SECURITY INTELLIGENCE
REVIEW COMMITTEE

Annual Report
2010–2011

Checks and Balances

Viewing Security Intelligence Through the Lens of Accountability

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. PS105-2011E-PDF
ISSN 1912-1598

Security Intelligence Review Committee

Comité de surveillance des activités de renseignement de sécurité

September 30, 2011

The Honourable Vic Toews
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 2010–2011, 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.

About 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). It conducts reviews of CSIS activities and investigates complaints from the public about the Service. In doing so, SIRC provides assurance to Parliament and to all citizens of Canada 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. For more information on SIRC, consult www.sirc-csars.gc.ca.

About CSIS

The Canadian Security Intelligence Service (CSIS) is responsible for investigating threats to Canada, analyzing information and producing intelligence.

To protect Canada and its citizens, CSIS advises the Government of Canada on issues and activities that are, or may pose, 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.

A legal framework for both SIRC and CSIS

By virtue of the *CSIS Act*, Canada became one of the first democratic governments anywhere 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, and created accountability mechanisms to keep those considerable state powers in check—a model that, by and large, has stood the test of time.

Contents

MESSAGE FROM THE COMMITTEE MEMBERS **2**

ABOUT THIS REPORT **4**

SECTION 1: THE YEAR IN REVIEW **5**

SECTION 2: SUMMARIES OF SIRC REVIEWS AND COMPLAINTS **9**

A. Reviews **9**

CSIS's Use of the Internet 12

CSIS's Private Sector Relationships 13

CSIS's Intelligence-to-Evidence Process 15

CSIS's Investigation of Cyber Threats 17

CSIS's Relationship with a "Five Eyes" Partner 19

The Role of CSIS in the Interviews of Afghan Detainees 21

How CSIS Evaluates the Reliability of Human Sources 23

B. Complaints **25**

Alleged Improper Conduct by CSIS 27

Alleged Delay in Providing a Security Assessment 28

Alleged Unjust, Unfounded and Unethical Assessment of an Applicant for Permanent Residency 29

SECTION 3: SIRC AT A GLANCE **30**

Committee Membership 30

Staffing and Organization 30

Committee Activities 31

List of SIRC Recommendations 32

Message from the Committee Members

Building and maintaining trust in public institutions are tenets of a free, democratic society. This task is especially challenging when an institution cannot be subject to rigorous public scrutiny because much of its work must be carried out under the veil of secrecy. Such is the case with the Canadian Security Intelligence Service (CSIS), which has a responsibility to collect intelligence relating to threats to Canada's national security.

For over 25 years, the Security Intelligence Review Committee (SIRC) has worked to ensure that this powerful organization is accountable to Parliament and to the citizens of Canada. The same legislation that established the legal authority for CSIS's activities also created an elaborate system of checks and balances on its powers. SIRC's role, therefore, is to help ensure that the Service respects the fundamental rights and freedoms of Canadians while it investigates threats to national security.

Specifically, SIRC strives to ensure that CSIS carries out its duties in a lawful, effective and appropriate manner. It does so through continuous review of CSIS's activities and through the investigation of complaints against the Service, and by making findings and recommendations to the Minister of Public Safety and the Director of the Service. Our work is summarized, to the fullest extent permitted by law, in this annual report.

Although the Service's mandate has remained unchanged since its creation, CSIS's work has taken on a complexity not foreseen 25 years ago—unavoidably so, in a world where international threats emerge and proliferate at sometimes dizzying speed.

While SIRC has adjusted the way it deploys its resources to meet these altered circumstances, we have not strayed from the basic tasks set for us in 1984 by Parliament. As we see it, our job is to make independent, meticulous and fair-minded assessments of the facts as we find them, and to provide cogent advice and recommendations to government based on those assessments.

Amidst the shifting sands of public opinion, and the rapid pace of international events and change, SIRC's role and composition take on special importance. As Members, we bring considerable and diverse expertise to our work, having served in a variety of public sector fields—politics, medicine, public administration and NGOs, to name a few. That expertise gives us a collective awareness of—and sensitivity to—matters of public importance, while our arm's-length status means that we can act in a scrupulously non-partisan fashion. Canadians expect our work to transcend events and politics, and we will remain vigilant to ensure that it does.

This year's report aims once again to engage parliamentarians and indeed, all Canadians, on a number of important issues relevant to security intelligence. These are highlighted in *The Year in Review* and *Summaries of SIRC Reviews and Complaints* (Sections 1 and 2 of this annual report, respectively). We hope to advance the goal set out in last year's report: to generate public discussion on the future role and challenges of security intelligence, as well as the review function in support of that role.

In today's heightened threat environment, it is important that Canada's security intelligence service has the authority and capacity to investigate new threats. Equally important, those activities need to be carried out within a framework that provides proper accountability. Collective security must not come at the expense of individual rights and freedoms, and SIRC will maintain that clear principle at the forefront of its work.

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.

About This Report

SIRC derives its mandate and functions from the same law that sets out the Service's legal framework: the *Canadian Security Intelligence Service Act*. In accordance with this legislation, SIRC annually prepares a public report of its activities, which is tabled before Parliament by the Minister of Public Safety.

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 in security intelligence and how these relate to select findings and recommendations by SIRC from the previous year.

Section 2

Summaries of SIRC Reviews and Complaints

A synopsis of the reviews completed by SIRC, as well as the complaint reports issued during the fiscal year covered by this annual report.

Section 3

SIRC at a Glance

Highlights the public engagement, liaison and administrative activities of SIRC. This includes details of its annual budget and expenditures.

SECTION 1:

The Year in Review

This year, SIRC expanded its public engagement activities in pursuit of a goal we set out in our 2009–2010 Annual Report: to stimulate public discussion on the future role of security intelligence and, as a corollary, the review function in support of that role. Again and again, these discussions touched on one theme: that, in the aftermath of 9/11, Canada has seen greatly enhanced operational cooperation among the almost two dozen federal departments involved in national security.

Yet Canada's system of checks and balances, designed decades ago to ensure the accountability of individual agencies, has not kept pace with these changes. The existing review mechanisms—including SIRC—are neither configured nor equipped to examine fully Canada's increasingly integrated national security activities. At the same time, many departments and agencies currently involved in national security are not subject to any form of independent review.

Review of Canada's national security activities

Three commissions of inquiry—O'Connor, Iacobucci and Major—have reported in the past five years on matters relating to Canada's national security activities, and all have come to the same conclusion. *The Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar* (also known as the O'Connor Commission), in particular, undertook an in-depth examination of Canada's national security accountability framework. Mr. Justice O'Connor proposed a greatly expanded role for SIRC, given its longstanding expertise in the review of national security activities. SIRC's new role would encompass ongoing, independent review of the national security activities of four departments in addition to CSIS, specifically the Department of Foreign Affairs and International Trade Canada (DFAIT), the Financial Transactions and Reports Analysis Centre (FINTRAC), Citizenship and Immigration Canada (CIC) and Transport Canada.

The key question in our minds is this: do these activities warrant permanent, independent and ongoing review? The national security activities of other federal entities certainly have the potential to have an impact on individuals. For example, Canada Border Services Agency (CBSA) can refuse a person entry into Canada, and CIC has the power to remove someone from Canada. Yet these powers do not compare to CSIS's capacity to collect intelligence in secrecy—activities that may have a direct impact on individuals' civil rights and liberties, but without their knowledge. CSIS's robust review mechanisms were designed as a

counterweight to the Service's ability to act covertly and in ways that can profoundly affect individual lives. Accordingly, we question whether the same level of permanent and independent review is required for departments and agencies whose mandates do not provide similar powers.

Looking ahead—retooling SIRC

The *CSIS Act*, which provides SIRC with the power and ability to review thoroughly every aspect of CSIS's activities and operations, is not broken. Still, the nature and extent of change within the security intelligence environment causes us to reflect on Canada's national security accountability structure and SIRC's role within it.

Justice O'Connor observed correctly that the national security activities of many federal entities have become largely intertwined in the aftermath of 9/11. SIRC's recent reviews have underscored this finding. CSIS now liaises and works closely with numerous federal partners on a daily basis, a trend that will likely intensify as the Service pursues a more active and intricate domestic and foreign agenda. CSIS's activities are examined exhaustively and reported on by SIRC through its reviews and investigation of complaints. The challenge is to provide Canadians with the same level of reassurance about all of the government's national security operations, writ large.

We believe that independent review of Canada's national security activities could be enhanced by retooling SIRC—achievable without major legislative amendments, expense or restructuring. This would allow for a proportionate yet effective system of broad, independent review for national security.

At present, in the context of reviews, SIRC cannot examine and assess national security matters that go beyond CSIS—even though they may be influenced by the Service's actions or advice. A slight adjustment to SIRC's mandate could address this gap, allowing for more comprehensive reviews of CSIS's information-sharing and interactions with domestic partners. Further, it would enable SIRC to examine the actions of other federal entities when they connect with, or relate to, CSIS. Additionally, a minor amendment to the *CSIS Act* could permit SIRC—at the request of the Minister of Public Safety and with the concurrence of the appropriate Minister—to undertake a national security review of an agency or agencies other than CSIS. These modest changes would be cost-effective, and could help to alleviate public concerns regarding Canada's existing system of national security accountability.

This year's review of CSIS's role in interviewing Afghan detainees is a case in point. SIRC's ability to review the actions of other involved departments would have resulted in a more comprehensive examination and, by the same stroke, helped to build a broader public account of Canada's national security activities abroad. Whether or not structural change occurs, SIRC will continue to ensure that its reviews provide the fullest assessment possible of CSIS's activities.

SIRC'S observations

SIRC has responded to the changing national security environment by looking at CSIS's operational activities in novel ways, and delving into new lines of inquiry. SIRC also is committed to making its work and findings public to the fullest extent possible as a way of contributing to the public discussion on national security.

In this spirit, this year featured several "baseline" reviews on new topics, including one that focused on the evolving nature of CSIS's interactions with the private sector. Although SIRC regularly examines CSIS's relationships with domestic and foreign counterparts and other public sector partners, we chose for the first time to take an in-depth look at CSIS's cooperation with the private sector. The review concluded that, despite the impetus towards greater cooperation with the private sector, especially with the owners and operators of some of the nation's critical infrastructure, there are significant legal and practical limitations on the Service's ability to work closely with the private sector.

Of note, the review revealed an emerging gap between CSIS's legal framework, created three decades ago during the height of the Cold War, and the post-9/11 operational reality. The idea of CSIS working closely with non-government actors was not envisaged when the *CSIS Act* was passed in 1984. At that time, intelligence activities were focused largely on countering espionage and subversion threats, and did not require the extensive networks that have since been established to counter the global terrorist threat. Thus far, CSIS has managed to work within the existing framework, but SIRC is concerned that these gaps may begin to strain the Service's operational effectiveness or lead it to carry out activities that fall outside its mandate.

"SIRC has responded to the changing national security environment by looking at CSIS's operational activities in novel ways, and delving into new lines of inquiry."

At the same time, CSIS has been modernizing its traditional investigative techniques to keep pace with new threats. This process was underscored in SIRC's examination of CSIS's investigation of cyber threats, which is among the federal government's intelligence priorities. The review looked at the innovative strategies and tools CSIS is using to move forward with this important investigation. Similarly, through our review of the Service's use of the Internet, we gained an appreciation of the way in which this medium supports CSIS's activities.

SIRC also followed through on its commitment to pay close attention to CSIS's expanding foreign investigative activities. This year, we did so by examining a very public issue, CSIS's role in the interviews of Afghan detainees, within the framework of its overall operational activity in Afghanistan. SIRC concluded that CSIS should assess and qualify, with care and consistency, information originating from agencies that may engage in human rights abuses—concerns that have animated previous SIRC reviews.

More broadly, we found that the Service's involvement with the Afghan detainees provides lessons that can be applied

to other operations abroad. Although overseas operations unfold in unique circumstances and present different challenges, CSIS should strive to ensure that the management of its operations abroad mirrors, to the extent practicable, the standards of administration and accountability that are maintained domestically.

This year's review of CSIS's cooperation with a "Five Eyes" partner offered insight into another dimension of the Service's work abroad. SIRC found that the expansion of CSIS activities abroad requires a more integrated approach with its domestic partners. Specifically, we urged CSIS to give further consideration to how it keeps the Department of Foreign Affairs and International Trade—which is ultimately responsible for managing Canada's international relations—regularly apprised of its overseas activities.

Information sharing and cooperation with domestic partners are obviously core components of CSIS's intelligence work, and therefore run through this year's reviews. SIRC looked at one of the Service's most important relationships—with the RCMP—through the lens of one of the intelligence community's most important contemporary challenges: the use of intelligence as evidence. The Committee was left with a positive impression of RCMP–CSIS cooperation, and a strong appreciation of the complexities and challenges of reconciling the need to protect secret intelligence with the need to share it with law enforcement in support of criminal prosecutions.

These findings are only a few highlights of our reviews. Detailed summaries of all the reviews undertaken in the last year are found in the following pages.

Conclusion

Our perspective on a possible future role for SIRC and the results of our reviews are offered here as part of our contribution to a public dialogue on national security. Indeed, Parliament conceived this advisory role for us in 1984 by anticipating that SIRC would play a "vital role in the functioning of the security intelligence system" by promoting "adequate debate, where necessary, in the area of security." Should the government proceed to implement a broader system of independent review for agencies involved in national security, SIRC hopes that its views will assist decision-makers in achieving improvement and in building the confidence of Canadians in their national security apparatus.

SECTION 2:

Summaries of SIRC Reviews and Complaints

A. REVIEWS

SIRC's reviews are designed to provide Parliament and the Canadian public with a broad understanding of the Service's operational activities. In carrying out its reviews, SIRC examines how CSIS has performed its duties and functions to determine if the Service was acting appropriately, effectively and in accordance with the law.

SIRC's reviews provide a retrospective examination and assessment of specific CSIS investigations and activities. Our research program is designed to address a broad range of subjects on a timely and topical basis.

The difference between oversight and review

Outside Canada, intelligence oversight bodies, such as the select committees of the United States Senate and Congress, examine on a continuous basis the actions of the intelligence agencies. They have the mandate to evaluate current investigations or decisions in "real time," and usually monitor budget and administration, as well. As a result, oversight bodies can be implicated in the decision-making process of intelligence agencies because they have the capacity to influence those decisions as they are being made.

In Canada, by contrast, SIRC reviews past operations of the Service. SIRC is not involved in the day-to-day operational or administrative decisions and activities of the Service, nor is SIRC implicated in those decisions. Reviews give us the distinct advantage of being able to assess fully CSIS's performance, unfettered by any earlier involvement on our part.

In deciding which matters to review, SIRC considers:

- events or developments with the potential to represent threats to the security of Canada;
- intelligence priorities identified by the Government of Canada;
- 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 and initiatives announced by or affecting CSIS; 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 case. 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. SIRC can also examine files relating to CSIS's cooperation and operational exchanges with foreign and domestic agencies and partners, among other sources, that may be review-specific. The goal is to look at a diverse pool of information so that we can ensure that we have thoroughly reviewed and completely understood the issues at hand.

Find out more about SIRC's earlier reviews

Over the years, SIRC has reviewed a wide range of CSIS activities. A complete listing of SIRC's past reviews can be found on our website (**www.sirc-csars.gc.ca**).

Throughout the years, SIRC has reviewed a wide range of CSIS activities, both domestically and abroad. We have done so by looking at:

- activities undertaken at various CSIS stations around the world;
- activities and investigations of CSIS regional offices;
- CSIS's cooperation and exchanges of information with domestic and foreign partners; and
- specific operational techniques such as CSIS's use of human sources and covert intercepts.

The Committee's reviews include findings and, where appropriate, recommendations. These reviews are forwarded to the Director of CSIS, the Inspector General of CSIS, and Public Safety Canada.

Accountability matters

SIRC is one of several mechanisms designed to ensure CSIS's accountability. 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 of Canada, the Information Commissioner of Canada and the Privacy Commissioner of Canada.

SIRC's recommendations

Each year, SIRC requests a status report from CSIS on the recommendations arising from the previous year's reviews and complaint decisions. This update gives SIRC the opportunity to track the implementation of our recommendations and to learn about the practical impact of those recommendations on CSIS. This process also allows CSIS to respond formally to SIRC's reviews and decisions, thereby contributing to the ongoing discussion between CSIS and SIRC.

Previously, during the 2009–2010 review period, SIRC made 12 recommendations addressing a wide range of issues. SIRC is pleased to note that CSIS has responded to several of these recommendations. For example, in response to recommendations made in SIRC's review of CSIS's relationships with select domestic front-line partners, CSIS has revamped the primary reporting tool it uses to gauge the status of its domestic relationships, and it is also examining the idea of adding a category in its reporting to indicate when intelligence found in reporting originated from law enforcement partners. Furthermore, in response to SIRC's recommendation that CSIS seek Ministerial guidance on the use of disruption to counter national security threats, CSIS responded that it has brought the issue to the Department of Public Safety for consideration.

SIRC REVIEW:
CSIS's Use of the Internet

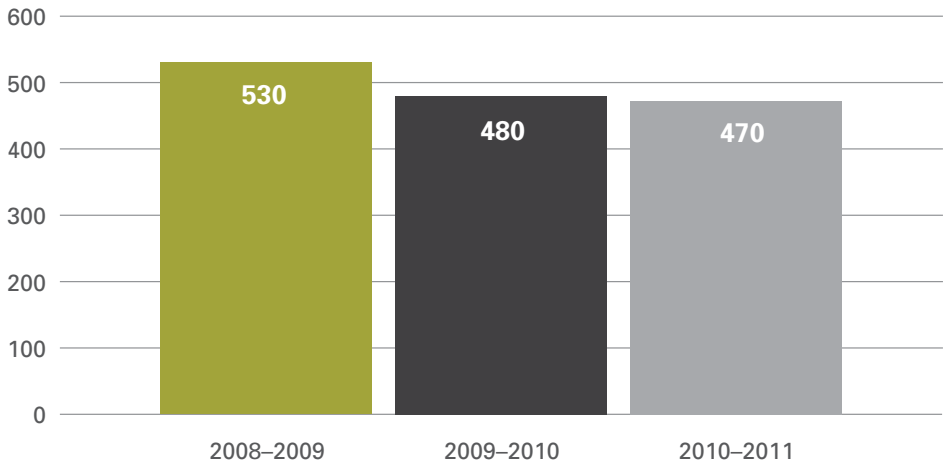
Over the span of a generation, information available via the Internet has grown exponentially. Today, it is a vast, interactive medium that offers significant anonymity to people who communicate online.

Of particular concern to security intelligence agencies and law enforcement is the growing role that online activities play in the radicalization of individuals who may become threats to Canadian interests. Today, people who may never have met can create networks, mobilize and plan threat-related activities—all without ever having to leave home. For those who pose a threat to Canada and its allies, online activities play an important role at every stage of radicalization, giving direct access to unfiltered extremist ideology, as well as providing a nearly anonymous meeting place for like-minded radical individuals.

As a result, threat-related online activities have moved to the forefront of many national security investigations. This medium has come to play an important operational role in CSIS investigations: for example, key targets of the "Toronto 18" group were initially detected through the monitoring of material posted online.

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. The figures below indicate the number of targets (rounded to the nearest 10) investigated by CSIS in the past three fiscal years.



SIRC's review

This review examined the strategies, policies and processes that guide CSIS's use of the Internet by focusing on the role of a specialized unit established in 2001. SIRC looked specifically at how this unit's work helps to generate leads and push investigations forward. SIRC's review also looked at the information collected online by the Service.

SIRC's review found that CSIS's use of the Internet has become increasingly common. It is therefore important that the Service have the resources in place to deal with the workload. In that regard, SIRC supports the findings of an internal audit that recognized the importance of addressing these resource issues.

Overall, SIRC found CSIS's approach to its online work to be sound and flexible. SIRC also noted that the Service had developed useful guidelines for certain Internet-based activities. These guidelines incorporate lessons learned and best practices into a useful reference tool.

SIRC identified two issues concerning CSIS's use of the Internet.

First, CSIS's interactions with young Canadians will no doubt increase as extremists continue to use the Internet to attempt to radicalize youth. Indeed, much of the extremist content posted online to recruit and radicalize individuals is targeted at youth—one of the largest groups of Internet users in Canada and elsewhere. SIRC did not take issue with CSIS collecting information online. However, SIRC believes that the Service needs to give special consideration when dealing with information concerning youth. At issue was the volume of information pertaining to young people being retained by CSIS as part of its operational reporting. SIRC believes that CSIS should impress upon its employees the need to exercise added caution when collecting and retaining information relating to youth.

Second, SIRC underscored the importance of CSIS applying the "strictly necessary" test when collecting and retaining information online. The Internet offers vast amounts of easily accessible information, and care should be taken to ensure that such information is subject to the same "strictly necessary" test as information collected from other sources.

SIRC REVIEW:
CSIS'S Private Sector Relationships

Increased collaboration with non-traditional partners is a growing trend in security intelligence in Canada and elsewhere. Traditionally, CSIS's relationships were with domestic and foreign partners in the public sector, such as domestic police services, other Canadian government departments and agencies, or governments or institutions of foreign states. Today, the Service is also reaching out to non-traditional partners, such as the private sector.

SIRC's review

This review examined CSIS's growing relationship with the private sector in the context of national security. SIRC examined the Service's general liaison and outreach efforts with private sector organizations, which are conducted primarily at the regional level. CSIS has two main programs through which most of these interactions take place:

- the Public Liaison and Outreach Program—briefings intended to sensitize the public sector to CSIS's mandate and to establish CSIS as a point of contact for potentially threat-related information; and
- the Liaison and Awareness Program—more focused briefings on specific threats.

SIRC concluded that CSIS's interactions with the private sector are important and can be helpful when pursuing more specific investigative leads.

SIRC looked at a few instances where CSIS was able to capitalize on private sector relationships. Overall, the Committee found that developing rapport within that milieu is key to CSIS capitalizing on private sector information. In particular, it recognized the efforts of CSIS liaison officers in this regard.

SIRC learned that, in the past, the Service employed a more coordinated and strategic approach with respect to building its private sector relationships. In the interests of leveraging the limited resources available for these activities, and of capitalizing on the experience already gained, **SIRC recommended that CSIS expand on the efforts undertaken in regional offices by articulating a Service-wide strategy on managing its relations with the private sector**. In SIRC's opinion, an effective strategy would involve identifying those

Rules on sharing information regarding security intelligence

The *CSIS Act* prohibits disclosure of information obtained by the Service in the course of its investigations, except in the performance of its duties and functions under the *Act*, or the administration or enforcement of the *Act* or other laws.

Section 19 specifically identifies situations where such sharing of information is permitted:

- disclosures to law enforcement and to officers of the court in an investigation or prosecution;
- disclosures to the Minister of National Defence or of Foreign Affairs, or departmental officials, when the information is relevant to matters relating to Canada's defence or international affairs; or
- disclosures authorized by the Minister of Public Safety that are considered to be in the public interest.

sectors with the greatest potential to be of investigative value to the Service.

At the same time, there are limitations on CSIS working more closely with the private sector because of the strict laws that govern official information-sharing. The *CSIS Act* does not authorize disclosure of information collected by the Service to non-traditional or non-governmental partners, such as private sector organizations. Section 12 of the *CSIS Act* limits CSIS's responsibility to report to and advise the Government of Canada on national security threats. Although operational policies have been developed to govern information-sharing with the private sector, the policies are appropriately restrictive and provide strict parameters for what information can be shared.

For these reasons, the Service strives to engage and support the private sector's security needs in other ways. For example, it tries to share more unclassified information, namely through its participation in the Integrated Threat Assessment Centre, which produces threat assessments that are distributed to the private sector, among others. Efforts are also underway to increase the number of security clearances for individuals in the private sector, to allow for more meaningful exchanges on issues relating to national security threats.

Finally, CSIS conducts security clearances for the private sector when such requests are sponsored by a federal department or agency, or by an appropriate provincial authority. Under the Sensitive Site Screening program, for example, CSIS provides clearances for individuals seeking to obtain access to sensitive locations, including nuclear sites, international airports and special events, such as the 2010 Winter Olympics.

SIRC will continue to examine CSIS's relationships with the private sector in future reviews and will pursue, where appropriate, the issues raised in this study to enhance its understanding of the benefits and challenges of the Service's relationships with non-traditional partners.

SIRC REVIEW:
CSIS's Intelligence-to-Evidence Process

Cooperation and information-sharing among members of Canada's security and intelligence community have always been key characteristics of Canada's national security efforts. The relationship between CSIS and the RCMP, in particular, has moved to the forefront following the passage of the *Anti-terrorism Act* (2001). As a result of this legislation, CSIS and the RCMP have had to work more closely together since activities related to terrorism can constitute both a threat to the security of Canada and a crime under the *Criminal Code*.

In the intervening decade, intelligence has been disclosed in a growing number of criminal proceedings—a process that some have called the "judicialization of intelligence" or the "intelligence-to-evidence" process.

In 2008, the Director of CSIS publicly acknowledged that intelligence agencies have had to confront a "range of legal issues such as disclosure, evidentiary standards, and the testimony of intelligence personnel in criminal prosecutions," all of which have had profound implications for how intelligence work is undertaken and carried out in Canada.

SIRC's review

SIRC's review examined how CSIS has responded to the increased use of security intelligence in criminal proceedings. It explored how the Service and the RCMP cooperate while still respecting each other's roles in counter-terrorism investigations, and what lessons have been learned from recent terrorism prosecutions.

"SIRC found that CSIS and the RCMP have implemented a process that allows for an effective operational partnership."

First, SIRC's review looked at the framework governing cooperation between CSIS and the RCMP, as well as the approaches and tools that the Service—either separately or in conjunction with the RCMP—has developed to manage this important relationship. SIRC found that significant progress had been made in this area. In particular, it found that CSIS and the RCMP have implemented a process that allows for an effective operational partnership.

Next, SIRC took a closer look at how this approach was put to the test during the Toronto 18 investigation—one of the first major prosecutions under the *Anti-terrorism Act* to have worked its way through the criminal justice system. In SIRC's view, this case demonstrated CSIS's ability to work effectively with the RCMP under the new law.

SIRC also examined in detail two judgments rendered by the Ontario Superior Court of Justice in the course of the Toronto 18 trials, focusing on CSIS's operational coordination and information exchanges with the RCMP. Overall, SIRC found that the Service's response to both rulings provides useful guidance for future counter-terrorism investigations and prosecutions.

Recognizing that discussions concerning intelligence-to-evidence are ongoing, SIRC identified three issues that CSIS may wish to examine more closely.

First, SIRC looked at the two-letter mechanism (i.e., disclosure and advisory letters) currently used by the Service to disclose information to law enforcement. Typically, a disclosure letter is treated as a tip or an investigative lead to initiate or advance a criminal investigation, and is not to be used by police to obtain a warrant. An advisory letter, on the other hand, is the formal means by which CSIS authorizes law enforcement to use its information in applications to the courts to obtain a warrant.

To improve the quality and value of the information that CSIS provides to its law enforcement partners, and to bring consistency to the way in which CSIS discloses information to law enforcement, **SIRC recommended that CSIS adopt a one-letter disclosure model that incorporates the standards of rigorous legal review currently set for advisory letters**.

Second, the importance of cooperation—both early and often—with the RCMP was a recurrent theme. Cooperation in an active investigation entails exchanges at multiple levels, both formal and informal. In its review, SIRC found a gap in the Service's records of daily operational and strategic exchanges with the RCMP. It is important that CSIS keep proper records of verbal exchanges, consistent with recent jurisprudence on the subject of retention, as well as CSIS's own approach to the retention of records.

Third, the Toronto 18 trial demonstrated that the courts in Canada are prepared to challenge the means by which CSIS acquires information disclosed to the RCMP, such as through warrant intercepts. This underscores the importance of ensuring that the principle of full, fair and frank disclosure is entrenched in the CSIS warrant application process. SIRC believes that the obligation to provide full, fair and frank disclosure of all material facts to the courts should be fully understood by all CSIS employees.

The use of security intelligence in criminal proceedings will continue to evolve as CSIS and law enforcement gain more experience in working collaboratively in counter-terrorism investigations, and as more court decisions provide guidance. Further direction may also come from the federal government: in its December 2010 response to the *Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182*, the government committed to undertake initiatives to improve the relationship between the use of intelligence and its application as evidence in criminal proceedings. SIRC will continue to examine CSIS's relationship with the RCMP, as it is the Service's most important domestic partner.

SIRC REVIEW:
CSIS's Investigation of Cyber Threats

Post 9/11, Western security intelligence agencies have focused their efforts on countering terrorism. Recently, however, the Director of CSIS stated that Canada is experiencing levels of espionage comparable to the height of the Cold War. Indeed, recent events, such as the discovery of a Russian spy ring operating in the United States in the summer of 2010, serve as a reminder that the threat of espionage is still very real.

Complicating the work of intelligence agencies is the fact that espionage activities have, much like terrorism, changed in nature. Today, individuals, groups and state-sponsored agencies are increasingly using cyberspace to break into government and private sector networks to steal secrets. Accordingly, protecting Canada against cyber threats has become increasingly important to the Government of Canada.

SIRC's review

This review examined CSIS's investigation of a cyber threat and, more broadly, how CSIS's efforts contribute to Canada's cyber security. First, SIRC examined the nature of the cyber threat in question, as well as some of the key challenges associated with investigating the threat. SIRC then took a closer look at the strategies and tools CSIS was using to move the investigation forward, especially with regards to human source recruitment. Finally, SIRC explored CSIS's role within a broader "whole-of-government" approach to countering the cyber threat.

SIRC noted that CSIS's role in investigating cyber threats is limited by its mandate, which is to collect information on threats to the security of Canada and to advise government. To fulfill this goal, CSIS has developed a two-pronged approach to its cyber investigations: first, to seek to attribute cyber attacks against Canada, and second, to determine the motivation behind the attacks.

SIRC's review found that the migration of espionage threats into the cyber realm has required an expansion of CSIS's efforts and, over time, the introduction of new methods and powers to use in both the physical and virtual world. For example, CSIS has sought a new range of court-approved warrant powers that are designed to keep pace with the rapidly changing cyber threat environment and, at the same time, to generate investigative leads. SIRC noted that the Service's new approach appears to have established clear benchmarks for the future success of cyber investigations. In addition, CSIS has tried to optimize operational resources deployed against cyber threats.

CSIS is one of many players that support wider government efforts to mitigate cyber

Warrants

The power to authorize intrusive investigative techniques rests strictly with the Federal Court of Canada. The granting of a warrant provides CSIS with authorization to use investigative techniques that would otherwise be illegal, such as the monitoring of telecommunications activities. This table shows the number of Federal Court warrants that were approved in the past three fiscal years.

	2008–09	2009–10	2010–11
New warrants	26	36	55
Replaced or renewed	183	193	176
Total	**209**[†]	**229**	**231**

[†]*Included in this number were two urgent warrants.*

threats. The largest role falls to Communications Security Establishment Canada (CSEC), which is responsible for protecting the government's computer systems and networks, and for providing it with related mitigation advice. SIRC found that CSIS works very closely with CSEC on cyber incidents, and that their work is complementary. While CSEC's signals intelligence provides CSIS with investigative leads, information collected in the course of CSIS's investigations can enhance CSEC's ability to respond to cyber threats.

Finally, SIRC noted that CSIS conducts briefings with federal government departments and private sector organizations as part of a "whole-of-government" approach to raising awareness of cyber threats. Although this outreach is necessary and within CSIS's investigative duties, targeted outreach efforts hold the potential to develop into activities that could be seen as mitigation. Mitigation, which refers to advice provided to victims, or potential victims, from designated government agencies, does not fall within CSIS's mandate on this file. CSIS's role is consistently outlined as one of support, through its investigative activities, to the government's mitigative efforts which are led by CSEC.

SIRC recognizes that liaison activities are a complement to CSIS's investigative methods, and provide opportunities for CSIS to advance its investigation into cyber threats. However, as CSIS positions itself to keep pace with cyber threats, it should remain focused on its investigative role, and continue to use caution not to engage in activities that could be seen as mitigation.

In fall 2010, the federal government introduced *Canada's Cyber Security Strategy*, which defines the roles and responsibilities of departments and agencies on a range of cyber issues, including cyber-espionage. Given its expertise and mandate, Communications Security Establishment Canada (CSEC) plays a key role. The strategy calls on CSEC to enhance its capacity to detect and discover threats and to respond to cyber threats and attacks against government communications networks and information technology systems. For its part, CSIS is called upon to investigate and advise government on threats to the security of Canada, which includes cyber threats.

SIRC REVIEW:
CSIS's Relationship With a "Five Eyes" Partner

Collaboration with domestic and foreign counterparts is essential for any intelligence agency to fulfill its mandate. This is especially true following the events of 9/11, as intelligence agencies have had to cooperate even more closely to counter a global terrorist threat.

During the Second World War, Britain and the United States worked together closely in intercepting the communications of their enemies—what is commonly known as signals intelligence. In 1946, in the context of the emerging Cold War with the Soviet Union, the two major powers decided to institutionalize this cooperation through a formal agreement. Two years later, Canada joined this alliance, with New Zealand and Australia following suit in 1956. Over the years, the "Five Eyes" has expanded its networks and increased its partnerships with other agencies, leading to greater information-sharing on a variety of state and non-state threats to member countries.

In Canada, CSIS has recognized that the expansion of its investigative activities abroad has led to an unprecedented level of cooperation with foreign partners. Underpinning this collaborative work are the Service's foreign arrangements, which allow for cooperation and exchanges of information on issues of common concern. CSIS has implemented over 250 foreign arrangements with counterparts around the world; chief among these are the relationships the Service maintains with what is commonly known as its "Five Eyes" partners.

SIRC's review

This review examined the history and transformation of the Service's role within the Five Eyes community by undertaking an in-depth examination of CSIS's cooperation and exchanges with one Five Eyes partner. SIRC's review was complemented by a visit to the CSIS foreign station that is responsible for managing these partnerships abroad, and meetings with CSIS's domestic counterparts at the DFAIT Mission.

The Committee found that, in recent years, changes to the threat environment, fiscal pressures and technological advancements have underscored the importance of collaboration within the Five Eyes community. SIRC also found that CSIS's expansion of collection activities abroad has led to more information-sharing on targets of mutual concern to the alliance.

The review found a high level of cooperation between CSIS and its Five Eyes partner. Furthermore, cooperation and shared concerns over current issues such as radicalization, the growing use of the Internet and the challenges posed by the growing use of intelligence in criminal proceedings, have contributed to making this country's security and intelligence agencies key partners for CSIS.

In the course of this review, SIRC identified one issue for CSIS's consideration as it expands its collection capabilities and activities abroad. SIRC recognizes the

importance of effective interdepartmental communication, especially between CSIS and DFAIT, which is responsible for managing Canada's international relations.

CSIS shares information with DFAIT on a regular basis through several means, ranging from formal disclosures and cooperation at the Headquarters level to direct engagement by CSIS Heads of Station with DFAIT Heads of Mission and/or other DFAIT employees at the Mission. In recent years, the scope of this relationship has expanded with CSIS undertaking more operational activities abroad. In 2005, as CSIS planned to increase its foreign operations, it recognized that a new Memorandum of Understanding (MOU) would have to be struck with DFAIT to help manage issues of mutual interest. The MOU signalled CSIS's recognition that it was a member of a larger Canadian contingent operating abroad, with associated responsibilities.

Yet, SIRC found that there were limited exchanges on CSIS's foreign operational activities with DFAIT, despite the MOU advocating "close cooperation, consultation and coordination" with respect to intelligence activities in Canada and abroad. Building on this observation, **SIRC recommended that CSIS adopt a broader interpretation of its disclosure commitments to DFAIT, to allow the department to prepare itself in the event of an adverse development arising from CSIS's foreign operations**.

SIRC REVIEW:
The Role of CSIS in the Interviews of Afghan Detainees

Within months of 9/11, Canada became involved in a United Nations-led mission to overturn the government of, and stabilize, Afghanistan. One aspect of Canada's involvement in that conflict—the processing of Afghan detainees—has been a flashpoint of public discussion. In 2009, the Canadian public, media and Parliament became aware of CSIS's involvement in the interviewing of detainees in support of Canadian operations in Afghanistan. In recognition of the importance of this file, SIRC announced during an appearance before the Standing Committee on Public Safety and National Security in May 2010 that it would conduct a review of CSIS's involvement in this matter.

CSIS Director Richard Fadden also commissioned an internal study of the Service's participation in the interviews of Afghan detainees, the key findings of which were reported in the media in February 2011. The purpose of the CSIS study was to provide an overview of CSIS's role in this matter: to review its knowledge (or lack thereof) of the abuse/mistreatment of detainees, and to ascertain the legal risk regarding its involvement in these interviews. Overall, SIRC found that CSIS's study achieved its goals, and that the report accurately reflected the nature and extent of CSIS's involvement in Afghanistan. In particular, SIRC's review found no indication

that, in the period during which CSIS conducted detainee interviews, CSIS officers posted to Afghanistan had any first-hand knowledge of the alleged abuse, mistreatment or torture of detainees by Afghan authorities.

SIRC's review

The focus of SIRC's review was broader than the internal CSIS study, and was designed to explore the larger context within which CSIS activities, policy and decision-making evolved with respect to Afghan detainees. SIRC examined the role of the detainee interviews within the framework of the Service's operations in Afghanistan; the nature, utility and effectiveness of CSIS's relationship with its Afghan partners, as well as its exchanges of information with those partners; and finally, any lessons learned that could have a bearing on CSIS's future involvement in these types of overseas operations.

"Overall, SIRC found that the Afghan detainee experience provided opportunities for CSIS to enhance its approach to managing operations overseas."

SIRC noted two issues that warranted further consideration: first, the need for CSIS to assess and to qualify, with care and consistency, information originating from agencies that may engage in human rights abuses; and second, the need for CSIS to ensure that the management of its operations abroad mirrors, to the extent that is practicable, the standards of administration and accountability that are maintained domestically.

On the first issue, SIRC found that the information gathered by CSIS's local partners to identify threats to Canada and Canadian operations in Afghanistan was of operational value to the Service. Given ongoing human rights concerns and the possibility that information provided to CSIS could have been derived from torture, it was important that CSIS address this risk by managing its relationship and exchanges of information carefully. One of CSIS's standard risk-mitigation techniques is to use caveats, that is, qualifying statements which accompany information sent from CSIS to a partner agency. SIRC found that it took almost five years after CSIS became involved in Afghanistan for CSIS to caveat these exchanges properly.

The manner in which CSIS should engage with foreign agencies that may not share Canada's stance on human rights has been outlined in Ministerial Direction, as well as in the 2008 CSIS Deputy Director Operations Directive. SIRC believes that CSIS's Directive makes great strides to promote consistent awareness of the possibility of torture-derived information, and to enhance accountability surrounding the exchange and use of such information. However, the Committee found that the wording of the preamble may leave CSIS vulnerable to potential challenges or criticism regarding its policy on information-sharing with

agencies that have a poor human rights record. As a result, **SIRC recommended that CSIS reword the preamble of the Directive governing exchanges with agencies suspected of human rights abuses, to eliminate any possible misunderstanding**.

The second issue addresses lessons learned for future overseas operations from CSIS's interviews of Afghan detainees. SIRC noted that CSIS did not comprehensively document its role in the interviews of Afghan detainees by keeping records that would confirm the numbers and details of all of the detainee interviews. SIRC believes that, should CSIS continue to expand its activities abroad and to provide support to Canadian efforts in volatile regions of the world, it will need to improve its record management practices in those regions to enhance its own internal accountability.

Along similar lines, SIRC found that, early in CSIS's involvement, there was enough information available on the situation in Afghanistan for the Service to have appreciated the complexity of the environment in which it was operating. As a result, SIRC believes CSIS could have moved more quickly to put in place additional direction or guidelines to promote greater accountability.

Overall, SIRC found that the Afghan detainee experience provided opportunities for CSIS to enhance its approach to managing operations overseas. If CSIS continues to expand its operations abroad, it should take all reasonable measures to ensure that the management of operations meets, as far as is practicable, the standards of administration and accountability that are maintained domestically. This would include strengthening CSIS's ability to consider the potential implications of those operations prior to undertaking them, and increasingly embracing the notion that, while overseas operations present a different set of challenges, those challenges can be anticipated and planned for and do not have to be conceived as "exceptions" in CSIS's overall strategic planning.

SIRC REVIEW:
How CSIS Evaluates the Reliability of Human Sources

In carrying out its investigations against threats to the security of Canada, CSIS draws upon multiple sources of information, including human sources. Human intelligence is obtained from people who are not professionally trained as intelligence agents, but instead are recruited to provide information to which they have access. Human source operations are extremely sensitive and can be dangerous and difficult. For these reasons, special controls are required to ensure sources' security and safety, as well as to mitigate risks to the Service.

CSIS has long regarded its human source program as the most cost-effective and efficient means of accessing privileged information. Recent successful human source operations reinforce this point: human sources' penetration of, and

reporting on, the Toronto 18 terrorist cell, for example, were instrumental in the successful prosecution of the main conspirators.

SIRC's review

Past SIRC reviews have examined a number of human source issues, but generally with a focus on assessing the degree to which CSIS conducted human source operations in conformity with legislation and operational policy. This review moved beyond these considerations to an assessment of the efficiency and effectiveness of CSIS's human source "validation" process, meaning the way in which CSIS assesses a source's information access, reliability and reporting history to determine the value or weight of information he/she provides.

The validation process is crucial to CSIS's recruitment, development and management of successful human source operations. Accordingly, CSIS officers are guided by various instruments and techniques outlined in the Service's operational policies. To complement this framework, CSIS officers also seek advice from senior investigators and/or managers, as well as from the branch at CSIS HQ that is responsible for providing operational support services, policy guidance and operational security relating to human source issues.

SIRC's review noted that a fast-changing and more complex domestic and international operational environment compelled CSIS to take a closer look at its human source validation process. As a result of this exercise, CSIS identified a need to improve its ability to cope with demographic pressures, employee training and issues related to managerial supervision and mentorship.

Building on CSIS's own observations, the Committee made three recommendations designed to enhance the Service's validation process. **First, SIRC recommended that CSIS develop more rigorous criteria, or seek to establish best practices, with respect to human source validation. Second, CSIS should create a human source "lessons learned" database that is accessible to all intelligence officers to enhance their professional development. Finally, SIRC recommended that CSIS conduct a more systematic method of human source file reviews to help ensure that best practices are being followed and that any findings and/or recommendations are incorporated into the lessons learned database.**

B. COMPLAINTS

In addition to its review function, SIRC conducts investigations into complaints concerning CSIS made by either individuals or groups. The types of complaints that SIRC investigates are described in the *CSIS Act* and can take several forms. Under Section 41 of the *CSIS Act*, SIRC investigates "any act or thing done by the Service"; under Section 42, SIRC investigates complaints about denials of security clearances to federal government employees and contractors. SIRC may also conduct an investigation in relation to referrals from the Canadian Human Rights Commission and Minister's reports in regards to the *Citizenship Act*.

The complaints process at SIRC

Complaint cases may begin as inquiries to SIRC—either in writing, in person or by phone. Once a written complaint is received, SIRC staff advise a prospective complainant about what the *CSIS Act* requires to initiate a formal complaint.

Once a formal complaint is received in writing, 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 and SIRC's legal team which will provide legal advice to members on procedural and substantive matters. Pre-hearing conferences may be conducted with the parties to establish and agree on preliminary procedural matters, such as the allegations to be investigated, the format of the hearing, the identity and number of witnesses to be called, the production of documents in advance of the hearing and the date and location of the hearing.

The time to investigate and resolve a complaint will vary in length depending on a number of factors, such as the complexity of the file, the quantity of documents to be examined, the number of hearing days required (both in the presence and the absence of the complainants), and the availability of the participants.

The *CSIS Act* provides that SIRC hearings are to be conducted "in private." All parties have the right to be represented by counsel and to make representations at the hearing, but no one is entitled as of right to be present during, to have access to, or to comment on, representations made to SIRC by any other person. A party may request an *ex parte* hearing (in the absence of the complainant and possibly other parties) to present evidence which, for reasons of national security or other reasons considered valid by SIRC, cannot be disclosed to the other party or their counsel. During such hearings, SIRC's legal team will

cross-examine the witnesses to ensure that the evidence is appropriately tested and reliable, in order to provide the presiding Member with the most complete and accurate factual information relating to the complaint. Once the *ex parte* portion of the hearing is completed, SIRC will determine whether the substance of the evidence can be disclosed to the excluded parties. If so, SIRC will prepare a summary of the evidence and provide it to the excluded parties once it has been vetted for national security concerns.

When SIRC's investigation of a complaint made under Section 41 is concluded, it provides a report to the Director of CSIS and to the Minister of Public Safety, as well as a declassified version of the report to the complainant.

On completion of an investigation in relation to a complaint under Section 42 of the *CSIS Act*, SIRC reports its findings and any recommendations to the Minister, the Director of CSIS and the Deputy Head concerned, and provides a declassified version of the report to the complainant.

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).

Table 1
Complaints directed to SIRC

	2008–09	2009–10	2010–11
Carried over	15	22	31
New	30	32	17
Total	**45**	**54**	**48**
Closed[†]	23	23	32

[†]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 complaint was discontinued.

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 under Section 41 of the *CSIS Act* in which two complainants alleged that CSIS employees, in attempting to interview one of them, conducted themselves in an inappropriate, harassing and disrespectful manner.

The CSIS employees in question went to the home of one of the complainants on a number of occasions over a period of several days, until they were able to meet with the complainant. SIRC found that the Service had a legitimate interest in interviewing the complainant, and that it was necessary to return to that individual's residence until they were successful in securing an interview.

SIRC determined that questioning by CSIS employees can sometimes appear to be aggressive and pressing without being improper or constituting harassment. In the circumstances of this complaint, SIRC found that the interview conducted by the CSIS employees was within the bounds of propriety and did not constitute harassment.

Further, the two complainants alleged that the CSIS employees minimized the significance of the interview by suggesting that the presence of a lawyer was not required. On this point, SIRC agreed with the Service's position that the presence of a lawyer is not always necessary, especially when conducting preliminary interviews. SIRC also maintained, however, that if an individual wishes to have a lawyer present, those wishes should be respected.

In addition, the complainants alleged that the CSIS employees failed initially to identify themselves properly by indicating only that they were representatives of the federal government. SIRC found that the CSIS employees acted appropriately in this regard. Not identifying themselves to members of the complainant's family as CSIS employees is done, in part, to protect the privacy interests of the complainant.

SIRC also concluded, however, that the CSIS employees could have left a business card, and that this would likely have helped expedite a meeting with the complainant. Similarly, when the complainant indicated that he would not speak to the Service without a lawyer, SIRC found that the reaction of the CSIS employee—which was to refer the complainants to the phone book for CSIS's general number—was unprofessional.

The final component of the complaint involved an allegation that the conduct of the CSIS employees constituted a violation of the *CSIS Act* as well as Sections 7, 9 and 15 of the *Canadian Charter of Rights and Freedoms*. Although SIRC found certain aspects of the CSIS employees' conduct to have been unreasonable or unprofessional, the evidence did not support a claim that the complainants' rights under the *Charter* were engaged.

SIRC INVESTIGATION:
Alleged Delay in Providing a Security Assessment

SIRC investigated a complaint regarding the alleged delay by the Service in providing its security assessment for a complainant's site access clearance, required for the purpose of employment.

In its investigation, SIRC found that the Service spent over 15 months processing the request for a security assessment, which was eventually cancelled when the complainant was laid off, due to circumstances unrelated to the clearance.

Although SIRC considered that the Service was justified in the steps it took to provide its security assessment, it found that the overall processing time involved in conducting the complainant's security assessment was not reasonable, notwithstanding the

Service's explanation for the delays incurred during the various steps of the process.

CSIS indicated it had made changes in the Security Screening Branch with regard to site access clearances. SIRC was satisfied that this contributed to an improvement to the Service's overall processing time of such clearances. Nevertheless, **SIRC recommended that a tracking system be implemented so that priority can be given to files that fall outside the average processing times**.

SIRC INVESTIGATION:

Alleged Unjust, Unfounded and Unethical Assessment of an Applicant for Permanent Residency

SIRC investigated a complaint concerning advice given by CSIS to Citizenship and Immigration Canada (CIC). The complainant alleged that the Service provided unjust, unfounded and unethical advice to CIC regarding his application for permanent resident status in Canada under the former *Immigration Act*.

SIRC determined that the Service's assessment was not unjust, unfounded or unethical.

SIRC also found the Service interviewer was well-prepared for the complainant's interview and that the resulting report was fully documented and well-balanced.

However, **SIRC recommended that:**

- **the Service identify the facts in support of each of the legislative requirements within a provision when making its assessments, and that it provide its analysis for each of the provisions on which it relies;**
- **the Service not include certain information unless it has been corroborated, and that it include all relevant information when reporting statements made by the subject of the assessment; and**
- **the Service include information that could be relevant to a determination as to whether the admission of an individual to Canada would not be detrimental to the national interest.**

SECTION 3:

SIRC at a Glance

Committee Membership

SIRC is chaired by the Honourable 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 Philippe Couillard, P.C., M.D.; and the Honourable Carol Skelton, P.C.

Staffing and Organization

SIRC is supported by an Executive Director, Susan Pollak, and an authorized staff complement of 20, located in Ottawa. This includes a Deputy Executive Director, a Research Director, 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 executive and staff, and other 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 debates affecting Canada's national security landscape.

Committee Members and staff also visit CSIS regional offices to understand and assess the day-to-day work of investigators in the field. These visits give SIRC an opportunity to be briefed by regional CSIS staff on local issues, challenges and priorities. They also provide an opportunity to communicate SIRC's focus and concerns. During the 2010–2011 fiscal year, SIRC visited three regional offices.

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 2010–11 ($ millions)

	2010–11 (Estimates)	2010–11 (Actual)
Personnel	2.06	2.05
Goods and Services	1.06	0.64
Total	**3.12**	**2.69**

Committee Activities

October 14–15, 2010: Several staff attended a conference of the Canadian Association of Security and Intelligence Studies (CASIS), held in Ottawa.

October 26, 2010: SIRC's Chair gave an interview on CBC Radio One's show, *As it Happens*. An audio copy of the interview is available online at www.cbc.ca/asithappens/episode.

January 21, 2011: SIRC senior staff participated in a bi-annual Review Agencies Forum meeting hosted by the Inspector General of CSIS.

February 2011: The Executive Director, along with representatives from CSIS, the Department of Justice, and Foreign Affairs and International Trade Canada, participated in a capacity-building exercise in Bogotá, Colombia.

February 2011: SIRC's Chair gave an interview to the *Ottawa Citizen* in which he discussed SIRC's role and his views on a number of Canadian intelligence matters.

March 3, 2011: The Committee met with members of the United Kingdom's parliamentary oversight body, the Intelligence and Security Committee.

March 29, 2011: The Chair and Executive Director led a panel discussion entitled "The Challenges of National Security Accountability," organized by the Centre for International Policy Studies at the University of Ottawa. Panelists included: Senator Pamela Wallin, Chair of the Senate Committee on National Security and Defence; Mel Cappe, President of the Institute for Research on Public Policy; Paul Kennedy, former Chair of the RCMP Public Complaints Commission; and Professor Reg Whitaker, distinguished Professor Emeritus at York University. The discussion addressed the democratic challenges inherent in maintaining accountability of the operations of Canada's national security agencies, as well as post-9/11 security practices.

March 31, 2011: The Executive Director participated in a Department of Justice National Security Group training day, presenting an overview for the lawyers present of SIRC's role and functions.

April 10, 2011: SIRC's Chair gave an interview on CBC Radio One's show, *Sunday Edition*. An audio copy of the interview is available online at www.cbc.ca/thesundayedition/shows.

List of SIRC Recommendations

During the 2010–2011 review period, SIRC made the following recommendations stemming from the reviews it conducted, as well as from the complaints it investigated.

Report	SIRC Recommendations
CSIS's Private Sector Relationships	In the interests of leveraging limited resources and of capitalizing on the experience already gained, SIRC recommended that CSIS expand on the efforts undertaken in regional offices by articulating a Service-wide strategy on managing its relations with the private sector.
CSIS's Intelligence-to-Evidence Process	To improve the quality and value of the information that CSIS provides to its law enforcement partners, and to bring consistency to the way in which CSIS discloses information to law enforcement, SIRC recommended that CSIS adopt a one-letter disclosure model that incorporates the standards of rigorous legal review currently set for advisory letters.
CSIS's Relationship with a "Five Eyes" Partner	SIRC recommended that CSIS adopt a broader interpretation of its disclosure commitments to DFAIT, to allow the department to prepare itself in the event of an adverse development arising from CSIS's foreign operations.
The Role of CSIS in the Interviews of Afghan Detainees	SIRC recommended that CSIS reword the preamble of its Directive governing exchanges with agencies suspected of human rights abuses to eliminate any possible misunderstanding concerning CSIS's policy on information-sharing with such agencies.
How CSIS Evaluates the Reliability of Human Sources	SIRC recommended that CSIS develop more rigorous criteria, or seek to establish best practices, with respect to human source validation. SIRC recommended that CSIS create a human source "lessons learned" database that is accessible to all intelligence officers to enhance their professional development. SIRC recommended that CSIS conduct a more systematic method of human source file reviews to help ensure that best practices are being followed and that any findings and/or recommendations are incorporated into the lessons learned database.

Report	SIRC Recommendations
Alleged Delay in Providing a Security Assessment	SIRC recommended that a tracking system be implemented within CSIS's security assessment process so that priority can be given to files that fall outside the average processing times.
Alleged Unjust, Unfounded and Unethical Assessment of an Applicant for Permanent Residency	SIRC recommended that CSIS identify the facts in support of each of the legislative requirements within a provision when making its assessments, and that it provide its analysis for each of the provisions on which it relies. SIRC recommended that CSIS not include certain information unless it has been corroborated, and that it include all relevant information when reporting statements made by the subject of the assessment. SIRC recommended that CSIS include information that could be relevant to a determination as to whether the admission of an individual to Canada would not be detrimental to the national interest.