



SECURITY INTELLIGENCE  
REVIEW COMMITTEE



# Annual Report 2008–2009

---

Accountability in a new era of  
security intelligence

Security Intelligence Review Committee  
P.O. Box 2430, Station D  
Ottawa, ON K1P 5W5  
(613) 990-8441

Visit us online at [www.sirc-csars.gc.ca](http://www.sirc-csars.gc.ca)

Collect calls are accepted between 8:00 AM and 5:00 PM, EST

© Public Works and Government Services Canada 2009

Catalogue No. PS105-2009E-PDF

ISBN 978-1-100-13085-9



September 30, 2009

The Honourable Peter Van Loan, P.C., M.P.  
Minister of Public Safety  
House of Commons  
Ottawa, Ontario  
K1A 0A6

Dear Minister:

We are pleased to present you with the annual report of the Security Intelligence Review Committee for the fiscal year 2008–2009, as required by Section 53 of the *Canadian Security Intelligence Service Act*, for your submission to Parliament.

Sincerely,

A handwritten signature in black ink that reads "Gary Filmon".

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

Chair

A handwritten signature in black ink that reads "Raymond A. Speaker".

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

A handwritten signature in black ink that reads "Denis Losier".

Denis Losier, P.C.

A handwritten signature in black ink that reads "Frances Lankin".

Frances Lankin, P.C.

A handwritten signature in black ink that reads "Arthur T. Porter".

Arthur T. Porter, P.C., M.D.

## WHAT IS SIRC?

The Security Intelligence Review Committee (SIRC, or the Committee) is an independent review body that reports to the Parliament of Canada on the operations of the Canadian Security Intelligence Service (CSIS, or the Service). By conducting reviews of CSIS activities and by investigating complaints, SIRC provides assurance to Parliament that the Service investigates and reports on threats to national security in a manner that respects the rule of law and the rights of Canadians.

## WHAT IS CSIS?

CSIS is responsible for collecting and analyzing security intelligence and other related information within Canada and abroad. It advises the Government of Canada on issues and activities that are a threat to national security. CSIS also provides security assessments to all federal departments and agencies, with the exception of the Royal Canadian Mounted Police.

See Appendix B of this annual report for more information on some of CSIS's key activities.

# CONTENTS

<b>MESSAGE FROM THE COMMITTEE MEMBERS</b> .....	<b>2</b>
<b>ABOUT THIS REPORT</b> .....	<b>4</b>
<b>SECTION 1: THE YEAR IN REVIEW</b> .....	<b>5</b>
<b>SECTION 2: SUMMARIES OF SIRC REVIEWS AND COMPLAINTS</b> .....	<b>8</b>
<b>A. REVIEWS</b> .....	<b>8</b>
CSIS's Role in the Matter of Omar Khadr .....	9
CSIS's District Office Activities at Canadian International Airports ....	13
A CSIS Human Source Operation .....	15
CSIS Activities at a Foreign Station .....	17
CSIS's Scientific and Technical Services .....	18
CSIS's Investigation into Domestic Extremism .....	19
The Case of Paul William Hampel .....	21
<b>B. COMPLAINTS</b> .....	<b>22</b>
Investigation of Alleged Profiling .....	24
<b>SECTION 3: SIRC AT A GLANCE</b> .....	<b>26</b>
Committee Activities .....	26
Committee Membership .....	26
Staffing and Organization .....	27
Budget and Expenditures .....	27
<b>APPENDIX A: LIST OF RECOMMENDATIONS</b> .....	<b>28</b>
<b>APPENDIX B: CSIS AT A GLANCE</b> .....	<b>29</b>
<b>A. SECURITY INTELLIGENCE ACTIVITIES</b> .....	<b>29</b>
Targeting .....	29
Warrants .....	30
<b>B. SECURITY SCREENING ACTIVITIES</b> .....	<b>30</b>
Government Screening .....	30
Site-Access Screening .....	32
Immigration Screening .....	33

# MESSAGE FROM THE COMMITTEE MEMBERS

Security intelligence operates in an ever-changing environment. The nature and pace of that change today is on a scale that has not been seen for several decades in Canada and elsewhere. Faced with a diverse threat environment of state and non-state actors, increased foreign investigations, growing demands from government stakeholders, as well as numerous public inquiries and court decisions pertaining to national security, the world of security intelligence has become increasingly complex.

It is against this backdrop that the Security Intelligence Review Committee (SIRC, or the Committee) continues to serve Canadians to ensure the democratic accountability of one of our country's most secretive institutions. Our mandate remains firmly rooted in assuring Parliament that the Canadian Security Intelligence Service (CSIS, or the Service) investigates and reports on threats to national security in a manner that respects the rule of law and the rights of Canadians. However, the range of security intelligence-related issues that we must understand and review continues to evolve in nature and scope.

At SIRC, we take great pride in being an organization that makes full use of the range of tools at our disposal to fulfill our mandate. Through the *Canadian Security Intelligence Service Act (CSIS Act)*, Parliament gave this Committee a broad mandate to review the Service's performance in carrying out its duties and functions. Since it was first established in the 1980s, SIRC has endeavoured to fulfill this responsibility by responding to the changing priorities of CSIS and to the evolving expectations of Canadians for security intelligence in a democratic society. From the Committee's perspective, the *CSIS Act* has provided SIRC with a model framework to carry out its mandate.

Our annual report is a vital component of how we meet those expectations—maintaining a proud tradition of providing insight and analysis with probity and fairness. Given the nature and scope of the changes in the security intelligence environment, we feel this year is a fitting time to offer Canadians a new approach to the way we report our findings and recommendations.

This year's annual report includes an analysis section that identifies the main themes reviewed by SIRC in the past year and engages readers in a discussion about the importance of accountability in this new era of security intelligence. We are confident this undertaking will provide Parliament and all Canadians with a renewed understanding of SIRC's role in reviewing the operations of CSIS.

SIRC itself has also experienced important changes over the past year. We recently welcomed three new members to the Committee: the Honourable Frances Lankin, P.C., the Honourable Denis Losier, P.C., and the Honourable Dr. Arthur T. Porter, P.C., M.D. We all look forward to serving Canadians with the same level of commitment that has characterized SIRC's work since its inception. The Committee would also like to thank



Members of SIRC  
(from left to right):  
The Honourable  
Raymond Speaker,  
The Honourable Arthur  
T. Porter, The Honourable  
Gary Filmon (Chair),  
The Honourable Frances  
Lankin, The Honourable  
Denis Losier.

*Photo: Couvrette/Ottawa*

those members whose terms ended recently: the Honourable Roy Romanow, P.C., O.C., Q.C., the Honourable Baljit S. Chadha, P.C., and the Honourable Aldéa Landry, P.C., C.M., Q.C. We thank them for their dedication and wish all of them well in their future endeavours.

On a final note, the Committee would like to take this opportunity to send our best wishes to Jim Judd, who, after serving as the Director of CSIS, retired from the public service in June 2009. From our perspective, Mr. Judd conscientiously guided the Service through some of the most challenging issues that the organization has faced in recent years. All Members of SIRC extend their thanks to Mr. Judd for his professionalism in meeting with the Committee on a number of occasions to discuss CSIS's work and the state of security intelligence. We look forward to working with his successor, Mr. Richard B. Fadden, and wish him well in his new position.

We are proud to share with Parliament and all Canadians our summaries of reviews and complaints investigations undertaken during the 2008–2009 fiscal year. It is our hope that this annual report will help inform Canadians about SIRC's roles and responsibilities and the constructive role we play in ensuring that CSIS is effective in investigating and reporting on threats to national security, while respecting the rights and freedoms of citizens. This is an integral part of the scheme of accountability that was established in 1984 by Parliament—a framework that has stood the test of time, and a responsibility that we look forward to continuing to fulfill with great pride.

# ABOUT THIS REPORT

SIRC provides assurances to Parliament—and through it, to Canadians—that CSIS investigates and reports on threats to national security in a manner that respects the rule of law and the rights of Canadians.

The *CSIS Act* gives SIRC full access to any information under the control of the Service. As a result, SIRC may examine all of CSIS's files and all of its activities—no matter how highly classified that information may be. The sole exception is Cabinet confidences (e.g., written and oral communications that contribute to the collective decision-making of Ministers).

This annual report summarizes SIRC's key analyses, findings and recommendations arising from its reviews and complaints investigations. It has three sections:

## **SECTION 1: THE YEAR IN REVIEW**

An analysis of prominent developments within the security intelligence milieu, and of how these relate to select findings and recommendations by SIRC from the past year.

## **SECTION 2: SUMMARIES OF SIRC REVIEWS AND COMPLAINTS**

A synopsis of reviews completed by SIRC as well as the complaint reports it has issued during the period covered by this report.

## **SECTION 3: SIRC AT A GLANCE**

Details about the outreach, liaison and administrative activities of SIRC, including its annual budget and expenditures.

## **A NEW LOOK FOR SIRC'S ANNUAL REPORT**

As part of SIRC's ongoing efforts to understand and report on new challenges and responsibilities in security intelligence in Canada, a revised layout has been developed for the organization's annual report. Key elements of these changes include:

### **MORE IN-DEPTH ANALYSIS FROM SIRC**

The revised SIRC report explores the changing environment in which security intelligence operates. This includes observations about key trends and challenges that CSIS will need to address in the coming years.

### **EASY ACCESS TO FACTS AND RECOMMENDATIONS**

This report features a revised layout to help you find the facts and information you're looking for, including: recommendations made during the review period and important information on the Committee.

### **BACKGROUND INFORMATION WHEN AND WHERE YOU WANT IT**

Look for the caption boxes throughout this report. These contain valuable background information on various legal- and policy-related matters regarding SIRC's review and complaints functions.



## SECTION 1: THE YEAR IN REVIEW

In less than two decades, the global environment in which Canada's security intelligence operates has undergone a fundamental transformation.

The end of the Cold War appeared to promise a more peaceful world with an expanding number of democracies and more widespread economic prosperity. It soon became clear, however, that the emerging global environment was both more complex and less secure than when there was a clear demarcation of interests between Western and Communist states.

The rise of global terrorism has played a significant role in shaping today's world, underscored most prominently by the rise of al Qaida as a globally capable terrorist platform. The 9/11 attacks on the United States, along with subsequent attacks in Europe and Asia, have changed how countries around the world perceive, and respond to, terrorism's destructive potential.

The contemporary threat environment is characterized by a constant danger of meticulously planned terror attacks designed to inflict mass casualties and destroy infrastructure. Canada has been openly threatened with attacks by al Qaida. It has also been subject to domestic and self-radicalizing terrorist cells. The arrest and trial of the Toronto 18 is reflective of this complex and evolving threat environment.

SIRC recognizes that CSIS must respond to these terrorist threats while still pursuing its traditional counter-intelligence priorities. For example, investigating the national security implications of the clandestine activities of foreign governments remains an important issue of concern. Likewise, counter-proliferation continues to be a top CSIS priority as the global community faces a number of unstable regimes with nuclear ambitions.

As the threat environment in which CSIS operates changes, so too does the corresponding legal environment. Recent court proceedings have lifted the veil of secrecy on the inner workings of the intelligence community. As part of this process, judicial rulings have required that the information CSIS brings to the courts meet the highest legal standards.

SIRC believes that the security intelligence environment will continue to be characterized by multiple threats and a high degree of unpredictability. Although global terrorism might shift its focus, it can be expected to continue to breed disorder and instability. Within this context, anticipating and defusing terrorist plans, while at the same time investigating other threats to national security, requires an effective security intelligence service.

When security agencies are faced with a multi-dimensional threat environment—and the need to protect society's fundamental values must be maintained—the role of a review body is equally complex. SIRC must comment on CSIS's capacity to carry out its mandate and on the tools that it has to undertake its work. Equally important, SIRC recommendations must be practical and reflect the values of Canadians.

## SECTION 1: THE YEAR IN REVIEW

SIRC is the only independent review body with the mandate to comment on all aspects of the Service's operations. It can respond to complaints or, on its own initiative, review specific aspects of CSIS. It can also respond to requests from the Minister of Public Safety to review the Service's performance of its duties and functions.

Each year, SIRC reviews a selection of the Service's operational activities to determine if it acted appropriately, effectively and in accordance with the law. This year's annual report covers a range of CSIS's operational activities and deals with some of the complex issues that confront the Service. Section 2 of this report summarizes the Committee's reviews and complaint decisions.

In SIRC's view, CSIS has made important progress in developing policies to guide itself on human rights issues when investigating threats to national security. However, as SIRC's review of the Service's role in the matter of Omar Khadr reveals, there are additional issues to be addressed. Of particular note, CSIS must consider the principles of national and international law in regards to the treatment of minors when interviewing a Canadian detainee abroad.

Security agencies cannot investigate terrorist activities unless they exchange information efficiently across borders. Some of the countries that may possess vital intelligence on threats to Canada's security do not respect the human rights valued by Canadians. Canada does not use torture or approve of its use. Less straightforward, however, is whether CSIS should cooperate and interact with countries that may engage in human rights abuses to collect threat-related intelligence. As a result, it is increasingly important for SIRC to review the Service's interactions with foreign intelligence agencies.

A related issue arises if a CSIS representative interviews a Canadian detained abroad. The priority for CSIS is the collection of security intelligence. At the same time, it must consider suspicions of torture or other human rights abuses—whether a detainee is able to directly confirm them or not.

From SIRC's perspective, it is important for CSIS to address the many difficult issues that arise in conducting security intelligence work in a contemporary democracy. Most importantly, although intelligence collection is the Service's *raison d'être*, the Khadr review underscores how extra-intelligence matters must become an integral part of CSIS's decision-making processes. As part of this transition, CSIS must draw on the guidance of the Minister in addition to its own experience and resources.

In a separate review, the Committee examined CSIS's activities at Canadian airports. These locations can be targets for terrorist attacks because they concentrate large numbers of people and are a vital part of Canada's transportation infrastructure. CSIS activities at Canadian airports support the aviation security framework by providing national security advice and conducting interviews of persons suspected of posing a threat to national security. In reviewing the Service's activities at these airports, SIRC found that CSIS's presence enhances the security environment.

SIRC also examined the impact of legislation passed after 9/11 on CSIS's activities. For instance, one of the goals of the 2001 federal *Anti-Terrorism Act* (ATA, or the *Act*) was to address terrorism financing. However, the *Act* raised some difficult issues for CSIS in terms of managing its human source program. In particular, due to the ATA's provisions, activities related to CSIS's human source program that could benefit organizations listed as terrorist entities were, by definition, potentially criminal acts. Although CSIS has taken steps to address these issues, SIRC believes more accountability to the Minister of Public Safety is needed with respect to certain aspects of the Service's human source program.

SIRC's review of CSIS's investigation into domestic extremism found that key elements of the Service's strategy for dealing with the domestic threat environment needed to be reviewed and reformulated. The Committee believes this is necessary to ensure there is a clear and common understanding of both the threat environment and the terminology used to describe it. This task will become more pressing over the coming months in advance of the 2010 Olympic and Paralympic Winter Games in Vancouver—an event that will be a major test of Canada's security infrastructure.

SIRC has the power to comment on the manner in which CSIS has used its authorities, as well as whether those authorities are fair, reasonable and appropriate to the threat. The Committee's review of CSIS's Scientific and Technical Services commented on the continuing lack of lawful-access legislation and its impact on Service operations. This legislation is needed. It would require that Internet service providers include intercept capabilities in their networks. SIRC hopes that the government's latest legislative efforts on this matter are successful in achieving this goal.

The role of SIRC as a review agency would be straightforward if there were public successes and failures that could be analyzed for lessons learned. In the fortunate absence of an actual attack or a major security incident, SIRC examines aspects of CSIS operations, which can serve as valid indicators of the organization's capability, efficiency and effectiveness.

In the past, SIRC focused much of its review activity on CSIS operations within Canada. As CSIS moves to expand its capacity to operate outside of Canada, SIRC will accordingly allocate more of its resources to review these activities. As well, SIRC will continue to investigate complaints—not only to see if they are justified, but to determine whether they signal more systemic issues for review.

Because of its extensive powers to investigate CSIS, SIRC takes very seriously the duty to understand the complex challenges that CSIS confronts and to thoroughly review its activities.

SIRC's annual report is a vital component in meeting this expectation—one that has been entrusted to SIRC by Parliament, on behalf of Canadians.

# SECTION 2: SUMMARIES OF SIRC REVIEWS AND COMPLAINTS

## A. REVIEWS

For more than 25 years, SIRC's reviews have provided Parliament and Canadians with a comprehensive picture of the Service's operational activities. It has also scrutinized CSIS's performance of its duties and functions to determine if the Service acted appropriately, effectively and in accordance with the law.

SIRC's reviews provide a retrospective examination and assessment of specific CSIS investigations and functions. The Committee's reviews include findings and—where appropriate—recommendations for the Service. Upon completion, all reviews are forwarded to both the Director of CSIS and the Inspector General of CSIS. SIRC is also authorized 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 asks SIRC to undertake.

### SIRC'S EARLIER REVIEWS

In past years, SIRC has reviewed a wide range of CSIS activities. For example, SIRC has examined how the Service carries out its mandate abroad by looking at activities undertaken at its various Stations around the world, the activities and investigations of CSIS regional offices, CSIS's cooperation and exchanges of information with domestic and foreign partners and specific operational activities such as CSIS's use of human sources. A complete listing of SIRC's past reviews can be found on the Committee's website ([www.sirc-csars.gc.ca](http://www.sirc-csars.gc.ca)).

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

- events with the potential to represent threats to the security of Canada;
- particular activities by CSIS that could have an impact on individual rights and freedoms;
- priorities and concerns identified by Parliament or in the media;
- issues identified in the course of SIRC's complaints functions;
- new directions or initiatives announced by, or affecting, CSIS;
- the CSIS Director's annual classified report submitted to the Minister of Public Safety; and
- the need to assess regularly each of the Service's branches and regional offices.

Each review results in a snapshot of the Service's actions in a particular context. This approach allows SIRC to manage the risk inherent in being able to review only a small number of CSIS activities in any given year.

SIRC's researchers consult multiple information sources to examine specific aspects of the Service's work. As part of this process, researchers may arrange briefings with CSIS employees, as well as examine individual and group targeting files, human source files, intelligence assessments and warrant documents, plus files relating to CSIS's cooperation and operational exchanges with foreign and domestic agencies and partners, among other sources that vary between reviews. The goal is to create a diverse pool of information so that SIRC can ensure it has thoroughly reviewed and completely understood the issues at hand.

### **ACCOUNTABILITY MATTERS**

SIRC is one of several mechanisms designed to ensure CSIS's accountability. In addition to the reviews and complaints investigations conducted by the Committee, the Service also remains accountable for its operations through the Minister of Public Safety, the courts, the Inspector General of CSIS, central agencies of government (e.g., Privy Council Office, Treasury Board Secretariat), the Auditor General, the Information Commissioner and the Privacy Commissioner of Canada.

## **SIRC Review: CSIS's Role in the Matter of Omar Khadr**

---

### **CONTEXT**

Many Canadians are familiar with the story of Omar Ahmed Khadr—a Canadian citizen held at the United States detention facility at Guantanamo Bay, accused of killing a United States army medic during a firefight in Afghanistan in 2002. The American legal case against Khadr, his treatment while in US custody, his status as a child soldier, and the Canadian government's stance on his repatriation—all of these topics have garnered widespread media coverage and commentary. In July 2008, Khadr's story was thrust onto the international stage when his lawyers released a videotape showing CSIS officials interviewing their client at Guantanamo Bay in February 2003. The video prompted questions in the public domain about the nature and extent of CSIS's involvement in this matter, including the reasons for the Service's decision to interview Khadr.

### SIRC'S LEGAL AUTHORITY IN THIS CASE

SIRC's review of CSIS's role in the matter of Omar Khadr was undertaken pursuant to Section 54 of the *CSIS Act*, which allows the Committee to forward to the Minister of Public Safety a special report on any matter that relates to CSIS's performance of its duties and functions. In most cases, these reports are reserved for matters that raise particularly difficult or high-profile issues that SIRC believes need to be brought to the Minister's direct attention. Examples of SIRC's previous Section 54 reviews include: the case of Mohammed Mansour Jabarah, the case of Maher Arar, the Heritage Front Affair, and CSIS activities in regard to the bombing of Air India Flight 182.

### SIRC'S REVIEW

SIRC's objective was to conduct an in-depth review of CSIS's involvement in the case of Omar Khadr. The Committee looked back as far as mid-August 2002—when Canadian officials, including CSIS, were informed by American authorities that Khadr had been captured by US forces—to the federal court injunction in September 2005, prohibiting further interviews with Khadr by Canadian authorities.

In February and September 2003, CSIS officials travelled to Guantanamo Bay to meet with Khadr. SIRC noted that, from the Service's perspective, there were compelling operational reasons to interview him, given the threat posed by Sunni Islamic extremism in the months following 9/11. Khadr's father, Ahmed Khadr, was allegedly the highest-ranking Canadian al Qaida member. When the Americans granted Canadian intelligence and law enforcement officials access to Khadr, the Service seized the opportunity to gather intelligence that would advance their own investigation.

The driving force behind CSIS's interest in interviewing Khadr was to collect intelligence on a potentially serious terrorist threat and to provide advice to the Government of Canada accordingly. Although SIRC understands CSIS's position—that it had reasonable grounds to travel to Guantanamo Bay to gather threat-related information—the Committee found that the decision to interview Khadr was prompted primarily by intelligence considerations.

As a result, SIRC believes that CSIS failed to give proper attention to two important extra-intelligence matters: human rights issues and Khadr's age at the time that CSIS conducted its interview with him.

With respect to the first matter, SIRC examined the issues relating to the Service's handling of situations where it interacts and shares information with foreign partners when there are potential human rights considerations. CSIS's exchanges and cooperation with foreign

partners have come under closer scrutiny since 9/11, as it has become apparent that intelligence agencies need to work together to combat terrorist threats that transcend geo-political boundaries. Although information-sharing with foreign partners is crucial for CSIS to fulfill its mandate, it has created some new difficulties, specifically when working with countries that do not share Canada's respect for human rights.

The Canadian government fully supported CSIS's visit to, and interview of, Khadr at Guantanamo Bay in February 2003, as this initiative was part of a whole-of-government effort to gain access to him while in detention.

When CSIS interviewed Khadr in February 2003, there was widespread media reporting of alleged mistreatment and abuse of detainees in US custody in Afghanistan and at Guantanamo Bay. In mid-2002, allegations were made by several individuals relating to their treatment by American soldiers after being taken into custody in Afghanistan in late 2001 and 2002. Meanwhile, the US detention facility at Guantanamo Bay opened its door amid controversy as many countries denounced the American government's legal position, as well as its treatment of detainees.

SIRC did not find any evidence that CSIS took this into account in deciding to interview Khadr.

As a result of recommendations made by SIRC in 2004, and by Justice O'Connor in 2006 with respect to the case of Maher Arar, CSIS revised its policies governing the circumstances in which it shares information with foreign partners who are suspected of having questionable human rights records. CSIS and the Department of Foreign Affairs and International Trade (DFAIT) also signed a new protocol in 2007, to promote greater coordination and coherence across government in addressing issues that arise from consular cases involving Canadians detained abroad in cases related to suspected terrorism or national security. SIRC hopes that these developments will assist CSIS in the future in collecting intelligence while respecting human rights—particularly if confronted with situations similar to that of Khadr.

The second matter relates to Khadr's age. It is well recognized in Canadian and international law that youth are entitled to certain fundamental rights because of their status as a minor. In Canada, this is expressed in provisions of the federal *Youth Criminal Justice Act*. The rights of children are also reflected in international conventions to which Canada is party, such as the *UN Convention on the Rights of the Child*.

### NO EASY SOLUTIONS

The issues raised in this case—such as information-sharing with foreign partners, human rights concerns when dealing with youth, and interacting with detainees in foreign jurisdictions—do not present simple remedies or easy answers. New mechanisms have been established to encourage CSIS to consider such issues as part of its decision-making process. However, in SIRC's view, it is becoming apparent that finding a solution to many of these complex post-9/11 issues will entail a thorough rethinking of intelligence work in light of recent social, policy and legal decisions.

SIRC found no evidence that CSIS, in deciding to meet Khadr at Guantanamo Bay, took into account the fact that their interview subject was still a youth at the time. In addition, youth radicalization is of growing concern to the Service. In light of these facts, SIRC recommended that the Service consider establishing a policy framework to guide its interactions with youth. As part of this, CSIS should ensure that such interactions are guided by the same principles that are entrenched in Canadian and international law.

Overall, SIRC believes that information-sharing with countries that have poor human rights records will continue to be a difficulty for CSIS until the Government of Canada resolves its seemingly contradictory position on information obtained from torture, versus the directions it provides to CSIS on carrying out its work.

This position places CSIS in an uncertain and vulnerable position when legal proceedings arise.

Such was the case in the matter of Omar Khadr, in which Canadian courts found that DFAIT and CSIS had violated Khadr's *Charter* rights by interviewing him and submitting the resulting information to US investigators. Underpinning the courts' message is that CSIS can no longer view the activities it undertakes strictly through the lens of intelligence-gathering. It must also consider the wider environment and implications within which its work is carried out.

There is general agreement among intelligence experts and academics that the world of intelligence changed dramatically after 9/11. Although CSIS has taken important steps to tackle some of these resulting challenges, the matter of Omar Khadr suggests that changes in policies and procedures are but one component of a broader transition that needs to take place.

The time may have come for CSIS to undertake a fundamental reassessment of how it carries out its work, and shift its operational culture to keep pace with the political and legal developments of recent years. It is also important for the Service to demonstrate that it has the professionalism, experience and know-how required to make the difficult



decisions that arise when conducting operations abroad. Indeed, there is mounting pressure and expectation on CSIS to consider extra-intelligence matters in fulfilling its mandate and carrying out its activities.

### RECOMMENDATIONS IN BRIEF

This review had two recommendations:

- The Service should consider establishing a policy framework to guide its interactions with youth. As part of this, CSIS should ensure that such interactions are guided by the same principles that are entrenched in Canadian and international law.
- CSIS should implement measures to embed the values stemming from recent political, judicial and legal developments in its day-to-day work to maintain its own credibility, and to meet growing and evolving expectations of how an intelligence agency should operate and perform in a contemporary democratic society. Guidance and advice from the Minister of Public Safety on how to accomplish this task would be helpful.

## SIRC Review: CSIS's District Office Activities at Canadian International Airports

---

### CONTEXT

A safe and secure civil aviation system is a vital component of Canada's economy. Its security is therefore of great importance. Following the 1985 bombing of Air India Flight 182 and the 9/11 terrorist attacks, a number of new measures were introduced across Canada to improve aviation security. These included new rules for aircraft and airport construction, enhanced screening of people and goods at airports, requirements for air carriers to provide basic information on specific passengers or flights, and assigning undercover police officers to provide security on Canadian aircraft. Although not an exhaustive list, these initiatives illustrate how civil aviation security has evolved into a broad network of players and responsibilities involving regional, provincial and federal agencies, as well as air carriers and private security firms.

## SECTION 2: SUMMARIES OF SIRC REVIEWS AND COMPLAINTS

### SIRC'S REVIEW

CSIS plays an essential role within the complex web of airport security stakeholders by investigating threats to national security, as well as screening passengers travelling to Canada or airport employees requiring access to restricted areas. In addition, CSIS activities at Canadian airports support the aviation security framework in their respective regions.

For this review, SIRC examined CSIS's activities at a selection of Canadian airports. The objective was to better understand and assess the role of CSIS at these airports, including how they manage their airport-related responsibilities and work with their airport partners.

Through constant contact with airport stakeholders, service personnel are able to transfer information to regions and headquarters, and act as conduits for information collection and sharing among airport partners. The effectiveness of their communications depends on maintaining solid relationships. SIRC observed that both of CSIS's District Offices spent considerable time and effort developing and maintaining contact with both government and non-governmental airport stakeholders.

Further, SIRC observed that government and law enforcement partners in the airport environment frequently request the assistance of CSIS personnel to obtain national security advice related to airport operations. CSIS airport personnel are called on by airport stakeholders to provide briefings on threat-related issues, including information concerning CSIS's national security mandate. Service personnel also provide advice to law enforcement agencies in response to any security breach or criminal incident occurring at an airport where a risk to national security is suspected. Airport immigration officers, as part of CSIS's role in the Port of Entry Interdiction Program, also request the presence of CSIS personnel when conducting interviews of air travellers who are suspected of posing a potential threat to national security. During these interviews CSIS personnel conduct background checks to determine if the person has a history of threat-related activities. This expert advice is vital in securing airport entry points.

CSIS staff also spend considerable time and effort building and maintaining relationships within the airport environment. Through the development of these relationships, CSIS airport personnel are able to support regional and headquarters operational desks that require access to the airport infrastructure to carry out operations.

SIRC noted that CSIS staff who carry out activities at airports would benefit from greater exchanges with their counterparts who serve airports in other regions of Canada, and who carry out day-to-day functions similar to their own. SIRC believes that Service personnel whose main functions are to support airport security should be given the opportunity to collaborate and share best practices with their counterparts at other airports.

Overall, SIRC found that CSIS activities at airports reinforce the Service's national security mandate. Moreover, this provides airport stakeholders with readily available access to CSIS expertise.

### RECOMMENDATIONS IN BRIEF

There were two recommendations arising from this review:

- CSIS should support efforts that encourage greater collaboration between Service personnel to enhance their operational activities at Canadian airports.
- The Service should ensure that their disaster management plans include activities at airports, so that procedures are in place to better ensure that the essential services that they provide are not interrupted in the event that their offices are rendered inoperable.

## SIRC Review: A CSIS Human Source Operation

### CONTEXT

CSIS's human source program is considered to be an effective and cost-efficient intelligence tool. Sources under this program are often able to provide insight about a target's intentions—something that cannot be gained through the Service's other methods of information gathering.

Legislative steps taken to date to fight terrorism have presented the Service with unique challenges in terms of the management of the human source program. One such challenge arose as a result of the *Anti-Terrorism Act* (2001). Due to its provisions, activities related to CSIS's human source program that could benefit organizations listed as terrorist entities were, by definition, potentially criminal acts.

### ABOUT THE *ANTI-TERRORISM ACT*

The *Anti-Terrorism Act* gives the Government of Canada legal authority to create a list of entities believed to be involved in terrorist activities. The *Act* also makes it a criminal offence to, among other things, directly or indirectly collect or make available property or financial or other related services knowing they will be used by—or will benefit—a terrorist group.

## SECTION 2: SUMMARIES OF SIRC REVIEWS AND COMPLAINTS

Aware of the legal complexities of this situation, CSIS determined that its human source program was carried out within the confines of the law.

### SIRC'S REVIEW

The Committee had briefly examined this issue in previous reviews. At that time, SIRC accepted the Service's position that CSIS operational policy was sufficient to cover all aspects of human source management. Nevertheless, SIRC maintained that it would continue to monitor the matter to identify challenging issues when required.

As part of this commitment, SIRC believed it was important to re-examine the matter at this time. For this review, SIRC placed special emphasis on the appropriateness and adequacy of the human source program's level of accountability within CSIS, and to the Minister of Public Safety.

In terms of accountability within CSIS, operational policy has not been updated to include any of the emerging factors that must be considered prior to determining whether actions carried out within the human source program are lawful. Nevertheless, SIRC found that a reporting structure was in place to ensure meaningful discussions take place within the Service about significant matters affecting management of the human source program.

In terms of accountability to the Minister of Public Safety, SIRC found that as a result of CSIS's interpretation—and by extension, its implementation—of operational policy, there was no venue by which it could inform the Minister of the implications of the *Anti-Terrorism Act* on human source operations. SIRC suggested a process of regularly updating the Minister on this matter.

Since the passage of the *Anti-Terrorism Act*, the Government of Canada has listed over 40 entities. As Canada's list of terrorist entities grows longer, commensurate growth is expected in the number of CSIS human source operations that could benefit listed organizations. It is important that CSIS be held to account for these activities.

### RECOMMENDATIONS IN BRIEF

There was one recommendation arising from this review:

- CSIS should inform the Minister of Public Safety of the implications of the *Anti-Terrorism Act* as it relates to the Service's human source program and any future related developments.

## SIRC Review: CSIS Activities at a Foreign Station

---

### CONTEXT

In fulfilling its legal and operational responsibilities, CSIS maintains a presence outside of Canada. With the exception of three CSIS Stations—London, Paris and Washington—the locations are classified. Traditionally, the primary function of each Station was to liaise with CSIS's foreign partners and to conduct immigration screening. In addition, CSIS officials at headquarters used to manage operations abroad. Today, however, CSIS Stations take on larger roles in these operations. This expanded role coincides with an increase in the number of CSIS operations abroad, as underlined by former CSIS Director Jim Judd, who publicly acknowledged the Service's involvement in operations in Afghanistan, Iraq and Lebanon.

### SIRC'S REVIEW

This year, the Committee examined the activities of a CSIS Station responsible for the Service's relationships with agencies in a number of countries. While not one of CSIS's busiest Stations, its work suggested that there was a high level of cooperation and information sharing. Although the Station under review was actively involved in operations, most continued to be managed by Canadian-based officials. Therefore, liaison work remained the Station's mainstay. Nevertheless, SIRC noted that the Station is well positioned to fulfill its mandate in liaison and operations.

To be effective in managing foreign relationships, all CSIS Stations need to have efficient methods of exchanging information—both with CSIS and its partner agencies. SIRC identified three communications-related challenges at the Station under review. In two instances, the challenges posed an inconvenience but did not prevent the Station from doing its work. SIRC also noted that CSIS had already indicated that it is exploring options to address these matters.

The third challenge related to the exchange of information directly from CSIS Headquarters to foreign agency representatives—as opposed to the accepted practice of sending the information through the respective CSIS Station. SIRC indicated that it would like to see a more consistent use of the accepted practice for exchanging information (i.e., all messages should go through the respective CSIS Station).

When the Service engages in operations abroad, senior-level approval is required from within CSIS. In recent years, this approval process was delegated downwards. The new process, however, was ambiguous and in some instances led to an inconsistent approach when seeking approval. New processes were recently instituted by CSIS, but these were outside of the scope of SIRC's work during the period under review. Nevertheless, it is worth noting that, in SIRC's estimation, the devolution of authority is a significant development that warrants ongoing examination.

## SECTION 2: SUMMARIES OF SIRC REVIEWS AND COMPLAINTS

As CSIS Stations become more active operationally, they are addressing some of the needs that a separate foreign intelligence service would otherwise address. SIRC will continue to monitor the activities of both the Service and the Stations as they take on greater operational roles.

### RECOMMENDATIONS IN BRIEF

There was one recommendation arising from this review:

- CSIS should ensure there is a more consistent use of the accepted practice for exchanging information with foreign partners in which all messages go through the appropriate CSIS Foreign Station.

## SIRC Review: CSIS's Scientific and Technical Services

### CONTEXT

Of all the strategies used by CSIS to collect and access information, those that are technology-based are considered to be the most resource-intensive. Designing and deploying these technologies requires a wide range of specialties including forensics, mechanical engineering, programming and laboratory analysis. These are all within the responsibilities of CSIS's Scientific and Technical Services (STS) Branch.

Although previous SIRC studies have examined aspects of the Service's technical operations, the Committee believed it was appropriate to conduct a more thorough analysis of what goes on behind the scenes within CSIS before an operation takes place.

### SIRC'S REVIEW

The goal of this review was to better understand the nature and scope of the STS Branch's work, including the challenges it faces in completing its work and how it cooperates with various partners. Intelligence technology is a complex business that requires continued access to new talent and innovative research and development, as well as the ability to develop products in a timely fashion—all while dealing with budgetary constraints. The STS Branch manages these challenges by working with Government of Canada partners and contracting-out to industry.

During the review, it became apparent to SIRC that not all of the challenges STS faces are within its control to address. Primary among these is the need to keep pace with rapidly

developing technologies in a variety of disciplines. Associated with this is the absence of lawful-access legislation—requiring telecommunication service providers to design their products with built-in intercept capabilities. This is in sharp contrast to the experience of CSIS’s counterparts in the United States and Europe, where governments have legislated cooperation between the service providers and security intelligence agencies.

In Canada, opponents to lawful-access legislation cite a number of concerns, including:

- the appropriateness of compelling service providers to create intercept solutions;
- the scope of information that would be obtained and how it would be used; and
- whether restrictions or oversight would exist to prevent abuse.

Canada’s Privacy Commissioner has argued against various iterations of the proposed legislation, most recently stating that “lawful access raises fundamental issues for rights such as privacy and the ability to communicate freely.” The Committee recognizes it is important that Canadians engage in a healthy debate on this issue. However, SIRC is concerned that STS’s ability to perform certain investigative procedures will be constrained until the government is successful in enacting appropriate legislation.

There were no recommendations arising from this review.

On June 18, 2009, during preparation of SIRC’s 2008–2009 Annual Report, the federal government tabled the *Technical Assistance for Law Enforcement in the 21<sup>st</sup> Century Act*. If enacted, this legislation would require that internet service providers include intercept capabilities in their networks. SIRC will follow the development of this legislation to determine its potential impact on the Service’s intelligence-gathering mandate and priorities.

## SIRC Review: CSIS’s Investigation into Domestic Extremism

---

### CONTEXT

The Government of Canada considers domestic extremism a national intelligence priority. For this reason, CSIS identifies domestic, politically motivated violence as one of its highest priorities. The investigation of domestic extremism, however, presents a unique challenge to the Service. While it must gather information required to fulfil its mandate, CSIS must also refrain from infringing on Canadians’ protected rights to lawful advocacy, protest and dissent. Successfully negotiating the line between legal

## SECTION 2: SUMMARIES OF SIRC REVIEWS AND COMPLAINTS

protest and activist extremism requires a specialized and in-depth understanding of advocacy movements, protest tactics and the ways in which otherwise well-intentioned protesters can become radicalized.

### SIRC'S REVIEW

This study had two objectives. First, SIRC examined CSIS activities in relation to domestic extremism, taking into account the overlap with criminal investigations and lawful advocacy, protest and dissent. SIRC found that CSIS had allocated appropriate resources to deal with the potential threat from domestic extremism. Moreover, CSIS had developed significant expertise regarding potential threats from domestic extremism, as well as a series of balanced measures to ensure Canadians' right to legal dissent.

However, SIRC found that some of the strategies employed by the Service to analyze the threat environment could benefit from reformulation. Several key concepts to evaluate the potential threat are not universally understood, commonly defined or used consistently. SIRC recommended that the Service establish an accepted terminology and gain a deeper understanding of the parameters of the threat environment to isolate and identify indicators of radicalization.

The second objective was to examine CSIS investigations of special events (i.e., an event that provides a heightened opportunity for carrying out threat-related activities). In that regard, the Committee examined the plans and priorities put in place by the Service for the 2010 Olympic and Paralympic Winter Games in Vancouver, and found them to be on-schedule and well-conceived. However, several of the concerns raised in the context of domestic extremism investigations—key concepts not being commonly defined or used consistently—applied equally to the Service's assessment of the threat environment surrounding the Olympic and Paralympic Games.

It is important to note that CSIS's understanding of the Olympics threat environment continues to evolve and its efficiency during the 2010 Games will depend on its ability to assess accurately the movements associated with domestic extremism. SIRC believes that the strategies recommended to address the concerns highlighted in the domestic extremism investigation will also inform CSIS's preparations for the Olympics.

### RECOMMENDATIONS IN BRIEF

There was one recommendation arising from this review:

- CSIS should take steps to develop stronger definitions and a better understanding of the multi-issue extremism environment. The objective should be to build a more effective model to isolate and identify indicators of activist extremism and their potential for violence.



## SIRC Review: The Case of Paul William Hampel

---

### CONTEXT

Former CSIS Director Jim Judd has publicly acknowledged that foreign powers are becoming more sophisticated in conducting espionage within Canada's borders. A recent case of Russian espionage in Canada underlines this concern. In November 2006, a Russian spy, who had been using the name Paul William Hampel, was detained by Canadian officials in Montreal as he was about to board an international flight. The circumstances surrounding Hampel's detention received significant media attention, which reported that he was a Russian intelligence officer who had been residing in Canada under a false identity since 1995. However, there was no reporting of the nature and scope of CSIS's involvement in this high-profile and sensitive matter.

### SIRC'S REVIEW

The objective of SIRC's review was to understand CSIS's involvement in the Hampel case. The Committee found that after becoming aware of Hampel's existence, CSIS conducted an investigation to determine the nature and scope of his espionage activities.

During the course of the investigation, the Service gathered important information to advise the Ministers of Public Safety and Citizenship and Immigration that Hampel was a known member of Russia's Foreign Intelligence Service and had used a fraudulent Canadian identity to further Russian espionage activities. In accordance with the *Immigration and Refugee Protection Act*, the Ministers signed a security certificate, thereby initiating the process by which Hampel was eventually deported to Russia.

As a result of the Hampel investigation, CSIS gained additional insights into the espionage threat posed to Canada by the activities of the Russian Intelligence Services. This will assist CSIS in investigating similar threats should they arise in the future.

There were no recommendations arising from this review.

# SECTION 2: SUMMARIES OF SIRC REVIEWS AND COMPLAINTS

## B. COMPLAINTS

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

### WHAT IS THE DIFFERENCE BETWEEN A REVIEW AND A COMPLAINT INVESTIGATION?

A **review** is initiated by SIRC and entails in-depth research of CSIS's performance in carrying out its duties as described in the *CSIS Act*. A **complaint** investigation is initiated by an individual or group who may make a complaint to SIRC with respect to: "any act or thing done by the Service" (Section 41); denials or revocation of security clearances to government employees or contractors (Section 42); referrals from the Canadian Human Rights Commission; and Minister's reports in regards to the *Citizenship Act*. While reviews constitute SIRC's research function, complaint investigations are conducted as part of a quasi-judicial process.

Once a written complaint is received, SIRC conducts a preliminary 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. A complainant has the right to be represented by counsel and to make representations at the hearing. Pre-hearings may be conducted to establish and agree on procedures with the complainant and/or the complainant's counsel.

SIRC's 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.

### TYPES OF COMPLAINTS

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 or potentially under Section 41 of the *CSIS Act*.

When SIRC's investigation of a complaint made under Section 41 is concluded, it provides a report to the Director of CSIS, the Minister of Public Safety and the complainant.<sup>1</sup> Summaries of these reports, edited to protect national security and the privacy of complainants, are also included in SIRC's annual report to Parliament.

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*.

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., via an administrative review).

<b>TABLE 1 RESOLUTION OF COMPLAINTS</b>			
	<b>2006–07</b>	<b>2007–08</b>	<b>2008–09</b>
Carried over	24	20	15
New	37	32	30
<b>Total</b>	<b>61</b>	<b>52</b>	<b>45</b>
Closed <sup>†</sup>	41	37	23
Carried forward to subsequent year	20	15	22
Reports issued	5	6	1

<sup>†</sup> Closed files include those where reports were issued, the Committee did not have jurisdiction, the preliminary conditions of the complaint were not met, or the complaints were withdrawn. In the past year, the Committee dealt with an increased number of files raising complex jurisdictional issues.

<sup>1</sup> The complainant receives a declassified version of the report.

### 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.

## SIRC Complaint: Investigation of Alleged Profiling

SIRC investigated a complaint in which the complainant was required to obtain an airport restricted-access security clearance for the purposes of employment. In this case, Transport Canada requested that CSIS undertake a security assessment to appraise this individual’s loyalty to Canada and reliability as it relates to such loyalty. The complainant was subsequently contacted by CSIS and a security-screening interview was conducted.

In the complaint to SIRC, filed pursuant to Section 41 of the *CSIS Act*, the complainant alleged profiling by CSIS. In addition, the complainant objected to the use of questions during the interview, which the complainant alleged solicited political opinions and were believed prohibited under the *Charter of Rights and Freedoms*. The complainant sought an apology and written assurances that CSIS would stop asking these questions at future security-screening interviews.

For its part, CSIS argued that it is not unusual to conduct interviews as part of the security screening process. Interviews may be conducted for cause when it is determined that there is insufficient information regarding an individual to complete a security assessment. In conducting its security assessment, CSIS is required, as per the *CSIS Act*, to appraise a person's "loyalty to Canada and reliability as it relates to such loyalty." In doing so, it will consider a range of factors when completing these assessments, including personal beliefs and associations—matters the Service considers to be consistent with the Treasury Board Secretariat's Government Security Policy.

SIRC's investigation included a detailed review of CSIS's documentation, as well as testimony from the complainant and representatives from CSIS plus a Treasury Board Secretariat representative who spoke about the purpose of the Government Security Policy. As a result of this information, SIRC was satisfied that CSIS acted in accordance with the Government Security Policy, the Government Security Policy Standard, as well as CSIS's applicable operational policies in requesting that the complainant attend a security-screening assessment interview. In addition, SIRC found that the complainant was not profiled on grounds prohibited by the *Charter of Rights and Freedoms*, and found that questions in the security-screening interview relating to the complainant's opinions and beliefs did not infringe on the complainant's rights under the *Charter*.

### SIRC'S LEGAL AUTHORITY TO INVESTIGATE COMPLAINTS

Under Section 41 of the *CSIS Act*, SIRC has the authority to investigate complaints made by "any person" with respect to "any act or thing done by the Service." The Committee must also be satisfied that the complaint is not trivial, vexatious or made in bad faith.

### ABOUT THE GOVERNMENT SECURITY POLICY

The Government of Canada must ensure that individuals who have access to government information and assets are reliable and trustworthy. Ensuring loyalty to Canada is essential for protecting Canadians and Canadian assets from threats posed by terrorism and espionage, or from malicious or improper activities, such as the unauthorized disclosure of classified and protected information that can have a serious impact on the safety of Canadians and on the effective functioning of society. Federal departments must therefore ensure that individuals are appropriately screened before commencing their duties. CSIS plays a vital role in this process, providing security assessments for government departments and institutions (see Appendix B of this report for further information on CSIS's security screening activities.) For more details on the Government Security Policy, visit the Treasury Board of Canada Secretariat's website ([www.tbs-sct.gc.ca](http://www.tbs-sct.gc.ca)).

## SECTION 3: SIRC AT A GLANCE

### COMMITTEE MEMBERSHIP

SIRC is chaired by the Honourable Gary Filmon, P.C., O.M., who was appointed as Chair on June 24, 2005. The other Committee Members are the Honourable Frances Lankin, P.C., the Honourable Denis Losier, P.C., the Honourable Dr. Arthur T. Porter, P.C., M.D., and the Honourable Raymond Speaker, P.C., O.C.

All Members of SIRC are Privy Councillors. Each is 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.

### COMMITTEE ACTIVITIES

**October 5–8, 2008:** The Chair, the Executive Director, and a Member of SIRC attended the International Review Agencies Symposium, hosted in Auckland, New Zealand, by the Inspector-General Intelligence and Security.

**October 30–November 1, 2008:** The Executive Director and several staff attended a conference of the Canadian Association of Security and Intelligence Studies, held in Ottawa.

**November 4, 2008:** At Carleton University, the Executive Director gave a lecture to students of a course on national security, providing an overview of SIRC's role and mandate.

**March 5, 2009:** The Executive Director appeared before the House of Commons Standing Committee on Public Safety and National Security.

**March 24, 2009:** The Acting Senior Counsel and the Senior Advisor met with officials from the New Zealand Security Intelligence Service.

**March 26, 2009:** The Acting Senior Counsel and the Senior Advisor met with officials from the Intelligence Security Committee (United Kingdom).

## 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 Advisor, a Senior Counsel, a Corporate Services Manager, Counsel, a Senior Paralegal, plus researchers and administrative staff.

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

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

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

SIRC also visits CSIS regional offices on a rotating basis to better understand and examine 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 2008–09 fiscal year, SIRC visited three 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 2 below presents a breakdown of actual and estimated expenditures.

	2008–09 (Estimates)	2008–09 (Actual)
Personnel	\$1,900,000	\$1,700,000
Goods and Services	\$1,000,000	\$700,000
Total	\$2,900,000	\$2,400,000

## APPENDIX A: LIST OF RECOMMENDATIONS

During the 2008–2009 review period, SIRC made the following recommendations stemming from the range of reviews it conducted, as well as from the complaint it investigated.

CASE <sup>2</sup>	SIRC RECOMMENDED THAT...
CSIS'S ROLE IN THE MATTER OF OMAR KHADR	<p>The Service should consider establishing a policy framework to guide its interactions with youth. As part of this, CSIS should ensure that such interactions are guided by the same principles that are entrenched in Canadian and international law.</p> <p>CSIS should implement measures to embed the values stemming from recent political, judicial and legal developments in its day-to-day work to maintain its own credibility, and to meet growing and evolving expectations of how an intelligence agency should operate and perform in a contemporary democratic society. Guidance and advice from the Minister of Public Safety on how to accomplish this task would be helpful.</p>
CSIS ACTIVITIES AT CANADIAN INTERNATIONAL AIRPORTS	<p>CSIS should support efforts that encourage greater collaboration between Service personnel to enhance their operational activities at Canadian airports.</p> <p>The Service should ensure that their disaster management plans include activities at airports, so that procedures are in place to better ensure that the essential services that they provide are not interrupted in the event that their offices are rendered inoperable.</p>
A CSIS HUMAN SOURCE OPERATION	CSIS should inform the Minister of Public Safety of the implications of the <i>Anti-Terrorism Act</i> as it relates to the Service's human source program and any future related developments.
CSIS ACTIVITIES AT A FOREIGN STATION	CSIS should ensure there is a more consistent use of the accepted practice for exchanging information with foreign partners in which all messages go through the appropriate CSIS Foreign Station.
CSIS'S INVESTIGATION INTO DOMESTIC EXTREMISM	CSIS should take steps to develop stronger definitions and a better understanding of the multi-issue extremism environment. The objective should be to build a more effective model to isolate and identify indicators of activist extremism and their potential for violence.

<sup>2</sup> Consult the SIRC website at [www.sirc-csars.gc.ca](http://www.sirc-csars.gc.ca) for a list of all SIRC reviews conducted since 1984.



# APPENDIX B: CSIS AT A GLANCE

Each year, as part of SIRC’s annual report, the Committee presents important information and statistics related to CSIS operations. This data, provided by the Service, provides readers with insight into some of the Service’s key duties and functions, as well as highlights any major changes or developments within CSIS.

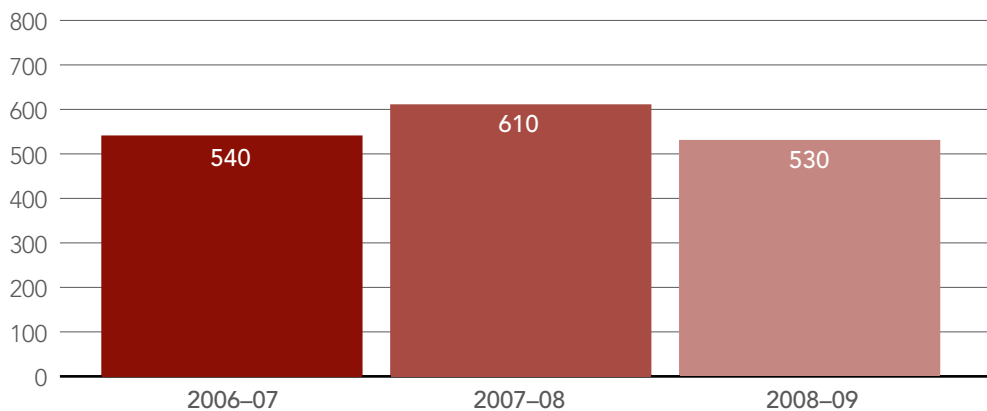
For SIRC’s 2008–2009 Annual Report, this information is grouped in two categories: security intelligence activities and security screening activities.

## A. SECURITY INTELLIGENCE ACTIVITIES

### Targeting

When the Service has reasonable grounds to suspect that an individual or an organization could pose a threat to Canada, it must first establish an investigation in which it exercises its powers proportionate to the threat that is posed. Figure 1 indicates the number of targets investigated by CSIS during the period under review, relative to previous fiscal years.

**FIGURE 1**  
TARGETING STATISTICS\*



Note: \* Figures have been rounded to the nearest 10.

## Warrants

The power to authorize intrusive investigative techniques rests strictly with the Federal Court of Canada. If the Court grants a warrant, it provides CSIS with authorization to use investigative techniques that would otherwise be illegal, such as the monitoring of telecommunications activities. Table 3 shows the number of federal court-approved warrants that CSIS had during the period under review, relative to previous years.

**TABLE 3**  
WARRANT STATISTICS

	2006–07	2007–08	2008–09
New warrants	42	71	26
Replaced or renewed	134	182	183
Total	176 <sup>†</sup>	253 <sup>††</sup>	209 <sup>†††</sup>

<sup>†</sup> Included in this number were 25 urgent warrants.

<sup>††</sup> Included in this number were 19 urgent warrants.

<sup>†††</sup> Included in this number were 2 urgent warrants.

## B. SECURITY SCREENING ACTIVITIES

Security screening is one of the most publicly visible functions provided by CSIS. This activity consists of government screening (which includes site-access screening) and immigration screening.

### Government screening

This type of screening provides security assessments—an appraisal of the loyalty to Canada and (so far as it relates thereto) the reliability of an individual—for all government departments and institutions, except the Royal Canadian Mounted Police (RCMP).

CSIS does not decide who receives a security clearance. Rather, it advises the requesting department or agency of information that could have an impact on their decision to grant a clearance. On rare occasions, CSIS will recommend to a requesting agency that the threshold in the Government Security Policy has been met to deny a clearance. However, it is the responsibility of the requesting agency to grant, revoke or deny a clearance.

Table 4 reports the number of requests for government screening that CSIS received over a three-year period. Table 5 reports the median turnaround time for CSIS to complete these assessments.

<b>TABLE 4</b> REQUESTS FOR CSIS GOVERNMENT SECURITY SCREENING*			
	2006–07	2007–08	2008–09
Requests from Department of National Defence (DND)	13,100	8,800	15,300
Requests from other clients	38,100	41,500	46,400
<b>Total</b>	<b>51,200</b>	<b>50,300</b>	<b>61,700</b>
Assessments issued to DND	13,100	8,300	14,400
Assessments issued to other clients <sup>†</sup>	41,800	40,500	46,300
<b>Total</b>	<b>54,900</b>	<b>48,800</b>	<b>60,700</b>

\* Figures have been rounded to the nearest 100.

<sup>†</sup> This number includes assessments performed for provincial governments and for access to nuclear facilities.

<b>TABLE 5</b> MEDIAN TURNAROUND TIME (IN CALENDAR DAYS) FOR CSIS TO COMPLETE SECURITY ASSESSMENTS						
		2006–07 <sup>†</sup>	2007–08		2008–09	
			New	Updates	New	Updates
DND	Level I (Confidential)	40	23	9	74	57
	Level II (Secret)	40	28	23	61	62
	Level III (Top Secret)	82	164	29	126	57
Non-DND	Level I (Confidential)	32	18	13	18	6
	Level II (Secret)	21	13	12	15	16
	Level III (Top Secret)	47	186	4	145	8

<sup>†</sup> For 2006–07, median turnaround times for new and update security assessments were not available. The time reflected in this column is therefore for both types of assessments.

## Site-access screening

This type of screening allows an individual access to certain secure areas—such as airports, port and marine facilities, the Parliamentary Precinct and nuclear power facilities—and provides accreditation for special events and assessments to provincial departments. These programs are meant to enhance security and reduce the potential threat from terrorist groups and foreign governments, which may seek to gain unauthorized access to classified information or other assets, materials and sensitive sites. Table 6 reports the number of requests that CSIS received for site-access screening over the past year, relative to the previous two years.

**TABLE 6**  
REQUESTS TO CSIS FOR SITE-ACCESS SCREENING\*

	2006–07	2007–08	2008–09
Parliamentary Precinct	1,100	1,100	1,000
Airport restricted-access area (Transport Canada)	39,300	36,800	31,400
Nuclear facilities	17,900	9,200	11,100
Free and Secure Trade (FAST)	23,100	10,700	6,400
Special events accreditation	0	1,300	16,300
Marine Transportation Security Clearance Program <sup>†</sup>	N/A	6,300	5,200
Other government departments	2,500	2,100	2,600
<b>Total</b>	<b>83,900</b>	<b>67,500</b>	<b>74,000</b>

\* Figures have been rounded to the nearest 100.

<sup>†</sup> The Marine Transportation Security Clearance Program became operational in December 2007 to provide security assessments in relation to the security of Canada's ports.

## Immigration screening

This type of screening helps to ensure that individuals who pose a threat to security and/or are inadmissible under the *Immigration and Refugee Protection Act* do not gain entry or obtain status in Canada. If an individual meets one or more of these criteria, CSIS will issue a brief. Table 7 reports the number of citizenship and immigration screening requests received by CSIS, as well as the number of briefs issues in relation to these requests.

	Requests*			Briefs		
	2006–07	2007–08	2008–09	2006–07	2007–08	2008–09
Permanent resident†	62,800	66,000	67,300	201	195	213
Front-end screening††	17,900	21,800	26,800	143	117	108
Refugee determination†††	11,600	6,600	6,600	153	142	102
<b>Subtotal</b>	<b>92,300</b>	<b>94,400</b>	<b>100,700</b>	<b>497</b>	<b>454</b>	<b>423</b>
Citizenship applications	227,300	190,000	169,500	155	109	169
<b>Total</b>	<b>319,600</b>	<b>284,400</b>	<b>270,200</b>	<b>652</b>	<b>563</b>	<b>592</b>

\* Figures have been rounded to the nearest 100.

† This includes permanent residents inside 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.

## APPENDIX B: CSIS AT A GLANCE

Table 8 reports the time it took for CSIS to complete notices of assessment, which are issued in those government and immigration screening cases when CSIS finds no adverse information on an applicant.

**TABLE 8**  
TURNAROUND TIME (IN DAYS) FOR CSIS TO COMPLETE NOTICES OF ASSESSMENT

	2006–07	2007–08	2008–09
Citizenship	1	1	1
Immigration (Canada) <sup>†</sup>	78	59	95
Immigration (USA) <sup>††</sup>	29	45	65
Overseas immigration	14	20	26
Refugee determination	98	64	89
Front-end screening	19	28	29

<sup>†</sup> This includes certain classes of individuals who apply for permanent resident status from within Canada.

<sup>††</sup> 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.