SECURITY INTELLIGENCE
REVIEW COMMITTEE

Meeting the Challenge

MOVING FORWARD IN A CHANGING LANDSCAPE

ANNUAL REPORT 2011–2012

Canada

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

Visit us online at **www.sirc-csars.gc.ca**

Catalogue No. PS105-2012E-PDF
ISSN 1912-1598

Security Intelligence Review Committee

Comité de surveillance des activités de renseignement de sécurité

September 30, 2012

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 2011–2012, as required by Section 53 of the *Canadian Security Intelligence Service Act*, for your submission to Parliament.

Sincerely,

Chuck Strahl, P.C.
Chair

Frances Lankin, P.C., C.M.

Denis Losier, P.C., C.M.

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

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).

SIRC 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. Visit SIRC online at **www.sirc-csars.gc.ca** for more information.

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. These include terrorism, the proliferation of weapons of mass destruction, espionage and foreign-influenced activity. It also provides security assessments of individuals 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. By the same stroke, it created accountability mechanisms to keep those considerable state powers in check.

Contents

Message from the Committee Members

For nearly 30 years, the Security Intelligence Review Committee (SIRC) has served as a fundamental check on the extraordinary powers granted by Parliament to the Canadian Security Intelligence Service (CSIS).

This year, we are again pleased to present our annual report to Parliament and through it to the Canadian public, summarizing the Committee's work during the past year and providing as much detail as the law allows us to disclose. The report includes the summaries of eight comprehensive reviews carried out this year on specific CSIS activities, investigations and programs, as well as summaries of those complaints cases that were concluded during the year. Further, as we have done in past reports, we have included certain operational statistics related to CSIS's investigations.

SIRC's work this year has continued at a steady and productive pace. In the past three years, we have made some 30 recommendations aimed not only at ensuring the Service's compliance with the law—which we would see as a minimum expectation—but also, and more importantly, at enhancing its performance and effectiveness. We keep track of whether and to what extent CSIS implements our recommendations, not because it is our job to direct the Service but because we need to know whether we are making a positive contribution as Parliament intended. We have found that, historically, CSIS has adopted roughly 70 percent of SIRC's recommendations, in whole or in part—a percentage we believe reinforces the effectiveness of SIRC's role and the utility to the Service of our analysis and recommendations.

Readers of this report will already be aware that the regime designed in 1984 to ensure the accountability of CSIS has recently undergone some significant changes. In June 2012, Parliament transferred some of the responsibilities previously held by the Inspector General of CSIS (IG CSIS), to SIRC. Starting in the next fiscal year, SIRC will be responsible for evaluating and certifying the annual report provided to the Minister by the Director of CSIS, thereby helping to ensure ministerial responsibility for CSIS, as well as the Service's accountability to the Minister. SIRC, therefore, has some important shoes to fill. We see this as an opportunity.

Previous years have witnessed both cooperation and coordination between SIRC and the IG CSIS in terms of ensuring the most efficient coverage of CSIS's activities, and of sharing best practices. Bringing responsibility for some of the IG CSIS's work under SIRC's roof will allow a single, expert entity to produce reports both for Parliament as a whole, as well as a specialized product for the eyes of the Minister alone. The main challenge, as we see it, will be to maintain the arm's length independence embodied in our core mandate, while simultaneously meeting the new expectations of government.

The legal parameters under which SIRC and CSIS operate have also been shifting. Of particular note, the Federal Court recently produced two decisions that affect and validate SIRC's complaints process. In a ruling by Justice Simon Noël, the Court ruled that SIRC has jurisdiction to hear complaints about CSIS actions where violations of the *Charter of Rights and Freedoms* have been alleged. The Federal Court ruling means that complaints to SIRC alleging *Charter* violations will now become part of the Committee's investigations. As the Federal Court stated, SIRC's investigating of *Charter* violations had always been envisioned in the original CSIS legislation, and the Committee welcomes the clarity that this ruling provides.

In a separate ruling by Justice Noël, it was found that Section 41 complaints reports could indeed be reviewed by the Federal Court, thus confirming the position advanced by SIRC. This decision makes SIRC more accountable through judicial oversight and, at the same time, flags the importance of our complaints process.

Last year, the Committee proposed a regime that would respond to the recommendations of Justice Dennis O'Connor, calling for review of all national security activities across government. We proposed that, with some slight adjustments to SIRC's mandate and corresponding amendments to the *CSIS Act*, SIRC would be able to address and assess national security matters that involve CSIS but go beyond the strict confines of that agency. For instance, SIRC has noted—with interest—the points raised in the annual report of the Office of the Communications Security Establishment Commissioner. Over the past year, SIRC has met with the Commissioner to discuss the expanding relationship between the Communications Security Establishment (CSE) and CSIS, and we indicated that we plan to make CSE–CSIS collaboration one of SIRC's main areas of focus for the 2012–2013 review cycle. To date, SIRC is awaiting government direction as to any possible change in SIRC's review capacity, which would necessitate an accompanying adjustment to our resources.

Finally, the make-up of the Committee has also undergone some significant changes this past year. We recently welcomed a new Chair, the Honourable Chuck Strahl, P.C. Mr. Strahl's reputation for integrity, commitment and fair-mindedness long precedes him, and the Members look forward to productive collaboration under his leadership. The Committee also wishes to recognize two former chairs, the Honourable Dr. Arthur Porter, P.C., and the Honourable Carol Skelton, P.C. We thank both for their contributions to the work of the Committee.

Chuck Strahl's appointment helps underscore a fundamental strength of the SIRC model: as a former Minister of the Crown and parliamentarian, Mr. Strahl joins a Committee,

all of whose Members have been ministers and parliamentarians. As such, we have years of expertise in weighing the public interest across a broad spectrum of policy and program areas, yet we can do so as Members of SIRC without the partisan preoccupations that colour the day-to-day reality of those still holding public office. The Committee is thus able to draw upon a diverse range of informed perspectives emerging from multiple regions, political backgrounds and portfolio expertise, seated at a single, non-partisan table.

As always, SIRC presents its work with pride, and we are pleased to share our findings, recommendations and analysis both with Parliament and with the wider Canadian public. We trust that the Committee's work during 2011–2012 will continue to contribute to the ongoing discussion of national security—and of the integral role of review and oversight in it. We hope to demonstrate the fundamental importance of CSIS's role in maintaining Canada's national security, and the utility and reliability of accountability provided through SIRC since 1984.

Members of the Committee

The Honourable
Chuck Strahl

The Honourable
Denis Losier

The Honourable
Frances Lankin

The Honourable
Dr. Philippe Couillard

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 prepares an annual report of its activities, which is tabled in Parliament by the Minister of Public Safety.

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

SECTION 1
The Year in Review

An analysis of key 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 complaints decisions 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.

EASY ACCESS TO BACKGROUND INFORMATION WHERE AND WHEN YOU WANT IT

Look for caption boxes throughout this annual report. These contain valuable background information on various legal and policy matters related to SIRC's review and investigatory functions.

SECTION 1

The Year in Review

The past year has, once again, proven to be a challenging one for both CSIS and SIRC. Both organizations have made considerable effort not only to maintain, but to increase output and production in a period of growing fiscal restraint. For CSIS, this has meant developing enhanced tools for risk management, increasing centralization of intelligence analysis and expanding into new areas effectively and efficiently. For SIRC, it has meant honing its more thematic and horizontal approach to review, and producing a series of papers and analyses that examine CSIS's intelligence cycle from start to finish, and which reinforce past SIRC recommendations and observations.

In all of these cases, the themes of efficient resource management, effective risk management, and the benefits of drawing upon existing areas of strength, have served as guideposts for both organizations.

International Intelligence Review Agencies Conference

Sharing best practices and learning from the experience of others is vital for any organization, but for those of us working in the field of national security, the strict limitations on what we can divulge, and to whom, can sometimes make it feel as though we are working in isolation. This past fiscal year ended with the final planning for SIRC to host, in conjunction with the Office of the Communications Security Establishment Commissioner (OCSEC), the 8th International Intelligence Review Agencies Conference (IIRAC). IIRAC is a biannual conference that allows delegates from several Western democracies to share concerns, ideas and best practices in fulfilling their responsibilities for ensuring the accountability of their country's security and intelligence agencies. This year's conference was held in Ottawa, under the theme of "Strengthening Democracy Through Effective Review," and was attended by over 60 delegates from 10 countries.

Although each organization represented at IIRAC has its own mandate, structure and reporting relationships, the conference provided a unique opportunity to explore the broader issues that affect review and oversight organizations. We discovered that participants from all of the countries present are grappling with similar issues, such as the impact of court decisions, balancing national security and individual rights, and the challenges of sharing information across jurisdictions and among agencies.

Having heard from a full range of speakers representing academia, the media, the courts and government, as well as from former senior decision-makers from the Canadian intelligence community, SIRC and OCSEC were pleased to wrap up a successful conference. SIRC has since been preparing a package of conference proceedings and planning materials to pass on to the 2014 host country.

SIRC Reviews

Some of the discussion at IIRAC also noted that many countries are moving well past the changes wrought by 9/11; in many ways, this is beginning to restore a pre-9/11 balance in intelligence gathering. In CSIS's early days, most of its resources went towards investigating espionage networks. Since 2001, counter-intelligence has largely been overshadowed by counter-terrorism activities. However, counter-intelligence, counter-proliferation and new and emerging areas have begun to push their way to the fore once again.

SIRC is ideally placed to observe recent shifts, to tie them into longer-term trends, and to ensure that CSIS remains within its mandate as it addresses various types of threats to Canada's national security. As has been the case since 1984, this year's annual report provides unclassified summaries of a full range of in-depth reviews that SIRC carried out over the past year. Each review is the result of months of intensive research by our expert staff, all of whom have direct access to CSIS personnel and to all CSIS documentation, with the exception of Cabinet confidences.

Two of this year's reviews noted that the Service is positioning itself to collect and analyze information to fulfill a growing Government of Canada expectation that it function in a "think tank" role. CSIS has placed its analytical branch at the centre of the intelligence process. It is moving away from what many saw as a tendency for CSIS to "collect for itself," toward responding to the needs of external clients. Nonetheless, there may be limits to what CSIS is able to do—both from a resource and a mandate perspective; SIRC notes in this year's annual report that the search for wider knowledge for external clients may push CSIS to collect information that could fall beyond its core mandate of security intelligence, or else stretch its capacity beyond what is tenable.

A familiar theme also surfaced in several other reviews this year: the Service's interaction with minors. The phenomenon of domestic radicalization has made it more likely that CSIS will come into contact with an increasing number of young people, as youth are often the target of radicalization efforts, particularly with regards to recruitment via the Internet. Although we recognized that CSIS has developed policies around its direct interaction with minors, two of SIRC's reviews nonetheless came to the same conclusion: the Service needs to have mechanisms in place to guide the sharing of information, particularly with foreign agencies, on the activities of minors.

"SIRC is ideally placed to observe recent shifts, to tie them into longer-term trends, and to ensure that CSIS remains within its mandate as it addresses various types of threats to Canada's national security."

A Range of Investigations

The proliferation of arms and the clandestine activities of foreign governments are not only national security threats, but also represent some of the most fertile areas for growth in the coming years. Having examined these threats in several reviews this year, SIRC is pleased to note that CSIS has made progress in its risk management strategies, which in turn places it in a stronger position when following threats abroad. However, SIRC stressed that as the Service engages in more overseas activities, there will be greater and more lethal potential risks that cannot be fully managed or mitigated, and CSIS must be prepared to handle the consequences.

Of course, the threat of terrorism remains viable, deadly and global. SIRC has commented in recent years on CSIS's expanding footprint abroad and its increased collection overseas, and this year was no different. Almost all of our reviews had an international component, and because cooperation with a variety of foreign partners is increasing, it is a regular part of the SIRC review process to examine both information exchanges and cooperation with foreign agencies. SIRC's review of a foreign station identified concerns with the Service's documentation of information exchanges with foreign partners. A separate review raised concerns with the Service's information-sharing practices, specifically the procedures used to mitigate the dangers of information-sharing.

Emerging issues are still drawing CSIS into new terrain. This year, SIRC examined the role of the Service in kidnapping and illegal migration cases, both of which involved working closely with domestic and foreign partners. In such cases, CSIS's traditional strengths—networks of human sources, and strong links with key foreign partners—have served to propel the Service into very useful roles. However, SIRC noted that new issues will demand both new resources and new areas of expertise, both of which return us once again to the potential pitfalls of rapid expansion.

Conclusions

SIRC's review of CSIS's activities this year stresses the movement of CSIS into processes or initiatives that go beyond what many would conceive of as its "traditional" role, though this movement can be seen as a legitimate response to growing government demands. That being said, SIRC remains ever mindful of the potential for CSIS's Government of Canada partners to ask too much of it, and of the risks of overextension on effectiveness, efficiency and staying within legally prescribed boundaries.

Similarly, SIRC must rise to the challenge of keeping pace with change in order to provide effective oversight. This will require careful stewardship and ongoing attention to ensure that SIRC continues to provide Parliament with the independent and expert analysis that it has come to expect from us.

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 retrospectively if the Service was acting appropriately, effectively and in accordance with the law.

What is the difference between an oversight and a review body?

An oversight body looks on a continual basis at what is taking place inside an intelligence service and has the mandate to evaluate and guide current actions in "real time." SIRC is a review body, so unlike an oversight agency, it can make a full assessment of CSIS's past performance without being compromised by any involvement in its day-to-day operational decisions and activities.

How reviews are conducted

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

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.

Find out more about SIRC's earlier reviews

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

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 SIRC can ensure it has thoroughly reviewed and completely understood the issues at hand.

The Committee's reviews include findings and, where appropriate, recommendations. These reviews are forwarded to the Director 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 central agencies of government (i.e., Privy Council Office, Treasury Board Secretariat), the Auditor General of Canada, the Information Commissioner of Canada and the Privacy Commissioner of Canada.

Tracking 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 its 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, and forms part of the ongoing dialogue between the two organizations. During the 2010–2011 review period, SIRC made 11 recommendations addressing a wide range of issues.

SIRC is pleased to note that CSIS has responded to several of these recommendations. For example, SIRC's 2010–2011 recommendation to establish more rigour in human source validation resulted in a review of existing policy. Likewise, SIRC's recommendation to articulate a Service-wide strategy on managing private-sector relationships resulted in a directional statement from senior executives to guide CSIS regional offices on just such liaison initiatives.

SIRC REVIEW: CSIS's Role in the Passenger Protect Program

Since 9/11, aviation security has taken on greater importance within the sphere of national security. As a result, countries around the globe have committed themselves to enhancing and strengthening national aviation security programs and processes.

In Canada, one of the more prominent components of the government's approach to aviation security has been the introduction of the Passenger Protect Program (PPP). It includes the Specified Persons List (SPL), or "no-fly list," implemented in June 2007 under the *Aeronautics Act*, which is similar to lists in other jurisdictions where the aim is to improve aviation security.

The PPP is intended to identify individuals who may pose a threat to aviation security, to disrupt their ability to cause harm or threaten aviation, and to prevent them from boarding an aircraft.

SIRC's Review

SIRC's review examined CSIS's participation in the PPP. The Service's activities in this regard consist primarily of nominating individuals whom it assesses as warranting inclusion on the SPL. Nominations are reviewed by an advisory group chaired by Public Safety Canada, which includes CSIS, RCMP, Transport Canada, CBSA and Justice Canada. When supported by the group, nominations are submitted to the Minister of Public Safety, who is the ultimate decision-maker with respect to the composition of the SPL.

The review looked first at the intent of the PPP, which was designed by its drafters as an "essential component in Canada's multilayered approach to security." The review then turned to CSIS's role in the SPL nomination process and looked at the internal processes and policies guiding CSIS in this role, the criteria CSIS uses to nominate an individual, and any "lessons learned" from the program's first five years.

Specifically, SIRC examined whether CSIS had developed appropriate policies or procedures, including clear and consistent criteria, to help guide its nomination process.

The review identified a number of substantial issues that have impeded the PPP's functioning.

SIRC found that the program's statutory threshold is difficult to meet in practice. This has led to uncertainty among nominating departments over the criteria for inclusion on the SPL. Under the PPP, a person on the SPL can be denied boarding if it is believed that he/she poses an "immediate threat" to aviation security, a threshold rooted in the *Aeronautics Act*. The concept of "immediate threat" is open to interpretation. As a result, nominating departments and agencies have struggled with the nomination process.

This lack of clarity has also been the subject of public debate, with civil liberties associations (among others) taking aim at what they see as the program's lack of clear boundaries and legislative mandate. SIRC found that these challenges and deficiencies have significantly undermined the potential of the SPL to be an effective aviation security tool.

Even though guidance materials were provided by Transport Canada that were intended to assist the nominating departments, uncertainty remains about the precise meaning of "immediate threat." Compounding this problem, SIRC noted that CSIS did not take the necessary steps to formalize explicit, consistent criteria to guide its nomination process.

SIRC found two notable inconsistencies in CSIS's overall approach to nominations to the SPL.

First, the nominations covered a wide spectrum in terms of the nominees' links to specific threats to aviation security. This appears to be a departure from past practice, when there was greater emphasis on establishing a direct link to aviation security. SIRC expressed concern at this lack of consistency and at the absence of clearly defined criteria for nomination.

A second area of inconsistency concerned whether—and under what circumstances—secret information should be used by SPL authorities to corroborate Service nominations. Initially, the Service took a measured approach by putting forward individuals whose nominations could be supported outside CSIS mainly through open source information. However, SIRC found that CSIS moved away from that initial posture, leading to a finding that there should be clear and explicit parameters addressing the trade-off between the risks associated with the disclosure of secret information, and achieving greater aviation security.

Overall, SIRC found that the PPP's deficiencies contributed to inconsistencies in the Service's approach to nominations.

Although SIRC is satisfied that the Service has employed a generally cautious approach, SIRC found that the lack of a clear statutory definition, as well as a lack of internal guidance, has resulted in a somewhat ad hoc approach by CSIS in nominating individuals to the SPL.

SIRC recommends that, in the near future, CSIS develop a consistent set of criteria to determine its potential nominations, recognizing that these may need to be amended regularly as the program evolves.

SIRC REVIEW: CSIS's Role in the Security Certificate Process

A security certificate is an administrative tool that allows the Government of Canada to detain and to deport non-Canadians (i.e., permanent residents or foreign nationals) deemed to be security threats. The security certificate process is set out in the *Immigration and Refugee Protection Act* (IRPA), and it entails an immigration proceeding, rather than a criminal one. Certificates can be issued on grounds of security, which include: espionage and terrorism; for violating human and international rights; and for involvement in serious or organized crime.

In recent years, the security certificate regime has become heavily litigated. A major Supreme Court of Canada decision in 2007 (*Charkaoui v. Canada*) struck down the certificate regime as unconstitutional because the individual named in the certificate could not be privy to the information used in the genesis of the certificate. This resulted in a significant reform that provided for the appointment of special advocates to represent the interests of the named persons during the closed security certificate proceedings. In the context of these legal challenges, the advice that CSIS provided to the ministers of Public Safety and Citizenship and Immigration has also come under heavy scrutiny.

SIRC's Review

This review focused on the Service's internal processes and policies related to its role in security certificates, which consists primarily of preparing a Security Intelligence Report (SIR), a document containing its information and assessment that an individual poses a threat to national security.

SIRC looked at how the Service has changed its practices to accommodate a number of issues raised by the courts in the context of security certificate proceedings, including the challenges posed by the increased use of CSIS intelligence in legal proceedings.

Specifically, the Committee examined CSIS's response to some of the issues identified by the Federal Court in selected security certificate cases. In doing so, SIRC also looked at how the Court challenged the Service to look critically at its involvement in security certificates, such as: how and what human source-derived information is provided to the courts; the guidelines related to the Service documents prepared in support of security certificates; the preparation of witnesses appearing before the Court; and CSIS's practices with respect to the presentation of intelligence in legal proceedings.

SIRC found that the Service responded to the Federal Court's concerns in three key ways.

First, CSIS developed policy to govern the preparation and approval of the human source précis, an important document that CSIS uses to convey information on human sources to the Court. CSIS recognized the gravity of its failure to disclose in a timely manner important human source information to the judge in one certificate case. To that end, the Service promptly initiated a thorough managerial review of the procedures surrounding the preparation of human source précis.

As a result, procedures for the preparation of source précis were formalized in a policy requiring all such précis to be submitted to a challenge session. This entails the participation of legal counsel to ensure the accuracy of information contained in the document. Moreover, the policy outlines the kind of information to be included in the précis—information that the Court needs so it can make an independent assessment of the reliability of a human source.

SIRC found that CSIS took action to determine the cause of the mistake cited above, and applied corrective measures to avoid a reoccurrence. Given that human source précis are also used to support warrant applications, this new policy has a broad application.

Second, the Service established guidelines for Service witnesses appearing before the courts in security certificate cases. For example, the Committee learned that CSIS's Department of Legal Services (DLS) has prepared a guide for witness preparation that covers issues specific to security certificates. This is especially important given that CSIS employees now must testify in court in the presence of special advocates, which has been described by the Service as an important "new reality."

CSIS has also created a new branch to house civil and immigration litigation under one roof, to build expertise and foster consistency in different aspects of Service litigation.

Third, CSIS has developed an extensive training program focused on promoting "rigour" in all activities, including court-related matters. To complement these efforts, DLS has developed a "judicial orientation module" for new intelligence officers. It covers a broad range of legal topics and issues, including: intelligence used as evidence; disclosure; giving testimony; and the Canadian *Charter of Rights and Freedoms*. DLS also provides legal training to current employees as appropriate. In addition, presentations are given to CSIS regional staff on issues that have been identified in the courts, and on their practical implications.

While signalling these important changes, SIRC is aware that there is declining interest—not merely at the Service, but across government—in the use of security certificates as a legal tool because of the challenges they pose, particularly in anti-terrorism cases. For its part, CSIS faces substantial disclosure obligations with the security certificate process

and, because some of the intelligence used in SIRs comes from foreign agencies, disclosure can be especially problematic.

SIRC believes that the courts provide important direction to the Service on how it must carry out its duties, which in turn will allow it to meet legal challenges successfully. Therefore, **SIRC recommends that CSIS undertake a comprehensive, forward-looking review of relevant court rulings to ensure a full understanding of their implications on Service operations, processes and resources**.

The Committee believes that CSIS will continue to be involved in other IRPA-related processes—some of which may require the preparation of a SIR. SIRC therefore believes that the Service should implement certain changes with respect to the preparation of SIRs. To that end, SIRC made a number of specific suggestions, including encouraging the Service to involve all sources of expertise at the Service's disposal in the SIR preparation process to ensure that the substance of SIRs keeps pace with legal expectations.

CSIS has expressed its commitment to find ways to adapt to the difficulties in presenting intelligence as evidence within the Canadian legal framework. Although the Service has taken steps to address the specific concerns raised in these cases, SIRC believes that the Service could be more strategic in managing its engagement in legal processes, and should undertake a more holistic examination of the issues and criticisms emanating from judicial rulings, to assess their cumulative impact on the processes and practices of the Service.

SIRC REVIEW: CSIS's Role in a Counter-Proliferation Investigation

This review examined CSIS's investigation of a serious proliferation threat, with a focus on the Service's collection and analysis of intelligence in relation to that threat. It also examined the advice provided to the Government of Canada in connection with this case. Given this investigation's international scope, SIRC focused on CSIS's cooperation with foreign intelligence partners, thereby gaining insight into the Service's planning and execution of foreign operations. It also provided insight into the management of human sources, the operational benefits CSIS derives from these activities, and how the Service has adapted its risk management strategies to cope with increasingly dangerous operating environments.

SIRC's Review

In the case under review, CSIS adopted a multi-faceted investigative strategy to meet short- and long-term objectives vis-à-vis a serious proliferation threat. Over the short term, CSIS focused on maximizing the collection efforts of every existing and potential human source. Yet, developing a large number of sources with good access is only a first step; being able to exploit and leverage the information collected is equally important.

Thus, CSIS's longer-term strategy involves building operational capabilities abroad and subject matter expertise on this threat. Favourable client feedback on the Service's intelligence products relating to this threat suggests that these strategies are helping CSIS to address the Government of Canada's intelligence requirements.

While conducting this study, SIRC learned of a serious operational failure that underscored the inherent risks in foreign operational activities. Following meetings with CSIS officials and careful documentation review, SIRC concluded that no single action by CSIS led to the ultimate failure of this particular foreign operation. Instead, there were a number of contributing factors, many of which were beyond the control of CSIS.

Given the importance of risk management in planning and executing operations abroad, SIRC chose to examine in closer detail the steps CSIS has taken to improve this process. These include how risk is identified, what internal consultations occur, the controls or mitigators used to help manage risk, and the role management plays in approving these endeavours.

SIRC has previously raised concerns about CSIS's Operational Risk Management (ORM) strategies.

In 2008, for instance, SIRC completed two reviews that concluded CSIS lacked criteria for conducting risk assessments. As a result, the Committee recommended that CSIS improve its risk definitions and standardize its assessments using detailed and consistent terminology. At the time, SIRC also questioned whether more transparency was required within CSIS's operational reporting to help explain the decision-making process surrounding CSIS's risk management.

Shortly thereafter, CSIS initiated an entirely new ORM process, designed to help meet intelligence requirements through the assessment and mitigation of risk to a level judged to be organizationally acceptable. The Service maintains that this new process produces risk assessments that are systematic, demonstrate decision-making transparency, include all relevant stakeholder viewpoints, and are grounded in common sense.

To assess the degree to which CSIS's new ORM process adheres to these principles, SIRC reviewed the risk assessments for all joint operations in this investigation. SIRC found that, although operational risk can never be entirely eliminated, a combination of policy and process changes by CSIS has indeed created a more systematic and methodological approach to managing risk. Among the more significant improvements: clear and concise risk definitions; specialized employee training; stakeholder identification and associated responsibilities; policy identifying the level of managerial approval for each risk level; risk matrices that require measurable inputs; and a designated responsibility centre for incorporating lessons learned from previous operations.

SIRC's review also found, however, that despite risk assessments being designed to reflect all operational considerations, there was a notable absence of detail on partner agencies. **SIRC therefore recommends that, in the future, risk assessments should—where appropriate—include a more nuanced and comprehensive appraisal of individual partner agencies.**

With time, this information would contribute to a more transparent and strategic appraisal of the unique benefits and potential challenges of partner engagement on a case-by-case basis.

SIRC was pleased to note that following completion of this review, CSIS advised SIRC that the ORM process now includes more information on foreign partner agency capabilities and intentions.

This review highlighted CSIS's steady progress in establishing itself as a significant foreign operational player to gain information on a serious proliferation threat. As a result of bringing this strategy to fruition, the Service has adopted new policies, practices and procedures for overseas activities. It has also increased its level of connectivity with allies—but also, as a consequence, increased operational risks.

SIRC will continue to follow CSIS's overseas activities to ensure that the Service is equipped to provide appropriate advice and support to the Government of Canada, while managing the attendant risks of doing so.

SIRC REVIEW: Domestic Radicalization

In past years, few threats to national security have provoked as much concern as the phenomenon of radicalization as it relates to Sunni Islamist terrorism. The term "radicalization" generally refers to the process by which an individual comes to legitimize the use of violence to achieve political goals. The Government of Canada's priority is to find ways to stop or prevent the radicalization process to reduce the likelihood of terrorism in Canada and of Canadians becoming involved in terrorist activity abroad.

This requires a "whole-of-government" approach, spearheaded by Public Safety Canada.

CSIS has an important role to play in broader government initiatives related to radicalization. In its latest public annual report, CSIS noted that the threat posed by the indoctrination and radicalization of young Canadians into the violent ideology espoused and inspired by al Qaeda, which is commonly referred to as "homegrown Islamist extremism," continues to be a key concern. CSIS has been working to understand the threat posed by the phenomenon of radicalization in Canada and to identify radicalized individuals and groups, and the means by which they have been radicalized.

The focus of CSIS's investigative and analytical work is on the threat once the radicalization process is complete—that is, the potential for violence and the threat it poses to national security.

SIRC's Review

The purpose of this review was to examine CSIS's understanding, investigation and analysis of the radicalization threat in Canada. It looked at what domestic radicalization is in the Canadian context, how it has evolved, and how CSIS has positioned itself to collect intelligence on this threat. SIRC also examined how CSIS analyzes the phenomenon of domestic radicalization, so as to broaden the Service's understanding of this process and advise government.

SIRC's review noted that domestic radicalization is not a stand-alone issue but one part of the overall threat that has evolved over this past decade. Initially, the primary threat was non-Canadians abroad seeking to carry out an attack on Canadians abroad or on Canada. More recently, it has shifted to Canadians joining terrorist organizations abroad and attacking other countries, Canada or Canadians, as well individuals who undergo radicalization within Canada and then seek to carry out violence in Canada or abroad.

Overall, SIRC found that CSIS's investigation and analysis of radicalization has evolved to reflect the Service's knowledge of the issue and to exploit available resources more effectively.

Nevertheless, SIRC noted three challenges that CSIS faces in investigating domestic radicalization: addressing the growing use of the Internet as a vehicle for radicalization; the collection and sharing of information on targets and individuals under the age of 18; and the prioritization of multiplying threats.

The Role of the Internet

Although the process of radicalization in Canada is driven largely by charismatic leaders, peer groups and family members, the Internet has been described by many as "a game changer," in part because it has

enabled the quick spread of extremist ideology to an international audience. Today, individuals may become radicalized almost entirely as part of online communities, without a great deal of face-to-face contact with others.

Not surprisingly, the ever-increasing volume of online, threat-related activities has created a significant investigative challenge for CSIS. Monitoring online activity is resource-intensive, and the Service recognizes that many individuals who appear to be radicalized online pose no actual threat. For CSIS to target someone based on their online activities, it must have reasonable grounds to suspect that the person is involved in actual threat-related activities.

Yet, when there is little real world interaction, it can be difficult to investigate these activities through traditional methods, such as physical surveillance. As a result, CSIS may decide to apply for a warrant earlier in the investigative process to avail itself of more intrusive powers and tools to push its investigation forward. Even in such cases, for the Service to obtain warrant powers, it must demonstrate convincingly that these intrusive powers will advance an investigation and that other investigative methods are not likely to succeed.

CSIS has therefore developed useful tools to assist investigators to determine whether to target an individual and whether there is justification for a warrant against an individual based on their online activities. SIRC supports CSIS's efforts to exhaust less-intrusive means of investigation before proceeding to a Section 21 warrant application with respect to investigations that have a heavy online component.

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.

	2009–10	2010–11	2011–12
New warrants	36	55	50
Replaced or renewed	193	176	156
Total	**229**	**231**	**206**

Increasing Interaction with Youth

The second challenge noted by SIRC: since youth are often the target of radicalization efforts, CSIS is very likely to come into contact with an increasing number of underage persons as individuals of concern or targets. Dealing with underage persons presents challenges for the Service, both in terms of its investigative approach, as well as practices concerning information collection, retention and dissemination.

SIRC found that CSIS exercised discretion and sensitivity in its interactions with underage persons, but believes this same level of consideration should be extended to information-sharing and operational reporting.

There is no clear approval process set out in operational policy when sharing information on minors, particularly with foreign partners. SIRC believes CSIS should develop policy to govern the sharing of information on underage persons to establish clear lines of responsibility and approval.

SIRC recommends that CSIS develop a new policy to govern the sharing of information on minors with foreign partners, or amend existing policy on information-sharing to reflect an appropriate sensitivity to youth.

Another issue with respect to information pertaining to minors relates to collection and retention in operational reporting by the Service. Currently, there is no requirement for CSIS to identify clearly in operational reporting that the information contained in a given message relates to a minor.

To ensure that appropriate attention and sensitivity are given to intelligence collected and retained on underage persons, SIRC recommends that all operational reporting containing information on a minor be flagged as such.

Prioritization of Threats

A third type of challenge to emerge in recent years has been the need for CSIS to be judicious in its management of resources, especially given the ever-increasing number of threats. To address this, CSIS has developed tools to assist in prioritizing its investigations and associated resources.

CSIS's investigations remained focused on radicalization as a developing part of the threat, a phenomenon that adds a new dimension to its outreach efforts, analysis and advice to government. Indeed, although terrorism squarely constitutes a threat under Section 12 of the *CSIS Act*, radicalization, as a process, does not. CSIS may legitimately collect on the threat posed by radicalized individuals, but other information, such as "root causes," may fall beyond the scope of the Service's mandate.

CSIS recognizes there are limitations to the information and advice that it can provide to government on this issue, due in large part, "to the nature of the Service's mandate, which directs it to investigate threats to national security (and hence individuals already showing signs of violent radicalization)."

Still, SIRC is concerned that in the search for wider knowledge, CSIS may be pushed both internally and externally to collect information that does not fall squarely within the boundaries of Section 12. As such, SIRC encourages CSIS to maintain its current conceptualization of radicalization as one part of a complex threat picture, and not a driver of investigations in its own right.

SIRC REVIEW: CSIS Support to Emerging Issues and Government of Canada Intelligence Priorities

CSIS's intelligence collection efforts are guided by the Government of Canada's intelligence priorities. In recent years, in response to a heightened and changing threat environment, these priorities have included new and emerging security intelligence requirements that have led CSIS to expand its operational activities into non-traditional areas, such as assistance to government in foreign kidnapping cases and illegal migration operations.

The government has directed CSIS to provide intelligence on kidnappings of Canadians abroad when linked to extremist groups. As a result, a new operational niche has been created within the Service. Illegal migration and human smuggling is another area of emerging importance. A number of terrorist groups use illegal migration networks to support their objectives. As part of its investigations into those groups and their activities that may

pose a threat to Canadian interests, CSIS is working with domestic partners to stop human smuggling involving maritime vessels destined for Canada.

A common characteristic in responding to these two emerging threats is the requirement for CSIS to work closely with other Canadian departments and agencies in a whole-of-government approach.

SIRC's Review

This review examined the impact that kidnapping and illegal migration cases have had on "traditional" Service operations and assessed whether CSIS has adequate resources and training to respond. More broadly, SIRC explored CSIS's contribution to whole-of-government approaches to emerging security intelligence matters by examining its cooperation and exchanges with domestic partners and foreign allies.

CSIS's interest in politically motivated kidnappings by groups or individuals that pose a threat to Canadian national security is not new. What is new, however, is the nature and extent of its operational involvement. The same can be said of CSIS's involvement in illegal migration cases. Overall, SIRC found that CSIS's intelligence collection and advice to government on these issues—through its investigations of threats to Canadian national security—were valuable and sound. In particular, SIRC found that CSIS's liaison and exchanges with foreign partners proved invaluable to government decision-makers.

The Canadian government's approach to hostage situations varies depending on the nature of the case. If a foreign kidnapping is deemed to constitute a threat to national security, an inter-departmental task force will be struck with all relevant departments and agencies, the main goal of which is to secure the hostages' safe release. Within this task force, CSIS's role echoes its mandate: to collect and provide intelligence on threats to national security—in this case, with the ultimate goal of facilitating the release of hostages. This work is carried out by ad hoc crisis units or teams, assembled in response to specific kidnapping cases.

Overall, CSIS contributes to the whole-of-government approach to kidnapping cases in two key ways.

First, CSIS collects information on the extremist group or individuals behind a kidnapping, using the investigative means at its disposal, and advises government of the same. Of particular value is the human intelligence that CSIS may obtain abroad as part of this collection effort, which can provide unique insight, albeit with challenges associated with foreign operations.

Second, and perhaps more importantly, CSIS may draw on the assistance of its foreign partners working around the world to acquire valuable information. Over the years, CSIS has developed and maintained relationships with numerous foreign intelligence agencies, many of which have a presence in countries where CSIS does not, and some of whom will only share information with intelligence counterparts (i.e., not law enforcement or Foreign Affairs officials). Through liaison, CSIS has been able to tap into these resources to gain information it would otherwise not be able to collect itself.

To ensure that CSIS is in a position to respond to kidnapping cases overseas, while not compromising its ability to fulfill other responsibilities, SIRC has noted three important challenges: addressing the issue of resource drain; establishing appropriate internal processes and procedures; and the impact of expanded foreign collection activities.

The first two issues have already been recognized by CSIS management. CSIS informed SIRC

that the Service's approach to dealing with kidnappings continues to be on a risk management basis. This allows greater flexibility from a resource and operational standpoint.

Although each kidnapping case is unique, SIRC questions the desirability of continuing to rely on an ad hoc approach. Although CSIS has addressed certain logistical challenges, there is little evidence that it has taken broader steps to develop standard operational procedures and strategies in its responses to such crises.

SIRC believes that the Service's approach to kidnapping cases should be the focus of broader strategic planning. **To enhance the effectiveness and sustainability of CSIS's involvement in such matters, SIRC recommends that CSIS develop appropriate operational procedures, as well as mechanisms to enhance operational and subject matter expertise.**

Moreover, SIRC's review confirmed the value-for-money in liaising with foreign partners. Although expanding CSIS's presence and operational activity abroad may be an appropriate response to a short-term crisis situation to counter a threat to Canadian national security, SIRC questions the feasibility of continuing to do so in difficult parts of the world without additional resources.

For this reason, as CSIS continues to respond to emerging issues within a whole-of-government framework, more strategic thinking and planning will be required.

The Service has been involved in illegal migration cases through its security screening role under Sections 14 and 15 of the *CSIS Act*. In recent years, however, as migrant smuggling has become a government security priority, CSIS has sought to enhance its operational capacity on the issue. CSIS is not the lead in such cases; its role is limited to providing information and advice related to national security threats. The key goal is to collect intelligence that could be exploited by domestic and foreign partners either to influence or disrupt illegal migration activities "in-theatre."

In recent years, CSIS launched several strategic initiatives to bolster its operational capabilities to address these emerging threats. It also created a dedicated unit to be the centre of responsibility for all matters related to illegal migration, while providing intelligence leads to relevant CSIS personnel in Canada and abroad. The unit aims to create in-house expertise and to act as a vehicle for information-sharing with relevant domestic partners. In the cases reviewed, SIRC noted the information that CSIS collects through its domestic investigations is key to its role in illegal migration cases.

Given that the government has made migrant smuggling a security priority, SIRC expects an increase in CSIS's operational involvement in illegal migration cases. To avoid putting a burden on other traditional operational activities both domestically and abroad, CSIS will need to approach illegal migration on a priority basis.

Overall, SIRC found that CSIS has been able to draw some operational benefits in support of broader intelligence requirements from participation in these whole-of-government operations.

Yet, as CSIS moves forward to fulfill those intelligence requirements, it will need to reflect on its strategies (both domestic and foreign) for meeting this demand. Key to CSIS's contribution is its unique access to the international intelligence community, and indeed, SIRC found that CSIS's liaison and exchanges with foreign partners proved to be its greatest asset in kidnapping and illegal migration cases.

Responding to new and emerging government intelligence requirements may demand a more efficient balance between leveraging existing liaison opportunities and increasing the Service's operational footprint abroad. SIRC believes that CSIS will need to undertake greater strategic thinking and long-term planning to ensure that it is, and remains, well-positioned to strike such a balance and therefore meet their requirements with available resources.

SIRC REVIEW: A CSIS Foreign Station

In recent years, the global threat environment has led CSIS to expand the nature and scope of its activities abroad to support the government's increased overseas collection requirements. In this period, CSIS entered into many new foreign arrangements, and several officers posted abroad were given the authority to collect information actively in support of CSIS operations.

SIRC's more recent post reviews have focused on larger, busier posts. This year, SIRC chose to examine one of CSIS's more modest stations. This review examined: CSIS's foreign arrangements and exchanges at station; the responsibilities of the CSIS Foreign Collection Officer (FCO); CSIS support to other Canadian departments and agencies at station; and site-specific developments, conditions, pressures and emerging issues.

SIRC's Review

SIRC took note of the hard work done by FCOs in recent years to try to transform this station into a more operational one. The country's strategic geographic location appears ideal for operational activities. However, this has proven extremely difficult, in part due to the host country's counter-intelligence activities.

The station had limited liaison relationships and information exchanges with the domestic agency despite the Service's efforts to engage it on issues of mutual interest. In the context of these exchanges, SIRC noted that CSIS displayed due diligence when considering sharing information related to Service targets, particularly when they were travelling to, or through the host country, owing to concerns over human rights abuses. SIRC also noted that appropriate caveats were attached to information that was shared with the domestic agency during the review period.

The FCOs placed additional effort on cultivating their Conscious Relationships (CRs) with other foreign partners stationed in the country. SIRC noted that in the past, information gleaned from these foreign partners was at least as valuable as what was received from the host country. In particular, SIRC saw important liaison work being undertaken with the CRs with regard to a priority CSIS investigation.

Overall, SIRC found the relationships between CSIS and its Canadian partners at the Station to be positive. Although both the Head of Mission and the incumbent FCO were relatively new, there appeared to be a spirit of cooperation and understanding of each organization's respective mandate. Briefings held during SIRC's on-site visit indicated that CSIS's relationships at the Station are positive, with each partner having a solid grasp of CSIS's mandate and role.

In the course of its review, SIRC came across two separate instances where information was improperly recorded in operational reporting. The outcome in both cases led to confusion over what information had been shared by an FCO with a foreign partner.

SIRC recommends that CSIS implement a practice whereby FCOs must alert operational desks when a request to share information with a foreign partner is not fulfilled for whatever reason, so that the report can be amended in operational reporting.

The importance of liaison was a highlight of this review. Although the FCO's focus is now on collection, traditional liaison work is still a valuable part of the work at this station. More broadly, this review underscored the need to ensure strong, effective communication between CSIS Headquarters and its foreign-based staff, particularly in carrying out operations that require coordination among different individuals. As the Service expands its overseas presence, effective communication with the FCOs and accurate operational reporting on information-sharing are crucial, particularly when dealing with agencies that may have questionable practices when it comes to human rights.

SIRC REVIEW: CSIS's Relationship with a Foreign Partner

The modern realities of intelligence require significant cooperation with foreign partners. Although there are many facets of such cooperation, information-sharing is what has attracted much of the public's attention in recent years. This year, SIRC examined the Service's cooperation with a particular foreign partner through the lens of information-sharing activities.

SIRC's Review

SIRC examined how CSIS's relationship with this partner has evolved in recent years. SIRC also looked at how such developments have the potential to generate particular challenges with respect to sharing information, including human rights concerns.

SIRC then looked at the strategies and procedures CSIS uses to manage its information exchanges with such a foreign partner, including seeking guarantees (or "assurances") from the partner concerning respect for human rights, the introduction of new policies to manage information-sharing, and the expanded use of caveats accompanying the transmission of information.

Overall, SIRC found that there has been significant discussion of the challenges of information-sharing and of the measures needed to manage these exchanges properly. However, SIRC found a lack of clarity and direction in applying those measures. In most cases, the implementation of clear, structured policy is long overdue. As a result, SIRC made recommendations to guide the completion of appropriate and clear guidelines that reflect current political direction on information-sharing, and the recommendations of independent Commissions of Inquiry.

SIRC's review found that CSIS has expended a significant amount of time and energy—especially at the highest levels of management—conveying to foreign partners its expectations surrounding information-sharing, especially as they relate to human rights.

These positive developments notwithstanding, SIRC found a number of areas in which CSIS policy did not meet the standard that the Committee would expect. In particular, SIRC identified concerns around the procedures employed by CSIS to mitigate the dangers of information-sharing, specifically: the systematic gaining of assurances from foreign partners when receiving information from them; the attachment of caveats to CSIS information when providing it to a foreign partner; and the sensitive issue of sharing information on young offenders.

First, there remains a lack of clear understanding about what "assurances" actually are, when they are to be used, and how they should be documented. Given the lack of clarity and absence of guidelines on the issue of assurances from foreign partners when information-sharing presents a substantial risk of torture, **SIRC recommends that CSIS develop policy and direction on the practical application of assurances, such as when and how they should be sought, under whose authority, and how this process should be documented in operational reporting.**

Second, SIRC's review found that although the use of specific caveats meant to mitigate the dangers of sharing sensitive information with non-Canadian entities stretches back to 2003, their application was inconsistent: up to a dozen different caveats have been used in recent years.

SIRC believes that one of the reasons caveats have not been applied in a uniform manner is because CSIS's policy on the use of caveats dates back to 2005, and has not been updated to reflect more recent practices and recommendations on information-sharing with foreign partners. **SIRC believes that a revised policy on caveats is overdue and, as such, recommends that this policy be updated to reflect current information-sharing practices and processes with foreign partners, and be finalized without further delay.**

Third, in the course of the review, SIRC paid special attention to practices surrounding information-sharing about youth. SIRC was told that decisions about sharing information on minors and young offenders with foreign partners are made on a case-by-case basis. What SIRC observed, however, suggests a degree of uncertainty about sharing information on these individuals.

Given what appears to be a lack of clarity surrounding what information can or should be shared on young offenders, SIRC encouraged CSIS to seek legal advice to assist in developing specific parameters when dealing with foreign partners.

In summary, SIRC recognizes that sharing intelligence between states is a clear requirement of effective national security, especially in an era of global terrorism and terrorist networks. However, enhanced information-sharing presents a number of challenges, not the least of which is the need for agencies like CSIS to reconcile Canadian democratic values with international intelligence practices.

CSIS has acted to develop an information-sharing framework with an emphasis on foreign partners who give rise to human rights concerns. SIRC encourages the Service to finalize that framework as soon as possible.

SIRC REVIEW: CSIS Intelligence Production and Dissemination

In addition to collecting information on threats to the security of Canada, CSIS also produces and disseminates intelligence products to various Government of Canada partners and foreign allies. In recent years, CSIS has attempted to bolster this function by granting a more significant role to the Intelligence Assessments Branch (IAB), which is the analytical and dissemination arm of the Service. This change has led to the development of new methods to address how intelligence demands are heard, processed, analyzed and disseminated, placing IAB at the centre of CSIS's intelligence process.

SIRC's Review

This review examined IAB's efforts to work more closely with CSIS operations and to integrate Government of Canada intelligence priorities into CSIS's collection efforts.

SIRC specifically looked at: how CSIS has changed its mechanisms for receiving feedback from federal departments; the various initiatives IAB has undertaken to improve its intelligence assessments; the drivers and demand for different CSIS intelligence products; and elements of training offered to analysts.

To fulfill its new central role, IAB has undergone structural and organizational changes. Its core responsibilities are for the most part performed by three different streams of analysts: Strategic Analysts, Requirements Officers, and Tactical Analysts. These positions were designed to help IAB meet its goals of assisting operations and of reaching out to external clients in the federal domain. The new structure has also helped to enhance and to bring more attention to intelligence analysis and production. However, each stream still faces a number of challenges that have been acknowledged by the Service.

In conjunction with its new structure, IAB has created the Intelligence Requirements Document (IRD), intended to drive both collection and production. The IRD acts as a framework to organize Government of Canada intelligence priorities, Ministerial Direction, Section 16 agreements, and input from clients.

IAB also produces the vast majority of CSIS's classified intelligence products, which it then disseminates to domestic and foreign partners as it deems appropriate. These products include:

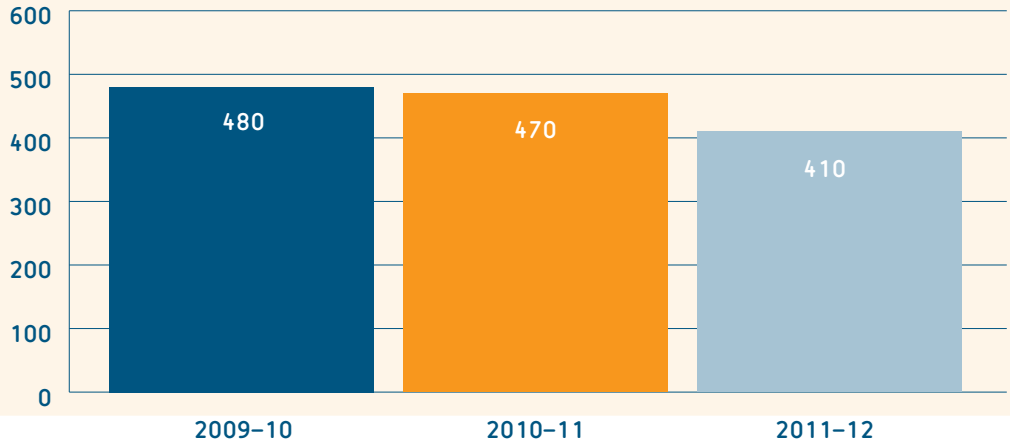
- Intelligence Assessments (IAs)—CSIS's flagship product, which provide the government with broad, strategic analysis;
- CSIS Intelligence Reports (CIRs)—non-assessed intelligence reports; and
- Threat and Risk Assessments (TRAs)—produced at the request of a federal department to assess the national security threats to a specific asset.

IAB is also responsible for disseminating Foreign Agency Reports (FARs), which are intelligence assessments and products from allies and other governments. Through solicited input from several of CSIS's clients, SIRC found that the Service's products dealing with national security issues and the domestic threat picture were indeed valued.

New record-keeping protocols have also been established to track the production of CIRs and, more importantly, the intelligence requirements to which they respond. However, the mechanisms to track the investigation authority as per the *CSIS Act* do not distinguish between the different types of authority employed in the creation of the product. **SIRC recommends that CSIS develop a more accurate means of tracking its production activity so as to accurately represent the proportions of Section 12 and Section 16 information.**

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. This figure indicates the number of targets (rounded to the nearest 10) investigated by CSIS in the past three fiscal years.



SIRC noted evidence of CSIS being in the midst of a "cultural shift" that is driven by three key factors: the influence of CSIS's close foreign partners; the Government of Canada's expectations and priorities; and feedback and demands of clients who receive and use CSIS's reports.

With respect to the first factor, some of the changes to products that have taken place as IAB has moved to the centre of the Service's intelligence cycle were modelled after foreign intelligence organizations, which presented some challenges. Foreign intelligence agencies do not make distinctions between security intelligence and foreign intelligence; they simply collect "intelligence." For CSIS, however, the distinction between these two is a vital part of its mandate. In emulating foreign intelligence agencies and their products, CSIS runs the risk of obscuring the distinctions within its collection mandate. This represents not only a cultural shift for production, but also for collection. For this reason, SIRC believes that as CSIS seeks best practices from allies, it should also turn to other domestic security intelligence organizations.

With respect to the second factor, the Government of Canada's expectations and priorities also heavily influence CSIS's collection priorities. What the government may deem as a high-priority intelligence requirement may not be well aligned with CSIS's core mandate. This situation carries the potential to push CSIS collection increasingly towards broader Government of Canada intelligence priorities, possibly to the detriment of fulfilling its core function.

With respect to the third factor—client feedback and demands—IAB has worked over the past few years to develop an active client-feedback strategy, whereby CSIS solicits input from federal departments. A client-driven strategy, while useful to a degree, could increase demands on CSIS, as not all clients seek intelligence that falls within CSIS's purview. In an effort to try to meet client demands, CSIS runs the risk of collecting and producing intelligence that takes away from its security intelligence focus.

The IAB's new centralized role was geared to alleviate certain challenges with respect to growing intelligence priorities and increased, client-driven foreign and security intelligence demands, but also to assist with CSIS operations. However:

SIRC is concerned that the combination of CSIS's attempts to emulate the reporting and dissemination structure of foreign intelligence organizations, its efforts to respond to broader Government of Canada intelligence priorities, and CSIS's more active client feedback process, may take the focus away from its core mandate: security intelligence.

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, although two predominate. 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 or revocations of security clearances to federal government employees and contractors. Far less frequently, SIRC conducts investigations in relation to referrals from the Canadian Human Rights Commission, or 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 will 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. This 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 hearings 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. This provides 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. In the case of complaint under Section 42, SIRC will also provide its report to the Deputy Head concerned.

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

	2009–10	2010–11	2011–12
Carried over	22	31	16
New	32	17	17
Total	**54**	**48**	**33**
Closed[†]	23	32	11

[†]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 Delay in Providing a Security Assessment

SIRC investigated a complaint regarding an alleged delay by the Service in providing an immigration security screening assessment as part of an application for permanent resident status in Canada. The complainant alleged that the delay created both financial and career difficulties.

In its investigation, SIRC found that the Service took over two years to process the complainant's file. SIRC found that CSIS was justified in taking each of the steps it did to process the complainant's file and that the complainant was not unfairly targeted.

The file was, in fact, completed within the median time for completion of similar files. However, the time it took for the Service to complete its immigration security screening assessment of the complainant and provide advice to Citizenship and Immigration Canada was not reasonable. SIRC found that the delay appeared systematic and, therefore, was not the result of any wrongdoing on CSIS's part, but was the result of a combination of work overload and insufficient human resources in the unit handling the complainant's file during the period investigated.

SIRC encourages the Minister to follow up directly with CSIS to discuss ways of ensuring that appropriate resources are allocated to avoid unreasonable delays in the future.

SECTION 3

SIRC at a Glance

Committee Membership

SIRC is chaired by the Honourable Chuck Strahl, P.C. The other Committee Members are: the Honourable Frances Lankin, P.C., C.M.; the Honourable Denis Losier, P.C., C.M.; and the Honourable Philippe Couillard, P.C., M.D.

Staffing and Organization

SIRC is supported by an Executive Director, Susan Pollak, and an authorized staff complement of 15, located in Ottawa. This includes a Director of Research, a Senior Counsel, a Corporate Services Manager and other professional and administrative staff.

The Committee provides 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.

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 2011–12 ($ MILLIONS)

	2011–12 (Estimates)	2011–12 (Actual)
Personnel	2.02	1.84
Goods and Services	0.82	0.73
Total	**2.84**	**2.57**

Committee Activities

October 12–14, 2011: SIRC's Chair participated in a panel discussion on accountability of security and intelligence agencies at the annual conference of the Canadian Institute for the Administration of Justice, entitled "Terrorism, Law and Democracy: 10 Years After 9/11," held in Montreal. SIRC's Executive Director and senior staff also attended the conference.

November 8–10, 2011: The Chair, Executive Director and senior staff travelled to London, UK, to meet with British counterparts and government officials to discuss issues of mutual interest.

April 24, 2012: The Executive Director accepted an invitation to give a presentation on the importance of security intelligence accountability at a NATO-sponsored conference on the "Promotion of Democratic Values and Compliance with Human Rights in the Activity of Special Services," in Kiev, Ukraine.

May 27–30, 2012: SIRC co-hosted the International Intelligence Review Agencies Conference (IIRAC), along with the Office of the Communications Security Establishment Commissioner. Under the theme "Strengthening Democracy Through Effective Review," the conference reunited delegates from Australia, Belgium, Germany, the Netherlands, Norway, South Africa, the United Kingdom and the United States. The conference was held at Ottawa's Chateau Laurier, and featured panels on Legal Development in Review and Oversight, Media as a Form of Review/Oversight, Engaging the Public, and Balancing National Security and Individual Rights. Featured speakers for the conference included Senator Hugh Segal, Mel Cappe (former Clerk of the Privy Council), Jim Judd (former Director of CSIS), David Walmsley (Managing Editor of the *Globe and Mail*), and Federal Court Justice Simon Noël, among many others.

List of SIRC Recommendations

During the 2011–2012 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 Role in the Passenger Protect Program	SIRC recommends that, in the near future, CSIS develop a consistent set of criteria to determine its potential nominations, recognizing that these may need to be amended regularly as the program evolves.
CSIS's Role in the Security Certificate Process	SIRC recommends that CSIS undertake a comprehensive, forward-looking review of relevant court rulings to ensure a full understanding of their implications on Service operations, processes and resources.
CSIS's Role in a Counter-Proliferation Investigation	SIRC recommends that, in the future, risk assessments should—where appropriate—include a more nuanced and comprehensive appraisal of individual partner agencies.
Domestic Radicalization	SIRC recommends that CSIS develop a new policy to govern the sharing of information on minors with foreign partners, or amend existing policy on information-sharing to reflect an appropriate sensitivity to youth. To ensure that appropriate attention and sensitivity are given to intelligence collected and retained on underage persons, SIRC recommends that all operational reporting containing information on a minor be flagged as such.
CSIS Support to Emerging Issues and Government of Canada Intelligence Priorities	To enhance the effectiveness and sustainability of CSIS's involvement in such matters, SIRC recommends that CSIS develop appropriate operational procedures, as well as mechanisms to enhance operational and subject matter expertise.
A CSIS Foreign Station	SIRC recommends that CSIS implement a practice whereby Foreign Collection Officers must alert operational desks when a request to share information with a foreign partner is not fulfilled for whatever reason, so that the report can be amended in operational reporting.

CSIS's Relationship with a Foreign Partner	SIRC recommends that CSIS develop policy and direction on the practical application of assurances, such as when and how they should be sought, under whose authority, and how this process should be documented in operational reporting. SIRC believes that a revised policy on caveats is overdue and, as such, recommends that this policy be updated to reflect current information-sharing practices and processes with foreign partners, and should be finalized without further delay.
CSIS Intelligence Production and Dissemination	SIRC recommends that CSIS develop a more accurate means of tracking its production activity so as to accurately represent the proportions of Section 12 and Section 16 information. SIRC is concerned that the combination of CSIS's attempts to emulate the reporting and dissemination structure of foreign intelligence organizations, its efforts to respond to broader Government of Canada intelligence priorities, and CSIS's more active client feedback process, may take the focus away from its core mandate: security intelligence.
Alleged Delay in Providing a Security Assessment	SIRC encourages the Minister to follow up directly with CSIS to discuss ways of ensuring that appropriate resources are allocated to avoid unreasonable delays in the future.