BRIDGING THE GAP

Recalibrating the Machinery of Security Intelligence and Intelligence Review

ANNUAL REPORT 2012–2013

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**

Catalogue No. PS105-2013E-PDF
ISSN 1912-1598

Security Intelligence Review Committee

Comité de surveillance des activités de renseignement de sécurité

September 30, 2013

The Honourable Steven Blaney
Minister of Public Safety
House of Commons
Ottawa, Ontario
K1A 0A6

Dear Minister:

We are pleased to present you with the annual report of the Security Intelligence Review Committee for the fiscal year 2012–2013, as required by Section 53 of the *Canadian Security Intelligence Service Act*, for your submission to Parliament.

Sincerely,

Chuck Strahl, P.C.
Chair

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

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

Deborah Grey, P.C., O.C.

L. Yves Fortier, P.C., C.C., O.Q., Q.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 Service. In doing so, SIRC provides assurance to Parliament and to all citizens of Canada that the Service investigates and reports on threats to national security in a manner that respects the rule of law and the rights of Canadians.

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

ABOUT CSIS

CSIS is responsible for investigating threats to Canada, analyzing information and producing intelligence.

To protect Canada and its citizens, CSIS advises the Government of Canada on issues and activities that are, or may pose, a threat to national security. These include terrorism, the proliferation of weapons of mass destruction, espionage and foreign-influenced activity.

It also provides security assessments of individuals to all federal departments and agencies, with the exception of the Royal Canadian Mounted Police.

A legal framework for both SIRC and CSIS

By virtue of the *CSIS Act*, Canada became one of the first democratic governments anywhere in the world to establish a legal framework for its security service. With this *Act*, Canada clearly defined in law the mandate and limits of state power to conduct security intelligence. By the same stroke, it created accountability mechanisms to keep those considerable state powers in check.

CONTENTS

MESSAGE FROM THE COMMITTEE MEMBERS

The Security Intelligence Review Committee (SIRC) exists to help ensure that security intelligence in Canada is conducted lawfully, effectively, appropriately, and with sufficient accountability. Over the past year, SIRC has engaged in, and encouraged, a process renewal and realignment in its pursuit of these key objectives. Throughout this process, the Committee has remained loyal to the duties and functions of SIRC, which has, since 1984, served as the fundamental check on the extraordinary powers granted by Parliament to the Canadian Security Intelligence Service (CSIS). Our work, summarized in this annual report to Parliament, and through it to the Canadian public, stands as our commitment to provide Canadians with as much detail as the law will allow.

SIRC's authority stems from the same legislation that created CSIS and gave that organization its role and powers: CSIS is mandated to investigate threats to national security as defined in the *CSIS Act*, while SIRC is mandated to help ensure that CSIS respects the fundamental rights and freedoms of Canadians while it does so. As an independent body reporting to Parliament, SIRC is committed to the highest level of transparency concerning our operations and the conclusions of our work, while ensuring that we maintain the strictest of standards as applied to information concerning national security. These commitments have represented SIRC's core values for almost 30 years.

Naturally, SIRC does nonetheless evolve, and this past year has seen us reach a number of significant milestones: our Committee has welcomed new Members and worked on its first products under its newest Chair, the Honourable Chuck Strahl; we have witnessed the expansion of our mandate to include the certification of the Director of the Canadian Security Intelligence Service's annual report to the Minister of Public Safety; we have hired our first new Executive Director in over a decade; and we have taken up the challenge of reintroducing and reintegrating SIRC into the broader community of Canadian intelligence and security.

As a result, we are pleased to present nine summaries of the comprehensive reviews carried out by our agency this past fiscal year, as well as summaries of the complaints cases that were concluded during that same time frame.

When producing such a document, it is important to take a moment to recognize the individuals who helped us get to where we are today, as well as those who will bring us forward into the future. First and foremost, the Committee would like to take this opportunity to extend its most profound gratitude to former SIRC Executive Director, Susan Pollak. To say that in her 14 years of leadership, Ms. Pollak's name and that of SIRC had become interchangeable is to understate what all of us in the security and intelligence community know instinctively. Ms. Pollak shepherded SIRC and its staff through five Chairs, four CSIS Directors, the tumultuous wave of change following 9/11, two turns as host of the International Intelligence Review Agencies Conference (IIRAC), and more than 100 SIRC reviews and complaints cases. We wish her a most pleasant and serene retirement, and thank her deeply for her years of dedicated service.

On another note, the Committee would like to take the opportunity to thank former Director Richard Fadden for his years of cooperation and his cordiality. Mr. Fadden has been generous with his time and frank in his approach to SIRC over the past four years, and the Committee will look back fondly on its relationship with him as Director of CSIS. We wish Mr. Fadden success in his new position, and we look forward to working with his successor.

With an eye towards what lies ahead, the Committee would like to welcome its new Executive Director, Michael Doucet. Mr. Doucet comes to SIRC via the Communications Security Establishment, Correctional Services Canada and the RCMP, where he served as the CIO for the country's national police force. The Committee has already been impressed with Mr. Doucet's enthusiasm and leadership, as has SIRC's staff, and we look forward to the coming years of innovation and advancement under his stewardship.

SIRC has also recently welcomed Deborah Grey, P.C., O.C., to the ranks of Committee Member. Ms. Grey brings with her an incredible wealth of experience in promoting and defending the public interest on a national scale. In addition, SIRC has just welcomed L. Yves Fortier, P.C., C.C., O.Q., Q.C., as its newest Committee Member. M. Fortier's extensive background as an international arbitrator, diplomat and director of numerous Canadian corporations brings an exceedingly valued and valuable range of expertise to the Committee. It is an understatement to remark that the Chair is pleased and excited at the prospect of drawing upon the knowledge and talent of Ms. Grey and M. Fortier over the coming years.

As predicted in the 2011–2012 annual report, the Committee spent some of its time and energy this past year taking up a new challenge, namely, guiding SIRC through an evolution of its responsibilities and mandate that saw it take on the task of certifying the CSIS Director's annual report to the Minister. SIRC was quite suited to the task of meeting this legislative requirement, and a symbiotic relationship has already begun to develop between SIRC's review function and the certification process whereby both are able to inform the other. Ultimately, it was SIRC's established expertise in the production of research reviews that facilitated this transition.

This consistency of approach between SIRC's long-standing review work and the certification process also addressed the issue of how to maintain the arm's length independence embodied in SIRC's original mandate, while simultaneously fulfilling SIRC's new legislative requirements. Since the methodology employed in SIRC's certification process is quite similar to the approach required to fulfill its other legislative responsibilities, there is no inherent conflict between SIRC's responsibility to report to Parliament and its provision of a Certificate to the Minister. Indeed, the issues identified in SIRC's certification of the 2011–2012 Director's report were addressed in recent SIRC studies and described in SIRC's 2011–2012 annual report to Parliament.

As we move forward, we also recognize the need to reinvigorate the promotion of SIRC and its staff to the wider environment of security and intelligence. Domestically, this will mean stronger ties with like review and oversight bodies, and increased consultation with the appropriate intelligence and security experts. Internationally, this will mean following up on the crucial links forged at events like IIRAC.

Finally, SIRC remains committed to promoting and enriching the critical national conversation on the aims and limits of security intelligence, and of CSIS's duties and functions in support of those endeavours. As will be reflected in this report, which we offer with pride, we are encouraging CSIS to realign and recalibrate a range of policies and approaches to effectively and efficiently support its crucial investigative activities, thus promoting the ongoing safety and security of the Canadian public, while maintaining the freedoms and rights Canadians justifiably expect and enjoy.

MEMBERS OF THE COMMITTEE

The Honourable
Chuck Strahl

The Honourable
Frances Lankin

TheHonourable
Denis Losier

The Honourable
Deborah Grey

The Honourable
L. Yves Fortier

MESSAGE FROM THE EXECUTIVE DIRECTOR

When the Honourable Chuck Strahl appointed me as SIRC's Executive Director in December 2012, I was struck by how little was publicly known about this Committee of Privy Councillors. Having been in my new role for the better part of a year, it now seems appropriate for me to clarify what SIRC does, how it does it, and what parliamentarians and Canadians can expect of us in the future.

The Committee is composed of exceptional Canadians who leverage their previous experiences in public and private life to assess information presented to them about the activities of CSIS. Members, who are generally appointed to the Committee for five-year terms, work part-time throughout this period. As Privy Councillors, SIRC Members receive all of their information and advice about CSIS's activities from a dedicated team of full-time national security experts or through complaint hearings.

The Committee Chair delegates to the Executive Director the responsibility for the day-to-day running of SIRC. This means I am responsible for having the right people, processes and procedures in place to ensure that the Committee is adequately informed. I am additionally entrusted with ensuring the sound fiscal management of government funds provided to SIRC.

Allow me to underscore the key principles I believe are central to the work my staff and I perform on behalf of the Committee and, through them, for parliamentarians and, hence, all Canadians.

The most important principle is our independence. The architects of the *CSIS Act* understood that SIRC had to exist as a body external to the executive branch of government to ensure that our findings and recommendations were never influenced for either bureaucratic or political reasons. The *CSIS Act* gives voice to this requirement in two complementary ways: first, SIRC employees are not members of the core public administration—the Committee functions as a separate employer. Instead, SIRC employees retain their positions at the pleasure of the Committee, meaning that their duty is to SIRC—not, for the most part, to the wider government establishment. Second, Committee Members are appointed as Privy Councillors by the Prime Minister of Canada, after consultation with the other political parties, and cannot be serving Members of Parliament. This means that although Committee Members have diverse political and regional backgrounds, they sit on SIRC in positions of trust where partisan predispositions are unwelcome.

I am well aware that one of the risks to our independence is becoming unduly influenced by the culture of secrecy, or what spy novelist John le Carré described as becoming entrapped by the "magic circle." SIRC must therefore—and on an ongoing basis—balance the need for transparency concerning CSIS activities with the attendant requirement to protect national security information. Let me be clear: we will never jeopardize the security of Canadians by releasing information that could serve

only to buttress the Committee's image as a relevant and topical entity. Although I am confident that we always have our fingers "on the pulse" of CSIS, being responsible with the information we are entrusted with necessitates discretion.

That said, to help maintain our independence from CSIS, SIRC's main office is located in downtown Ottawa. This location also acts as "neutral" territory for the quasi-judicial process of investigating complaints, requiring that CSIS representatives come to SIRC to present their case. SIRC also has working space at CSIS headquarters; this is where SIRC staff access CSIS's corporate and operational information (hard copy and electronic formats), ranging from health services data to raw intelligence on the most classified operations. Meetings are held with CSIS employees and management, as required, including travel to CSIS regional offices and overseas stations. In short, we can gain access to whatever we need, wherever it is located. Next year, for the first time, I will be travelling to a classified foreign station; I do so as much for the information I will obtain while there as for the message it sends about SIRC's unencumbered reach.

Given this comprehensive access to national security information, I acknowledge that the confidence placed in our work is rooted in the competency of the people charged with performing the legal and research activities on behalf of the Committee.

This leads me to my second principle: maintaining a highly competent and professional workforce. As one would expect, my staff is well educated (as an example, analysts have a minimum of two post-secondary degrees). My team is composed of individuals from different academic and professional backgrounds, with many approaching, or eclipsing, 10 years of experience in handling the most sensitive national security issues. I have spent my career in the areas of intelligence and law enforcement, having had the pleasure of working with a wide cross-section of domestic and international professionals from these fields over the past 25 years. Therefore, I can say with confidence that I am impressed by the expert assessments produced by SIRC staff. Copies of our classified reports are sent to CSIS and the Minister of Public Safety and, historically, roughly 70 percent of our recommendations are accepted by CSIS, even though they are non-binding.

As a complement to the capacity of my staff, **our third principle calls for SIRC to act as a productive and informed member of the national security community**. Although I am satisfied by the work done by my small and nimble group of experts, I am equally committed to continuously enhancing their professional capacities. As part of this, I have embarked upon a program of modernization by which additional technological and analytical systems will provide employees with updated resources to manage their legal and research processes.

In addition, I am aware that part of further evolving the expertise of my employees is through SIRC's outreach initiatives. Employees are being encouraged, whenever possible and appropriate, to liaise with academic, legal, intelligence, auditing and policing professionals. The purpose of these liaison efforts is to help ensure that SIRC staff stay well informed of issues related to their professional discipline. These exchanges also allow staff to take advantage of a large and growing body of work and experts in Canada with whom we have the privilege of consulting. This strategy serves to counteract the risk of groupthink by ensuring that employees can place CSIS's activities within the broader context in which they operate.

As I concentrate on moving forward, I am reminded that SIRC's unimpeded access to CSIS information is our *raison d'être*, and that this access has been further leveraged by incorporating certain duties previously performed by the former Office of the Inspector General of CSIS. Indeed, SIRC is now required to certify the accuracy of the CSIS Director's annual report to the Minister of Public Safety.

To ensure that my team can hone their professional understanding of CSIS to the greatest extent possible, our short- and medium-term goals involve further integrating our three core information pillars: complaints, reviews and certification.

Speaking more broadly, SIRC continues to play an important role alongside Canada's intelligence community by contributing to both the classified and non-classified dialogue on national security. I envision expanding our contribution in both of those realms over my tenure as SIRC's Executive Director. This will take time and will be dependent on whether SIRC's statutory reach is expanded to pursue national security information linked to CSIS within other federal departments and agencies. Even absent of legislative change, however, I remain confident that our efforts to evolve our work will be received by CSIS, and by Parliament, as a constructive undertaking.

In subsequent annual reports and departmental performance reports, I will continue to provide further context concerning the progress being made on advancing our capabilities in support of the Committee's mandate.

Let me state unequivocally that our independence and professionalism will never be points of compromise. We are committed to performing our duty on behalf of the Committee so that Parliament and Canadians remain confident that Canada's human intelligence spy agency is fully accountable in the performance of its duties and functions.

Sincerely,

Michael Doucet

ABOUT THIS REPORT

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

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

SECTION 1

The Year in Review

An analysis of key developments in security intelligence and how these relate to select findings and recommendations by SIRC from the previous year.

SECTION 2

Summaries of SIRC Reviews and Complaints

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

SECTION 3

SIRC at a Glance

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

EASY ACCESS TO BACKGROUND INFORMATION WHERE AND WHEN YOU WANT IT

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

SECTION 1

THE YEAR IN REVIEW

In its 2009–2010 annual report, SIRC observed that, "periods of intense change often result in substantial policy gaps." At that time, SIRC challenged CSIS, and Parliament, to formulate a series of questions concerning the goals and limitations of an expanded, international realm of CSIS operations and intelligence collection. In the following few years, both the Service and Parliament helped shape a framework in which those goals and limits were conveyed with greater precision—through revised intelligence priorities, more substantive guidelines on information sharing, and mechanisms to promote more effective domestic partnerships.

Having made significant strides to articulate a sharpened expression of CSIS's current intelligence goals and priorities, the time has now come to backfill the regulations and best practices that will ensure those goals are met by employing a regime of appropriate, accountable and efficient measures. After establishing a far more directed and pronounced presence overseas, drawing upon much more vigorous and productive domestic partnerships, and reshuffling domestic priorities to foster more potent lines of collection, CSIS must now reach back into many of its programs in order to identify and align its objectives with updated policies, regulations and operational procedures.

Complementing such developments must be a commensurate shift in SIRC's capacity to fully assess the work of the Service; since our 2010–2011 Annual Review, SIRC has put forward an argument that its current limitations in the area of review—that is, limited to CSIS's information holdings and personnel—is falling increasingly out of step with the *modus operandi* of contemporary intelligence. Greater cooperation with domestic partners and more comprehensive regimes of information sharing mean that CSIS's investigations now feed into and receive feedback from an increasingly large network. This theme spans the majority of reviews this year, and was evident in regard to the RCMP, DFAIT,

DND, CBSA and, in particular, CSEC. Moreover, all government departments and agencies—to say nothing of Canada's close allies—are becoming more technologically integrated. Governments across the Western world have responded and adapted, further integrating formerly separate intelligence capacities. As the technological barriers between information systems and previously stove-piped databases continue to fall, the sharing of data has become not merely possible, but routine. In the material explored in this annual report, we examine how there are both advantages and risks in this development, and we will highlight the growing challenges for their complete and effective review.

As CSIS moves to take advantage of this new capacity, SIRC must also be able to respond. It must be flexible enough to follow up and effectively review CSIS activities and investigations, even when they cross over with other agencies and departments. Given the inevitability of technological interconnectivity, SIRC must be ready with the legislative tools and matching government resource commitments to ensure that the checks and balances enshrined in the Committee remain relevant and effective.

SIRC REVIEWS

One of SIRC's largest reviews this past year delved into our ongoing interest in the increased collaboration between CSIS and Communications Security Establishment Canada (CSEC). Clearly anticipated as one of the most important intelligence partnerships of the next decade, SIRC's review highlighted both the significant potential efficiencies of closer cooperation—from shared services to filling in intelligence gaps—as well as the areas where results were not yet meeting expectations. When the focus turned to the realm of intelligence sharing, SIRC found limitations in the application of established Human Intelligence (HUMINT) procedures when applied to the Signals Intelligence (SIGINT) process; one significant risk of increased HUMINT/SIGINT collaboration is the potential erosion of control over the information shared.

Given the inevitable—and desirable—growth of cooperation between the two agencies, SIRC identified what we found to be a need to backstop many of the individual programs with a more comprehensive string of policies and procedures to address the growing volume of challenges, as well as the need to ensure that each organization continues to respect its individual and unique mandates.

In another review on a new Section 21 warrant power, SIRC similarly found that, given the current need to leverage international partnerships in order to keep track of CSIS targets when they travel outside Canada, the Service set out to maximize existing mechanisms and partnerships so as to increase its collection capacity. However, the resulting increased volume of shared information also introduced a reduced level of control over the flow—and, potentially, the use—of CSIS-originated information once it was passed off. Although this risk has already been identified by the Service in regards to one of its allies, SIRC recommended that the use of "caveats"—articulated limits and conditions on the use of CSIS information—be extended to a wider range of international partners.

SHORING UP LIMITS AND THRESHOLDS

As both SIRC and CSIS have been stating for several years, while counter-terrorism remains one of the highest intelligence priorities, counter-espionage has returned to the forefront of intelligence work. Echoing levels last seen during the Cold War, CSIS's long-standing role to advise government of threats emanating from state-sponsored offensive intelligence efforts has evolved from more straightforward "classic" counter-intelligence strategies and activities (e.g. political and military), to gathering information on commercial and financial data, following webs of influence and, perhaps most formidably, parcelling out terabytes of information to identify the occurrence and origin of foreign-sponsored attacks in the cyber realm. SIRC found that one of the foremost challenges of collecting and analyzing espionage-based information is, as it has often been, sorting out the "legitimate"

efforts of another state acting within Canada from the "clandestine" range of activities.

Given the seemingly endless range of platforms and techniques within which espionage can now take place, the challenge CSIS faces in remaining within the boundaries of the "strictly necessary" limitations of the powers accorded to them in the *CSIS Act* is significant. As a result, SIRC recommended that CSIS fine-tune its existing policy and practice in this area to assist investigators in identifying common and consistent thresholds, and create firmer indicators and tools to help define when an activity has crossed over into the clandestine realm.

Another SIRC review examined some of the initiatives now underway to support CSIS's foreign collection programs. Having now firmly established the need and mandate for such collection, CSIS has moved into a phase of evaluating and improving the tools and policies that underscore and establish its capacity to do so. SIRC was satisfied with what it perceived was a consistent and constant message throughout the branches of the Service that maintained that foreign collection is always firmly anchored to a Canadian nexus, and that such collection is never allowed to take priority over domestic investigations. However, given the increased challenges—operational and legal—of operating outside Canada's borders, SIRC did find that CSIS had gaps to fill, both in regards to the availability of training (particularly for individuals deployed to dangerous environments), and in regards to the legal limitations of intelligence options. As CSIS's overseas operations bring the Service into new scenarios, the opportunities they represent—and the potential risks they carry—are going to require CSIS to develop a more comprehensive legal framework that will clearly delineate what kinds of activities will be acceptable, and which will be prohibited.

In an additional review—SIRC's annual foreign post review—we took the view that CSIS's operations abroad are not expanding as much as they are evolving. The ongoing restrained fiscal environment has meant that CSIS cannot pursue with equal vigour every potential operational lead to which it is privy overseas (and there are many), but must decide which leads to explore, and to what extent. Again, having received government direction and having established guidelines on information sharing with both trusted allies and agencies suspected of human rights violations, CSIS must now fill in the procedural gaps that present themselves when such arrangements begin to produce intelligence. In some instances, such expectations have been met, while in other instances, SIRC found that some specific tools CSIS utilizes to inform its own decision-making were somewhat deficient.

INSTITUTIONALIZING RESPONSIBILITY

As a final kind of "gap" that emerged as SIRC examined the reshuffling of priorities and investigations, the need to establish a firm and consistent chain of responsibility was noted in several reviews. One such review, which centered on CSIS's support to Canada's Northern Perimeter Security, noted how the issue shifted over the past few years, given the need to strike a balance between the government's emphasis on the Arctic as a prescient security concern, and the historic dearth of intelligence collection in that region. Ultimately, SIRC found that despite some gained efficiencies, CSIS's northern strategy was still too dependent on a mix of serendipity and the personal engagement of a string of internal Service champions. Over the long term, CSIS, which under centralized rather than regionalized leadership, will have to develop a concentrated strategy that hammers out a concrete, multi-year strategy, backed up by the appropriate resources.

On the other side of the coin, SIRC examined CSIS activities related to domestic investigations and emerging issues. Over the past few years, long-standing domestic concerns such as environmental extremism, white supremacy, and secessionist extremism, have, to varying degrees, faded from view. As a result, CSIS reassessed and retooled those investigations to draw down on areas that were showing few signs of active threat, while at the same time re-imagining the categorization of extremist ideologies (left, right, etc.) so as to

be less concerned with the philosophical orientation but as concerned with the potential for violence. The result was the efficient termination of reporting and investigation of some long-standing but increasingly inactive targets. The remaining risk involves the possibility of a sudden flare-up of domestic violence, prompting an immediate request on the part of government for information. To help mitigate that risk, SIRC noted and encouraged CSIS's strategy of maintaining active liaison with its domestic partners—especially in law enforcement—who maintain an awareness of the same groups due to their spill over into criminal behaviour.

The last example reviewing the institutionalization of responsibility emerges from SIRC's first production of the certification of the CSIS Director's annual report to the Minister of Public Safety. Overall, SIRC emerged from this intense exercise largely satisfied with the quality and completeness that characterized the Director's report. However, when it came to describing CSIS's overseas operations, SIRC found that the quantity and detail of what was included in the report was not as comprehensive as it could have been. Given that the object of that section would be to provide the Minister with a strong understanding of the increasingly elevated threats to the lives of Service employees and its operations overseas, SIRC noted that more detailed information would provide a more accurate and representative description of CSIS activities. SIRC noted that the Director of CSIS may wish to include more information in this area next year, and that the issue is of sufficient concern to warrant the Minister's attention and continued consideration.

WRAPPING UP COMPLAINTS

This year also saw the completion of five complaints cases; as with SIRC's reviews, the recommendations stemming from these cases concerned the filling of gaps and an increased measure of standardization across CSIS practices. For example, in the case of one complaint surrounding the immigration interview process, SIRC recommended that CSIS adopt the practice of one region—to consistently prepare and test the recording devices prior to such interviews—and apply it to all regions of the Service. In a separate case, SIRC noted that some government employees require, from time to time, a review of the instances and conditions under which they can and cannot divulge the identity of their employer.

COMING FULL CIRCLE: THE CASE OF ABOUSFIAN ABDELRAZIK

The past year also witnessed the completion of SIRC's review of CSIS's role in the matter of Abousfian Abdelrazik. In that review, SIRC concluded there was no indication that CSIS requested Sudanese authorities to arrest or detain Abdelrazik, but found that CSIS kept its allies informed of fresh intelligence concerning his case once he departed Canada. Moreover, SIRC found that the two Canadian government organizations most heavily involved in this case carried out their respective consular and intelligence work concurrently—sometimes at odds—with each other. SIRC also raised concerns surrounding: the inappropriate disclosure of classified information; the creation of an intelligence assessment that exaggerated and inaccurately conveyed information to Government of Canada's partners; and the excessive reporting in operational databases of information not related to the threat, originating from individuals who were not targets.

However, given that it has been a decade since the events described in much of SIRC's report took place, the remedies and recommendations that would adequately address SIRC's concerns have already been covered in previous SIRC reports, as well as other venues such as Commissions of Inquiry. Although SIRC encouraged CSIS to use this review as an opportunity to revisit the applicable range of SIRC recommendations provided over the last decade, we did not provide any novel (and likely duplicative) recommendations.

THEN AND NOW

In regards to the broader themes identified in the rest of SIRC's reviews discussed above, it is interesting to note a contrast. The review of the case of Abousfian Abdelrazik centred on CSIS's activities in the first half the 2000s, a period in which most of the guidelines and decisions concerning overseas operations were yet to be made. As SIRC emphasized in that review, it should be unsurprising that SIRC did not make any new recommendations in that case, given that a combination of CSIS policy shifts and previous SIRC recommendations had already addressed the concerns raised by the review. In the early and mid-2000s, CSIS, the government and the Canadian public were still wrestling with questions concerning whether CSIS's activities should expand overseas, the extent to which that expansion should occur and what it meant for both the Service and the Canadian intelligence community as a whole.

In 2013, that debate has moved to the next stage. The discussion now turns to how best that job should be done, what gaps remain in CSIS policy and procedure to operate in the current security intelligence environment, and what measures remain in place and are enforced to ensure the continued exercise of the Service's powers within the limitations of its mandate.

SECTION 2

SUMMARIES OF SIRC REVIEWS AND COMPLAINTS

A. REVIEWS

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

WHAT IS THE DIFFERENCE BETWEEN AN OVERSIGHT AND 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.

HOW REVIEWS ARE CONDUCTED

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

In deciding which matters to review, SIRC considers:

- events or developments with the potential to represent threats to the security of Canada;
- intelligence priorities identified by the Government of Canada;
- activities by CSIS that could have an impact on individual rights and freedoms;

- issues identified in the course of SIRC's complaints functions;
- new directions and initiatives announced by or affecting CSIS; and
- the CSIS Director's classified annual report, which is submitted to the Minister of Public Safety.

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

SIRC's researchers consult multiple information sources to examine specific aspects of the Service's work. As part of this process, researchers may arrange briefings with CSIS employees, as well as examine individual and group targeting files, human source files, intelligence assessments and warrant documents.

SIRC can also examine files relating to CSIS's cooperation and operational exchanges with foreign and domestic agencies and partners, among other sources, that may be review-specific. The goal is to look at a diverse pool of information so that we can ensure we have thoroughly reviewed and completely understood the issues at hand.

FIND OUT MORE ABOUT SIRC'S EARLIER REVIEWS

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

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

ACCOUNTABILITY MATTERS

SIRC is one of several mechanisms designed to ensure CSIS's accountability. The Service also remains accountable for its operations through other mechanisms such as the Minister of Public Safety, the courts, the central agencies of government (i.e. Privy Council Office, Treasury Board Secretariat), the Auditor General of Canada, the Information Commissioner of Canada and the Privacy Commissioner of Canada.

TRACKING SIRC'S RECOMMENDATIONS

Each year, SIRC requests a status report from CSIS on the recommendations arising from the previous year's reviews and complaint decisions. This update gives SIRC the opportunity to track the implementation of its recommendations and to learn about the practical impact of those recommendations on CSIS.

This process also allows CSIS to respond formally to SIRC's reviews and decisions, and forms part of the ongoing dialogue between the two organizations. During the 2011–2012 review period, SIRC made nine recommendations addressing a wide range of issues.

SIRC is pleased to note that CSIS has responded to several of these recommendations. For example, CSIS agreed with SIRC's 2011–2012 recommendation to revise the Service's policy on caveats so as to reflect current information-sharing practices and processes with foreign partners.

SIRC REVIEW

CSIS'S RELATIONSHIP AND EXCHANGES WITH COMMUNICATIONS SECURITY ESTABLISHMENT CANADA (CSEC)

Background

The government's decision to locate CSEC headquarters alongside CSIS headquarters is illustrative of a global trend in which the once-solitary worlds of Human Intelligence (HUMINT) and Signals Intelligence (SIGINT) have increasingly merged. This trend has been driven by expanded demands from the government for timely and relevant information, to maximize operational efficiency in an age of fiscal restraint, and to address an evolving and increasingly technologically complex global threat environment.

This review explored the benefits to CSIS from increased cooperation with CSEC, both through an examination of operational and non-operational initiatives. The review examined combined efforts at coordinating corporate services, ensuring sufficient inter-organizational knowledge transfer, how operational risks are managed, the collection of non-threat-related information (cf. *CSIS Act*, Section 16), and the adequacy of direction and policies used to help guide CSIS's information sharing with CSEC.

SIRC's Review

The review found that a number of challenges prevent CSIS and CSEC from fully capitalizing on the opportunities presented by the new proximity of their respective headquarters. For intelligence agencies faced with increasingly limited resources, shared services allow for efficient and effective resource management. Unfortunately, SIRC found that the initial expectations for shared services between CSEC and CSIS may have been too optimistic.

Although the new CSEC facility has not yet been completed—leaving open the possibility for greater-than-expected returns—to a significant extent, the potential efficiencies have thus far been offset by managerial issues, budgetary restrictions and complications related to CSEC site development.

More generally, SIRC found that CSIS and CSEC had gaps in understanding the other organization's respective mandate and/or responsibilities. This impediment to cooperation was raised at both the working and managerial levels across CSIS's operational branches, and acknowledged at joint CSIS/CSEC meetings. Moreover, these gaps in understanding resulted in instances where CSIS policies or procedures were not followed, an outcome that could have negatively impacted operational risk.

For its part, CSIS acknowledged the challenges associated with overlapping mandates and, quite often, the unique demands of the overlapping activities involved in the deployment or use of sensitive CSEC technology or CSIS human sources. Solutions presented to SIRC to address these problems include further educating CSEC and CSIS operational desks on relevant policies, as well as the creation of a joint CSIS and CSEC senior management operational board to provide strategic-level management on these activities.

FOREIGN INTELLIGENCE COLLECTION

Section 16 of the ***CSIS Act*** defines foreign intelligence as any information about the capabilities, intentions or activities of a foreign state, foreign national or foreign organization (i.e. non-threat-related information). By contrast, Section 12 of the ***CSIS Act*** defines security intelligence as information and intelligence related to "threats to the security of Canada." Despite considerable cooperation with CSEC on foreign intelligence collection activities within Canada, there remained some internal debate within the Service about the extent to which these activities negatively impact CSIS's primary mandate to collect security intelligence. As a result of the varying accounts provided by CSIS on this issue, SIRC cautioned the Service to be prudent when deciding the extent to which it continues to seek CSEC's assistance in the Section 16 process. Unless changes to the ***CSIS Act*** are made, CSEC, not CSIS, remains the organization primarily mandated with providing the Government of Canada with foreign intelligence information.

Information Sharing

The above notwithstanding, a large proportion of the review was focused on how CSIS and CSEC share information. Normally, whenever CSIS shares information, it uses caveats and/or assurances. Caveats stipulate that the information being provided is CSIS property and cannot be forwarded to another agency or altered without CSIS's direct consent. Assurances are formal, bilateral agreements made with foreign agencies stipulating that CSIS's information will not be used in a manner that runs contrary to international human rights conventions. The extent to which caveats and assurances are effective depends on the degree of trust between CSIS and the agency receiving the information. SIRC found, however, that a significant risk of increased HUMINT to SIGINT collaboration is the potential erosion of control over the information shared.

The Committee reached this conclusion because CSIS's caveats and assurances were never designed for SIGINT collection. Unlike HUMINT agency collection, which is often done in isolation (i.e. collecting information from a human source and, if desired, subsequently sharing that information with an allied agency), SIGINT collection is instead more of a collective undertaking. CSEC belongs to a special alliance that includes the United States National Security Agency, the United Kingdom's Government Communications Headquarters, the Australian Defence Signals Directorate, and the New Zealand Government Communications Security Bureau. The CSEC Commissioner's Office, in its 2011–2012 annual report, described these partnerships as being potentially "more valuable now than at any other time, in the context of increasingly complex technological challenges."

For its part, CSIS believes that exchanges with CSEC are low-risk endeavours. This is premised on the fact that allied SIGINT agencies, irrespective of the broad sharing that transpires among them, are primarily focused on their own national intelligence priorities. However, of concern to SIRC are those instances when allied collection priorities have coalesced with Canada's—such as in counter-terrorism cases.

Although ministerial direction to CSIS and associated Service policies are designed to prevent the misuse/abuse of information, both from a security and human rights perspective, it is not clear how CSIS can comply with ministerial direction stipulating that caveats must be used when sharing information with domestic and foreign recipients, when SIGINT collection and dissemination functions run contrary to this expectation.

CSIS has acknowledged to SIRC that addressing these concerns is a complex subject that remains a work in progress; considering that the collaboration between CSIS and CSEC is increasing, SIRC will revisit this issue in subsequent reviews in order to assess what progress has been made in addressing this challenge.

A Final Issue: Cyber Security

The final section of the review identified an anomaly of the CSIS/CSEC relationship, namely, a noted lack of cooperation on cyber security. In 2010, Public Safety Canada created a whole-of-government strategy, the Cyber Security Strategy, which asserts that there can be no ambiguity in terms of who does what. The Strategy confirms the respective roles of CSEC and CSIS: the former has the recognized expertise in dealing with cyber threats and attacks, while the latter is broadly tasked to analyze and investigate domestic and international threats. The Strategy notwithstanding, SIRC's review found that there is still work to be done to coordinate CSIS's cyber-related activities with CSEC, especially with respect to the protection of information and infrastructures of importance to the Government of Canada.

Given the inevitability of growth in CSIS/CSEC collaboration, **SIRC recommends that CSIS develop clearer and more robust overarching principles of cooperation with CSEC. These principles should address the growing volume of challenges that have arisen between the two bodies, while respecting the individual mandates of each organization.**

SIRC REVIEW

REVIEW OF A NEW SECTION 21 WARRANT POWER

Background

This review was SIRC's first examination of a new warrant power under Section 21 of the *CSIS Act*, which was initially authorized by the Federal Court in 2009. This new power was introduced in order for the Service to maintain coverage of targets who represented a threat to Canada as they travelled or, in some cases, resided, overseas. The review examined the processes, policies and controls that CSIS has put in place to manage the new power, as well as CSIS's cooperation and exchanges with domestic partners. The review also sought to evaluate how important the information obtained from this power has been to the Service's investigations thus far.

SIRC's Review

During the review period, 35 warrants (plus seven supplemental warrants) that included the new power were issued. The Committee found that CSIS encountered several challenges, including the efficacy of collection; control of the information collected; and possibly unrealistic future expectations. Indeed, it was noted that by relying on partner agencies—both domestic and foreign—for collection, some efficiency will ultimately be sacrificed. There has been substantial progress since the first warrant was issued; however, CSIS is still in a learning phase and it will need to manage expectations against the realities, meaning limitations, of reporting from this collection.

In order to maximize collection under the new warrant power, CSIS, in almost every case, leverages the assets of the Five Eyes community (Canada, plus the United States, the United Kingdom, Australia and New Zealand). SIRC noted that even with the assistance of allies, the collection or intelligence yield under this power has provided different gains and challenges than the Service initially expected.

The arrangements with partners and allies also present possibilities for other agencies to act independently on CSIS-generated information. In practice, if an allied agency were to pick up intelligence on a Canadian citizen, a Canadian agency would ideally take the lead based on an informal agreement governing interactions amongst the Five Eyes partners. Nonetheless, it is understood that each allied nation reserves the right to act in its own national interest. National security legislation in both the United States and the United Kingdom, for example, gives these countries the authority to retain and act on intelligence if it relates to their national security, even if it has been collected on behalf of another country, such as Canada.

WARRANTS

	2010–11	2011–12	2012–13
New warrants	55	50	71
Replaced or supplemental	176	156	165
Total	**231**	**206**	**236**

The risk to CSIS, then, is the ability of a Five Eyes partner to act independently on CSIS-originated information. This, in turn, carries the possible risk of detention or harm of a target based on information that originated with CSIS. SIRC found that while there are clear advantages to leveraging second-party assets in the execution of this new warrant power—and, indeed, this is essential for the process to be effective—there are also clear hazards, including the lack of control over the intelligence once it has been shared.

Conclusions

SIRC has seen indications that the Service has started using caveats that require allied agencies to contact CSIS in the event that information based on Service information is to be acted upon. The caveats, as they currently stand, are still considered a "work in progress" by the Service, but they do not yet address the wider reality of this type of collection. Nonetheless, they are a useful tool and do provide some measure of CSIS coverage. This coverage, however, comes with several challenges, including control of the information CSIS seeks to collect. SIRC advised CSIS to devise appropriate protections for the sharing of Service information, and to keep itself as informed as possible concerning the potential uses of CSIS information.

Moreover, for the most part, these caveats, as part of the wider "assurances" regime, were only considered with regard to one partner. **Therefore, SIRC recommends that CSIS extend the use of caveats and assurances in regards to this new warrant power to include the agencies of the entire Five Eyes community, in order to ensure that no dissemination occurs without the Service's knowledge.**

SIRC REVIEW

INVESTIGATING ACTIVITIES RELATED TO ESPIONAGE AND FOREIGN INFLUENCE

Background

Countering terrorist threats continues to be the number one priority for CSIS; however, Canada has been experiencing levels of espionage comparable to the height of the Cold War and nations involved in such state-sponsored activities are changing their tactics. In response, CSIS's primary role is to advise Government of Canada departments to better understand the emerging threats linked to newer forms of espionage and counter-intelligence, thereby maintaining an awareness of the foreign policy, trade and intelligence interests of specific nations.

SIRC's Review

This study reviewed how CSIS is dealing with the rapidly changing threat posed by espionage and foreign-influenced activities. From CSIS's perspective, the new challenges and complexities of investigating such activities are also seen as opportunities to look beyond traditional forms of espionage and delve into new operational domains. SIRC focused on CSIS's provision of advice when dealing with different forms of foreign-influenced activities.

Within Canada there exists a long history of diplomats, intelligence officers and foreign national business leaders conducting covert activities in order to advance the interests of their respective countries. Such foreign-influenced activities become more serious when high-ranking Canadian officials or prominent members of the business community are strategically targeted. Although some of the strategic relationships pursued by foreign national representatives are mere extensions of diplomacy, the activities are considered to be threat-related and of interest to CSIS when they covertly try to obtain information or to influence decision-making.

One of the challenges for CSIS is continuing to make the distinction between what is considered clandestine and what is legitimate diplomacy. In the past, detecting covert forms of foreign influence may have been more straightforward, since much of the activity was done through traditional approaches, and foreign agents of influence were usually the focus of CSIS investigations. However, methods used by foreign actors are continuously evolving.

In the cases of foreign-influenced activities examined for this study, the negative elements are clear: democratic principles are being challenged and direction is coming from a foreign government; however, the clandestine elements are not so apparent. From the Committee's perspective, a number of the activities being investigated appear to be more overt than clandestine. SIRC noted that although activities by foreign states may be organized and focused, such approaches are not, in and of themselves, indicators of secret activity.

As investigations into espionage and foreign-influenced activities continues to grow in size and complexity, so too will the challenge of distinguishing between what is clandestine and what is legitimate. SIRC believes that clarifying this distinction is important, since collecting information on threat-related issues must, according to the *CSIS Act*, be "strictly necessary." **SIRC recommends that CSIS carry out the appropriate fine-tuning, in policy and practice, to assist investigators and analysts in identifying common and consistent thresholds, and in judging when an activity has crossed over into the clandestine realm.**

Adjusting the Approach

In recent years, agents of foreign interference have been targeting individuals and groups within smaller subsections of Canadian society in order to leverage those relationships into greater domestic influence. To take one example, some foreign elements have attempted to reach out to some subsections in an attempt to potentially bypass other jurisdictions, such as federal, provincial or municipal governments. CSIS will often alert affected parties (e.g. politicians, corporate executives, academics and other influential individuals) by providing security briefings and advice; however, such measures are not afforded to all affected communities.

CSIS is using this "wait and see" approach for several reasons: in addition to not having enough specific information on the potential targets or the intended offensive strategy, the Service is also concerned about how its message—any message—may be received by some communities, and whether those messages will be viewed as a positive. SIRC recognizes the Service's concerns; nonetheless, not informing all Canadian communities about the security issues around a particular threat, while informing other sectors of society, is problematic. By trying to gather information on foreign-influenced activities without informing all communities, CSIS could actually increase distrust, especially if these communities become informed of CSIS activities through other channels. As such, **SIRC recommends that CSIS develop a strategy to deliver the same cautionary messages about foreign-influenced activities for all potentially affected sectors.**

A Growing Concern

In recent years, the potential risks to national security from state-owned enterprises (SOEs) originating from foreign countries has been of increasing interest to the Government of Canada. CSIS informed SIRC that advice to the Government of Canada that touches on SOEs is not aimed at stopping investment; rather the Service provides information so that the government can make a fully informed decision on trade and relations with foreign partners. CSIS also participates in the *Investment Canada Act* (ICA) process. In 2009, the *National Security Review of Investments Regulations* provisions within the ICA were registered and became a new business line for CSIS. One purpose of the ICA is to review significant investments in Canada by non-Canadian entities. Despite the short timelines within which this activity takes place, CSIS is an important part of the larger process whereby the Minister of Public Safety assists the Minister of Industry in determining whether the proposed investment could or would be injurious.

Canada's recent foreign policies and international trade agreements will likely result in greater client demands for information on SOEs, and other economic/prosperity issues. SIRC will monitor the evolution of CSIS's involvement in such processes with interest in the years to come.

On this file overall, SIRC found that CSIS has acted appropriately under current operational policies; however, some adjustment may be required as new strategies by foreign nations emerge. SIRC will be interested to see how CSIS's investigation into threats posed by espionage and foreign-influenced activities of foreign governments develops in the future.

SIRC REVIEW

CSIS INITIATIVES FOR FOREIGN COLLECTION

Background

CSIS Director Richard Fadden noted in February 2013 that the Service is "aware of dozens of Canadians" who have travelled or attempted to travel to engage in terrorist activities. CSIS is hoping that foreign collection initiatives will help to close this information gap. Indeed, SIRC has also seen how ministerial direction and emerging issues such as kidnappings and illegal migration have placed demands on the Service to report on overseas activities. Foreign collection operations help CSIS identify threats before they reach Canada. They also help decrease the Service's dependence on allied reporting, focusing collection efforts on Canadian-related foreign-based threats.

SIRC's Review

This review centred on efforts by two branches to enhance their overseas intelligence collection abilities. The review continued SIRC's ongoing examination of how CSIS is operating abroad with partner intelligence services, while also independently working to fill information gaps. Both branches worked with the various CSIS regional offices to create frameworks for the intelligence collection priorities, methods and goals of overseas collection, and to connect them back to Canadian concerns. The documents outlining such initiatives are frequently updated to reflect the ongoing evolution of the threat, or changes with regard to intelligence gaps.

In March 2012, the Service created a dedicated unit to provide training related to operations, in part because CSIS recognized that it was increasingly venturing into more dangerous areas. Training modules are tailored to the individual operation and include a feedback mechanism. Incorporating such a mechanism as a routine task is an excellent method of ensuring a better product; SIRC found that the lessons learned and the iterative approach adopted in the development of the training modules to be good practice.

An important benefit of having these training modules is that it allows CSIS to take an ongoing critical look at any operational shortcomings. The training and evaluation can also provide a measure of objectivity and help mitigate any differences of opinion when it comes to deciding to operate in a potentially dangerous environment. **SIRC supports the development of operational training and recommends that the Service ensure that all persons who are identified as a priority for training receive it, particularly if they are operating in a dangerous environment.**

Overall, SIRC found that CSIS is taking a measured and cautious approach with the initiatives examined in this review. Safety continued to be a paramount consideration and was mentioned at all of SIRC's briefings; SIRC saw no indication that people would be brought into any new initiative if it was felt they would be in jeopardy or would not meet with some measure of success. SIRC was also reassured to find a consistent message highlighting the fact that the primary focus of the regional offices and collection programs was always domestic collection, and that such collection is never to be sacrificed in order to collect abroad. With regard to overseas activities, **SIRC recommends that CSIS develop a legal framework outlining acceptable and prohibited activities, including the corresponding levels of approval within and outside the Service**.

SIRC REVIEW

CSIS'S EVOLVING FOOTPRINT ABROAD

Background

CSIS foreign stations are strategically located in order to meet Government of Canada intelligence needs, which include: the provision of security screening support to Citizenship and Immigration Canada offices abroad, liaising with other partners (both international and domestic) located abroad, and collecting intelligence on possible threats to Canada or Canadian interests. With the exception of Paris, Washington and London, and CSIS's presence in Afghanistan, the location of foreign stations remains classified. Typically, past SIRC reviews have examined liaison efforts and operational activities within a single station abroad. This year, SIRC took a broader focus and looked at CSIS's overseas presence writ large, focusing on the decision-making surrounding the Service's overall approach to its representation abroad.

SIRC's Review

This review was guided by some key items, including: the criteria for opening and closing stations, the challenges of operating overseas, and the assessment of arrangements with foreign agencies. Overall, SIRC found that CSIS, in attempting to broaden its operational role overseas, is being strategic and capitalizing on both its liaison and operational functions. Nonetheless, SIRC outlined a few noteworthy issues concerning: the accuracy of information provided in some of its foreign arrangement profiles; how priorities are determined when collecting on specific intelligence requirements abroad; and the implications surrounding the long-term sustainability of playing a more operational versus a liaison-centric role.

The broader question of whether CSIS is being asked to do more with less was not a question that could be answered within this review. Rather, SIRC notes that CSIS's footprint abroad is evolving rather than merely expanding, and that the requirements of the Government of Canada, including fiscal restraint, have encouraged a more dynamic approach to this evolution. New strategies are in place, which CSIS hopes will provide the flexibility required to respond to its ongoing collection requirements, as well as any emerging issues that may arise and require attention.

However, there are other challenges associated with stepping into rich areas of collection, and SIRC outlined that existing opportunities do not completely counter them. For instance, the staff in one of the stations examined found challenges in managing the competing demands that CSIS faces in relation to not only day-to-day administrative duties, but key liaison functions and complex operational activities. This underscores some of the differences that exist between liaison-centric posts and the more operational posts located in other parts of the world.

An evolving operational presence abroad has also meant a changing dynamic of how CSIS is dealing with foreign intelligence agencies. This has translated into the enhancement of existing arrangements, the re-activation of suspended or dormant relationships, and the pursuit of new partnerships. The requirement to work and deal with a limited pool of potentially problematic partners in certain parts of the world is inevitable, and poses additional challenges. This reality is nonetheless juxtaposed with reasonable questioning and research on the questionable track record of some of these agencies and its personnel.

As per Section 17 of the *CSIS Act*, the Service may enter into arrangements with foreign entities. Another illustrated challenge, both in terms of liaison and conducting operations abroad, is the possible corruption within some of these agencies. In one arrangement profile that SIRC examined, previous concerns with respect to corruption had led to temporarily suspending this relationship. In an attempt to revive this arrangement to meet some operational requirements, corruption issues were still deemed to be a potential concern; however, CSIS relied on an incremental risk-based approach. SIRC found that prior to the Service re-engaging with the foreign agency, CSIS took appropriate steps to assess current corruption concerns.

Information related to foreign arrangements is contained in the *CSIS Act*, Section 17 "Arrangement Profile." These arrangement profiles are used to brief the Director, the executive, the branches and regional offices, as well as external departments and entities, including SIRC. As such, the accuracy and relevancy of such profiles is of utmost importance. SIRC found some deficiencies regarding content within three arrangement profiles it examined. SIRC also found that in at least one case, critical information contained in a source file was not used to keep an arrangement profile accurate and up-to-date.

SIRC has commented in the past on the accuracy and maintenance of Section 17 profiles and further found that although progresses have been made with regards to regular updates, there is still a need for significant improvements, particularly in regards to populating the content of the documents. As SIRC was informed throughout this review, operations abroad are no longer the exception but now the norm. As such, accurate and up-to-date information on foreign agencies is crucial not only to the success of the operation, but also to maintaining positive liaison relationships.

As overseas operations expand and evolve, the accuracy of information contained within these arrangement profiles becomes more important than ever. As such, **SIRC recommends that CSIS take immediate action to ensure that Section 17 profiles are consistently accurate, complete, up-to-date and relevant.**

SIRC REVIEW

CSIS'S SUPPORT TO CANADA'S NORTHERN PERIMETER SECURITY

Background

Canada's North is undergoing rapid transformation: from the impacts of climate change, to advances in oil, gas and mineral exploration and development, as well as the growth of northern and Aboriginal governments and institutions. Not all of the interest in this vast region, however, is benign: national security concerns in the North—long perceived as a bygone threat of the Cold War—are once again receiving media, academic and government attention.

Each of the eight circumpolar states (i.e. Canada, Finland, Greenland [Denmark], Iceland, Norway, Russia, Sweden and the United States) has its own definition of what constitutes the circumpolar region, the Arctic, and the North. Canada tends to differentiate between the "near north" and the "far north." The near north is typically defined as constituting the landmass between 50° and 60° latitude, while the far north is generally regarded as encompassing all areas north of 60° latitude (i.e. the Arctic). These distinctions are important for CSIS, as there are different liaison, operational and financial considerations between operating in the near north versus the far north of Canada.

SIRC's Review

Advancing the government's northern interests has become a priority in recent years; as such, this study focused on the rationale(s) underscoring CSIS's efforts at securing Canada's northern perimeter. In particular, the study examined the extent of the threat(s) as understood by the Service, how resources devoted to this issue are managed (at headquarters and within CSIS's regional offices), CSIS's liaison activities with relative northern partners, and how operational initiatives have been developed and acted upon.

In particular, SIRC found that CSIS faced a number of unforeseen challenges following the government's decision in 2010 to designate the Arctic as an intelligence and security "issue" in its own right. To begin, the Service had traditionally not played a significant role in working collaboratively with relevant stakeholders on northern issues. Absent a dedicated "Arctic portfolio," what resources that were expended on the subject were devoted to investigating what had historically been a limited number of threats. Therefore, CSIS was forced to confront a topic that had hitherto been viewed as a fairly low priority.

Despite being encouraged by the government to realign its resources alongside this northern-focused priority, SIRC found that CSIS's efforts at addressing this direction were difficult to implement due to an additional government priority calling for fiscal restraint. The problem with the resulting curtailment in resources is that it occurred precisely when CSIS was trying to reassess the relative importance of threats in the North, their complexity, and how resources should be focused for targeting and source recruitment.

In 2011, CSIS received new and more specific direction on what was expected vis-à-vis Canada's North. This was followed by an internal reorganization of responsibilities within the Service aimed at increasing the efficiency and effectiveness of resources devoted to this subject. SIRC found that as a result of this new direction and regional reorganization, CSIS's strategic management of the northern question became more consistent with the approach taken for other regional responsibilities.

Despite the directional and the resulting organizational changes, challenges remain. First, there is the larger and general prevalence of a pervasive ("southern") attitude of indifference towards Canada's North that must be overcome each time investigative considerations (or the subsequent request for associated funding) is discussed; second, there are pressing operational priorities in Canada's south (and overseas)

that take up the lion's share of CSIS's resources; and, finally, there are continuing financial pressures limiting operational options. Added to this is the absence of an official CSIS headquarters strategy guiding the Service's northern efforts; instead, there is a reliance on shared regional responsibilities, which can complicate the prioritization of northern initiatives.

Although SIRC found there was general agreement among CSIS managers that the *status quo* was satisfactory, looking over the longer term (i.e. five years and more), some senior officials believed that a stronger role by CSIS headquarters would become necessary. SIRC agrees; one initial initiative would be for CSIS to conduct an internal study on establishing a long-term operational strategy for Canada's North, paralleling sound efforts undertaken prior to the Service's expansion overseas. Such an approach would be consistent with the importance the government places on this issue and, further, would better position the Service to react to national security requirements when (not "if") they become more prominent within Canada's northern frontier.

Regardless of the specific manner in which it is implemented, however, **SIRC recommends that CSIS "institutionalize responsibility" for northern initiatives by setting out headquarters-driven liaison and operational objectives over a multi-year period, and ensure that these objectives are sustained with an appropriate resource commitment.**

SIRC REVIEW

CSIS ACTIVITIES RELATED TO DOMESTIC INVESTIGATIONS AND EMERGING ISSUES

Background

CSIS characterizes domestic extremism as the willingness of individuals or groups in Canada to use violence or the threat of violence for political and/or ideological purposes. While CSIS dedicates most of its counter-terrorism resources to religious extremism, the Service also continues to monitor individuals and organizations that might be involved in other forms of terrorism, including violence related to issues such as: animal rights, the environment, anti-globalization and white supremacy. Violence associated with these domestic themes tends to fluctuate and often revolves around events or current issues; moreover, the vast majority of activities related to these issues or events falls well within the realm of legitimate protest. In recent years, the level of threat associated with a number of such domestic investigations has been reassessed, particularly in light of the conclusion of key, large-scale events in 2010 (e.g. the Vancouver Olympics and Paralympics, and the G8 and G20 summits) that may have temporarily attracted violence, or the increased threat of violence. Accordingly, CSIS has made changes to the ways it investigates non-religious domestic extremism in the wake of this threat reassessment.

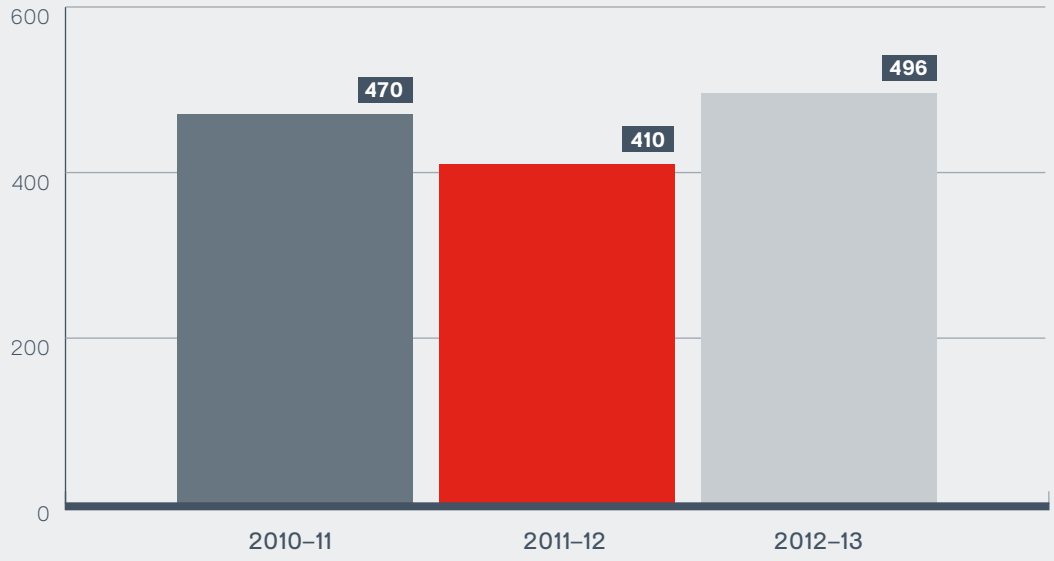
SIRC's Review

This review concentrated on CSIS's new framework and post-2010 investigations. To inform this review, SIRC visited a regional office where there were active investigations related to domestic extremist activities. SIRC was interested in how changes in the Service's approach to domestic extremism affected both national strategy and local investigations. SIRC found the recently revised investigative framework under which the Service is now operating provides more flexibility to collect and report on these threats, regardless of ideology or group membership, and to be logical and sound from the perspective of investigative efficiency. SIRC also examined select files and operational reporting to ensure that investigations were handled in an appropriate and reasonable manner—i.e. that they adhered to internal policy and the CSIS mandate. SIRC found that activities related only to legitimate protest and dissent were not investigated, and that detailed operational reporting on a range of former targets ceased. SIRC also found that CSIS moved quickly to terminate investigation of those individuals who were no longer considered threats after the major events of 2010, and encouraged the Service to be as vigilant regarding future events or issues.

One remaining challenge concerns the inevitable need on the part of the government for information on threats that are mainly inactive today, but which may suddenly rush back to the surface tomorrow;

Targeting

When the Service has reasonable grounds to suspect that an individual or organization could pose a threat to Canada, it must first establish an investigation. This figure indicates the number of targets (rounded to the nearest 10) investigated by CSIS in the past three fiscal years.



the Service must therefore remain abreast of possible flashpoints or triggers that may involve a threat to national security from domestic extremism. In addition, CSIS must ensure that by maintaining this awareness they do not intrude on legitimate forms of protest. Ultimately, it is the Service's partnerships with law enforcement agencies that can act as a potent source of information: law enforcement officials may be aware of individuals involved in ongoing criminal activity who may, at some point, pose a threat according to CSIS's mandate to investigate domestic extremism. SIRC saw examples of fruitful liaison with law enforcement, both in older threats areas where the Service no longer had investigations, and within emerging areas that CSIS needs to be aware of in case a national security nexus develops. Overall, **SIRC encourages the direction the Service is taking in liaising with its domestic partners.**

SIRC REVIEW

CSIS'S USE OF A CLANDESTINE METHODOLOGY

Clandestine methodologies (also frequently referred to as "intelligence tradecraft") include a wide range of specific risk-managed techniques that provide the necessary secrecy and security to assist CSIS in the performance of its duties and functions. As the Service's operations have expanded at home and abroad against increasingly sophisticated targets, there has been a corresponding need to enhance clandestine methodologies to help further protect the identities of its employees, processes and sources of information. This review was concerned with one of these specialized CSIS methodologies.

SIRC's Review

SIRC reviewed relevant documents and spoke to the CSIS employees responsible for the creation, management and ongoing logistics involved with this classified tradecraft. The following key issues were addressed: the justifications for its use; the types of scenarios in which it is applied; the extent of, and SIRC's satisfaction with, the auditing, access and reporting controls used to ensure that the tradecraft is not abused by employees; and finally, an examination of the various relationships that CSIS must maintain to ensure the efficient and effective management of this methodology.

CSIS's Internal Audit Branch had previously performed an assessment on this clandestine methodology and, as such, an additional goal behind SIRC's review was to examine the level to which CSIS responded to the recommendations stemming from that audit. Overall, our review found that CSIS has made many improvements since the audit, including the development of a more comprehensive policy framework and a set of guidelines to better support the expanding use of this covert methodology.

Accountability over the use of this tradecraft is a shared responsibility across CSIS's regional offices. This approach provides regional managers with the necessary flexibility to apply this methodology according to their operational needs, albeit with a sufficient number of headquarters controls, including the creation of a centrally administered database, as well as the formation of a specific unit acting as the policy centre guiding the use of this tradecraft. Prior to CSIS's internal audit, there were a number of challenges associated with financial accountability. SIRC found that additional financial reporting requirements have been put into place and other improvements are underway.

SIRC was informed that there were no instances during the review period in which a CSIS employee was found to have been in violation of security procedures and/or involved in a breach of security with respect to the use of this tradecraft. However, SIRC found there had been one compromise of this covert methodology in recent years, albeit one that was procedural/administrative in nature and which resulted in no injury or significant risks. The situation was addressed by the appropriate internal stakeholders and the details about the specific compromise were retained on file, as per CSIS policy. As a result, and although generally satisfied with how this compromise was addressed, SIRC found that there was no established procedure requiring that other CSIS regions be informed in a timely manner about the lessons learned following a security breach involving this tradecraft. In light of this, **SIRC recommends that CSIS policy be changed to ensure that all stakeholders be informed about lessons learned stemming from a suspected or confirmed security breach pertaining to the use of this covert methodology.**

Growing concerns about the need to further safeguard CSIS's employees, processes and sources of information have spurred increased use of this tradecraft. Yet, this in turn has created various management challenges, one of the more pressing being the need to maintain the necessary human resources to ensure its effective use. One solution being developed by CSIS is to utilize a complementary tradecraft/program to help offset this managerial burden. Although this new initiative suggests some promising attributes, SIRC found the policy guiding this accompanying program was insufficient and contradicted tenets of other connected policies. For this reason, **SIRC recommends that CSIS immediately update its policy on the use of this new program so that it is more in line with other operational policies.**

CSIS's use of covert methodologies has come a long way since the creation of the Service in 1984. Indeed, a cornerstone of any successful intelligence agency is to be operationally active without being observed. Without the use of clandestine methodologies, CSIS would not be able to operate effectively nor efficiently. As CSIS embarks on innovative measures to provide greater security to its various activities domestically and abroad, newer challenges will undoubtedly emerge. For this reason, SIRC will be examining other aspects of CSIS's covert methodologies in future reviews.

SIRC REVIEW

THE ROLE OF CSIS IN THE MATTER OF ABOUSFIAN ABDELRAZIK

Background

Abousfian Abdelrazik, a dual Canadian-Sudanese citizen, was arrested by Sudanese authorities in September 2003; he remained in exile in Sudan for six years, unable to secure travel back to Canada. In early 2009, Canadian media reported that his arrest and detention had come at the request of Canadian security intelligence officials, an accusation that CSIS has consistently denied. The allegation also prompted the CSIS Director to publicly write to the Chair of SIRC, asking SIRC to investigate and report on the performance of CSIS's duties and functions with respect to this case.

In the spring of 2011, SIRC launched a review intended to examine CSIS's involvement in the matter of Abousfian Abdelrazik from the months leading up to his departure from Canada for Sudan in March 2003, to his eventual return to Canada. Our review looked at CSIS's investigation of, and interactions with, Abdelrazik both in Canada and abroad, including any role CSIS may have played in his arrest and detention by Sudanese authorities. It also examined the information that CSIS received from, or provided to, domestic and foreign partners in relation to him. More broadly, SIRC explored CSIS's role and advice in the "whole-of-government" approach that was ultimately used in Abdelrazik's case.

Methodology

SIRC requested all relevant information held by CSIS relating to Abdelrazik that fell within the review period, specifically: operational reporting, internal correspondence, and information relating to CSIS's exchanges with domestic and foreign partners. Further to our review of documentation, SIRC submitted questions seeking clarification on a number of issues and asked to speak to certain key individuals who were directly involved in the investigation and management of this case.

As the review unfolded, CSIS apprised SIRC of legal concerns it had arising from the fact that SIRC's review was running concurrent with Abdelrazik's ongoing civil litigation against the Canadian government. As a result, SIRC's access to the relevant personnel was significantly delayed. Furthermore, CSIS originally provided answers to only some of SIRC's written questions, and, in a number of these cases, those answers were not complete. After extensive internal deliberation and consultation, it was reiterated to CSIS that SIRC's mandated activities and any ongoing court proceedings were distinct and separate processes, with neither affecting nor impeding the progress of the other.

In time, SIRC did receive full answers and full cooperation from the Service. SIRC was also ultimately able to speak with several of the key persons involved in the file, although the passage of time since the original events meant that some of these individuals no longer worked for the Service. In light of the delays we encountered, SIRC chose to narrow the primary focus of its review: it mostly scrutinizes the earlier phase of this case (specifically, from March 2003 to December 2004), which corresponded to CSIS's most intense involvement. Following that period, Abdelrazik's case became much more complex, and began to draw a number of other Canadian agencies into significant roles.

Because of the nature of the issue and the direct and public request by the former CSIS Director, the Committee decided to submit its report directly to the Minister of Public Safety under Section 54 of the *CSIS Act*.

Findings

SIRC found no indication that CSIS had requested Sudanese authorities to arrest or detain Abousfian Abdelrazik. CSIS did, however, in the months leading up to Abdelrazik's departure and eventual arrest abroad, keep its foreign intelligence allies up to date on any fresh information gleaned from their investigation of him.

As this case unfolded, SIRC found that Sudanese authorities remained under the mistaken impression that Canada, including CSIS, had supported the original decision to arrest and detain Abdelrazik. This confusion could perhaps be explained by the fact that the genesis of this case put it front and centre as an intelligence issue, and it remained so (according

to reporting) in the minds of the Sudanese. Further complicating matters was the fact that, originally, the two Canadian government agencies most heavily involved in this case—DFAIT and CSIS—carried out their respective consular and intelligence work concurrently, though sometimes at odds with each other. SIRC's review concluded that upon learning of Abdelrazik's detention in Sudan, CSIS should have been more forthcoming with DFAIT in regards to what it knew so as to ensure a more informed and coordinated Canadian response to this case.

SIRC's review did raise a number of concerns. First, following Mr. Abdelrazik's initial incarceration, CSIS was allowed to interview him in Sudan. CSIS followed proper authorities in seeking approval for conducting this interview; SIRC found, however, that in the context of its interview and its subsequent report, CSIS inappropriately and, in contravention of CSIS policy, disclosed personal and classified information.

Second, in mid-2004, and in preparation for Mr. Abdelrazik's possible release, CSIS updated its government partners on information the Service possessed. Although these updates would not be the final word concerning the Service's assessment of the situation, and although it would be years before Abdelrazik left Sudan (thus mitigating the impact of what the assessments had asserted), SIRC found that these assessments contained exaggerated and inaccurately conveyed information.

Third, SIRC had concerns with respect to CSIS's investigation, notably, that CSIS excessively reported, and hence retained in its operational databases, a significant amount of information not related to the threat, originating from individuals who were not targets.

Preparing Our Report

SIRC has found it challenging to put the findings of this review into the appropriate context. It has been nearly a decade since Abdelrazik first left Canada for the Sudan, and it is an understatement to note that since the events of 2003 and 2004, much has changed in Canada's security and intelligence landscape.

To begin, multiple Canadian Commissions of Inquiry, including the O'Connor (2006), Iacobucci (2008) and Major (2010) reports have commented extensively on a wide spectrum of security and intelligence issues. Although not related directly to Abdelrazik's case, the numerous recommendations flowing from these inquiries attempted to improve the professional standards expected of the government departments and agencies generally involved in security and intelligence matters and, in many cases, were directed specifically at improving the policies and practices of CSIS.

Another consideration is the wide spectrum of jurisprudence that has steadily been developed over the past decade and which comments on the roles and responsibilities of government(s), citizens and immigrants (permanent residents) when national security is the fulcrum of debate. Pointedly, Mr. Abdelrazik's own stilted progression through Canada's legal system is well publicized, such that it does not require repeating here.

For its part, SIRC has not been an idle bystander as the preceding tumultuous decade unfolded. In fact, many of the Committee's previous recommendations have covered issues that are germane to the Abdelrazik case. Some of these include:

- That CSIS, in its collection of information, avoid extensive reporting of non-targeted individuals (cf. SIRC 2002–2003 annual report: Domestic Threats in Conjunction with Lawful Advocacy, Protest and Dissent);
- That CSIS amend operational policy outlining the procedures for documenting contact with agencies known or reputed to have engaged in human rights abuses (cf. SIRC 2005–2006 annual report: CSIS Liaison with Foreign Agencies: Review of a Security Liaison Post);
- That CSIS review its use of investigative techniques to ensure they reflect established best practices (cf. SIRC 2005–2006 annual report: Electronic Surveillance and Information-Gathering Techniques);

- That CSIS and DFAIT update their MOU to designate the latter as the lead agency in cases involving Canadian citizens detained abroad, including reflecting the protocol, described by Justice O'Connor, of "timely and open consultation among Canadian agencies" involved with Canadians detained abroad; and "a coherent and unified approach," led by DFAIT; and "accountability for the course of action adopted" in such cases (cf. SIRC 2006–2007 annual report: The Case of Mohammed Mansour Jabarah);
- That CSIS implement measures to embed the values stemming from recent political, judicial and legal developments in its day-to-day work in order to maintain its own credibility, and to meet growing and evolving expectations of how an intelligence agency should operate and perform in a contemporary democratic society, and that CSIS seek guidance and advice from the Minister (cf. SIRC 2008–2009 annual report: The Role of CSIS in the Case of Omar Khadr);
- That CSIS adopt a broader interpretation of its disclosure commitments to DFAIT (cf. SIRC annual report 2010–2011: CSIS Relationships with Partners).

When considered holistically, these points and other SIRC recommendations have fundamentally affected how CSIS conducts its business, including the implementation of new ministerial direction and policies guiding CSIS's information collection, retention, analysis and dissemination functions, as well as how the Service's relationships with domestic and foreign agencies are expected to be managed. As a result, CSIS's entire program of operations—both at home and, especially, abroad—do not resemble what it was in the years focused upon in this review.

Perhaps of equal importance is the fact that Abdelrazik's case became much broader and more complex as the years went by: at the same time as CSIS's investigation of him was significantly reduced (given his apparent indefinite inability to leave Sudan), a raft of other Canadian government departments—notably DFAIT, the RCMP, CBSA and Transport Canada—(as well as foreign government agencies) commenced wrestling over his fate. SIRC is unable to ascertain the extent to which any of these entities may or may not have acted on CSIS's advice, or to what extent CSIS information factored into the decision-making of others. Indeed, SIRC has no review jurisdiction beyond CSIS and, therefore, had to limit its commentary to what the Committee knows solely as it pertained to the Service's involvement.

Conclusions

For all of these reasons, SIRC elected not to present any recommendations to policy or practice as part of this review. Indeed, most of the relevant CSIS policies have already changed, and/or operational practices have evolved over the past decade, meaning that SIRC would, in effect, be resubmitting recommendations already covered by Commissions of Inquiry or by decisions of Canadian courts or the Committee itself.

Nonetheless, we believe there are a number of valuable lessons to be drawn from SIRC's review of CSIS's role in the case of Abousfian Abdelrazik. That CSIS produced threat assessments based on incorrect and exaggerated information should be of concern, as should the fact that classified information was improperly provided, despite existing policy and specific preventative senior management direction. There are also important concerns in regard to CSIS's relationship with its Government of Canada partners, especially, in this case, DFAIT.

As SIRC has pointed out in a range of recent studies (with some of the pertinent recommendations cited above), CSIS is rapidly expanding abroad and is becoming a much more frequent and integrated partner with other large government agencies. As it pursues that role, however, CSIS will be facing the increased responsibilities and expectations that accompany them. For example, CSIS told SIRC in 2012 that existing legislation and MOUs "allow but do not require" CSIS to share information that would be of critical importance

to the work of government partners; that statement is technically correct but greatly minimizes—if not undermines—the entire intention of fostering closer and more integrated working relationships among government agencies. SIRC strongly encourages CSIS to view this report as a detailed retrospective, and an opportunity to re-evaluate its posture and approach to being party to a whole-of-government approach.

On a final note, the inability of this study to move beyond the confines of CSIS is a limitation on which this Committee has publically commented previously. Although the 1984 Special Senate Committee, which reviewed the draft legislation that would become the *CSIS Act*, anticipated SIRC would provide a "vital role in the functioning of the security intelligence system" by promoting "adequate debate, where necessary, in the area of security," this function is curtailed by the practical limitations of our mandate.

Therefore, although we stand by our review of CSIS's role in the Abdelrazik case, this study does not constitute the definitive or complete picture on this subject. Other information is likely to emerge from the broad range of documents or reports held by other Government of Canada departments and agencies that were equally involved, as well as from ongoing legal processes. As it stands, Abousfian Abdelrazik's story has yet to be fully written.

CERTIFICATION OF THE DIRECTOR OF CSIS'S ANNUAL REPORT TO THE MINISTER OF PUBLIC SAFETY: OVERVIEW

As per its new statutory requirements, SIRC engaged in the certification of the Director of CSIS's annual report to the Minister of Public Safety. The statements required by Section 38(2) of the *CSIS Act* amount to significant assurances regarding the legality, reasonableness and necessity of the Service's operational activities. Moreover, the Director's report has been, in recent years, a useful and comprehensive overview of the whole of CSIS operations. The report for fiscal year 2011–2012 was no exception, and it provided a summary of the major operational accomplishments and challenges faced by the Service over the previous year. As a result, SIRC found that certifying the "operational activities described in the report" meant certifying a high-level description of almost the whole of CSIS's activities for fiscal year 2011–2012.

With the exception of three issues, SIRC is satisfied with the Director's report on the Service's operational activities for the 2011–2012 reporting period. In addition, it is SIRC's opinion that the operational activities, as they are described in the Director's report, did not contravene the *CSIS Act* or ministerial directives, nor did they involve the unreasonable or unnecessary use of the Service's powers.

CHANGES TO THE *CSIS ACT*

In 2012, the Government of Canada amended the ***CSIS Act*** to require that SIRC complete some of the responsibilities formerly assigned to the Inspector General of CSIS. Primary among these was the requirement that SIRC submit to the Minister of Public Safety a certificate stating the degree to which the Committee is satisfied with the report. In addition, 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 ***Act***, or involved any unreasonable or unnecessary exercise of the Service's powers.

Satisfaction with the Report

The purpose of the Director's report, submitted pursuant to Section 6(4) of the *CSIS Act*, is to provide the Minister with information to assist him in exercising ministerial responsibility for CSIS. Accordingly, SIRC's satisfaction with the report was based on whether the Director's report fulfilled that function. SIRC measured this against three criteria: first, whether the report met the ministerial reporting requirements set out in the 2008 Ministerial Directives on Operations and the 2011–2012 Ministerial Directives on Intelligence Priorities; second, whether the report was factually accurate; and, third, whether, in SIRC's opinion, the report provided an accurate representation of CSIS activities during the 2011–2012 fiscal year.

With respect to ministerial reporting requirements, SIRC found that the Director's report addressed them all but one. During the certification process, SIRC learned that although this issue was not specifically addressed in the Director's report, the Service did provide the Minister with this information as part of a Memorandum to Cabinet. Accordingly, this omission did not detract from SIRC's overall satisfaction with the Director's report.

Regarding the accuracy of the Director's report, SIRC is of the opinion that the information provided by the Director's report was, on the whole, factually accurate. SIRC reviewed the statements in the report against CSIS information holdings, and, where warranted, SIRC submitted written requests for additional documentation and clarification. On the basis of this review, SIRC determined that, with the exception of two statements, the Director's report was fully supported and appropriately documented. The errors identified related to the inaccurate characterization of the status of the Service's relationship with another agency and the omission of one operation from the total number of these types of operations.

SIRC considered whether the Director's report provided an accurate representation of CSIS activities during the 2011–2012 reporting period. To make this determination, SIRC submitted written requests for information on CSIS operational activities. This included requests for statistics on the Service's core activities such as targeting, human source operations and warrant applications as well as information on foreign and domestic liaisons, technical and operational support, foreign operations and security screening. The Service's responses enabled SIRC to construct a comprehensive picture of the extent of Service activities, and permitted SIRC to assess the Director's report against this bigger picture.

SIRC found that the Director's report was a useful and comprehensive overview of the whole of CSIS operations. Nevertheless, SIRC determined that the Director's report did not contain a detailed description of the Service's activities in support of Section 16 collection of information concerning foreign states and persons. As these activities are an integral part of the Service's operations, SIRC believes that a more detailed description was warranted.

SIRC also found that the Director's report did not contain a sufficiently detailed description of the Service's foreign operations. SIRC is of the opinion that more detailed information would have provided a more accurate and representative description of the Service's foreign operations and would help provide the Minister with a better understanding of the elevated threats to the lives of Service employees in this environment. As such, the Director may wish to consider including such information in next year's report; SIRC believes that this issue is of sufficient concern that it warrants the Minister's attention and continued consideration.

Compliance with the *CSIS Act* and Ministerial Directives, and Exercise of Service Powers

In addition to requiring SIRC to state its satisfaction with the Director's report, Section 38(2) of the *CSIS Act* requires SIRC to state whether, in its opinion, the operational activities described in the Director's report contravened the *Act* or ministerial directives and whether the activities involved any unreasonable or unnecessary use of the Service's powers.

To make this assessment, SIRC conducted an extensive examination of the review environment. This included a review of recent changes to the *CSIS Act*, the authorities for the Service to collect Section 16 information, and relevant ministerial directives and intelligence priorities. It also included an examination of the Service's internal governance framework, including internal directives and the Service's operational policies.

SIRC found that, with one exception, the Service's internal governance structure upholds the *CSIS Act* and ministerial directives. SIRC determined that the Service's practice of sharing information with domestic and foreign signals intelligence (SIGINT) agencies is potentially problematic in terms of compliance with ministerial directives on information sharing. This was not an issue that came to light during the certification process exclusively. Rather, it first came to light in the context of a SIRC review entitled "CSIS's Relationship and Exchanges with Communications Security Establishment Canada," which examined the issue during the period covered by the 2011–2012 Director's report. For the purposes of certifying the Director's report, SIRC did not characterize this issue as an instance of non-compliance with ministerial directives. Nevertheless, SIRC believes that it is of sufficient concern that it warrants the Minister's consideration.

With the exception of this one area, SIRC is of the opinion that the activities, as they are described in the report, comply with the *Act* and ministerial directives and constituted a reasonable and necessary exercise of the Service's powers. Specifically, SIRC determined that the activities described in the report 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 on operations, information sharing and intelligence priorities.

B. COMPLAINTS

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

The Complaints Process at SIRC

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

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

If jurisdiction is established, complaints are investigated through a quasi-judicial hearing presided over by one or more Committee Members. They are assisted by staff and by SIRC's legal team, which provides legal advice to Members on procedural and substantive matters.

Pre-hearing conferences may be conducted with the parties to establish and agree on preliminary procedural matters, such as the allegations to be investigated, the format of the hearing, the identity and number of witnesses to be called, the production of documents in advance of the hearing and the date and location of the hearing.

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

The *CSIS Act* provides that SIRC hearings are to be conducted "in private." All parties have the right to be represented by counsel and to make representations at the hearing, but no one is entitled as of right to be present during, to have access to, or to comment on, representations made to SIRC by any other person.

A party may request an *ex parte* hearing (in the absence of the complainant and possibly other parties) to present evidence which, for reasons of national security or other reasons considered valid by SIRC, cannot be disclosed to the other party or their counsel. During such hearings, SIRC's legal team will cross-examine the witnesses to ensure that the evidence is appropriately tested and reliable. This provides the presiding Member with the most complete and accurate factual information relating to the complaint.

Once the *ex parte* portion of the hearing is completed, SIRC will determine whether the substance of the evidence can be disclosed to the excluded parties. If so, SIRC will prepare a summary of the evidence and provide it to the excluded parties once it has been vetted for national security concerns.

When SIRC's investigation of a complaint made under Section 41 is concluded, it provides a report to the Director of CSIS and to the Minister of Public Safety, as well as a declassified version of the report to the complainant. In the case of a complaint under Section 42, SIRC will also provide its report to the Deputy Head concerned.

Table 1 provides the status of all complaints directed to SIRC over the past three fiscal years, including complaints that were misdirected to SIRC, deemed to be outside SIRC's jurisdiction, or investigated and resolved without a hearing (i.e. via an administrative review).

TABLE 1: COMPLAINTS DIRECTED TO SIRC

	2010–11	2011–12	2012–13
Carried over	31	16	22
New	17	17	17
TOTAL	**48**	**33**	**39**
Closed†	32	11	14

† 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.

HOW SIRC DETERMINES JURISDICTION OF A COMPLAINT...

...under Section 41

Under Section 41 of the *CSIS Act*, SIRC shall investigate complaints made by "any person" with respect to "any act or thing done by the Service." Before SIRC investigates, two conditions must be met:

1. The complainant must first have complained in writing to the Director of CSIS and not have received a response within a reasonable period of time (approximately 30 days), or the complainant must be dissatisfied with the response; and
2. SIRC must be satisfied that the complaint is not trivial, frivolous, vexatious or made in bad faith.

SIRC cannot investigate a complaint that can otherwise be addressed under existing grievance procedures of the *CSIS Act* or the *Public Service Labour Relations Act*.

...under Section 42

With respect to security clearances, Section 42 of the *CSIS Act* says SIRC shall investigate complaints from:

1. Any person refused federal employment because of the denial of a security clearance;
2. Any federal employee who is dismissed, demoted, transferred or denied a transfer or promotion for the same reason; and
3. Anyone refused a contract to supply goods or services to the government for the same reason.

These types of complaints must be filed within 30 days of the denial of the security clearance.

SIRC may extend this period if valid reasons are presented.

SIRC INVESTIGATION

ALLEGED HARASSMENT, RACIAL PROFILING AND SHARING OF MISLEADING INFORMATION

SIRC investigated a complaint under Section 41 of the *CSIS Act* in which the complainant alleged that a CSIS employee had, during an interview with him, conducted himself in a manner that constituted harassment, used inappropriate interview tactics, made threats and lied about the impact of the interview on the complainant's security clearance. He also alleged that CSIS was using racial profiling and that other CSIS employees, during interviews in relation to the government security clearance assessment process, had interfered with his freedom of religion. Finally, the complainant further alleged that CSIS's investigation for his security clearance assessment was inadequate, had led to the sharing of misleading information about him with a government department, and had been marred by undue delay.

SIRC found that the first CSIS employee's conduct amounted to neither harassment nor inappropriate tactics, but that his choice of discussion topics and tone had created unnecessary tension at the interview. SIRC also found that the employee was deceptive in that he did use the security clearance process as a ruse to get the complainant to provide information. **SIRC made recommendations to CSIS to address this issue at an operational and policy level to minimize the likelihood of such a scenario occurring again.**

SIRC found that there was no evidence of racial profiling in this case and that CSIS was fully justified in pursuing its security screening investigation of the complainant as it did on the basis of the information it had in order to fulfill its mandate. Nevertheless, SIRC also found that it is not unreasonable for people, such as the complainant, who don't have access to classified information, to perceive that they are being profiled. In this respect, **SIRC recommends that CSIS engage in outreach with minority communities to explore the issue of racial data collection as a possible way to reassure the public that CSIS does not racially profile individuals.**

SIRC found that there was no interference with freedom of religion in the context of the government security clearance assessment process, and that CSIS's investigation was adequate under the security screening policy in force. SIRC found the allegation of undue delay to be unfounded.

While SIRC did not find that CSIS shared misleading information about the complainant, SIRC estimated that the information provided to the other government department was incomplete in that it excluded some of the assessment's findings. **SIRC recommends that CSIS remedy the situation by sending the previously excluded information to the department concerned.**

Finally, the complainant also alleged that there were many examples of profiling in documents about him produced internally by the other department concerned following the sharing of information from CSIS, and that the same department had failed to formally deny his clearance application, thereby preventing him from seeking a remedy under Section 42 of the *CSIS Act*. Because of the limitations on SIRC's mandate in this investigation under Section 41 of the *CSIS Act*, SIRC was not able to make findings on this issue.

SIRC INVESTIGATION

ALLEGED DENIAL OF BASIC RIGHTS AND INSUFFICIENT CULTURAL KNOWLEDGE

SIRC investigated a complaint under Section 41 of the *CSIS Act* in relation to the conduct of a CSIS employee at a permanent resident application-screening interview. The complainant alleged that the CSIS employee had denied him certain basic rights, had behaved improperly, and lacked sufficient knowledge of the complainant's cultural background and country of origin.

SIRC found that, while no rights of the complainant had been violated, the CSIS employee should have shown flexibility to accommodate certain demands of the complainant at the interview. Similarly, SIRC did not find evidence of improper conduct on the part of the employee, but it did find that the employee, in one instance, could have been more sensitive to the complainant's apprehensions. SIRC reminded CSIS that its employees should show sensitivity when interviewing persons who come from countries where intelligence agencies are feared, and should avoid any actions that could be construed as crossing the line or as being manipulative.

SIRC also found that the CSIS employee was adequately prepared before entering the interview, and that his knowledge of the complainant's culture and country was sufficient.

Finally, **to avoid rescheduling immigration interviews and causing further undue delay, SIRC recommends that CSIS issue an operational directive to all regional offices, consistent with the direction taken by the Toronto region, requiring investigators to take recording devices to all immigration interviews, and to ensure that such devices are in working order.**

SIRC INVESTIGATION

ALLEGED DELAY IN PROVIDING A SECURITY ASSESSMENT

SIRC investigated a complaint under Section 41 of the *CSIS Act* regarding the alleged delay by CSIS in providing its security assessment for the complainant's site access clearance. The complainant argued that the delay had caused him to lose work opportunities.

SIRC found that the process, decisions and actions taken by CSIS in the course of the assessment were reasonable. The case officer and investigator afforded attention to details to ensure that the assessment was appropriate.

Notwithstanding the above, SIRC found that there were delays and periods of inactivity on the file which, when added together, rendered the overall delay unreasonable. SIRC reiterated a past recommendation that a tracking system be put in place to identify files falling outside average processing times to ensure that priority be given to such files. In addition, **SIRC recommends that time management systems and reminders be implemented to avoid such situations.**

SIRC INVESTIGATION

REVOCATION OF SECURITY CLEARANCES

SIRC separately investigated two related complaints under Section 42 of the *CSIS Act* made by complainants who were government employees and whose security clearances had been revoked on the basis of their association with a third-party entity.

SIRC found that there were reasonable grounds to question the complainants' reliability as it relates to loyalty on the basis of the complainants' associations with persons or groups of concern. In this respect, the complainants could act or be induced to act in a way that would constitute a threat to the security of Canada. **For these reasons, SIRC recommends that the decision to revoke the complainants' security clearances be upheld.**

Also as a result of these investigations, **SIRC recommends the review of certain policy guidelines for employees on the issue of what they can disclose to third parties with respect to the identity of their employer, recommending a more consistent policy that defines the situations where such disclosure is appropriate.**

SECTION 3

SIRC AT A GLANCE

COMMITTEE MEMBERSHIP

SIRC is chaired by the Honourable Chuck Strahl, P.C. The other Committee Members are: the Honourable Frances Lankin, P.C., C.M.; the Honourable Denis Losier, P.C., C.M.; the Honourable Deborah Grey, P.C., O.C.; and the Honourable L. Yves Fortier, P.C., C.C., O.Q., Q.C.

STAFFING AND ORGANIZATION

SIRC is supported by an Executive Director, Michael Doucet, and an authorized staff complement of 17, located in Ottawa. This includes a Director of Research, a 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 discussions with the CSIS executive and staff, and other members of the security intelligence community. These exchanges are supplemented by discussions with academics, security and intelligence experts and other relevant organizations. 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 opportunity to communicate SIRC's focus and concerns.

With respect to human resources, SIRC continues to manage its activities within allocated resource levels. Staff salaries and travel within Canada for Committee hearings, briefings and review activities represent its chief expenditures.

Table 2 below presents a breakdown of actual and estimated expenditures.

TABLE 2: SIRC EXPENDITURES 2012–13 ($ THOUSANDS)

	2012–13 (Tot. Auth.)	2012–13 (Actual)
Personnel	2,349	2,050
Goods and services	732	852
Total	**3,081**	**2,901**

SIRC ACTIVITIES

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

July 23–27, 2012: The Executive Director, along with representatives from CSIS, the Department of Justice, and Foreign Affairs and International Trade Canada, participated in a capacity-building exercise in Trinidad and Tobago.

October 11, 2012: SIRC's Executive Director met with a delegation of the French government in Ottawa, including the coordonnateur national du renseignement.

November 19–20, 2012: SIRC Chair and Committee Members visited CSIS's British Columbia and Prairie regional offices.

January 22, 2013: The Executive Director met, in a follow-up meeting, with members of the Délégation parlementaire française – Contrôle de la communauté du renseignement, in Ottawa.

February 6–8, 2013: The Executive Director attended the 14th Annual Privacy and Security Conference in Victoria, British Columbia.

March 27–28, 2013: The Executive Director attended the Institute on Governance's Public Governance Exchange Conference.

LIST OF SIRC RECOMMENDATIONS

During the 2012–2013 review period, SIRC made the following recommendations stemming from the reviews it conducted, as well as from the complaints it investigated.

REPORT	SIRC RECOMMENDATIONS
CSIS's Relationship and Exchanges with CSEC	SIRC recommends that CSIS develop clearer and more robust overarching principles of cooperation with CSEC. These principles should address the growing volume of challenges that have arisen between the two agencies, while respecting the individual mandates of each organization.
Review of a New Section 21 Warrant Power	SIRC recommends that CSIS extend the use of caveats and assurances in regards to this new warrant power to include the agencies of the entire Five Eyes community.
Investigating Activities Related to Espionage and Foreign Influence	SIRC recommends that CSIS carry out the appropriate fine-tuning, in policy and practice, to assist investigators and analysts in identifying common and consistent thresholds, and in judging when an activity has crossed over into the clandestine realm. SIRC also recommends that CSIS develop a strategy to deliver the same cautionary messages about foreign-influenced activities for all potentially affected sectors.
CSIS Initiatives for Foreign Collection	SIRC recommends continued support for the development of operational training, and that the Service ensure that all persons who are identified as a priority for training receive it, particularly if they are operating in a dangerous environment. SIRC also recommends that CSIS develop a legal framework outlining acceptable and prohibited activities, including the corresponding levels of approval within and outside the Service.
CSIS's Evolving Footprint Abroad	SIRC recommends that CSIS take immediate action to ensure that Section 17 profiles are consistently accurate, complete, up-to-date and relevant.
CSIS's Support to Canada's Northern Perimeter	SIRC recommends that CSIS "institutionalize responsibility" for northern initiatives by setting out headquarters-driven liaison and operational objectives over a multi-year period, and ensure that these objectives are sustained with an appropriate resource commitment.
CSIS's Use of a Clandestine Methodology	SIRC recommends that CSIS policy be changed to ensure that all stakeholders be informed about lessons learned stemming from a suspected or confirmed security breach pertaining to the use of this covert methodology. SIRC also recommends that CSIS immediately update its policy on the use of this new program so that it is more in line with other operational policies.
Alleged Harassment, Racial Profiling and Sharing of Misleading Information by CSIS	SIRC recommends that CSIS engage in outreach with minority communities to explore the issue of racial data collection as a possible way to reassure the public that CSIS does not racially profile individuals. SIRC also recommends that CSIS remedy the situation by sending the previously excluded information to the department concerned.

REPORT	SIRC RECOMMENDATIONS
Alleged Denial of Basic Rights and Insufficient Cultural Knowledge on the Part of CSIS	To avoid rescheduling immigration interviews and causing further undue delay, SIRC recommends that CSIS issue an operational directive to all regional offices, consistent with the direction taken by the Toronto region, requiring investigators to take recording devices to all immigration interviews, and to ensure that such devices are in working order.
Alleged Delay in Providing a Security Assessment	SIRC recommends that time management systems and reminders be implemented to avoid such situations.
Revocation of Security Clearances	SIRC recommends that the decision to revoke the complainants' security clearances be upheld. SIRC also recommends the review of certain policy guidelines for employees on the issue of what they can disclose to third parties with respect to the identity of their employer, recommending a more consistent policy that defines the situations where such disclosure is appropriate.