

gation or otherwise, to the extent that it is strictly necessary, and ana
information and intelligence respecting activities that may on reaso
nds be suspected of constituting threats to the security of Canada an
thereto, shall report to and advise the Government of Canada. The
collect, by investigation or otherwise, to the extent that it is strictly n
d analyse and retain information and intelligence respecting activitie
on reasonable grounds be suspected of constituting threats to the se
ada and, in relation thereto, shall report to and advise the Governm
. The Service shall collect, by investigation or otherwise, to the exte
strictly necessary, and analyse and retain information and intelligence

Lifting the Shroud of **SECRECY**

Thirty Years of Security Intelligence Accountability
Annual Report 2013–2014



SECURITY INTELLIGENCE
REVIEW COMMITTEE

Canada



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

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

© Public Works and Government Services Canada 2014
Catalogue No. PS105-2014E-PDF
ISSN 1912-1598

Security Intelligence
Review Committee



Comité de surveillance des activités
de renseignement de sécurité

September 30, 2014

The Honourable Steven Blaney
Minister of Public Safety and Emergency Preparedness
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 2013–2014, as required by Section 53 of the *Canadian Security Intelligence Service Act*, for your submission to Parliament.

Sincerely,

A handwritten signature in cursive script that reads "Deborah Grey".

Deborah Grey, P.C., O.C.
Interim Chair

A handwritten signature in cursive script that reads "L. Yves Fortier".

L. Yves Fortier P.C., C.C., O.Q., Q.C.

A handwritten signature in cursive script that reads "Gene McLean".

Gene McLean, 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, certifies the Director of CSIS's annual report to the Minister of Public Safety, and investigates complaints from the public about the activities of the Service and denials of security clearances, reports made pursuant to the *Citizenship Act*, and matters referred pursuant to the *Canadian Human Rights Act*.

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

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 Statutory Framework for Both SIRC and CSIS

By virtue of the *Canadian Security Intelligence Service Act (CSIS Act)*, Canada became one of the first democratic governments anywhere in the world to establish a statutory framework for its security service. With the *CSIS 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. SIRC derives its mandate and functions from the same law that sets out the Service's statutory framework.

CONTENTS

MESSAGE FROM THE COMMITTEE	2
MESSAGE FROM THE EXECUTIVE DIRECTOR	7
ABOUT THIS REPORT	9
1 SECTION	CERTIFICATE 10
2 SECTION	REVIEWS 12
	Security Screening – Section 54 Report 13
	CSIS’s Surveillance Capabilities and Functions 14
	A Counter-Intelligence Investigation 17
	A Sensitive CSIS Activity 19
	CSIS Operational Support and Its Use Overseas – Section 54 Report 20
	CSIS’s Use of an Emerging Area of Expertise 24
	Review of a CSIS Foreign Station 24
3 SECTION	COMPLAINTS INVESTIGATIONS 27
	Revocation of a Security Clearance 28
	Alleged Discrimination, Improper Conduct and Delay 30
	Revocation of a Security Clearance 31
	Alleged Wrongdoing and Violations of Rights 32
4 SECTION	SIRC AT A GLANCE 34
	Staffing and Organization 34
	SIRC Activities 35
LIST OF SIRC RECOMMENDATIONS	36

Message from the COMMITTEE

It is with great honour and pride that we present to Parliament, and to all Canadians, the work that was undertaken by SIRC for the fiscal year 2013–2014.

This report provides an annual assessment of CSIS's performance through SIRC's three key activities—certification, reviews and complaints investigations. As a whole, it also provides important insight into the nature and breadth of Canada's security intelligence activities.

The CSIS Director's Annual Report to the Minister of Public Safety offered a high-level overview of CSIS's key operational activities in the past year. This year, our certificate expressed overall satisfaction with the Director's Report and found that the activities described in the report complied with the CSIS Act and Ministerial Directives and did not constitute an unreasonable or unnecessary exercise of the Service's powers.

SIRC's certification process was complemented by its reviews, which provided in-depth examinations of a wide-range of CSIS's activities within and beyond our national boundaries. In most of its reviews, SIRC was satisfied with the manner in which CSIS carried out its mandate to investigate threats to the security of Canada. In others, however, the Committee raised concerns; indeed, the findings and recommendations arising from these reviews highlighted several areas for improvement. Of note, in two reviews, SIRC felt that the significance of the issues it found warranted sending the reports directly to the Minister of Public Safety as special reports under section 54 of the CSIS Act.

In most of its reviews, SIRC was satisfied with the manner in which CSIS carried out its mandate to investigate threats to the security of Canada. In others, however, the Committee raised concerns; indeed, the findings and recommendations arising from these reviews highlighted several areas for improvement.

The first report stemmed from our examination of CSIS's security screening activities. In this review, SIRC stressed the importance of CSIS exercising due diligence when using personal information, especially that collected under its security screening mandate. Our review identified a serious concern that changes CSIS has undertaken with respect to the internal use of information collected for security screening purposes could be in contravention of the *Privacy Act*, or could leave room for abuse of such information.

The second report examined CSIS's operational support capabilities overseas, with a dedicated focus on CSIS's decision to allow the arming of employees working in dangerous operating environments. SIRC first examined CSIS's use of firearms abroad in 2010, at which time it had recommended that should CSIS seek to change the scope of its policy on firearms, it should do

Under subsection 54(2) of the *CSIS Act*, the Committee may, on request by the Minister or at any other time, furnish the Minister with a special report concerning any matter that relates to the performance of its duties and functions.

so only after additional careful study and after consultation with, and approval of, the Minister of Public Safety. Four years later, in this report, SIRC raised a number of serious issues with respect to the management and accountability of CSIS's firearms program.

SIRC weighs carefully the decision to send a special report to the Minister; in the past, it has done so regarding issues that were the focus of substantial public attention. The decision to provide two such reports in the past year emphasizes the importance of the issues raised in these reviews.

This year, SIRC also noted concerns of a different nature, with respect to information provision and disclosure. In two reviews, SIRC encountered significant delays in receiving requested documentation and had to press the Service to obtain complete and consistent answers to several questions. With effort, SIRC was eventually provided all the relevant information it required to carry out and complete its reviews, but these difficulties and delays caused the Committee concern.

SIRC encountered similar disclosure difficulties in the investigation of two complaints. In one investigation, SIRC found that it had been seriously misled by CSIS and that CSIS had violated its duty of candour during *ex parte* proceedings by not proactively disclosing in its evidence its rejection of the reliability of a source of information. In a second complaint report, SIRC was critical of CSIS for failing to proactively highlight a highly relevant document. SIRC reminded CSIS that its disclosure obligations went beyond producing a

large quantity of documents for SIRC's review and included the duty to proactively present the most relevant pieces of evidence before any presiding Member.

SIRC communicated to CSIS its dissatisfaction regarding the way in which these reviews and complaints investigations had unfolded. The Committee is supportive of efforts undertaken by management to find a resolution to this problem, and it is hopeful that the situation is being dealt with appropriately.

Finally, SIRC came across a few issues within the scope of its reviews that, it felt, warranted focussed future examination. A number of these issues touched on CSIS's activities abroad, which SIRC has committed to examining closely on a yearly basis. Accordingly, SIRC has decided to explore these matters in a more meaningful and comprehensive manner as part of its upcoming research cycle.

In presenting the work that was undertaken last year, the Committee would like to extend its profound gratitude to SIRC's outgoing Chair, the Honourable Chuck Strahl, P.C., for his dedication and leadership in giving SIRC a stronger voice in the critical dialogue on national security. We also wish to thank the Honourable Frances Lankin, P.C., C.M. and the Honourable Denis Losier, P.C., C.M., whose terms expired this past year. Their engagement and input helped to enrich our discussions and enhance the value of our work. Following these departures, SIRC was very pleased to welcome a new Member, Mr. Gene McLean, P.C., whose in-depth knowledge of Canada's national security environment will undoubtedly be of tremendous benefit to us.

Past, Present and Future

This year marks SIRC's 30th anniversary. It is with great optimism that the Committee looks ahead, especially as we reflect on the course that has been travelled in the past three decades.

The Committee believes strongly that SIRC has remained faithful to the vision that was put forward by the McDonald Commission and to the mandate that was later defined by the architects of the CSIS Act. A member of the team working within the Privy Council Office on implementing the McDonald Commission recommendations recalls the challenge for those involved in creating Canada's new civilian security intelligence organization: to build public confidence in the new secretive organization by clearly defining the limits of its powers in law, but also implementing accountability mechanisms to keep these powers in check. To this end, SIRC would be given the independence and broad powers needed to provide assurance to Parliament and, by extension, to all Canadians, that CSIS was operating lawfully and appropriately.

This year marks SIRC's 30th anniversary. It is with great optimism that the Committee looks ahead, especially as we reflect on the course that has been travelled in the past three decades.

Although SIRC's fundamental *raison d'être* has not changed, the world in which we live today is very different from the Cold War environment in which CSIS was born. The rise of the global and borderless terrorist threat, the proliferation of initiatives designed to enhance collective security and the growth of Canada's national security apparatus has compelled SIRC to adapt its work to keep pace with these developments.

In this process, SIRC has been guided by a number of important legal developments. In addition to statutory amendments, the engagement of the courts in national security issues has produced a number of landmark judicial decisions, some of which have dealt specifically with SIRC.

For example, in 1992, the Supreme Court of Canada interpreted the word "recommendation" of the CSIS Act in the context of an investigation report in relation to the denial of a security clearance. In the same year, the Supreme Court of Canada determined in another matter that SIRC's proceedings pursuant to its Rules of Procedure and the CSIS Act did not violate the principles of fundamental justice.

More recently, in 2007, in examining the security certificate regime in place at the time, the Supreme Court of Canada looked to the SIRC model and processes as an example of a scheme which strikes a balance between the protection of sensitive information and the protection of an individual's procedural rights. Four years later, the Federal Court determined that since a complainant's rights, if not his interests, were at stake, SIRC investigation reports could be reviewed by the Federal Court. Confirming the position advanced by SIRC before the Federal Court, this decision makes SIRC more accountable through judicial oversight and, at the same time, reinforces the importance of our complaints investigation process.

Also, in 2012, the Federal Court ruled that SIRC had the jurisdiction to consider, in the course of its investigations, allegations raising issues of law, including the *Canadian Charter of Rights and Freedoms*. It found that in order to carry out its mandate of scrutinizing the activities of CSIS for the purpose of ensuring that it operates in accordance with the law, SIRC must have the jurisdiction to determine questions of law. The Court's analysis demonstrated that it was Parliament's intention that this jurisdiction include the *Charter*.

Overall, the rulings in these cases have had significant, positive, impacts on SIRC's investigation of complaints and have helped the Committee assume its role as a competent tribunal. These rulings have also, the Committee believes, served to validate the SIRC model of intelligence accountability.

At the same time, the post-9/11 security environment has brought about collective reflection on the possible need to fine-tune Canada's national security accountability apparatus. There have been mounting calls for Canada to achieve greater review or oversight of its national security activities, but there has not been consensus on how to best achieve this goal. Options have ranged from tweaking the enabling legislation of Canada's existing review bodies to asking Parliament to take on a more active oversight role.

The work of the *Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar* (commonly referred to as the *O'Connor Commission*) offered the first comprehensive analysis into how Canada's existing national security accountability framework had fallen out of sync with post-9/11 national security activities. The Commission noted how existing review bodies, designed to examine the activities of national security agencies that once worked mostly in silo, were now ill-equipped to review increasingly integrated national security activities. As a result, the Commission recommended the establishment of statutory gateways to allow national security review bodies to exchange information, to conduct joint investigations and to coordinate the preparation of reports.

Of particular concern to the *O'Connor Commission* was the fact that a number of federal departments or agencies actively engaged in national security were not subject to any form of independent review or oversight. The recommended solution was to give SIRC expanded powers to undertake ongoing review of the national security activities of the Department of Foreign Affairs, Trade and Development (DFATD), the Financial Transactions and Reports Analysis Centre, Citizenship and Immigration and Transport Canada.

SIRC has commented publicly on this recommendation, questioning whether the activities of these departments warrant the same level of permanent, independent and

ongoing review as those of CSIS, which can act covertly and in ways that can profoundly affect individual lives. Following reflection, SIRC put forward its own proposal for a proportionate yet effective system of broad, independent review for national security. This proposal aimed at allowing SIRC, through legislative amendment, to examine national security matters that go beyond CSIS by looking at the actions of other federal entities when they connect or relate to CSIS. SIRC still believes this proposal to be sensible.

The post-9/11 security environment has brought about collective reflection on the possible need to fine-tune Canada's national security accountability apparatus.

The discussion on accountability has intensified in the aftermath of widespread media reporting on the surveillance activities of intelligence agencies in various countries. As expected, these allegations have fuelled public criticism about intelligence work encroaching on citizens' privacy and have renewed calls for greater scrutiny of intelligence activities.

At home, these calls have taken the form of proposals to institute greater parliamentary oversight of Canada's national security activities. The argument put forward has been that Canada lags behind its close allies on the issue of parliamentary oversight as the only country that lacks a dedicated parliamentary committee with substantial powers of review over matters of national security and intelligence. Accordingly, there have been various efforts made to introduce legislation that would create such a committee to provide Canadians with "a full appreciation of what their intelligence agencies are doing considering the importance of intelligence-gathering work."

In the fall of 2013, SIRC was asked to comment on this initiative when it appeared before the Senate Committee on National Security and Defence. At that time, SIRC's Chair suggested that while it was desirable that Parliament play an active role in overseeing Canada's national security activities, careful consideration should be given to the mandate, responsibilities and structure of any future parliamentary committee to ensure that its activities complement rather than duplicate the work of existing intelligence review bodies.

Indeed, SIRC believes that its model offers three important benefits: independence, expertise and continuity. SIRC acts autonomously in its decision-making, meaning it decides which matters to investigate and report on, and may also question appropriateness of direction from the Government to CSIS. SIRC also has dedicated full-time research and legal staff who review CSIS activities in all areas, keep abreast of changes taking place at the Service, and carry out environmental scans to stay informed of relevant developments. Our model of ongoing and methodical review also has the distinct advantage of allowing for a full and impartial assessment of CSIS's performance,

arguably better positioning it to detect potential problems earlier.

As the merits of parliamentary oversight are debated, SIRC will continue to view its relationship with Parliament as an integral component of its mandate. In its first annual report, tabled in 1985, SIRC noted it believed that "Parliamentarians intended it to act on its behalf" in ensuring that CSIS carried out its activities appropriately, and further noted the following year that, "in some respects, the Committee may be seen as an extension of Parliament." SIRC still very much subscribes to this view today.

In the end, it seems reasonable for Canadians to ask whether the intelligence accountability framework that was designed 30 years ago is still appropriate to deal with the realities of contemporary intelligence work. Should decision-makers choose to modernize this framework by giving SIRC greater responsibilities, the Committee is confident that it has the expertise and ability to effectively take on new challenges. In the absence of change, the Committee has confidence in its ability to adapt to ensure that it remains relevant and effective in providing proper accountability of Canada's security intelligence activities.

MEMBERS OF THE COMMITTEE



The Honourable
Deborah Grey



The Honourable
L. Yves Fortier



The Honourable
Gene McLean

Message from the **EXECUTIVE DIRECTOR**

Having completed my first full year as SIRC's Executive Director, I would like to take the opportunity to follow up on the three key principles I underscored in my message from last year.

I remain firmly of the opinion that SIRC's most important principle is its independence. In a first instance, SIRC is independent from government to ensure that its priorities are not dictated by government decisions or party politics. In addition, SIRC has full autonomy in deciding its work and methodology, and in making its findings and recommendations.

Evidently, SIRC's independence underpins its dealings with the Service. SIRC has often described its relationship with CSIS as one of "healthy tension." Indeed, while we strive to maintain a cordial and professional relationship with our CSIS counterparts, our foremost objective is always to ensure that we receive all the relevant information we require to effectively carry out reviews and complaints investigations.

This past year, SIRC encountered challenges in this respect; in some instances, I had to personally intervene to ensure that staff received complete information. Having brought these issues to the attention of the Service's senior management, I am confident in CSIS leadership's ability to take the necessary steps to resolve the situation.

SIRC's independence is upheld on a daily basis by our staff, who carry out their activities with the utmost professionalism. Our research and legal staff recognize the significance of their work; for this reason, they are committed to ensuring the comprehensiveness, thoroughness and accuracy of every review and complaint investigation. To achieve this, they demonstrate tenacity and persistence in seeking to obtain the required information, but also diligence in combing through thousands of pages of documentation.

Finally, SIRC has stepped up its outreach efforts at home and abroad. In the past year, SIRC was invited to speak at a number of conferences and public events (on our website at www.sirc-csars.gc.ca, under "newsroom"); we seized a number of opportunities to talk about SIRC's work and to stimulate discussion on the importance of intelligence review. The Committee and I also attended the International Intelligence Review Agencies Conference, which was hosted by the United Kingdom's Intelligence and Security Committee. This conference, held every two years and attended by a number of our international counterparts, gave us a tremendous opportunity to discuss issues of mutual interest and exchange best practices.

It is with much enthusiasm that I look forward to fulfilling the ambitious agenda that we have laid out for the coming year. The research plan we developed contains a number of timely, topical and comprehensive reviews designed to further deepen our knowledge of CSIS's activities in Canada and overseas. With respect to our investigation of complaints, our newly adopted Rules of Procedure will help provide a more streamlined access to our complaints processes. Next year, SIRC will also focus on its underlying support systems by implementing a more robust and modern information management system aimed at improving efficiency and effectiveness on both internal services and core programs.

Sincerely,



Michael Doucet

I am committed to ensuring that SIRC remains fully engaged in broader public discussions on national security-related issues, such as those pertaining to the possible implementation of a broader system of independent review for agencies involved in national security. Our *raison d'être*, as outlined 30 years ago in debates leading to our creation was, and still is, to play a vital role in the functioning of the security intelligence system by promoting "adequate debate, where necessary, in the area of security."

ABOUT THIS REPORT

In accordance with its governing legislation, SIRC prepares an annual report of its activities that is tabled in Parliament by the Minister of Public Safety. This annual report summarizes SIRC's key findings and recommendations arising from its reviews and its investigation of complaints. It has four sections:

Section 1: **Certificate**

An overview of SIRC's certification of the CSIS Director's annual report to the Minister of Public Safety.

Section 2: **Reviews**

A synopsis of the reviews completed during the fiscal year covered by this annual report.

Section 3: **Complaints**

A synopsis of the complaints investigations completed during the fiscal year covered by this annual report.

Section 4: **SIRC at a Glance**

Highlights of SIRC's public engagement, liaison and administrative activities. This section also includes details of SIRC's annual budget and expenditures.

Monitoring SIRC's Recommendations

Each year, SIRC requests a status report from CSIS on the recommendations arising from its reviews and complaints investigations. This exercise allows SIRC to track the implementation of its recommendations and to assess their practical impact on CSIS.

This year, for the first time, SIRC is giving greater insight into this exercise by including CSIS's responses to recommendations at the end of each respective review or complaints investigation summary.

CERTIFICATE

In SIRC's 2011–2012 annual report, the Committee expressed the view that transferring responsibility for the Certificate upon the dissolution of the Office of the Inspector General had the advantage of allowing a single, expert entity to produce reports both for Parliament as a whole, as well as a specialized product for the Minister of Public Safety. At the same time, SIRC identified a challenge associated with this change: maintaining the arms' length independence of SIRC's core mandate, while simultaneously, as per the amended legislation, briefing the Minister on any matter relating to the performance by the Service of its duties and functions "at least once a year, and at any other time at the Minister's request."

With two years of experience operating in this new environment, the Committee can say with confidence that any concerns with respect to the encroachment of SIRC's independence, real or perceived, have not materialized. As required under the *CSIS Act*, SIRC's interactions with the Minister have become more frequent. Far from compromising its independence, however, this relationship has substantially added to SIRC's role in the system of accountability and has, if anything, deepened SIRC's ability to reassure Parliament and Canadians regarding the activities of the Service. In the future, the Committee will continue to engage with the Minister and the Department as appropriate.

The process of certifying the CSIS Director's annual report is a component of the system of accountability that was devised for CSIS upon its creation in 1984. In 2012, the Government of Canada amended the *CSIS Act*, requiring that SIRC take on some of the responsibilities formerly assigned to the Inspector General of CSIS.

The Certification Process at SIRC

The *CSIS Act* requires SIRC to submit to the Minister of Public Safety a Certificate stating the degree to which the Committee is satisfied with the CSIS Director's annual report to the Minister. As part of that process, SIRC is to discuss whether any of the Service's operational activities described in the report were not

authorized by the *CSIS Act*, contravened any Ministerial directions issued under the *CSIS Act*, or involved any unreasonable or unnecessary exercise of the Service's powers. Our certification process relies on a carefully designed and rigorous research methodology that is grounded in our understanding of the purpose of the Director's report: to provide the Minister with information necessary to support Ministerial responsibility for CSIS.

Satisfaction with the Director's Report

This year's Certificate expressed SIRC's overall satisfaction with the Director's report. The Committee found that it fulfilled Ministerial reporting requirements and was factually accurate. With respect to whether the report provided the Minister with an accurate representation of CSIS activities, SIRC found two areas—foreign operations and section 16 investigations—that should have been described in greater detail. Specifically, SIRC is of the view that the Director's report

should make clear to the Minister that there are unique risks associated with foreign operations, and that CSIS's activities with respect to section 16 investigations should be the focus of a more detailed discussion.

Compliance and Exercise of Powers

This year's Certificate also reflected SIRC's finding that the activities described in the Director's report complied with the *CSIS Act* and Ministerial Directives and did not constitute an unreasonable or unnecessary exercise of the Service's powers. With respect to the operational activities described in the report, SIRC determined that these activities were consistent with the duties and functions specified in sections 12 to 20 of the *CSIS Act* and complied with relevant section 16 requests from the Ministers of Department of Foreign Affairs and National Defence and with Ministerial Directives.

CSIS's activities are outlined in three distinct sections within the *CSIS Act*: section 12 permits the investigation of threats to the security of Canada, sections 13 to 15 authorize the provision of security assessments, and section 16 establishes a mechanism for the Service to assist the Ministers of National Defence or Foreign Affairs, within Canada, in the collection of foreign intelligence. Each of these sections of the *CSIS Act* provides the Service with a distinct legal mandate and establishes the thresholds that must be met before the Service may act.

REVIEWS

What is the difference between an oversight and 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 immediate, day-to-day operational decisions and activities.

SIRC’s reviews are designed to provide Parliament and the Canadian public with the assurance that, in the performance of its duties and functions, the Service has acted appropriately, effectively and in accordance with the rule of law.

The Review Process at SIRC

SIRC’s reviews provide a retrospective examination and assessment of specific CSIS investigations and activities. The Committee’s review 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).

A typical review requires hundreds of staff hours and is completed over a period of several months. As part of this process, SIRC's researchers consult multiple information sources to examine specific aspects of the Service's work: researchers may look at individual and group targeting files, human source files, intelligence assessments and warrant documents. SIRC can also examine documents relating to CSIS's cooperation and operational exchanges with foreign and domestic partners.

In every review, the examination of documentation generates follow-up exchanges with the Service. For this reason, SIRC researchers often request meetings and briefings with CSIS employees to seek clarification on issues. SIRC's goal is to satisfy itself that 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 the Minister of Public Safety.

SIRC STUDY: Security Screening – Section 54 Report

Under subsection 54(2) of the CSIS Act, the Committee may, on request by the Minister or at any other time, furnish the Minister with a special report concerning any matter that relates to the performance of its duties and functions.

Security screening is one of CSIS's primary responsibilities and also one of its most visible. As part of this function, which is set out in sections 13 to 15 of the *CSIS Act*, CSIS advises and assists the Government of Canada in preventing individuals who may pose a threat to Canada from obtaining either status or entry into Canada, as well as individuals who represent such threats, from accessing sensitive sites, assets or information.

SIRC examines the security screening process on a continuous basis as part of its complaints function; under section 42 of the *CSIS Act*, SIRC investigates complaints about denials or revocations of security clearances. It had

been several years, however, since SIRC undertook a focussed review of the Service's Security Screening Branch. In the intervening time, there have been several changes to the security screening program, including initiatives to streamline the screening process in order to improve the quality and consistency of screening products.

Our review identified a serious concern that changes CSIS has undertaken with respect to the internal use of information collected for security screening purposes could be in contravention of the *Privacy Act*, or could leave room for abuse of such information.

Findings

SIRC's review examined the key responsibilities and activities of CSIS's Security Screening Branch (SSB), including changes that have been made to its security screening program. As the review unfolded, SIRC chose to also focus on the processes under which information collected for security screening purposes is used and accessed within the Service; SIRC looked at corporate, operational, legal and policy documents to explore this issue fully. In addition, SIRC held briefings with SSB and regional offices to gain a full understanding of the screening process.

Beginning in 2010, SSB instituted corporate changes to address several challenges including: an increasing volume of requests and growing demands for services; a lack of centralized accountability and corresponding performance standards; out-dated or disjointed tools; and "complex" business practices. Although changes are still ongoing, SIRC noted that they have contributed to enhancing SSB's effectiveness. SIRC also found the initiatives undertaken by SSB to be very productive, notably the establishment of a quality-control mechanism and increased standardization on screening procedures and products across the Branch and the Regions. Overall, SIRC found SSB to be

proactively attempting to adopt sound business practices, as well as incorporating internal and external stakeholder input in order to create a better, more valuable screening product.

SIRC paid close attention to how CSIS uses and accesses information collected for security screening purposes. CSIS collects a great deal of information through its distinct legislative authorities. Disclosure of personal information, even within an organization, is subject to protection under the *Privacy Act*. Whereas information collected under section 12 of the *CSIS Act* is done without the knowledge or consent of individuals, under sections 13 to 15 (which deal with government and immigration screening), individuals provide written, informed consent for the Service to collect information for a specific purpose.

The notion that CSIS has to protect personal information has been ingrained since its creation. In fact, the McDonald Commission stressed this point in its report, emphasizing that while the Privacy Commissioner could review complainants' allegations of improper disclosure, "it is of the essence of security intelligence investigations that the subjects of such investigations be unaware of the investigation." For this reason, "we believe a system of prior approval, involving judicious application of a strict test of necessity, is needed as a means of ensuring that government information about the personal details of one's private life, beyond those items that are generally public knowledge, is used for national security purposes only when a clear case for the necessity of such use has been made."

SIRC agrees that the secretive nature of CSIS's information collection is precisely the reason why CSIS must be diligent in its use of personal information, specifically information collected under its security screening mandate. For this reason, SIRC identified a serious concern that changes to the internal use by CSIS of the information it collects for security screening purposes could be in contravention of the

Privacy Act, or could leave room for abuse regarding the use of such information.

SIRC noted that when an organization brings about large systemic changes to how it shares and uses personal information, a Privacy Impact Assessment is required. SIRC was told that the Service was in the midst of preparing a Privacy Impact Assessment addressing broader information management matters, but it was unclear to SIRC if its specific concerns would be addressed in a full and timely manner. **Accordingly, SIRC recommended that CSIS consult with the Office of the Privacy Commissioner (OPC) before the end of 2013 on changes affecting the internal use of information collected for security screening purposes.**

CSIS Response

The Service wrote to the OPC in December 2013 to advise that a Privacy Impact Assessment was being prepared on a broader CSIS information-management initiative. According to CSIS, the OPC will be able to examine the privacy issues raised by SIRC in this review within the context of this larger Assessment.

SIRC STUDY: CSIS's Surveillance Capabilities and Functions

CSIS has five key pillars of information collection: human sources, technical intercepts, liaison with foreign partners, domestic partnerships and surveillance. In general terms, physical surveillance involves the act of watching or monitoring, discreetly, the movements and activities of a person or object in real time. Even though the definition is relatively straightforward, in practice, physical surveillance is extremely difficult to carry out. CSIS's surveillance officers are required to observe their target while managing an often complex and evolving environment to ensure that their activities remain inconspicuous. To do this, they must develop extensive area knowledge, exceptional driving and observational

skills and a comprehensive understanding of team tactics. Moreover, they must execute their skills under pressure and, often, in less than ideal circumstances.

Findings

Although CSIS's surveillance activities are regularly examined in the context of reviews of particular investigations, this year SIRC decided to undertake a more focussed look at CSIS's surveillance functions. This review included an in-depth examination of the processes, policies and controls in place to manage the Service's surveillance activities across the country.

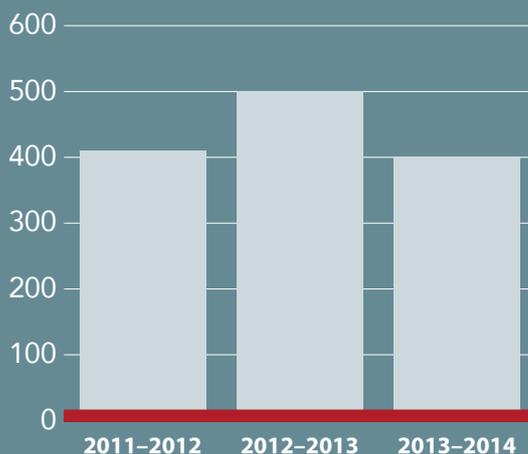
SIRC also paid close attention to recommendations flowing from a 2011 CSIS internal study that called for greater standardized surveillance practices, as well as centralization and modernization to advance overall performance. This initiative was consistent with other program renewals undertaken by CSIS in recent years to improve effectiveness, efficiency and operational output. This review thus sought to assess the extent to which CSIS has been successful in making proposed and, arguably, necessary changes to the surveillance program.

Overall, SIRC observed that surveillance officers carried out their work with professionalism and dedication. From coast to coast, SIRC found regional surveillance officers were uniform in their positive and introspective outlook towards their work. Indeed, members of SIRC's research team gained some practical perspective on the complexities involved in conducting surveillance while participating in a CSIS surveillance training scenario. This opportunity not only provided SIRC with insight into the expertise of surveillance officers but, equally important, the knowledge gained improved its overall assessment of CSIS's surveillance activities.

SIRC's extensive review of documentation and meetings with each of the regional surveillance teams across Canada revealed that, despite the

Targeting

As per its mandate, CSIS may investigate a person or group engaged in activities suspected of posing a threat to the security of Canada. Section 2 of the *CSIS Act* defines these activities as being in support of espionage, sabotage, foreign-influenced activity or terrorism. This figure indicates the number of targets (rounded to the nearest 10) investigated by CSIS in the past three fiscal years.



differences that exist between the various CSIS regions, these teams share similar managerial issues. For example, all regions must address issues relating to hiring standards, training, procurement in a time of fiscal constraint, attrition, the introduction of new technologies, and management of scarce resources. SIRC is of the opinion that these issues can best be addressed through standardization and that taking such action will improve the Service's

surveillance capability. As such, SIRC found the principal findings and recommendations from CSIS's 2011 internal study to be sound.

However, following the completion of the 2011 internal study, CSIS did not institute a strong management structure to implement its recommendations. Although the Service's internal study called for a dedicated manager with adequate staff to coordinate the centralization and standardization of the program, SIRC found that this recommendation was not acted on. In the absence of a strong central authority to lead the transition within the surveillance program, regions began implementing changes to their surveillance models according to their own needs and available resources.

One region, for instance, has worked towards improving its analytical capability in a way that enables more efficient deployment of surveillance officers, while another region has worked on improving the analysis of a target's movements. Although these initiatives are commendable, if they are continued in isolation from the other surveillance teams across the country, SIRC is concerned that it will be that much more difficult for CSIS to devise a truly "national" set of surveillance standards. Most significantly, SIRC believes that the absence of strong leadership to guide the surveillance program has meant that some of the issues that SIRC views as the most serious remain unaddressed.

For example, SIRC found that the Service does not have legal advice on how provincial laws apply to its surveillance teams, nor does it have a set of national driving standards to guide employees on important daily operational matters, such as the use of communications equipment while driving. Therefore, **SIRC recommended that CSIS prioritize the request for legal advice pertaining to its liability under distracted driving legislation across Canada.** Furthermore, following receipt of legal advice, CSIS should develop clear and standardized operating procedures outlining

the responsibilities of surveillance officers with respect to the performance of their duties and functions while driving.

SIRC was also concerned about the low level of communication that occurred between regions, as well as with CSIS HQ. With surveillance teams spread across Canada all sharing identical job functions, SIRC expected to see solid communication among surveillance practitioners. Instead, SIRC found that, for the most part, regional surveillance teams operate in total isolation from one another and communicate only sporadically with their HQ counterparts. That CSIS's surveillance teams do not routinely share lessons learned, nor keep the relevant practitioners within HQ consistently informed of operational developments, runs contrary to what SIRC believes are practical and necessary standards for a modern surveillance program.

Finally, given that CSIS's goal is to further entrench standardized approaches to surveillance training and development, SIRC expected to see synchronization between HQ and the regions on this objective. Instead, SIRC found that in certain instances a bifurcated training model persists, with HQ working towards the standardization of performance and learning objectives, while the regions remain focused on their own training agendas. In SIRC's opinion, this situation owes to an evident lack of coordination and consultation between HQ and regional surveillance teams.

Ultimately, SIRC found that the Service's failure to create a management structure and action plan to implement the recommendations outlined in the 2011 internal study has had two important repercussions. First, it has prevented the Service from achieving the standardization necessary for a modern, centrally coordinated surveillance program. Second and, more importantly, the failure to centralize and standardize the surveillance program has created a situation whereby the accountability structure is not as robust as SIRC believes it should be.

Accordingly, the **Committee recommended that CSIS devise a clear governance framework that addresses the foundations of a national and standardized surveillance program.**

Furthermore, this framework should be implemented through an action plan considering the following six points: clearly articulate the need for change and note precisely what change will transpire; commit leadership to guide the program forward; seek collaboration and engagement by relevant regional stakeholders; devise clear benchmarks for implementation; devote resources; reinforce to stakeholders that there is Executive-level commitment in achieving program results; and build in feedback processes to help assess progress.

CSIS Response

The Service has drafted a request for a legal opinion pertaining to its liability under distracted driving legislation across Canada. It has also initiated internal changes to further promote a standardized approach for surveillance activities and developed recommendations on various aspects of the surveillance program to form the basis of an action plan.

SIRC STUDY: A Counter-Intelligence Investigation

The end of the Cold War and the subsequent rise of the threat of terrorism have led to fundamental changes in intelligence priorities. In its most recent Public Report, CSIS confirmed that terrorism remains its “greatest preoccupation,” while at the same time reminding Canadians that the threat of espionage continues to be very real and that Canada “is a highly attractive target for hostile intelligence agencies.” In this review, SIRC looked at the goals and management of one of CSIS’s longest-running high-priority counter-intelligence investigations to assess how well the Service’s investigation has kept pace with current government direction and changes in the threat environment.

SIRC last looked at this investigation in 2007–2008, at which time the Committee assessed the Service’s performance in countering attempts by a foreign intelligence agency to cultivate sources of information within the Government of Canada, as well as its attempts to obtain economic intelligence and controlled technologies from Canadian businesses surreptitiously. SIRC concluded that the Service had positioned itself well to counter the threats posed by this foreign intelligence agency.

At the time of the 2007–2008 review, the Service was just beginning the process of broadening its investigation in recognition that the threat environment was changing. Although that review noted the Service had, to a degree, refocused its intelligence efforts to respond to a shift in the practices in the foreign intelligence service, the Committee was unable to comment further since this was a new development.

Findings

In this review, SIRC began its examination of the investigation by looking at the Service’s efforts to refine and refocus its approach to investigating this foreign intelligence agency. SIRC found that the modest refocusing of the CSIS investigation is justifiable given the fluidity and challenges inherent in a large counter-intelligence investigation. Still, the Committee found that, despite some success, the Service’s modest movements away from the traditional focus of its investigation have yet to yield substantial results. **For this reason, SIRC recommended that the Service commit to reassessing the resources devoted to this aspect of the investigation in due course to determine its continued sustainability.**

The review also looked at the more traditional elements of the investigation and concluded that the core of the investigation continues to be well managed, with several strong points and some notable successes. SIRC also found that CSIS worked well with traditional and non-traditional domestic partners and that these efforts served as a positive example of broader interdepartmental cooperation on an important issue.

In carrying out its mandate, CSIS collects threat-related information using various investigative techniques, some of which require CSIS to obtain a warrant from the Federal Court. These techniques would include, for example, intercepting communications or mail.

SIRC keeps abreast of CSIS's application for, and execution of, new warrant powers approved by the Federal Court. In 2012–2013, it reported on a power allowing the Service to maintain coverage of targets who represent a threat to Canada as they travel or, in some cases, reside overseas.

At the same time, SIRC looked at a sample of CSIS intelligence assessments of the threat associated with the foreign intelligence agency and found that the threat assessments produced by the Service should be more nuanced, but also provide more contextual information to better support any general characterization of the threat.

This review also gave SIRC an opportunity to examine a new warrant power that was approved by the Federal Court and employed in this investigation, among others. Overall, the Committee concluded that this power has significant value in a number of settings and that the Service has

acknowledged the potential privacy implications associated with it and has taken steps to minimize its intrusiveness.

The Committee also looked at the execution of the power in the specific context of this investigation. The review found that the Service exercised appropriate restraint in the execution of the warrant power given the level of intrusiveness associated with its use. At the same time, the review found a relatively high number of non-targeted communications that were incidentally intercepted. As a result, **the Committee recommended that CSIS's next warrant application include summary information similar to that which was compiled for SIRC so as to provide the Federal Court with additional information regarding the application and use of the power in this investigation.**

Going forward, the Committee made explicit its expectation that the Service demonstrate a continued sensitivity to issues of proportionality and operational necessity as it contemplates the expanded use of this power in other investigations.

CSIS Response

The Service will make a more concerted effort to prioritize its targets to ensure that this investigation is appropriately resourced and investigated. It has also agreed to provide a comprehensive overview of the warrant power used in this investigation as part of its next warrant application to the Federal Court.

TABLE 1: WARRANTS

	2011–2012	2012–2013	2013–2014
New warrants	50	71	85
Replaced or supplemental	156	189	178
Total	206	260	263

SIRC STUDY: A Sensitive CSIS Activity

In the course of its duties, CSIS undertakes operations and activities that sometimes require the guidance of specialized units or programs. This study marked SIRC's first in-depth examination of a specific program. Due to the nature of this program's activities, involvement and input from domestic partners is sometimes required, as is the assistance of foreign governments.

In the course of its review, SIRC encountered a number of significant delays and problems with respect to documentation provision.

Findings

At the outset of its review, SIRC was guided by a number of key considerations, such as: CSIS's decision-making process, the overall management of the program, CSIS's interactions with internal and external stakeholders, and activities that carry a potential for public controversy.

In the course of its review, SIRC encountered a number of significant delays and problems with respect to documentation provision. This led SIRC to find that a CSIS Branch had failed to adequately address SIRC's requests for documentation that was needed to carry out its review. As a result, the Committee requested CSIS to undertake a thorough examination into how SIRC's queries were addressed and to report back to SIRC in a timely manner. Following CSIS's response and action, SIRC is confident that it received all relevant materials for its review.

In 2010, the former Office of the Inspector General had recommended that CSIS make significant improvements to policies governing the activities in question, including Ministerial reporting requirements. CSIS subsequently revamped some of its relevant policies but, after careful examination, SIRC noted the need for further improvement, as the current policy still provides insufficient guidance. SIRC was told that CSIS is working to bring about further improvements.

Owing to the sensitivity of these activities, SIRC acknowledged the need for them to be handled on a case-by-case basis, with details and developments of each activity closely guarded and documented. Yet, SIRC noted that excessive safeguarding could lead to lost opportunities to learn from past lessons. For this reason, **SIRC recommended that the unit improve its information management methods and archiving practices.**

SIRC also noted that the unit is not playing as important a role in the approval process for these activities as outlined in policy. In the course of its review, SIRC came across a situation where better internal coordination and involvement from the unit at the initial decision-making stage could have proven beneficial. In light of these circumstances, **SIRC recommended that CSIS carefully examine the role of the unit within the larger process of operational discussions and decision-making, with a view of making the unit's involvement more explicit and formal.**

SIRC also raised concerns regarding the mechanisms through which the Minister of Public Safety is kept abreast of pertinent developments relating to these activities. Although the Minister may be informed of these activities *post facto* through the Director's annual report, there is no requirement in operational policy to report on an ongoing, active basis.

As SIRC noted, however, Ministerial direction requires the Director to report to the Minister, in a timely manner when there is a potential that a CSIS activity may have significant adverse impact on Canadian interests, such as discrediting the Service or the Government of Canada, giving rise to public controversy. SIRC believes that the activities reviewed often carry elements that could give rise to public controversy. Yet, SIRC found that the Minister of Public Safety is not always systematically advised of such activities, nor is he informed of them in a consistent manner. **SIRC therefore recommended that CSIS strive to ensure that reporting to the Minister of Public Safety be done in a formal and systematic manner.**

SIRC also learned that the CSIS Executive is kept apprised of major developments of the activities in question through an internal document; however, SIRC noted that CSIS had not used this process in over two years, despite developments that would have, in our opinion, warranted briefing to the CSIS Executive. For this reason, **SIRC recommended that appropriate mechanisms or processes be put into place to assist in systematically informing the CSIS Executive on developments related to the activities reviewed.**

Looking ahead, CSIS indicated that its current approach to managing these activities is sustainable and that it is well positioned to deal with a possible influx. Although CSIS noted that the introduction of new policies and procedures will provide better guidance on these activities, the issues raised in SIRC's review suggested that CSIS could benefit from more effective strategic planning on matters related to these activities.

CSIS Response

The Service has initiated changes to information-management practices surrounding the activities of this unit to allow for better record-keeping and tracking of issues, lessons learned and recommendations. It is also in the process of updating policies and developing guidelines to ensure that this unit's role in decision-making is made explicit and formal. On the issue of reporting to the Minister of Public Safety, CSIS will continue with its current protocol of briefing the Minister only when required, as the approval authority for this activity ultimately lies with the CSIS Director. Finally, CSIS has instituted formal biannual briefings to the Executive on this activity, with other briefings occurring as required.

SIRC STUDY: CSIS Operational Support and Its Use Overseas – Section 54 Report

For many years, CSIS employees stationed abroad mainly carried out liaison functions, namely receiving security intelligence from allied governments and relaying this information back to HQ. The changing threat environment post-9/11 compelled CSIS to rethink and redefine the nature and scope of its foreign work. This evolution also required the organization to pay more attention to the support functions necessary to run safe and effective operations abroad.

SIRC raised a number of serious issues with respect to the management and accountability of CSIS's firearms program.

Findings

The purpose of this review was to examine some of the physical, technical and planning support required for overseas operations, especially in higher-risk environments. SIRC examined the various changes to and developments in CSIS's foreign operations platforms, before exploring in-depth one of the most exceptional foreign support measures used by CSIS: the arming of personnel in high-risk/dangerous operating environments.

In the course of the review, SIRC encountered a few difficulties. SIRC staff received incomplete and inconsistent answers from CSIS on a number of issues related to the firearms program, leading it to believe that CSIS demonstrated a lack of candour.

In the end, SIRC's Executive Director wrote to CSIS requesting further information; these responses enabled the Committee to complete its assessment of the overall integrity of CSIS's firearms program.

On the evolution of CSIS's foreign operations platforms, SIRC noted the processes in place that are required to perform operations overseas have improved and are much more inclusive and comprehensive than in the past. SIRC also found that CSIS has worked on improving training offered to employees, developed new policy, approvals and authorities, enhanced its capabilities and equipment to deal with critical incidents, and designed new operational methods specific to the unique challenges associated with operating abroad. Still, SIRC recommended ways in which CSIS could further enhance its foreign operational support functions.

For example, with respect to training, a variety of specialized courses have recently been developed that are tailored to the needs of employees being sent overseas. Although these courses offer excellent training, none of them are actually mandatory prior to deployment. SIRC found this to be problematic since training is supposed to assist employees and mitigate any associated risks that they may encounter while performing and/or assisting in operations abroad. As such, **SIRC recommended that all necessary and relevant training be made mandatory prior to an employee's deployment abroad.**

Moreover, CSIS recently rolled out its Critical Incident Response Plan (CIRP), which outlines the main steps to be followed in the event an employee is involved in a critical incident impacting their health and well-being. Despite the clear benefits of this plan, SIRC found that not all employees posted abroad have been informed about the importance of

understanding the CIRP. **SIRC therefore recommended that CSIS HQ ensures that all employees be properly informed about the CIRP and any responsibilities they have under this Plan.**

Finally, SIRC noted that CSIS has paid appropriate attention to further augmenting the protective-support capabilities offered to employees working overseas. Known generically as Personal Protective Equipment (PPE), this refers to protective clothing, helmets, goggles or other garments or equipment designed to protect the employee's body from injury. SIRC found that there were instances of poor planning in deploying PPE products abroad. **SIRC recommended that CSIS apply consistent measures to ensure that personnel stationed abroad are adequately supplied with the appropriate personal safety equipment.**

CSIS has forged ahead with further changes to its foreign collection platform, which requires additional planning and operational support, as well as concerted efforts at both CSIS HQ and stations abroad. SIRC notes that the support systems in place to help facilitate foreign operations are being given considerable attention by CSIS; however, there remain some holistic challenges. CSIS HQ has acknowledged that it is working on all of these concerns, albeit within its fiscal limitations. SIRC will, in the future, revisit this subject to assess the degree to which these initiatives have affected operational support functions.

Overall, SIRC noted that the operational support mechanisms being developed overseas by CSIS are unique given the challenges associated with working within diverse foreign environments. Similar to Intelligence Officers in domestic operations who receive support from a number of different platforms, those operating abroad may at times deploy as members of a team, which

CSIS employees have been armed within Afghanistan since 2002. Until 2007, the arming and training of deployed CSIS personnel was the responsibility of the Canadian Forces (CF), who also ensured that all of CSIS's Afghan-related activities received Special Forces close protection. Equally significant, DFATD provided all CSIS employees in this country with diplomatic accreditation. As such, CSIS received excellent support from its Canadian military and diplomatic partners, in keeping with a whole-of-government strategy for operating within Afghanistan.

can include a host of various supports, including the possibility of armed protection for high risk/dangerous operating environments—a significant development that SIRC deemed to warrant close scrutiny in this review.

The catalyst for the adoption of one of CSIS's most exceptional operational support measures—the arming of Service personnel in high-risk/dangerous operating environments—is rooted in CSIS's entry into Afghanistan. The support functions used to advance CSIS's Afghan activities were initially unique yet, increasingly, the support capabilities came to be regarded as the preferred model for other theatres. Accordingly, CSIS launched its own firearms program, including the development of new firearms-specific policy and training. It also laid the foundations for its own armed operational support team. In 2010, CSIS acknowledged publicly that its intelligence officers could carry firearms in dangerous operating environments overseas.

That same year, SIRC undertook a review of CSIS's decision-making overseas, which included its use of firearms within Afghanistan. At the time, the Committee found that there were

strong measures in place to ensure proper training, accreditation and conditions under which firearms could be used. However, SIRC expressed caution about CSIS's possible future decision to use firearms outside of Afghanistan. The review concluded with a recommendation that, should CSIS expand its use of firearms abroad, it should be done “after consultation with, and approval of, the Minister of Public Safety.”

SIRC found that CSIS's new procedures provide improved direction to employees regarding their roles and responsibilities under the Service's firearms program, but there appears to be a disparity between policy and its practical application by employees. Furthermore, SIRC learned that not all employees who should have a sound understanding of CSIS's firearms program had knowledge of the policies or protocols. SIRC also found an instance where CSIS was not strictly following its own protocols on firearms. In light of these observations, SIRC impressed upon CSIS that its policy and protocols must be followed in the strictest possible terms, or be clearly written to indicate where there is latitude for interpretation.

SIRC also noted that CSIS's policy on firearms fails to adequately address the issue of an employee's liability, civil or criminal, under the laws of a foreign country and whether any mechanisms for immunity could be explored or what position the Government of Canada would take on helping to extract an employee from a certain situation. There is also no adequate advice on what course of legal action would be pursued domestically if an employee was believed to have acted negligently within a foreign environment, and consideration is not given on the extent to which certain types of firearms can be regarded as “defensive weapons.” Finally, there is also a lack of adequate advice on possible legal implications for Canada under international law.

In order to improve CSIS's management of its firearms program, **SIRC recommended that CSIS develop better guidelines on the sourcing and purchasing of weapons within**

dangerous operating environments, create a clear responsibility centre for the firearms program and obtain updated legal advice related to the reasonableness and necessity of carrying firearms within dangerous operating environments.

Finally, in 2010, SIRC had recommended that any expansion of CSIS's use of firearms beyond Afghanistan involve consultation with the Minister of Public Safety, as per criteria set out in Ministerial direction. Initially, our review was unable to conclude whether the Minister of Public Safety had been directly consulted and engaged on this issue. CSIS subsequently provided additional information to SIRC. After having carefully assessed this new information, SIRC remains of the opinion that the Service did not engage adequately with the Minister of Public Safety as the nature and scope of the firearms program evolved beyond Afghanistan.

SIRC believes that many of the issues raised in this review go to the heart of Ministerial accountability over CSIS. **SIRC therefore recommended that CSIS provide the Minister with written justification explaining under what legal authority CSIS officials are permitted to carry firearms outside of the unique legal context of Afghanistan.** Moreover, as part of this Ministerial consultation, SIRC would expect that the Service provide a full explanation of how the arming of some of its employees is consistent with CSIS's policy framework, which is rooted in the premise that activities are lawful and authorized, necessary and proportionate, and represent an effective and efficient use of public resources.

The difficulties encountered in trying to find documentation pertaining to CSIS's interactions with the Minister on this issue raised an additional issue of concern. There is wide acceptance of the importance of adhering to robust information-management practices among Canadian government departments and agencies, especially with respect to decision-making.

The Committee found it surprising, but also unacceptable, that CSIS had no record of a meeting between the CSIS Director and the Minister during which an issue as important as firearms was discussed. As such, **SIRC recommended that CSIS take immediate and appropriate steps to impress the importance of maintaining records of discussions and decisions to ensure proper accountability.**

CSIS Response

CSIS is working on a process that will provide standardized guidelines on the appropriate training recommended for each deployment, be it permanent or temporary; the determination of what is mandatory training will be made by the proper operational and security personnel. On the issue of the CIRP, CSIS has indicated that while it has already taken numerous steps to ensure that employees are aware of this Plan, it is taking further steps to improve all employees' awareness, namely through training, of their roles and responsibilities during all types of incidents and/or emergencies.

With respect to personal safety equipment, CSIS has indicated that it already equips employees at post with such equipment, but it will nonetheless incorporate existing requirements for personal safety equipment into policy and procedures before the end of this year. In this same timeline, it will also finalize a policy dealing with sourcing and purchasing of weapons in dangerous operating environments. CSIS has stated that it does not need to create a responsibility centre for its firearms program, as current procedures already have one in place. On the issue of documentation, CSIS agreed to take measures in the medium term to ensure the proper recording of decisions involving consultations with the Minister.

SIRC's recommendations pertaining to obtaining updated legal advice and to providing written justification to the Minister are still under consideration.

SIRC STUDY: CSIS's Use of an Emerging Area of Expertise

In recent years, SIRC observed that the Service has been turning increasingly to an emerging area of expertise to further its counter-terrorism and counter-espionage investigations. Although this form of assistance began in the mid-1990s in the form of requests from operational staff for target assessments, the work requested gradually expanded to also include human source assessments. Owing to mounting demand for services, this specialized unit within the Service grew over the years and its work has diversified. This unit currently divides its time between two major activities: direct contribution to operations and research and development.

Findings

SIRC's review explored how this team's insight and proficiency contributes to CSIS's understanding of the threat environment, and how this expertise is utilized and appreciated by different units in the Service.

Overall, SIRC found that the expertise provided by this unit has helped to enhance CSIS's operational capabilities and to mitigate certain corporate risks, particularly when the Service is operating in a dangerous environment. SIRC also found value in having a second set of eyes review certain activities, especially as the unit was able to provide additional insight from a specialized perspective.

SIRC was able to get some measure of the unit's usefulness by examining feedback provided by operational desks. This feedback was overwhelmingly positive, with the major concern being the length of time it took to get the end product. In the end, SIRC was left with the impression that this unit's work represents a valuable contribution to the Service's activities and operations.

The unit's research and development component is very active in a forum of professionals from allied countries who share ideas and expertise.

This forum also creates interesting opportunities for collaboration. SIRC found that the research and development team has made a respected contribution to the field and that CSIS's work is recognized and appreciated by its partners.

One challenge regarding the use of this expertise is that, currently, there are no standards of practice that guide the specific types of activities carried out by this unit in an intelligence setting. SIRC's review looked at how the unit endeavours to ensure that, in carrying out its work for CSIS, it does not act in a manner that could contravene any ethical codes or standards. SIRC found that the unit performed its duties with due care and regard for the potential ethical concerns that could arise from providing services to a security intelligence agency, and that it also had a proactive and methodologically sound approach to creating an ethical framework.

SIRC STUDY: Review of a CSIS Foreign Station

Each year, SIRC examines CSIS's activities overseas by reviewing, in-depth, the activities undertaken at a foreign station (the location of these stations remains classified, with the exception of Washington, London, Paris and Afghanistan). The activities that are facilitated by CSIS personnel posted abroad constitute important nodes for CSIS operations: indeed, CSIS's expansion overseas in the past decade has meant that its personnel stationed abroad have assumed more responsibility for taking on and coordinating the Service's overseas collection efforts.

SIRC's choice of a foreign station for review is usually rooted in the overlap between the regular duties and functions of the CSIS personnel posted at station, and the existence of leading-edge practice, a unique environment or a local partnership, any of which carries broader implications for CSIS's intelligence collection program.

Findings

This year, SIRC chose to review a foreign station whose work stood at the forefront of CSIS's evolving *modus operandi* overseas. Following an extensive review of documentation and numerous briefings at CSIS HQ, SIRC undertook a comprehensive on-site visit at station.

During its on-site review, SIRC took note of a security concern with respect to the protection of a communications network. In response to a technical issue, CSIS took reasonable steps to ensure the problem was solved while maintaining the necessary level of security; however, SIRC found that CSIS policy did not provide adequate procedures to deal with this situation. Moreover, documentation stipulates that CSIS must advise and seek approval from another partner prior to applying such a technical solution to this network. As a result, **SIRC recommended that CSIS update its security procedures to include additional guidelines and that it inform the appropriate authority of the solution it has implemented to resolve the technical problem.**

As SIRC has noted in recent years, the evolution of CSIS's operational footprint overseas had greatly enhanced its intelligence collection, but it has also created some challenges. For example, SIRC found that CSIS is not utilizing as many of the available techniques to validate intelligence collected overseas as it can and should, especially when operating in more secure overseas locations. As a result, **SIRC recommended that CSIS enhance its validation process for intelligence collected abroad by making increased use of the tools and techniques it already employs domestically.** In the absence of doing so, SIRC was concerned that the Service was relying heavily on techniques that may fall short of confirming the value and veracity of the information.

Finally, SIRC examined an important domestic partnership in the context of overseas operations, the Department of Foreign Affairs and Trade Development (DFATD). For several years now, SIRC has noted the evolution at DFATD's Global Security Reporting Program (GSRP), which was created post-9/11 to generate increased reporting on terrorism, non-proliferation and other security issues. GSRP officers, who are

Each year, SIRC reviews one of CSIS's foreign stations. Although the specific focus and objectives of a station review varies according to the location, these reviews do explore common elements:

- under section 38 of the *CSIS Act*, SIRC must review the Service's approved arrangements with foreign agencies, the details and intricacies of which are managed at station;
- each station also manages a range of relationships with Canadian domestic partners, the nature and scope of which may be affected by the history of Canada's presence in the country, as well as local conditions and events;
- the working and security conditions at each station may vary and, as

with any field operation, there is an operational context and environment that is only appreciated on-site; and

- observations flowing from individual station reviews may reveal patterns when analyzed and compared over time.

Overall, SIRC's ongoing reviews of foreign stations allow for a more complete analysis of CSIS's activities overseas. These reviews offer SIRC the unique opportunity to witness, first-hand, the day-to-day work of CSIS personnel posted abroad and provide valuable context for the operational strategies developed on the ground, as well as the policy discussions that take place at CSIS HQ.

not intelligence officers, collect information on security and stability issues, assess the evolving threat and risk environment at missions and work with whole-of-government reaction teams during crisis situations.

On the surface, there should be little overlap between the work of GSRP officers and CSIS officials: the former is looking for information concerning foreign developments, regardless of their connection to Canada, whereas the latter is collecting information that has a Canadian threat nexus. Nonetheless, there is a latent and real potential for conflict between the two programs, not the least of which can arise from both CSIS and DFATD “fishing in the same pond” for sources of information, and the possibility of running information-gathering programs with a similar focus vis-à-vis Canadian foreign or intelligence priorities. SIRC intends to keep this potential for conflict in mind as it moves forward.

While at station, SIRC was told by both GSRP and CSIS officials that they frequently meet to discuss situations that could become problematic. Both officials described the working relationship as cooperative, useful, professional and complementary to their own roles. While the relationship between the GSRP and CSIS officials at station appeared productive and positive, SIRC remains mindful of the fact that the GSRP’s goals and methods may lead to conflicting and overlapping initiatives with CSIS.

More broadly, however, SIRC’s impression of the relationship at station between CSIS and DFATD officials was not positive, with little awareness, appreciation or support for each other’s work. In one instance, SIRC noted a breakdown in communication that resulted in months of frustration, miscues and reduced information exchanges. SIRC found this situation unfortunate given efforts undertaken in past years to increase cooperation and coordination between the two organizations on national security or terrorism-related cases.

Recent SIRC reviews have made similar observations. In SIRC’s 2010–2011 review of CSIS’s relationship with a “Five Eyes” partner, the Committee found strong limitations on the exchange of information concerning foreign operations at station; as a result, it recommended that CSIS adopt a broader interpretation of its disclosure commitments in regards to the CSIS-DFAIT (now DFATD) Memorandum of Understanding (MOU). In light of these observations, SIRC will be taking a comprehensive examination of this relationship in the coming year.

CSIS Response

The Service has agreed to further update its communication protocols for technical solutions and will be looking at developing more accountability and stringent policy guidelines in regards to its validation process for intelligence collected abroad.

3

SECTION

COMPLAINTS INVESTIGATIONS

In addition to its review and certification functions, SIRC conducts investigations into complaints made against CSIS and denials of security clearances. Far less frequently, SIRC conducts investigations in relation to reports made in regards to the *Citizenship Act* and matters referred pursuant to the *Canadian Human Rights Act*.

The Complaint Process at SIRC

Complaint cases may begin as inquiries to SIRC either in writing, in person or by phone. SIRC staff will advise a prospective complainant about the requirements of the *CSIS Act* and SIRC's Rules of Procedure to initiate a formal complaint.

Once a formal complaint is received, 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 a Committee Member. They are assisted by staff and SIRC's legal team, which will provide legal advice to Members on procedural and substantive matters.

Pre-hearing conferences are 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 disclosure 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, the availability of the participants and the various procedural matters raised by the parties.

The *CSIS Act* provides that SIRC investigations are to be conducted "in private." All parties have the right to be represented by counsel, to present evidence, to make representations and to be heard in person at a 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 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.

On completion of an investigation, SIRC issues a final report containing its findings and recommendations, if any. A copy of the report is then provided to the Director of CSIS, the Minister of Public Safety and, in the case of a security clearance denial, to the deputy head concerned. A declassified version of the report is also provided to the complainant.

Table 2 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.

SIRC INVESTIGATION: Revocation of a Security Clearance

SIRC investigated a complaint under section 42 of the CSIS Act made by a government of Canada employee whose security clearance had been revoked after CSIS had contacted the relevant deputy head advising that it had new information on the complainant and recommended an update of his security clearance assessment. After that process was completed, the complainant was informed by his deputy head that adverse information concerning his loyalty to Canada had been received from CSIS and that his clearance was revoked.

In the course of its investigation, SIRC found that an unreliable source of information was used by CSIS to substantiate its assessment of the complainant. SIRC found that a more critical analytical assessment by CSIS would have prevented this from happening. SIRC also found that CSIS had internally discredited this source of information on some allegations against the complainant known to be false months before it actually chose to include and rely on such allegations in the assessment presented to the deputy head. Further, these allegations were portrayed to the deputy head as accurate but uncorroborated. SIRC found that this amounted to an intolerable misrepresentation in a report to a deputy head and that it seriously diluted the credibility of the Service’s security assessment.

TABLE 2: COMPLAINTS DIRECTED TO SIRC

	2011–2012	2012–2013	2013–2014
Carried over	16	22	24
New	17	17	9
TOTAL	33	39	33
Closed*	11	15	13

* Closed files include those where reports were issued, where the Committee did not have jurisdiction, where the preliminary conditions of the complaint were not met, or where the complaint was discontinued.

This investigation also found that SIRC had been seriously misled by CSIS on this same point. SIRC found that CSIS had violated its duty of candour during *ex parte* proceedings by not proactively disclosing in its evidence not only its rejection of the reliability of the source of information, but also the falseness of some allegations against the complainant. A witness had to be recalled by SIRC to speak to the matter and SIRC found CSIS's lack of candour most disturbing.

The investigation revealed further examples of inadequate assessment of the complainant's activity. It also revealed that the written reports derived from the complainant's security

screening interviews provided an inaccurate portrayal of the complainant's interview answers, which SIRC was able to ascertain by obtaining the original audio recordings.

In light of the preceding, SIRC found that weak intelligence, weak analysis and preconceptions contributed to the assessment of the complainant. Nevertheless, based on the remaining credible evidence, SIRC found that there were reasonable grounds to question the complainant's reliability as it relates to loyalty on the basis of the complainant's associations with persons or groups considered to be threats to the security of Canada, and in light of the complainant's dishonest features of character. For these reasons, SIRC found that the revocation

How SIRC determines jurisdiction of a complaint...

...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 of the *CSIS Act*,

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; or
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.

of the security clearance was warranted under the *Policy on Government Security* and recommended that the deputy head's decision to that effect be upheld.

SIRC made sure to address the issue of use of evidence and duty of candour. SIRC echoed the Federal Court's words in *Almrei (Re)* 2009 FC 1263, *Harkat (Re)* 2009 FC 1050, and those of Justice Mosley in *Further Reasons for Order* reported in *(X) Re* 2013 FC 1275. **SIRC also recommended that CSIS provide SIRC with a detailed update on the changes and initiatives undertaken since the events in question in this complaint to address the issue of rigour in assessments. SIRC further recommended that a policy directive be issued to all CSIS personnel about the importance of the duty of proactive candour in proceedings before SIRC.**

CSIS Response

The Security Screening Branch provided SIRC with a detailed description of various initiatives it has undertaken to promote greater rigour in security assessments and advice delivered to its domestic partners for government security clearances and immigration screening. Furthermore, the Director of CSIS sent a notice to all CSIS personnel reminding them about the importance of the duty of proactive candour in proceedings.

SIRC INVESTIGATION: Alleged Discrimination, Improper Conduct and Delay

SIRC investigated a complaint under section 41 of the *CSIS Act* in which the complainant alleged to have been discriminately targeted by CSIS to attend a security screening interview for the purposes of employment on the basis of religion and ethnicity, and that some of the questions asked during the process were inappropriate and discriminatory. Furthermore, the complainant claimed to have received conflicting information from CSIS regarding why the interview was being held and that the delay in processing the security clearance was unjustified.

SIRC found that the complainant was not discriminately targeted as there was a legitimate basis for CSIS to conduct an interview of the complainant. The adverse information available to CSIS needed to be clarified and it was entirely appropriate and reasonable for CSIS to seek clarification from the complainant.

SIRC also found that the overall line of questioning during the interview was not inappropriate or discriminatory. However, the CSIS investigator who conducted the interview did not have much experience in conducting security screening interviews and this appears to be reflected in the manner in which the interview was conducted, such as opening the interview with assumptions he made about the complainant that made the complainant uncomfortable. The investigator also refused to provide contact information that SIRC believes would have been reasonable to do in this context.

SIRC found the investigator did not follow CSIS policy with respect to the recording of security screening interviews by not ensuring that the recorder was functioning prior to the start of the interview. Furthermore, it would have been appropriate for the CSIS investigator to consult the other CSIS investigator who attended the interview in the preparation of the interview report. SIRC was also of the view that the second CSIS investigator should have taken notes as a backup to the lead interview investigator.

CSIS representatives who spoke with the complainant before, during, and after the security screening interview should not have provided the complainant with conflicting responses on why the interview was being conducted. **SIRC recommended that a generic reply be crafted so that a response may be provided in those circumstances where a subject of a security clearance enquires as to why he or she is being asked to engage in a security clearance interview.**

With regard to the delay in processing the security clearance, SIRC found the delay not to be unreasonable, particularly in light of the volume of requests that CSIS received during the time period.

CSIS Response

CSIS will disseminate operational guidance to regional investigators stipulating that, if queried by a subject of a security clearance as to why he or she is being asked to engage in an interview, they should provide the reason for the request if operationally practicable.

SIRC INVESTIGATION: Revocation of a Security Clearance

SIRC investigated a complaint under section 42 of the *CSIS Act* made by a Government of Canada employee whose Top Secret security clearance had been revoked, resulting in termination of employment.

Under subsection 39(1) of the *CSIS Act*, SIRC has the authority to determine the procedure to be followed in the performance of its duties and functions. Shortly after its creation, SIRC adopted Rules of Procedure in relation to its function under paragraph 38(1)(c) of the *CSIS Act*.

Although SIRC's Rules of Procedure have worked well since their adoption on March 9, 1985, SIRC underwent the process of reviewing them a few years ago with the purpose of providing further guidance in its processes, addressing the growing complexity of complaints and to reflect the quasi-judicial nature of its investigations. On May 1, 2014, SIRC's newly revised Rules of Procedure came into effect for complaints, reports and references made to SIRC under paragraph 38(1)(c) of the *CSIS Act* received on or after that date.

SIRC found that, based on a sound assessment provided to the deputy head through an independent evaluation, the complainant's features of character provided the deputy head with reasonable grounds to revoke the complainant's security clearance.

SIRC found that there was undisputed independent evidence that raised alarming conclusions as to the complainant's vulnerability to manipulation, providing the deputy head with reasonable grounds to believe that there was an issue with the complainant's reliability as it relates to loyalty under the Personnel Security Standard of the *Policy on Government Security*. As a result, SIRC found that the complainant may act or may be induced to act in a way that constitutes a "threat to the security of Canada"; or may disclose, may be induced to disclose, or may cause to be disclosed in an unauthorized way, classified information. For these reasons, SIRC recommended that the deputy head's decision to revoke the complainant's security clearance be upheld.

However, SIRC was critical of CSIS for failing to proactively highlight a highly relevant document in SIRC's investigation. SIRC had to remind CSIS that its duty of disclosure before SIRC goes beyond producing a large quantity of documents for SIRC's review. It also includes the duty to present the most relevant pieces of evidence proactively before any presiding Member.

In light of additional steps taken by the deputy head to address the likelihood that a situation similar to the complainant's reoccur in the future, SIRC found that no further recommendations were necessary.

SIRC INVESTIGATION: Alleged Wrongdoing and Violations of Rights

SIRC investigated a complaint under section 41 of the *CSIS Act* in which the complainant alleged that the Service undertook the following actions for the purpose of having the complainant collaborate with the Service: (1) that CSIS had exchanged information and/or made arrangements with a foreign entity, which led to the complainant's travel document being taken and retained, and to his arrest and detention in a foreign country; (2) that CSIS took part in an interrogation of the complainant by a foreign entity in the foreign country; (3) that CSIS contributed to pressure, intimidation and threats directed towards the complainant; (4) that CSIS intimidated and threatened the complainant in Canada, in the presence of an individual of the foreign entity; and (5) that CSIS participated in the violation of the complainant's constitutional rights and freedoms.

SIRC found that, with the exception of one allegation, the complaint was unfounded.

From the outset, SIRC noted that, except for one meeting between the complainant and two CSIS employees in the foreign country, the only evidence it received on the events alleged to have occurred in the foreign country between the complainant and the foreign entity was the complainant's evidence. SIRC did not receive any evidence from the foreign entity nor did it have the jurisdiction to investigate its actions.

SIRC heard evidence on information-sharing and cooperation agreements. The political and social context during which the alleged events took place was very different from today's environment. Information sharing was prevalent between foreign entities during the period in question. SIRC found that CSIS had acted within the authorities granted by the relevant legislative framework, Ministerial Directives, policies and agreements.

SIRC found no indication that CSIS made arrangements for the complainant's arrest and detention. In fact, the evidence demonstrated that CSIS was not aware that the complainant had left the country. SIRC did find, however, that once CSIS was made aware of the complainant's situation in the foreign country, it did not show any interest in ascertaining how the complainant's situation had evolved, nor did it take any steps to inform the Department of Foreign Affairs and International Trade. While CSIS's conduct in this sequence of events puzzled SIRC, in the absence of evidence of the motives behind the actions of the foreign entity, SIRC was unable to conclude that CSIS had arranged for, or that the sharing of information had led to, the complainant's travel document being taken and retained, his arrest or detention.

Although the evidence did show that two CSIS employees participated in a meeting with the complainant in the foreign country and that the meeting was attended by another person, SIRC found that the meeting was not inappropriate and that it was conducted within the authority of the legislation and Ministerial Directives and policies in place at the time. Notwithstanding, SIRC found that in the accomplishment of its mandate, CSIS must ensure that Canadians are

aware of the fact that they are free to meet with them or not. This requires an informed consent on the part of the individual, especially when the meeting is being held in a foreign country. It is CSIS's responsibility to ensure that the consent of the individual be informed and voluntary.

SIRC found that, with the exception of one instance, CSIS did not pressure, intimidate or threaten the complainant to obtain his collaboration. SIRC could only conclude on the actions of CSIS. SIRC found that during one meeting, CSIS did not obtain the complainant's informed consent when it met with the complainant in the presence of another person in Canada. In this regard, SIRC found that the presence of another person, which was not communicated to the complainant prior to the meeting, constituted undue pressure.

Overall, SIRC found that the evidence did not demonstrate that CSIS had participated in the violation of the complainant's rights.

In its report, **SIRC recommended that CSIS obtain the informed and voluntary consent from Canadians participating in a meeting with CSIS, in Canada or abroad.**

CSIS Response

The Service responded that when it seeks Canadians cooperation or assistance, it emphasizes the voluntary nature of discussions. Although CSIS employees usually identify themselves as such when conducting an interview with a Canadian citizen in Canada or abroad, there are occasions when pursuing this approach would not be operationally feasible.

SIRC AT A GLANCE

Committee Membership

SIRC's Interim Chair is the Honourable Deborah Grey, P.C., O.C. The other Committee Members are the Honourable L. Yves Fortier, P.C., C.C., O.Q., Q.C. and the Honourable Gene McLean, P.C.

Staffing and Organization

SIRC is supported by an Executive Director and an authorized staff complement of 17, located in Ottawa. This includes a Director of Research, Senior Counsel, a Corporate Services manager and other professional and administrative staff.

The Committee, in consultation with staff, approves 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 exchanges with the CSIS Executive and staff, and other members of the security intelligence and public safety community. These are supplemented by discussions with academics, security and intelligence experts, public safety professionals, and other relevant organizations.

Such activities enrich SIRC's knowledge about issues and debates affecting Canada's national security landscape.

Committee Members and, especially, SIRC 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 occasion for SIRC to communicate its 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 and review activities represent its chief expenditures.

Table 3 presents a breakdown of expenditures for the past two fiscal years, as well as planned expenditures for the coming fiscal year (rounded to nearest 100).

TABLE 3: EXPENDITURES

Program	2012–2013 Expenditures	2013–2014 Forecast Spending	2013–2014 Actual Spending	2014–2015 Planned Spending
Reviews	1,053,600	1,319,600	1,503,600	1,362,200
Complaints	513,800	688,600	513,800	682,900
Subtotal	1,567,400	2,008,100	1,567,400	2,045,100
Internal Services*	1,333,900	806,400	1,333,900	741,700
Total	2,901,300	2,814,500	2,901,300	2,786,800

* Internal Services are groups of related activities and resources that are administered to support the needs of programs and other corporate obligations of an organization (i.e., human resources management, financial management, information management, information technology). These services include only those activities and resources that apply across an organization and not those provided specifically to a program.

SIRC Activities

April 2013: SIRC staff met an expert from the International Cyber Security Protective Alliance for North America to discuss cyber security defence, namely its current state and future solutions for Canada and its close partners.

June 2013: SIRC staff met with the Queen’s University Canada Research Chair in Surveillance Studies on the current state of surveillance methodology among the Five-Eyes partners and the various tools for evaluating its effectiveness.

December 9, 2013: The Chair and Executive Director appeared before the Standing Senate Committee on National Security and Defence to discuss the findings and recommendations contained in SIRC’s annual report.

December 17, 2013: SIRC research staff attended the biannual Review Agencies Forum, which was attended by colleagues from the Office of the Communications Security Establishment Commissioner, the RCMP Public Complaints Commission and the Office of the Privacy Commissioner.

January 9–10, 2014: The Executive Director and senior staff met with a number of British counterparts and experts to discuss various security and intelligence matters.

February 6–7, 2014: The Executive Director presented on a panel discussion at the 15th Annual Privacy and Security Conference in Victoria, British Columbia. The conference brought together a large international audience of experts on policies, programs, laws and research and technology aimed at the protection of privacy and security.

LIST OF SIRC RECOMMENDATIONS

During the 2013–2014 fiscal year, SIRC made the following recommendations stemming from its reviews and complaints investigations.

Report	Recommendations
Review of Security Screening	<p>SIRC recommends that CSIS consult with the Office of the Privacy Commissioner before the end of 2013 on changes affecting the internal use of information collected for security screening purposes.</p>
CSIS's Surveillance Capabilities and Functions	<p>SIRC recommends that CSIS prioritize the request for legal advice pertaining to its liability under distracted driving legislation across Canada.</p> <p>SIRC recommends that CSIS devise a clear governance framework that addresses the foundations of a national and standardized surveillance program.</p>
A Counter-Intelligence Investigation	<p>SIRC recommends that CSIS commit to reassessing the resources devoted to an aspect of this investigation in due course to determine its continued sustainability.</p> <p>SIRC recommends that CSIS's next warrant application include summary information similar to that which was compiled for SIRC so as to provide the Federal Court with additional information regarding the application and use of the power in this investigation.</p>

A Sensitive CSIS Activity

SIRC recommends that the unit improve its information management methods and archiving practices.

SIRC recommends that CSIS carefully examine the role of the unit within the larger process of operational discussions and decision-making, with a view of making the unit's involvement more explicit and formal.

SIRC recommends that CSIS strive to ensure that reporting to the Minister of Public Safety be done in a formal and systematic manner.

SIRC recommends that appropriate mechanisms or processes be put into place to assist in systematically informing the CSIS Executive on developments related to the activities reviewed.

Operation Support and its Use Overseas

SIRC recommends that all necessary and relevant training be made mandatory prior to an employee's deployment abroad.

SIRC recommends that CSIS HQ ensures that all employees be properly informed about the Critical Incident Response Plan and any responsibilities they have under this Plan.

SIRC recommends that CSIS apply consistent measures to ensure that personnel stationed abroad are adequately supplied with the appropriate personal safety equipment.

SIRC recommends that CSIS develop better guidelines on the sourcing and purchasing of weapons within dangerous operating environments, create a clear responsibility centre for the firearms program and obtain updated legal advice related to the reasonableness and necessity of carrying firearms within dangerous operating environments.

SIRC recommends that CSIS provide the Minister with written justification explaining under what legal authority CSIS officials are permitted to carry firearms outside of the unique legal context of Afghanistan.

SIRC recommends that CSIS take immediate and appropriate steps to impress the importance of maintaining records of discussions and decisions to ensure proper accountability.

Report	Recommendations
<p>Review of a CSIS Foreign Station</p>	<p>SIRC recommends that CSIS update its security procedures to include additional guidelines and that it inform the appropriate authority of the solution it has implemented to resolve the technical problem.</p> <p>SIRC recommends that CSIS enhance its validation process for intelligence collected abroad by making increased use of the tools and techniques it already employs domestically.</p>
<p>Revocation of a Security Clearance</p>	<p>SIRC recommends that CSIS provide SIRC with a detailed update on the changes and initiatives undertaken since the events in question in this complaint to address the issue of rigour in assessments.</p> <p>SIRC recommends that a policy directive be issued to all CSIS personnel about the importance of the duty of proactive candour in proceedings before SIRC.</p>
<p>Alleged Discrimination, Improper Conduct and Delay</p>	<p>SIRC recommends that a generic reply be crafted so that a response may be provided in those circumstances where a subject of a security clearance enquires as to why he or she is being asked to engage in a security clearance interview.</p>
<p>Allegations of Wrongdoing and Violations of Rights</p>	<p>SIRC recommends that CSIS obtain the informed and voluntary consent from Canadians participating in a meeting with CSIS, in Canada or abroad.</p>