SECURITY INTELLIGENCE
REVIEW COMMITTEE

Annual Report 09/10

Time for reflection

Taking the measure of security intelligence

Canada

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

Catalogue No. PS105-2010E-PDF
ISBN 978-1-100-16147-1

Security Intelligence Review Committee

Comité de surveillance des activités de renseignement de sécurité

September 30, 2010

The Honourable Vic Toews, 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 2009–2010, as required by Section 53 of the *Canadian Security Intelligence Service Act*, for your submission to Parliament.

Sincerely,

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

Frances Lankin, P.C.

Philippe Couillard, P.C., M.D.

Carol Skelton, P.C.

Denis Losier, P.C.

P.O. Box / C.P. 2430, Station / Succursale "D"
Ottawa, Canada K1P 5W5
Tel: 613-990-8441 Fax: 613-990-5230

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 performance of the Canadian Security Intelligence Service (CSIS). 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?

The Canadian Security Intelligence Service (CSIS, or the Service) is responsible for investigating threats to Canada, analysing information and producing intelligence. To protect Canada and its citizens, CSIS advises the Government of Canada on issues and activities that are a threat to national security. It also provides security assessments to all federal departments and agencies, with the exception of the Royal Canadian Mounted Police. See the Appendix of this annual report for more information on some of CSIS's key activities.

A legal framework for both SIRC and CSIS

With the passage of the *CSIS Act* in 1984, Canada became one of the first democratic governments in the world to establish a legal framework for its security service. With this *Act*, Canada clearly defined in law the mandate and limits of state power to conduct security intelligence. Just as important, the *CSIS Act* gives SIRC full access to any information under the control of the Service. This framework keeps those state powers in check—an achievement that, by and large, has stood the test of time.

CONTENTS

MESSAGE FROM THE COMMITTEE MEMBERS

Ensuring that security intelligence in Canada is conducted appropriately, effectively and lawfully in protecting Canada and its citizens—these are responsibilities that the Security Intelligence Review Committee (SIRC) has effectively carried out for over a quarter of a century in Canada. Since 1984, SIRC has taken great care in how it conducts independent reviews and investigations into complaints related to the activities of the Canadian Security Intelligence Service (CSIS). We report our results in the fullest manner possible through this annual report.

SIRC is a core component in a system of checks and balances defined under the *CSIS Act* to keep CSIS accountable to Parliament and to all Canadians. Through the work of our Committee, we demonstrate the importance of conducting security intelligence with integrity both domestically and abroad.

However, SIRC's work doesn't end there. We also strive to show Canadians that our organization contributes to the security of Canada by conducting our work with diligence and

Photo: Couvrette/Ottawa

Members of SIRC (from left to right):
The Honourable Denis Losier, The Honourable Frances Lankin, The Honourable Dr. Arthur T. Porter (Chair), The Honourable Dr. Philippe Couillard and The Honourable Carol Skelton.

flexibility, and by demonstrating that a small organization such as ours can provide significant value in terms of public service.

Our Committee remains well positioned to respond to the changing threat environment. We have been keeping pace with the changing priorities of CSIS; this includes exploring important changes that have taken place in the relationship between the rights of citizens and the security of the state.

Readers of this year's annual report will also note how the scope and pace of change within the security intelligence field continue to grow. We ask those questions that Canadians expect to see asked in assessing how security intelligence is carried out in Canada. **The Committee believes it is time for a public discussion on the future role of security intelligence and, as a corollary, the review function in support of that role—and whether the status quo meets the goals of the Government of Canada along with the expectations of citizens**.

In September 2009, the Honourable Raymond Speaker completed his term on the Committee. Readers should also be aware that in June 2010, the Honourable Gary Filmon, P.C., O.C., O.M. completed his term as Chair of SIRC. All Members of the Committee wish to thank Mr. Filmon for his strong and effective leadership, and Mr. Speaker for his substantial contribution to security intelligence review in Canada. SIRC wishes them the very best in all their future endeavours.

SIRC carries out its mission and mandate with an enormous sense of pride and with a commitment to public service excellence. We are pleased to share with Parliament and all citizens of Canada summaries of our reviews and investigations undertaken during the 2009–2010 fiscal year. Through this annual report, we hope to demonstrate to all Canadians both the thoroughness of our work, and a recognition of the gravity of the task at hand for CSIS in carrying out its duties in helping to safeguard the security of Canada and its citizens.

ABOUT THIS REPORT

SIRC provides assurance to Parliament—and through it, to Canadians—that CSIS investigates and reports on threats to national security in a manner that is effective and 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 (i.e., 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 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 Decade of "The New Normal"

Nearly a decade has passed since the terrorist attacks of 9/11 fundamentally altered Canada's national security paradigm, and today Canadians see a security environment vastly different from the Cold War reality in which the Canadian Security Intelligence Service was created.

Decisions were taken and changes made post-9/11 to respond quickly to what was understood at the time about the threat of terrorism—sometimes without the benefit of much public debate. Indeed, Canada's *Anti-Terrorism Act* (ATA)—designed to improve Canada's ability to detect, investigate and stop terrorist activities at home and abroad—was enacted in the span of just three months.

Billions of dollars in new funds were identified in the 2001 federal budget on a range of activities under the Public Security and Anti-Terrorism Initiative, all with the objective of enhancing Canadian security. To put the magnitude of CSIS's growth during the past decade into perspective: in 2000, CSIS had a budget of $179 million. By 2009, CSIS's budget had more than doubled, reaching $430 million. As part of the broader anti-terrorism initiative, there was a significant reorganization of the security and intelligence community. This included the creation of multiple new structures to better integrate the intelligence community, consistent with the belief that better integration is the key to better intelligence. Moreover, all of this growth and change took place during a very short period of time.

Change came also from the legal environment in which CSIS operates. Intelligence gathered by CSIS is increasingly being used to support criminal prosecutions. The so-called judicialization of intelligence means that CSIS must manage a range of new issues that challenge the way it operates—from handling the testimony of intelligence officers in open court, to dealing with new evidentiary standards that significantly affect how it collects and retains information.

Nothing has changed so markedly as the pushing outwards of Canada's security intelligence activities. Indeed, CSIS has identified one of its top challenges as strengthening its capacity to be effective internationally in support of its national security mandate. Nowhere is the expanding international role of CSIS more apparent than in Afghanistan, where CSIS has been actively supporting the Canadian Forces since their deployment.

Action and Reaction

The magnitude of change that has taken place in the security and intelligence community, and the speed with which those changes have been implemented, have given rise to some unease. This reaction has been most visible in the O'Connor and Iacobucci Commissions of Inquiry and the engagement of the courts in national security issues, as expressed in a number of landmark judicial decisions.

Similar issues are emerging in open societies worldwide. For example, a judicial ruling in the UK challenged the long-standing principle of confidentiality of intelligence exchanges by ruling that certain pieces of intelligence that originated in the US could be summarized

and made public. British parliamentarians have also questioned the need for some of the legislation passed following 9/11, arguing that the post-9/11 environment led to the extension of previously unthought-of powers to those responsible for national security.

In the United States, meanwhile, there has been significant debate and discussion on the status and fate of the prisoners held at Guantanamo Bay. Indeed, this matter has become one of the most visible and potent reminders of the global reaction to 9/11.

Globally, efforts to make travelling by air more secure have resulted in a range of new measures and procedures—no-fly lists, full-body scanners, and greater restrictions on items permitted on board are all features of travel introduced since 9/11. For Canadians, there is now a requirement to have a passport to enter the United States at all border points.

Questions regarding the form and substance of Canada's national security apparatus have been raised in public and parliamentary debates, driven partly by the high-profile judicial inquiries cited above. Calls for taking stock have come from a range of sources, including CSIS itself. As former CSIS Director Jim Judd stated in 2008 at the Global Futures Forum Conference in Vancouver: "the key question for all of us is whether we are succeeding in matching the institutional changes with our environment. Are these the right changes? Are the transformations happening fast enough? Are we going far enough in changing our organizations and how we do business?"

SIRC's Observations

Throughout its history, SIRC has observed that periods of intense change often result in substantial policy gaps—events move more quickly than the ability of policy makers or parliamentarians to make appropriate or necessary statutory or policy reforms. This can lead to incrementalism in which a series of relatively small policy or operational adjustments made over time can culminate in large overall change—all in the absence of cohesive direction from government and without active public engagement.

SIRC has conducted several reviews in recent years to assess the challenges and opportunities that CSIS is facing as it expands its operational activities overseas. As the former Committee Chair stated in a recent parliamentary appearance, CSIS needs government direction on these matters to ensure that it is operating overseas in a way that reflects government priorities. SIRC accepts that the *CSIS Act* permits CSIS to collect security intelligence outside of Canadian borders. However, the *nature* of that activity has been changing—from one strictly of liaison to one that allows for operational activity.

Should CSIS exchange information with countries that may engage in human rights abuses? And if so, what should it do with the intelligence it collects? These questions have preoccupied public debate, and the Committee, for many years. SIRC committed in its last annual report to remain vigilant in reviewing this aspect of the Service's activities. SIRC also knows that as CSIS expands its operations internationally, these questions will become more pressing.

Closer to home, CSIS investigative activities regarding terrorism have become more complicated. Increasingly, successful counter-terrorism measures require close collaboration between intelligence and law enforcement personnel, especially since the introduction of the *ATA*. This complex threat and legal environment means that CSIS has had to engage in activities that extend beyond traditional collection and analysis. In particular, one of SIRC's studies this year found that CSIS has used investigative techniques that have the potential to disrupt terrorist acts. Although

SIRC believes that the use of disruption by CSIS is an appropriate response to the current threat environment, the Committee considers that the use of such measures requires appropriate Ministerial direction and guidance.

The closer cooperation of CSIS and law enforcement has raised additional questions. Examining CSIS's relationships with its domestic front-line partners, one review found that while the government has referenced the need for an integrated national security framework across Canada at a general level through the 2004 *National Security Policy*, more detailed direction through established channels would be required for CSIS to realize specific goals regarding integration.

Beyond law enforcement, there has been more demand from across government for CSIS's intelligence assessments and products. This spike in government interest in intelligence generally extends to the realm of foreign intelligence—a secondary mandate for CSIS. In one of this year's reviews, SIRC examined how CSIS's responsibilities in the area of foreign intelligence have evolved over time. SIRC learned that changes in this area have been extensive and found that the collection of foreign intelligence is no longer as limited at it once was. This raises questions about whether there should be a dedicated foreign intelligence service in Canada, consistent with past thinking on the need to maintain a distinction between foreign and security intelligence, as well as international practice in this regard. This is a question that SIRC has put to the Minister of Public Safety directly through its Section 54 review of CSIS's foreign intelligence program.

Conclusion

In SIRC's 1998–1999 annual report, the Committee wrote: "Canada's history in the field of security intelligence (not to mention sound public policy making) teaches us that it is foresight and opportunity, not crisis and scandal, which should be the spurs to building upon the achievements of recent years." Those sage words were written well before the events of 9/11 created an overwhelming need for action.

In that same annual report, the Committee stated that Canada's security intelligence apparatus was due for a thorough, evidence-based review. More than ten years have passed since then. In the intervening years, the Government of Canada has committed to continuing its efforts to enhance the framework that supports Canada's national security apparatus, including undertaking fundamental reform of the system of oversight and review of that national security apparatus.

SIRC suggests that it is time for a public discussion on what Canadians expect of their intelligence agencies and on the real risks and benefits that such work entails. This should include a discussion about what role is most appropriate for CSIS vis-à-vis foreign intelligence and overseas activities, and an acknowledgement of the tradeoffs that may be required for security intelligence to be effective well into the future.

SECTION 2:
SUMMARIES OF SIRC REVIEWS AND COMPLAINTS
A. Reviews

SIRC's reviews provide Parliament and Canadians with a comprehensive picture of the Service's operational activities. SIRC also carefully examines how CSIS performs its duties and functions to determine if the Service is acting appropriately, effectively and in accordance with the law.

SIRC's reviews provide a retrospective examination and assessment of specific CSIS investigations and activities. The Committee's reviews include findings and, where appropriate, recommendations for the Service and for the Minister of Public Safety. All of SIRC's reviews are forwarded to both the Director of CSIS and the Inspector General of CSIS. SIRC may also provide reports directly to the Minister of Public Safety on any matter which the Committee identifies as having special importance, or which the Minister asks SIRC to undertake.

Each year, SIRC requests a status report from the Service on its recommendations arising from the previous year's reviews and complaint decisions. The status reports give SIRC the opportunity of tracking the implementation of its recommendations and of learning about the practical impact of those recommendations on CSIS. The reports also give CSIS an opportunity to respond formally to the reviews and decisions. This process is thus an important part of the ongoing discussion between CSIS and SIRC and is a benefit to both. Though non-binding, over the years SIRC's recommendations have contributed to making CSIS a better and more accountable organization.

During the 2008–2009 review period, SIRC made seven recommendations from the reviews it conducted. These recommendations were included in the 2008–2009 Annual Report and are available on the SIRC website. Two of the recommendations stem from SIRC's review of CSIS's role in the matter of Omar Khadr. The main substance of the recommendations from this review was that CSIS should establish a policy framework to guide its interactions with youth, consistent with evolving expectations of how an intelligence agency should operate and perform in a contemporary democratic society. SIRC is pleased to report that CSIS has committed to integrating into its policies special considerations to govern its interactions with youth.

Find out more about SIRC's earlier reviews

Over the 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).

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

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

Each review results in a snapshot of the Service's actions in a specific area. 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, the central agencies of government (e.g., Privy Council Office, Treasury Board Secretariat), the Auditor General, the Information Commissioner and the Privacy Commissioner.

SIRC REVIEW: How CSIS Identifies and Addresses Intelligence Priorities

Context

CSIS's core mandate is to collect and analyse security intelligence and to advise the Government of Canada on threats to national security. To accomplish this, the Service must first define and prioritize the government's intelligence requirements. Recently, in response to growing demands for security intelligence across government, CSIS has initiated a multi-year re-engineering of its priority-setting and planning process so that it can continue to increase its collection capacity.

SIRC's Review

SIRC undertook a review of CSIS's 2007–2008 planning process, providing a snapshot of how the Service operated prior to implementing its re-engineering initiative. Specifically, it examined how CSIS defined, prioritized and monitored its intelligence priorities under Section 12 and Section 16 of the *CSIS Act*—in essence, the source of its legal authority to collect, analyse and retain information, and to assist in the collection of foreign intelligence in Canada. SIRC was particularly interested in how intelligence priorities are communicated to CSIS branches and regions.

Requirements under Section 12 are generally defined by CSIS independently through its planning process. However, Section 16 requirements are initiated outside the Service. They are defined through detailed discussions with Foreign Affairs and International Trade Canada and the Department of National Defence, who must formally request that CSIS collect information or intelligence to meet their needs.

Section 12 of the *CSIS Act*

This section authorizes CSIS to collect, analyse and retain information and intelligence on activities that are considered "threats to the security of Canada." It also is the basis on which the Service reports and advises the Government of Canada on its findings.

Section 16 of the *CSIS Act*

This section authorizes CSIS to assist in the collection of foreign intelligence in Canada.

SIRC noted several challenges in how the Service defined and monitored its own intelligence needs during the 2007–2008 planning cycle. These included the lack of a centralized planning document to integrate and prioritize branch intelligence requirements, and problems in engaging federal government stakeholders to define their specific intelligence requirements.

SIRC is pleased that the Service has undertaken to develop a more detailed intelligence requirements process, and believes this will help address many of the challenges identified in the course of this study. Changes being initiated by the Service to its planning process include enhanced dialogue with government stakeholders as a means of better directing Service collection activities to meet the Government of Canada's intelligence requirements. As part of these efforts, CSIS's Intelligence Assessments Branch will incorporate all intelligence needs into a centralized planning document. This will enable CSIS Regions to better allocate resources to meet the needs of its various investigations.

The effectiveness of CSIS's new intelligence requirements consultative process will depend on government partners who understand CSIS's capabilities and limitations, and who are actively engaged in articulating their needs to the Service. To help ensure the success of this re-engineering initiative, SIRC encouraged the Service to ensure that government stakeholders have a good understanding of the new intelligence planning process.

There were no recommendations arising from this review.

SIRC's REVIEW: CSIS's Relationships With Select Domestic Front-Line Partners

Context

It is widely acknowledged in Canada and abroad that the threat of terrorism is beyond the capacity of any one organization to address single-handedly. The Canadian government's *National Security Policy* (2004) acknowledges the need for integration, collaboration and effective partnerships among a range of security and intelligence partners to address threats to national security. For its part, CSIS has long recognized the need to work with its domestic partners as part of its efforts to investigate the contemporary threat environment.

SIRC Review

This study examined the relationship between CSIS and its front-line domestic partners, who together guard against threats to national security. The review focused on partner exchanges, the reasoning behind individual instances of cooperation, and the implications these partnerships might have for the Service. It also considered these relationships within the framework of increased cooperation and integration within Canada's security and intelligence community—a trend shaped by the *National Security Policy* (2004).

Given the very different roles, mandates and government-directed authorities of its domestic partners, and given the different imperatives that CSIS has in comparison to its partners (i.e., it is driven by long-term intelligence/information-gathering), this study asked how exactly those relationships are managed.

SIRC found that the larger the jurisdiction of the domestic agency, the higher the level of coordination and interaction the Service assigns to it. National partners, such as the Canadian Border Services Agency, were provided with liaison from CSIS Headquarters, who employed detailed tools to manage, maintain and analyse that relationship over a period of time. For partners at the provincial (e.g., Ontario Provincial Police) and municipal (e.g., Vancouver Police Department) levels, activity tended to be a regional-level responsibility, conducted most notably via CSIS liaison officers.

Overall, SIRC found that CSIS does very well at cooperating with its front-line domestic partners, meeting with them regularly, enjoying productive relationships and systematically tracking their information exchanges. However, there is still work for the Service to promote the further integration for joint planning activities with its domestic front-line partners—a strategy that is enunciated in the government's *National Security Policy*.

Recommendations In Brief

1) CSIS should reconceptualize its primary tool for managing federal relationships—a tool it calls the Domestic Liaison Program—given the lack of understanding of its function and utility within the Service, and given the absence of tangible results connected to the program thus far.

2) CSIS should take advantage of its access to high-quality information emanating from its law enforcement partners, by adding to its reporting a category to indicate that it received intelligence from those partners.

3) Should the Government of Canada wish to initiate cultural or procedural change concerning the manner in which CSIS interacts with its law enforcement partners, it should do so through the conventional tools that provide direction to the Service (e.g., Ministerial Direction or national priorities), rather than through public policy documents.

SIRC REVIEW: CSIS's Activities Involving Fundamental Societal Institutions

Context

CSIS has long exercised special care when undertaking intelligence investigations that affect—or even appear to affect—fundamental societal institutions. These include the academic, political, religious, media and trade union sectors—all of which were recognized in 1981 by the *McDonald Commission of Inquiry Concerning Certain Activities of the RCMP* as constituting a unique environment for the collection of intelligence. It is a key principle in Canada to weigh various investigative techniques against possible damage to either civil liberties or to these institutions themselves. This principle continues to shape the Service's investigative activities that affect fundamental societal institutions.

SIRC's Review

This review had two distinct yet related objectives. First, it examined CSIS's investigation of threat-related activities within fundamental societal institutions, focusing on the religious sector. Of particular interest was how the Service conducted its investigations without hindering the proper functioning of fundamental institutions or encroaching on individual liberties, as well as how they managed the delegation of decision-making authority overseeing those investigations. Second, it explored CSIS's liaison and outreach efforts with members of the community, many of whom are active members of fundamental societal institutions. In recent years, the Service has implemented a community outreach program to explain more effectively to Canadians its role and mandate.

CSIS's Outreach program

Beginning in 2005, CSIS launched a community outreach program, including what it described as a "strategic and coherent corporate function." Similar to outreach efforts of other federal departments and agencies, this was designed to communicate more effectively with Canadians and to explain its role and mandate to decision makers, citizens, media, academics, security stakeholders and cultural communities. CSIS's program objectives are to improve its public image and citizens' understanding of its role, and to enhance its operations in Canada's large urban centres. CSIS focused particularly on engaging groups who expressed concern that the enhanced security measures taken since 9/11 had violated their civil liberties or harmed their reputations.

With respect to the first objective, SIRC found that CSIS was collecting and retaining information concerning threat-based activities and events taking place within the religious sector. However, this information was related only to the activities of CSIS targets or to threat-related activities such as distributing literature that promoted violence.

SIRC also found that CSIS's fundamental institutions policy and its implementation were strong, and prevented the inappropriate

investigation of religious institutions. SIRC's study stressed that it is incumbent on the Service to maintain its vigilance with regard to investigations that have the potential to affect fundamental institutions.

With respect to the second objective, CSIS's main methods of community engagement include attending meetings of advisory committees representing various ethno-cultural groups, as well as making public presentations at various functions, such as information sessions and community events, on the Service's mandate and role. The goal is to build relationships while emphasizing that all Canadian citizens have a duty to inform authorities of threats to the security of Canada.

SIRC believes that CSIS can improve its outreach program and may be able to draw lessons from the community-policing model. There are valuable lessons to be learned from an approach that emphasizes an interactive, collaborative and mutually beneficial relationship between communities and law enforcement.

Successful outreach hinges on obtaining community support and cooperation. Studies have found that the selective use of community capital for national security reasons can easily undermine the fragile trust-based social relationships between local police and communities. Therefore, although increased interaction with ethnic communities clearly holds operational benefits for the Service, outreach does have its complexities and limitations.

In the long term, if CSIS wishes to sustain its outreach program, it must be clear in establishing benchmarks against which the program's success can be measured. Moreover, there must be a Service-wide understanding of what the program can and cannot achieve. Finally, successful and continued community engagement requires a mutually beneficial relationship—one that takes into consideration what the communities involved can gain from participating in CSIS's outreach efforts.

Recommendation In Brief

SIRC is concerned about the delegation of authority related to investigations involving fundamental institutions. Therefore, SIRC recommends that CSIS follow up within one year to ensure that recent changes to the delegation of authority have retained the challenge and balancing functions that had been embedded in policy.

SIRC REVIEW: Review of the Section 16 Program and the Use of Information Collected

Context

Canadian foreign intelligence capabilities have been a recurrent theme of discussion and debate in Canada for over half a century. Section 16 of the *CSIS Act* defines foreign intelligence as any information about the capabilities, intentions or activities of a foreign state, foreign national or foreign organization. By contrast, Section 12 of the *CSIS Act* defines security intelligence as information and intelligence related to "threats to the security of Canada."

A critical restriction placed on CSIS is that Section 16 information can only be collected within Canada, and cannot be collected on a Canadian citizen, a permanent resident of

SIRC's review of CSIS's Section 16 Program and the use of information collected, was completed 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. 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.

Canada, or a corporation incorporated by or under an Act of Parliament or the legislature of a province.

The creation of CSIS saw primacy given to security intelligence—reflected through National Intelligence Priorities—with a narrow secondary mandate to assist in the collection of foreign intelligence. This model distinguishes Canada from most other Western democracies: the Service has a dual role, and its Section 16 collection is constrained by domestic borders. By contrast, in most Western democracies security intelligence and foreign intelligence are carried out by separate agencies. In those situations, foreign intelligence agencies operate exclusively in foreign jurisdictions and by definition break the laws of those jurisdictions in order to collect information.

Over the decades, various governments as well as SIRC have examined the utility of Canadian agencies operating as spies in addition to spy catchers. The consensus has consistently been that the status quo should be maintained, with Canada receiving the vast majority of its foreign intelligence through open-source collection by the Department of Foreign Affairs and International Trade and by the Department of National Defence, or from technical source collection through the Communications Security Establishment.

SIRC's Review

This review examined the Service's Section 16 program, focusing on how cumulative changes have affected the once-rigid distinctions between Section 12 and Section 16.

The review found that CSIS's policies and procedures for collecting, analysing and disseminating products under Section 16 of the *CSIS Act* have evolved to reflect greater demands for intelligence across government. To meet these demands, the Committee found that the Service has increasingly linked Section 12 and Section 16 priorities—what CSIS refers to as *blended collection*.

SIRC is concerned at the potential implications of the melding of the Service's Section 12 and Section 16 mandates and concludes that these changes are of consequence for the future direction of the Service. If this were to continue, CSIS could become what Parliament never intended it to be: namely, a Service with equal security intelligence and foreign intelligence mandates. Such a development would not only go against public arguments to the contrary, but would additionally ignore the

Recommendation In Brief

The Committee recommends that the Government of Canada provide direction and/or guidance to the Service concerning its expanding role in foreign intelligence.

longstanding practice of respected allies who intentionally separated these divergent intelligence functions to help ensure government control and accountability.

SIRC REVIEW: CSIS's Use of Disruption to Counter National Security Threats

Context

The nature of terrorism today has complicated the ways in which CSIS conducts its investigative activities. Increasingly, successful counter-terrorism measures require close collaboration among intelligence and law enforcement personnel, especially since the introduction of the *Anti-Terrorism Act*.

This complex threat and legal environment means CSIS has had to engage in activities that extend beyond traditional collection and analysis. For example, whenever CSIS conducts investigations, an intended or unintended consequence can be to counter or disrupt a threat to national security. This may include making it generally known to targets that their activities are being investigated, thus reducing the likelihood that the targets will continue with their plans. It is also possible that a threat may be disrupted unintentionally, wherein an activity undertaken by the Service could dissuade an individual from pursuing future threat-related behaviour even though that result was not intended.

The Service recognizes that such tactics depart from typical forms of information collection, and that certain risks must be managed when undertaking this investigative activity. Despite this risk, CSIS regards these efforts to be in accordance with the *CSIS Act*.

SIRC's Review

SIRC understands that countering or disrupting is part of investigating threats to national security, and may even be necessary to protect Canadians. However, the Committee's review raised four issues concerning the Service's use of disruption. These require further consideration.

First, disruption potentially overlaps with efforts already exercised by police agencies in Canada. Second, although CSIS's mandate under Section 12 does not explicitly prohibit the use of disruption, neither does the authority to collect and analyse intelligence and report to and advise the Government of Canada thereon, appear to capture such activities. Third, SIRC believes that Ministerial knowledge of CSIS's use of disruption would be appropriate in certain circumstances. Fourth, there are no CSIS guidelines to help with the design and implementation of disruption operations, or to prepare for the potential consequences of such investigative activity.

The Service's statutory mandate resulted from a series of illegal acts and practices carried out by the RCMP, examined in the *McDonald Commission of Inquiry Concerning Certain Activities of the RCMP*. The *CSIS Act* and the *Security Offences Act* were designed to ensure that security offences would be investigated by the police and prosecuted in the courts, while security intelligence collection and analysis would be performed by CSIS. Additionally, Canadians were to take comfort in knowing that the federal government was clear on where the lines of demarcation lay between law enforcement and intelligence.

The McDonald Commission also recognized that government and police forces in Canada require *advance intelligence*—emphasis on those two words would later become key to CSIS's mandate, an organization devoted to information gathering, analysis and dissemination. As the McDonald Commission stated:

> *"The preventing or countering action is taken by a police force or government department exercising an authorized government function, and the security intelligence agency's contribution is confined to its proper role of collecting and reporting security intelligence."*

This view of an intelligence agency's role is consistent with the CSIS Director's May 11, 2010, testimony before a House of Commons Standing Committee. For example, when asked if CSIS has sufficient legislation powers in place to do its job, and if that meant that preventative arrest and investigative hearings were therefore not required, the Director responded:

> *"I would say that question is more appropriately answered by my colleague the Commissioner of the RCMP. From our perspective, what we try to do is collect information, make it available to the police and others and it's for them to decide whether they're going to do something to disrupt or counter."*

The nature of contemporary terrorism has complicated matters for federal departments and agencies. For the Service, it has meant adapting to novel threat environments, including a progression toward increased foreign activities and investigations within cyberspace. SIRC believes the use of investigative techniques that result in disruption is also a manifestation of CSIS's efforts at adapting to the changing threat and legal environment.

The Committee believes that if CSIS has determined it is necessary to disrupt threats to national security, then the Government of Canada should be made aware of this. This goes to the heart of Ministerial accountability for the Service and therefore should be conducted in accordance with the Minister's full knowledge.

Furthermore, while there is ample and well-tested CSIS policy on both the conduct of investigations and interviews, SIRC maintains that clear rules and procedures regarding deliberate or probable disruption are necessary for the Service to account for the use of its powers.

Recommendations In Brief

1) SIRC recommends that CSIS seek Ministerial guidance and direction regarding the use of disruption.

2) SIRC also recommends that CSIS develop formal guidelines regarding its use of disruption.

SIRC's REVIEW: CSIS's Decision-Making In Relation to Foreign Investigative Activities

Context

CSIS policy concerning Foreign Investigative Activities has evolved rapidly over the past few years, a reflection of the expansion of the Service's overseas activities that have become a significant source of the information and advice which they provide to government. As those activities have expanded, new challenges—from the management of foreign relationships and of CSIS personnel, to securing the personal safety of CSIS employees abroad—have all come to the fore.

SIRC Review

This review explored CSIS decision-making related to Foreign Investigative Activities by studying activities at three Foreign Offices, the locations of which are classified. A large portion of the review focused upon a new decision-making tool, which permits the delegation of operational decision-making downward to the Foreign Office from CSIS Headquarters when the level of risk is assessed as low. SIRC found that this delegation provided for improved and practical use of local expertise, had a positive effect on perceptions of the Service by its partners and allies, and increased the efficacy of local operations, while allowing adequate consultation with CSIS in Ottawa. Although the specific risks and cost of each case must be evaluated against its potential gains, this new tool for local authority has developed into a useful Service practice.

This review also explored a specific Service foreign relationship and found the relationship to be one that warrants further and careful consideration by CSIS. As the Service increases its activities overseas, such relationships will become increasingly central to the effectiveness of the information collected and provided to government, and hence, must be pursued with more attention to the level of risk that they carry.

Finally, this review examined elements of the Service's recent policies concerning the use of firearms. Because SIRC found certain elements of the policy to be underdeveloped, the Committee recommended several concrete steps to shore up Service practice and thinking on this subject.

Recommendations In Brief

1) The Service has made its case to DFAIT (and through this review, to SIRC) in support of a cautious resumption of operational exchanges with a particular foreign agency; CSIS is confident that the risks of human rights violations and other operational risks can be professionally managed, and that proper precautions can be taken. However, SIRC recommends that CSIS reconsider the utility of re-establishing exchanges of operational information with this foreign agency.

2) SIRC recommends that CSIS clarify its criteria for declaring a Dangerous Operating Environment.

3) SIRC recommends that, should CSIS seek to change the scope of its policy on firearms, it should do so only after additional careful study and after consultation with, and approval of, the Minister of Public Safety.

SECTION 2: SUMMARIES OF SIRC REVIEWS AND COMPLAINTS
B. Complaints

In addition to its review function, SIRC conducts investigations into complaints concerning CSIS. Complaint cases may begin as inquiries to SIRC—either in writing, in person or by phone. Once a written complaint is received, SIRC staff will advise a prospective Complainant about what the *CSIS Act* requires to initiate a formalized procedure for complaints investigations.

Process

Once a written complaint is received, SIRC conducts a preliminary review, which can include any information that might be in the possession of CSIS, except for Cabinet confidences. Where a complaint does not meet certain statutory requirements, SIRC declines jurisdiction and the complaint is not investigated.

If jurisdiction is established, complaints are investigated through a quasi-judicial hearing presided over by one or more Committee members, assisted by staff. A party 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, and with the respondent (CSIS) and the respondent's counsel.

SIRC's legal team provides advice on procedural and substantive matters, and will also cross-examine Service and other witnesses when, for national security reasons, evidence must be heard without the Complainant being present.

Once SIRC has established jurisdiction, the time to resolve a complaint can vary in length depending on a number of factors, including the complexity of the file, the quantity of documents to be reviewed, the number of hearings, and the availability of the participants.

What is the difference between a review and a complaint investigation?

A **review** is initiated by SIRC and entails in-depth research and analysis of CSIS's performance in carrying out its duties and functions as described in the *CSIS Act*, culminating in a report. 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*. Research and reports constitute SIRC's review function, while complaint investigations are conducted as part of a quasi-judicial process.

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 investigates "any act or thing done by the Service." Under Section 42, it investigates 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, the Committee provides a report to the Director of CSIS, the Minister of Public Safety and the Complainant.[1] 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.

Table 1 provides the status of all complaints directed to SIRC over the past three fiscal years. The total number of files include: those that are carried over from the past fiscal year; new complaints (including those that were deemed to be misdirected to SIRC, deemed to be outside SIRC's jurisdiction, or investigated and resolved without a hearing (i.e., via an administrative review); and those complaints that were resolved by means of a full hearing and a subsequent report. In 2009–2010, four such reports were issued.

Did you know that...
SIRC investigates complaints referred by the Canadian Human Rights Commission

According to the *Canadian Human Right Act*, if the Canadian Human Rights Commission receives written notice from a Minister of the Crown that a practice to which a complaint relates is a matter of national security, the Commission can either dismiss the complaint or refer the matter to SIRC. On receipt of such a referral, SIRC carries out an investigation and, after consulting with the Director of CSIS, reports its findings to the Canadian Human Rights Commission, to the Minister who referred the complaint, as well as to the Complainant.

Table 1: Complaints

	2007–08	2008–09	2009–10
Carried Over	20	15	22
New	32	30	32
Total	**52**	**45**	**54**
Closed	37	23	23

1 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 INVESTIGATION: Alleged Improper Conduct By CSIS

SIRC investigated a complaint pursuant to Section 41 of the *CSIS Act* in which the Complainant alleged disrespectful and inappropriate conduct by CSIS, and the Service's lack of interest regarding the Complainant's experiences in a foreign country.

As part of SIRC's investigation, a hearing was held. The Complainant testified that he had contacted CSIS by telephone to recount to a CSIS employee his experiences in a foreign country and had offered to provide additional written information. The Complainant further testified that after calling the CSIS employee a number of times and after sending the CSIS employee numerous letters, he received a call from a second CSIS employee who allegedly threatened him and who was rude and obnoxious on the phone. SIRC also heard the testimony of the CSIS employee whose conduct was alleged to be improper, and was left with two different versions of the facts.

In the absence of corroborating evidence to prefer one version over the other, SIRC found that the Complainant had not been able to demonstrate, on a balance of probabilities, that the CSIS employee in question had engaged

in disrespectful and inappropriate conduct. Further, with respect to CSIS's alleged failure to take seriously the Complainant's experiences in a foreign country, SIRC found the allegation to be unsubstantiated.

SIRC INVESTIGATION: Alleged Unauthorized Consultation By CSIS*

SIRC investigated a complaint, filed under Section 41 of the *CSIS Act*, in which the Complainant alleged that CSIS had consulted a third party entity without obtaining the Complainant's consent.

After its investigation, SIRC concluded that it was satisfied with the explanation provided by CSIS and found that CSIS had the proper authorization to consult with the third party entity on the Complainant's file and that it did not need the Complainant's consent.

Recommendation In Brief

SIRC recommended that CSIS approach the third party entity to request the removal of any CSIS reference in the Complainant's file to ensure that in the future, no one other than the Complainant will have knowledge of CSIS's inquiry with the third party entity.

SIRC INVESTIGATION: Alleged Harassment and Interference By CSIS In Obtaining Employment

SIRC investigated a complaint that CSIS interfered with the Complainant's efforts to obtain federal government employment by inducing her to provide CSIS with information, and that in the course of this interference, CSIS acted in a coercive, harassing and intimidating manner.

The Complainant sought to obtain a number of contract positions within the federal government. However, the Department of Public Works and Government Services (PWGSC)—the department that has the authority to confer an applicant's reliability status—would neither grant nor deny her that status.

PWGSC's refusal overlapped with a series of interviews of the Complainant by CSIS in which the Service expressed an interest in obtaining information from the Complainant concerning past associations and time spent abroad.

SIRC's investigation established that PWGSC's decision not to grant the Complainant's reliability status request was neither directly nor indirectly caused by CSIS. Although the status was granted shortly after the Complainant filed a complaint to CSIS, SIRC is satisfied in this instance as well that the decision to grant the status was independent of the Complainant's actions with respect to CSIS.

** Note: This report was signed in May 2010.*

An additional component of the complaint concerned the manner in which CSIS allegedly conducted interviews with the Complainant. Specifically, the Complainant alleged CSIS employees acted aggressively and in a manner that was improperly coercive and intrusive. Further, she maintained that alleged suggestions by CSIS during two of the interviews—that her cooperation would determine the outcome of her security clearance requests in the future—amounted to improper intimidation. SIRC took these allegations very seriously and reviewed the evidence carefully.

SIRC concluded that interviews can be aggressive and pressing and still be conducted within the bounds of propriety—as they were in this case. Although the Complainant found the interviews upsetting, SIRC found that the interviews were conducted appropriately.

SIRC also investigated the second point of the complaint, regarding CSIS's references to the Complainant's potential need for a security clearance. SIRC found that although CSIS interviewers agreed that they conveyed to the Complainant an explicit connection between her honesty during the interviews and the likelihood that she might obtain a security clearance in the future, the statements by the interviewers in this regard were correct. If a person is dishonest in an interview with CSIS, the ability to obtain a security clearance in the future could be seriously impaired. SIRC agreed with CSIS that this type of statement can be fair notice to the person being interviewed. That said, SIRC is well aware that threats can be both explicit and implied. In this situation, SIRC was satisfied the interviewers did not cross the line between giving fair notice and conveying threats.

Recommendation In Brief

SIRC recommended that CSIS approach the appropriate Treasury Board Secretariat officials to ensure that government departmental security officials are aware of and are encouraged to use the guidelines and approvals processes for making inquiries beyond those described in the Government Security Policy for reliability status.

SIRC INVESTIGATION: Alleged Improper and Unprofessional Conduct By CSIS*

In this case, SIRC investigated a complaint concerning the conduct of a CSIS employee. Specifically, the Complainant alleged that the CSIS employee acted improperly and unprofessionally and, as a result, there was a detrimental effect on his life.

SIRC's investigation included a detailed review of CSIS's documents as well as testimony from the Complainant, a member of the Complainant's family and representatives from CSIS. On the basis of the evidence, SIRC was unable to conclude that the CSIS employee's actions had the alleged detrimental effect on the Complainant's life. In particular, SIRC found that there had been sufficient external factors that could have contributed to the Complainant's misfortune.

Notwithstanding the fact that the CSIS employee in question was unable to testify and that no other CSIS official could testify on the conduct of the CSIS employee when meeting with the Complainant, SIRC concluded that there was credible evidence that the CSIS employee acted inappropriately during the period in question. SIRC found that the documentary evidence showed inconsistencies which could have been detected by CSIS management, and that this suggested a lack of effective oversight.

**Note: This report was signed in May 2010.*

SECTION 3: SIRC AT A GLANCE

Committee Membership

SIRC is chaired by the Honourable Dr. Arthur T. Porter, P.C., M.D. The other Committee Members are: the Honourable Frances Lankin, P.C.; the Honourable Denis Losier, P.C.; the Honourable Dr. Philippe Couillard, P.C., M.D.; and the Honourable Carol Skelton, P.C.

All Members of SIRC are Privy Councillors, and are given full access to highly classified government information. Members are appointed by the Governor-in-Council after consultation by the Prime Minister with the leaders of the opposition parties.

In addition to attending regular committee meetings, Members preside over complaint hearings. Reviews and complaint reports are prepared in consultation with SIRC staff. Members also visit CSIS regional offices, appear before 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 includes a Research Manager, a Senior Counsel, a Corporate Services Manager, and other professional 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 the CSIS

Committee Activities

October 2009: The Executive Director met with organizers of the International Intelligence Review Agencies Conference (IIRAC) in Sydney, Australia to design the program for the March 2010 conference.

October 2009: Several staff attended a conference of the Canadian Association of Security and Intelligence Studies, held in Ottawa.

November 2009: The Executive Director gave a lecture at a Carleton University course on National Security and Intelligence in the Modern State.

January 2010: The Executive Director, along with representatives from CSIS, including the Office of the Inspector General, the Department of Justice, and Foreign Affairs and International Trade Canada, participated in a capacity-building exercise in Costa Rica.

March 2010: The Chair, Committee Members and the Executive Director attended the International Intelligence Review Agencies Conference, hosted by the Inspector-General Intelligence and Security in Sydney, Australia.

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 affecting national security intelligence.

SIRC also visits CSIS regional offices on a rotating basis to understand and assess 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 2009–2010 fiscal year, SIRC visited two regional offices.

Performance

To fulfil its mandate, SIRC carries out activities to meet the following strategic outcome:

> *To ensure that CSIS performs its duties and functions in accordance with the law, policy and Ministerial Direction.*

With respect to human resources, 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.

Table 2: SIRC expenditures 2009 10 ($ millions)

	2009–10 (Estimates)	2009–10 (Actual)
Personnel	2.0	1.6
Goods and Services	0.9	0.8
	2.9	**2.4**

List of SIRC Recommendations

During the 2009–2010 review period, SIRC made the following recommendations stemming from the reviews it conducted, as well as from the complaints it investigated.

Report[2]	SIRC Recommendations
CSIS's Relationships With Select Domestic Front-Line Partners	CSIS should reconceptualize its primary tool for managing federal relationships—a tool it calls the Domestic Liaison Program—given the lack of understanding of its function and utility within the Service, and given the absence of tangible results connected to the program thus far. CSIS should take advantage of its access to quality information emanating from its law enforcement partners by adding to its reporting a category to signal that it received intelligence from those partners. Should the Government of Canada wish to initiate a cultural and procedural change concerning the manner in which CSIS interacts with its law enforcement partners, it should do so through the conventional tools that provide direction to the Service (e.g., Ministerial Direction or national priorities), rather than through public policy documents.
CSIS's Activities Involving Fundamental Societal Institutions	SIRC is concerned about the delegation of authority related to investigations involving fundamental institutions. Therefore, SIRC recommends that CSIS follow up within one year to ensure that the delegation of authority has retained the challenge and balancing functions that had been embedded in policy.
Review of the Section 16 Program and the Use of Information Collected	SIRC recommends that the Government of Canada provide direction and/or guidance to the Service concerning its expanding role in foreign intelligence.

continued...

2 Consult the SIRC website at www.sirc-csars.gc.ca for a list of all SIRC reviews conducted since 1984.

Report	SIRC Recommendations
CSIS's Use of Disruption to Counter National Security Threats	SIRC recommends that CSIS seek Ministerial guidance and direction regarding the use of disruption. SIRC also recommends that CSIS develop formal guidelines regarding its use of disruption.
CSIS's Decision-Making In Relation to Foreign Investigative Activities	The Service has made its case to DFAIT (and through this review, to SIRC) in support of a cautious resumption of operational exchanges with a particular foreign agency; CSIS is confident that the risks of human rights violations and other operational risks can be professionally managed, and that proper precautions can be taken. However, SIRC recommends that CSIS reconsider the utility of re-establishing exchanges of operational information with this foreign agency. SIRC recommends that CSIS clarify its criteria for declaring a Dangerous Operating Environment. SIRC recommends that, should CSIS seek to change the scope of its policy on firearms, it should do so only after additional careful study and after consultation with, and approval of, the Minister of Public Safety.
Alleged Unauthorized Consultation By CSIS	SIRC recommended that CSIS approach the third party entity to request the removal of any CSIS reference in the Complainant's file to ensure that in the future, no one other than the Complainant will have knowledge of CSIS's inquiry with the third party entity.
Alleged Harassment and Interference By CSIS In Obtaining Employment	SIRC recommended that CSIS approach the appropriate Treasury Board Secretariat officials to ensure that government departmental security officials are aware of and are encouraged to use the guidelines and approvals processes for making inquiries beyond those described in the Government Security Policy for reliability status.

APPENDIX: 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, and highlights any major changes or developments within CSIS.

For SIRC's 2009–2010 Annual Report, this information is grouped into two categories: security intelligence activities and security screening activities.

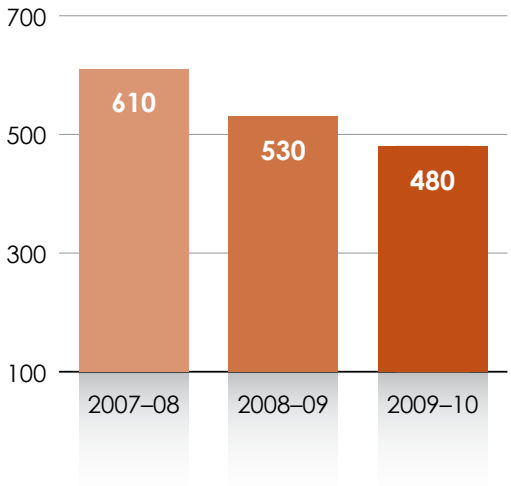
A. Security Intelligence Activities

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 suspected threat. Figure 1 indicates the number of targets investigated by CSIS during the period under review, relative to previous fiscal years.

Figure 1

Targeting statistics*



* Figures have been rounded to the nearest ten.

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

	2007–08	2008–09	2009–10
New warrants	71	26	36
Replaced or renewed	182	183	193
Total	**253†**	**209††**	**229†††**

† Included in this number were 19 urgent warrants.

†† Included in this number were 2 urgent warrants.

††† There were no urgent warrants reported this year.

B. Security Screening Activities

Security screening is one of the most publicly visible functions conducted 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 an individual's loyalty to Canada and (so far as it relates thereto) the reliability of that 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.

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.

Note: the total number of site-access screening requests received in 2009–2010 was significantly higher than in previous years, due to the volume of requests received related to the 2010 Olympic and Paralympic Winter Games in Vancouver.

Table 4 : Requests for CSIS government security screening*

	2007–08	2008–09	2009–10
Requests from Department of National Defence (DND)	8,800	15,300	15,000
Requests from other clients	41,500	46,400	49,300
Total	**50,300**	**61,700**	**64,300**
Assessments issued to DND	8,300	14,400	15,900
Assessments issued to other clients†	40,500	46,300	50,900
Total	**48,800**	**60,700**	**66,800**

* Figures have been rounded to the nearest 100.

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

Table 5: Median turnaround time (in calendar days) for CSIS to complete security assessments

		2007–08		2008–09		2009–10	
		New	Updates	New	Updates	New	Updates
DND	Level I (Confidential)	23	9	74	57	6	54
	Level II (Secret)	28	23	61	62	22	76
	Level III (Top Secret)	164	29	126	57	119	35
Non-DND	Level I (Confidential)	18	13	18	6	20	16
	Level II (Secret)	13	12	15	16	20	19
	Level III (Top Secret)	186	4	145	8	156	16

Table 6: Requests to CSIS for site access screening*

	2007–08	2008–09	2009–10
Parliamentary Precinct	1,100	1,000	1,100
Airport restricted access area (Transport Canada)	36,800	31,400	32,600
Nuclear facilities	9,200	11,100	9,500
Free and Secure Trade (FAST)	10,700	6,400	7,700
Special events—Olympics	N/A	N/A	200,100
Special events accreditation	1,300	16,300	720
Marine Transportation Security Clearance Program†	6,300	5,200	2,300
Other government departments	2,100	2,600	3,400
Total	**67,500**	**74,000**	**257,420**

* Figures have been rounded to the nearest 100.

† 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 (IRPA)* do not gain entry to—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 issued in relation to these requests.

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

Table 7: Requests to CSIS for Citizenship and Immigration screenings and briefs issued

	Requests*			Briefs		
	2007–08	2008–09	2009–10	2007–08	2008–09	2009–10
Permanent resident†	66,000	67,300	68,400	195	213	144
Front-end screening††	21,800	26,800	23,500	117	108	95
Refugee determination†††	6,600	6,600	9,200	142	102	116
Subtotal	**94,400**	**100,700**	**101,100**	**454**	**423**	**355**
Citizenship applications	190,000	169,500	175,500	109	169	60
Total	**284,400**	**270,200**	**276,600**	**563**	**592**	**415**

* 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.

Table 8: Turnaround time (in days) for CSIS to complete notices of assessment

	2007–08	2008–09	2009–10
Citizenship	1	1	1
Immigration (Canada)†	59	95	77
Immigration (USA)††	45	65	71
Overseas immigration	20	26	22
Refugee determination	64	89	72
Front-end screening	28	29	23

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