BroaderHorizons

PREPARING THE GROUNDWORK FOR CHANGE IN **SECURITY INTELLIGENCE REVIEW**

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. PS105-2015E-PDF

ISSN 1912-1598

Security Intelligence Review Committee

Comité de surveillance des activités de renseignement de sécurité

September 30, 2015

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

Dear Minister:

We are pleased to present you with the annual report of the Security Intelligence Review Committee for the fiscal year 2014–2015, as required by Section 53 of the *Canadian Security Intelligence Service Act*, for your submission to Parliament.

Sincerely,

Pierre Blais, P.C., Chair
Appointed May 1, 2015

L. Yves Fortier P.C., C.C., O.Q., Q.C.
Appointed August 8, 2013

Ian Holloway, P.C., C.D., Q.C.
Appointed January 30, 2015

Gene McLean, P.C.
Appointed March 7, 2014

Marie-Lucie Morin, P.C.
Appointed May 1, 2015

ABOUT SIRC

The Security Intelligence Review Committee (SIRC, or the Committee) is an external independent review body that reports to the Parliament of Canada on the operations of the Canadian Security Intelligence Service (CSIS, or the Service). It does so through its three core functions: certifying the CSIS Director's annual report to the Minister of Public Safety, carrying out in-depth reviews of CSIS's activities and conducting investigations.

SIRC has the absolute authority to examine all information under CSIS's control, no matter how classified or sensitive, with the exception of Cabinet confidences. Its work, edited to protect national security and privacy, is summarized in an annual report to Parliament.

SIRC exists to provide assurance to Parliament and to all citizens of Canada that the Service investigates and reports on threats to national security in a manner that respects the rule of law and the rights of Canadians. Visit SIRC online at **www.sirc-csars.gc.ca** for more information.

ABOUT CSIS

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

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

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

A STATUTORY FRAMEWORK FOR BOTH SIRC AND CSIS

By virtue of the *Canadian Security Intelligence Act* (*CSIS Act*), Canada became one of the first democratic governments anywhere in the world to establish a statutory framework for its security service. With the *CSIS Act*, Canada clearly defined in law the mandate and limits of state power to conduct security intelligence.

By the same stroke, it created accountability mechanisms to keep those considerable state powers in check. SIRC derives its mandate and functions from the same law that sets out the Service's statutory framework.

CONTENTS

MESSAGE FROM THE COMMITTEE

The Committee is pleased to present its thirtieth annual report to Parliament and to Canadians. Our report aims to provide meaningful insight into SIRC's work for the 2014–2015 fiscal year through the lens of our three key responsibilities: certification, reviews and investigations.

Our three responsibilities provide us with broad insight into CSIS's activities. In fact, each one of our functions offers a unique window into CSIS: our certification of the CSIS Director's annual report to the Minister of Public Safety provides us with a useful overview of CSIS's investigative priorities, organizational initiatives or developments, and operational challenges; our reviews allow us to "drill down" into CSIS's activities and to explore precise aspects of their activities in greater depth; and finally, our investigations give us an "outside" perspective on specific CSIS activities.

This year, with one exception, our Certificate found that the activities described in the CSIS Director's annual report did not contravene the *CSIS Act* or Ministerial Direction, and were reasonable and necessary. SIRC decided to ground its satisfaction of the Director's report in a broader appreciation of its original intent, namely, to support the Minister in his role. This reflection led us to recommend the issuance of a renewed Ministerial Direction that would outline more explicit instructions to the Service with respect to the format, content and timing of the Director's report.

SIRC's assessment of CSIS's performance was supplemented by its reviews, which were designed to examine a broad spectrum of CSIS's activities and operations within Canada and abroad. In addition to our reviews of CSIS's core activities—such as targeting, human source operations, warrant powers and exchanges of information—we expanded our knowledge through baseline reviews of activities that had not previously been the subject of a focused examination, namely, CSIS's collection and use of metadata.

In most of its reviews, SIRC was satisfied with the manner in which CSIS carried out its mandate to investigate threats to the security of Canada. This year again, however, the Committee raised concerns in two special reports that were sent directly to the Minister of Public Safety under section 54 of the *CSIS Act*.

The first report stemmed from SIRC's examination of CSIS's efforts at countering the "insider threat." SIRC's in-depth look at CSIS's own internal investigations revealed a number of deficiencies with respect to training, policy and procedures, investigative thresholds and recording of decision making. In one situation in particular, the Committee found that CSIS had failed to give a case the appropriate level of attention and scrutiny, and to take follow-up action. As a result, the Committee made a number of strong recommendations, several of which that, unfortunately, were not heeded by the Service.

The second report focused on SIRC's review of CSIS's relationship with the Department of Foreign Affairs, Trade and Development (DFATD). The Committee raised a potential legal concern with respect to CSIS's activities and Canada's obligations under international agreements. SIRC found that CSIS lacked procedures to systematically verify whether human source operations were in possible contravention of Canadian regulations implementing United Nations Security Council resolutions, namely, the *United Nations Al Qaeda and Taliban Regulations*. The Committee decided to invoke a rarely used clause in the *CSIS Act* to direct CSIS to conduct a review to gather information required for SIRC to take any follow-up action deemed necessary.

In other reviews, SIRC found issues that it felt required corrective action; in those instances, the Committee made recommendations that it will closely monitor going forward. SIRC also made note of several CSIS activities that it will need to re-examine in future reviews.

Finally, in presenting SIRC's work for the past year, the Committee must extend its profound gratitude to two individuals who helped to bring it to fruition. The Committee would like to thank the outgoing Interim Chair, the Honourable Deborah Grey, who brought profound dedication, passion and vision to her work at SIRC. We also wish to congratulate the Honourable Madam Justice Sylvie E. Roussel, who served as SIRC's Senior Counsel for eight years, for her appointment to the Federal Court of Canada.

In August 2014, the CSIS Director made an uncommon request to SIRC to review the circumstances surrounding an incident involving a CSIS Intelligence Officer who obtained taxpayer information from the Canada Revenue Agency absent a Federal Court warrant. SIRC agreed to conduct an inquiry into the incident. In its report to the CSIS Director (summarized in this annual report), the Committee noted that CSIS's management of the incident was not adequate and made several recommendations.

At the same time, the Committee was pleased to welcome a new Chair, the Honourable Pierre Blais, P.C., as well as two new Committee Members, the Honourable Ian Holloway, P.C., C.D., Q.C. and the Honourable Marie-Lucie Morin, P.C. Their impressive backgrounds and diverse experiences will surely contribute to enhancing SIRC's work.

In response to concerns expressed last year with respect to the provision and disclosure of information to SIRC by CSIS, we are pleased to note an overall improvement in this area. SIRC requires full and consistent information disclosure, in both its reviews and investigations, to ensure that its assessments are accurate, complete and fair. Consequently, this issue remains at the forefront of our discussions with the Service.

REVIEW VERSUS OVERSIGHT

In the context of recent debate surrounding new legislation, SIRC observed that the terms review and oversight have been used almost interchangeably. Yet, they mean different things: whereas "review" refers to retrospective assessments of performance against specific predetermined criteria, "oversight" means contemporaneous or "real-time command and control" of a given agency or organization.

Although review bodies, including SIRC, seek to improve future compliance or performance through forward-looking recommendations, they are not a form of "oversight." This means that SIRC can make a full assessment of CSIS's past performance without being compromised by any involvement in its day-to-day operational decisions and activities.

NEW LEGISLATIVE LANDSCAPE

The past year witnessed significant legislative developments in the national security area, with the adoption of new laws that brought important amendments to the *CSIS Act*. This report affords us an ideal opportunity to comment on the impact of this new legislation on SIRC.

In April 2015, the *Protection of Canada from Terrorists Act* (Bill C-44) received Royal Assent. This legislation introduced several amendments to the *CSIS Act*, notably making explicit that CSIS's investigations with respect to threats to the security of Canada or security assessments may be conducted outside of Canada. To this end, the *Act* also confirmed the Federal Court can issue warrants for CSIS to investigate threats to our national security outside of Canada.

For a number of years, SIRC has been paying steadily more attention to CSIS's evolving and expanding footprint abroad. At the turn of the new decade, SIRC examined an aspect of CSIS's overseas activities in one or two of its annual reviews; this year, over half of its reviews examined some component of these activities. Going forward, SIRC will need to further increase its coverage of CSIS's overseas activities by focusing, for example, on CSIS's relationships with foreign partners, information exchanges, operational risks, legal challenges and new warrant powers. SIRC may also need to increase the number of CSIS foreign stations it examines annually to fully appreciate the scope and complexity of CSIS's overseas role.

Still, it is the *Anti-terrorism Act* (Bill C-51), which received Royal Assent in June 2015 that will translate into a new and more complex workload for SIRC's research and legal teams. Of particular importance is CSIS's new "disruption" mandate, namely, the power to take measures, at home and abroad, to reduce threats when it has reasonable grounds to believe that a

particular activity constitutes a threat to the security of Canada. Moreover, under the new legislation, CSIS is required to seek a court warrant whenever proposed threat reduction measures contravene rights or freedoms guaranteed by the *Charter* or are otherwise contrary to Canadian law.

The new legislation will require the CSIS Director to include in his annual report to the Minister specific information concerning a general description of the threat reduction measures that were taken; the number of warrants issued and the number of applications for warrants that were refused; and, a general description of the measures that were taken under the warrants. SIRC will need to review and assess this additional information as part of its certification process.

SIRC reviews a sample of CSIS's application for, and execution of, warrant powers on an annual basis. SIRC will need to broaden its review sample to include threat reduction warrants, to examine whether the information underlying the warrant is accurate and whether the activities carried out under the authority of the Federal Court followed the parameters set out in the warrant. By the same stroke, SIRC will be largely involved in determining the legality of those threat reduction activities where CSIS did not seek a warrant from the Federal Court. This assessment of constitutionality and *Charter* rights will add an expansive element of legal support to research activities.

Finally, and importantly, SIRC now has the statutory obligation to annually "review at least one aspect of the Service's performance in taking measures to reduce threats to the security of Canada." This responsibility will require a significant resource commitment from SIRC: threat reduction activities are by their very nature potentially controversial and/or high risk, meaning SIRC will need to ensure these activities are examined annually in a focused and dedicated manner.

In light of the above, the Committee welcomed the announcement, made in the Government of Canada's Economic Action Plan of April 2015, providing additional funding to SIRC to enhance its review of CSIS. This budget increase will help to bolster SIRC's capacity to fulfil its new legislative requirements. At the same time, SIRC will look to expand its technological means to improve efficiency and productivity at this critical time of transformation.

It is clear that SIRC is willing and able to meet rising expectations. SIRC's work has evolved significantly in past years and, with recent developments, our pace of change will undoubtedly hasten in the months and years ahead. In this transformative process, however, we will remain focused on the principle that has guided our work since 1984: to serve as a cornerstone for ensuring the accountability of Canada's security intelligence activities.

From left to right: the Honourable Marie-Lucie Morin, the Honourable L. Yves Fortier, the Honourable Pierre Blais and the Honourable Gene McLean. Absent from photo: the Honourable Ian Holloway.

MESSAGE FROM THE EXECUTIVE DIRECTOR

SIRC had a positive and productive past year. In previous annual reports, I have emphasized what I believe to be SIRC's three main principles: our independence, our professionalism and our role as a valued member of the security intelligence community. This annual report illustrates how those principles underpinned all aspects of the work that was carried out last year.

The same principles will also help to guide us into a new era. The Government's intention to significantly increase SIRC's budget to tackle additional responsibilities means that our organization has begun a transformative process. The challenge lies in best preparing for the future in the most fiscally responsible manner, following clear business lines and a renewed focus on internal cohesiveness.

SIRC's transformation has to be led according to the organization's three business lines, which must work together to meet the challenges ahead. SIRC will need to grow its staff complement to handle the expanded workload, but it will also need to examine how it conducts its business. In short, SIRC will need to increase its operational capacity while setting clear objectives that align with its mandate and priorities.

SIRC's research team has been given the resources it needs to effectively carry out its new review responsibilities. Similarly, as SIRC's review function is rendered more complex with new legislation, we expect that active legal assistance will be required on a regular basis. As seen in this year's annual report, legal support to SIRC's research activities has become an integral component of our *modus operandi*. Meanwhile, our corporate services will strive to provide overall support to our organization and meet our various corporate needs.

As a result, SIRC's research, legal and corporate teams will grow together, working in tandem to achieve our common goals. The linkages between our three business lines have become more evident and important than ever with the passage of new legislation and the changing national security landscape.

Finally, in parallel with this internal transformation, SIRC will continue to find ways to increase its effectiveness and efficiency. This will be accomplished largely by harnessing technology: for example, in coming months, SIRC will implement new information and case management systems, seek greater electronic access to CSIS information holdings and move towards electronic hearings.

It is therefore with much confidence that we embark on next year's ambitious agenda. In so doing, my commitment to our three core principles remains steadfast.

Under the *CSIS Act*, SIRC must submit its annual report to the Minister of Public Safety no later than September 30. The Minister must then table SIRC's report in Parliament within 15 days in which the House is sitting.

ABOUT THIS REPORT

In accordance with its enabling legislation, SIRC prepares an annual report of its activities that is tabled in Parliament by the Minister of Public Safety. This annual report summarizes the work SIRC has undertaken through its three key functions, including its findings and recommendations. It has four sections:

SECTION 1:

Certificate

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

SECTION 2:

Reviews

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

SECTION 3:

Investigations

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

SECTION 4:

SIRC at a Glance

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

SIRC'S RECOMMENDATIONS

Each year, SIRC requests a status report from CSIS on the recommendations arising from its reviews and investigations. This exercise allows SIRC to monitor the implementation of its recommendations and to assess their practical impact. SIRC also includes a summary of the Service's response in its annual report, to provide Canadians with insight into the dialogue that occurs between the two organizations.

CERTIFICATE

SIRC's responsibility for certifying the CSIS Director's annual report to the Minister of Public Safety adds importance to its role in assessing the Service's activities and reporting practices from the point of view of Ministerial responsibility. This year, SIRC used the Certificate to offer its reflections on two important components of the system of Ministerial responsibility for CSIS: the Director's annual report and the process of Ministerial notifications.

In June 2012, SIRC inherited from the former Office of the Inspector General of CSIS the responsibility for certifying the CSIS Director's annual report to the Minister. Accordingly, SIRC is required to provide to the Minister a Certificate stating the extent to which it is satisfied with the CSIS Director's report; whether the operational activities described in the Director's report contravened the *CSIS Act* or Ministerial Direction; and whether the activities involved any unreasonable or unnecessary use of the Service's powers.

SIRC continues to reflect on how its role in the system of accountability has evolved in recent years. SIRC views its responsibility for the certification process as an opportunity to offer a more "global" assessment of the legality, reasonableness and necessity of the Service's operational activities. This assessment draws upon, and complements, the assessments offered in its reviews and investigations.

COMPLIANCE AND EXERCISE OF POWERS

SIRC's assessment rested on several review elements, including a sample of CSIS's core activities. SIRC also conducted a comprehensive review of the Government's direction to CSIS, with a particular focus on CSIS's implementation of the suite of Ministerial Directions. Finally, SIRC thoroughly canvassed the results of its ongoing review work to support the certification process.

For this year, SIRC found that the activities reviewed did not contravene the *CSIS Act* or Ministerial Direction and were reasonable and necessary. There was, however, one exception that bore pointing out to the Minister; this case is described in greater detail in SIRC's review "CSIS's Relationship with the Department of Foreign Affairs, Trade and Development."

SATISFACTION WITH THE DIRECTOR'S REPORT

In the three years since assuming responsibility for the certification process, SIRC has carefully considered whether the Director's report, in its present form, serves well the requirements of Ministerial responsibility, especially in the current context of rapid change. SIRC considered this question against the backdrop of the original intent of the Director's report; as a statutory requirement, it is one of the key elements of CSIS's accountability vis-à-vis the Minister, the purpose of which is to make available to the Minister important information as to the functioning of CSIS.

It remains the case today that the accountability of the Service requires an effective system of communication between the Service and the Minister and his or her Deputy to ensure the Minister is informed of CSIS activities that raise questions of legality or propriety. However, the Director's report, in its present form, contains long descriptions of the main investigations that do not change substantially from year to year. Far from being an aid to Ministerial accountability, the level of detail has the effect of obscuring the more important information for Ministerial consideration, including serious issues, challenges and potentially controversial activities.

SIRC is not the first to make this observation. In fact, in 2000, the Inspector General of CSIS (IG) set out to make the Director's report more readable and more focused on matters of Ministerial interest, concern or decision making. As a result of extensive discussions led by the IG, the Minister promulgated a new Ministerial Direction on Responsibility and Accountability that articulated his expectations regarding the responsibilities and accountabilities of the Director. The result was a substantive change in the form, focus and content of the Director's report, which resulted in more concise and effective support for Ministerial responsibility for the Service. Although this Ministerial Direction is still in force today, in recent years, the report has unfortunately drifted back to its previous format, with long descriptions and detail, and correspondingly less attention to high-level discussion.

SIRC also considered whether the Service is notifying the Minister, as required by Ministerial Direction, of all those activities with a potential to have an adverse impact on Canadian interests. To this end, SIRC reviewed the number of instances the Service reported to the Minister a certain category of investigative activity deemed to be of high risk. SIRC found that, from 2008, only one such activity was "deemed to be of high risk" and

MINISTERIAL NOTIFICATIONS

As part of its certification process, SIRC must assess whether CSIS provided, as set out in Ministerial Direction, an *ongoing* flow of information to the Minister on potentially serious issues through the system of Ministerial notifications. In particular, there is a requirement, based on a risk assessment, to notify the Minister when the Director determines that there is a potential for an activity to have an adverse impact on Canadian interests.

thus reported to the Minister. This result strongly suggests to SIRC that the Service's calculation of risk may be too narrow for the purposes of ensuring Ministerial accountability.

Although the system of Ministerial notifications is meant to supplement the Director's report with ongoing information about high-risk activities, SIRC found again that the flow of information was not adequate. As a result, the Minister runs the risk of being insufficiently apprised, even of higher-risk CSIS activities, and therefore prevented from taking appropriate corrective action. This consideration may well be magnified by the new powers that have been given to CSIS, which represent a whole new area of activity with its inherent risks.

SIRC therefore recommended that the Minister make his expectations explicit in the form of a new Ministerial Direction on Responsibility and Accountability with more specific instructions to the Service with respect to the format and structure, as well as the timing, of the Director's annual report. At the same time, the Minister should consider taking the opportunity to expand his expectations with respect to Ministerial notifications. In the absence of such direction, SIRC's own efforts vis-à-vis the Certificate, to the extent that they centre on a review of the Director's report, are not as effective as they might otherwise be in supporting Ministerial responsibility.

2 REVIEWS

SIRC's reviews are designed to provide Parliament and Canadians with the assurance that CSIS has acted appropriately, effectively and in accordance with the rule of law in the performance of its duties and functions. The recent increase in SIRC's budget means that, going forward, SIRC will be better positioned to provide a high level of assurance that its review work is both comprehensive and thorough.

THE REVIEW PROCESS AT SIRC

SIRC's reviews provide a retrospective examination and assessment of a representative sample of CSIS investigations and activities. 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.

At the outset of each fiscal year, SIRC develops a research plan that is presented to the Committee for approval. This research plan is designed to address a broad range of subjects on a timely and topical basis, taking into consideration such matters as the:

- importance and scope of CSIS investigations;
- potential for particular activities to intrude on individual rights and freedoms;
- priorities and concerns of Parliament and the Canadian people;
- CSIS Director's annual report to the Minister of Public Safety on operational activities; and
- importance of regularly reviewing each of the Service's branches.

SIRC has, in law, the absolute authority to examine all of the Service's activities and full access to all of its files, no matter how sensitive and no matter what the level of classification. The sole exception is Cabinet confidences, which is to say deliberations among Ministers.

SIRC's reviews cover all of CSIS's key activities—targeting, warrants, human sources, etc.—and program areas, including counter-terrorism,

counter-intelligence, counter-proliferation and security screening. SIRC also examines CSIS's arrangements to cooperate and exchange information with foreign agencies and with domestic organizations, as well as the advice the Service provides to the Canadian government.

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

In every review, the examination of documentation generates follow-up exchanges with the Service. For this reason, SIRC researchers often request meetings and briefings with CSIS personnel to seek clarification on issues to ensure the issues at hand have been thoroughly explored and completely understood. The review is then presented to the Committee for approval. Once this process is complete, SIRC sends its finalized reviews to the CSIS Director and the Minister of Public Safety.

SIRC'S METHODOLOGY

For a number of years, SIRC has made use of a combination of review types, carefully selected to cover CSIS's activities as effectively as possible:

Thematic reviews: these reviews are more horizontal in nature and are designed to get a broad view of a particular issue or theme that cuts across CSIS's programs or investigations. They often provide SIRC's most substantive findings and recommendations.

Investigation/program reviews: these reviews examine a particular CSIS investigation or area. They are valuable in that they allow SIRC to maintain knowledge of priority investigations on an ongoing basis.

In March 2015, the CSIS Director told the Standing Committee on Public Safety and National Security (SECU) studying Bill C-51 that, in his opinion, "SIRC is a robust review mechanism that has proven over 30 years its value, its impartiality. I've said publicly again a number of times that our organization is a better organization because of the work of SIRC."

Baseline reviews: these reviews are designed to gain insight into a CSIS activity that had not previously been the object of in-depth, focused review. They are valuable as they offer insight into a new activity, investigation or program.

Core reviews: these reviews offer insight into CSIS's main activities—targeting, warrants, human sources, etc.—through a larger sample analysis. They are valuable as they provide SIRC the opportunity to "drill down" more deeply into a specific type of activity.

Over the past few years, SIRC has turned to thematic reviews to provide a wider lens on CSIS's expanding activities. At the same time, thematic reviews cannot replace the "drilling down" that comes from more focused reviews. An ongoing challenge for SIRC is to find the right mix of review types to satisfy its review mandate.

Regardless of the review type, SIRC employs a common framework, or set of core criteria, that guide and support its examination of CSIS activities. Those criteria include legal thresholds contained in the *CSIS Act*, such as legality, necessity and reasonableness, as well as principles of good governance, such as compliance with Ministerial Direction and CSIS's policy framework.

RECOMMENDATIONS

SIRC's reviews include findings and, where appropriate, recommendations. SIRC has developed guidelines regarding its recommendations to ensure they are practical, action- and results-oriented, and constructive.

SIRC's recommendations, both those stemming from reviews and investigations, are non-binding. Indeed, Parliament did not intend to have SIRC substitute for the Director of the Service, who is accountable to the Minister of Public Safety, or for the Minister, who must answer to Parliament. In point of fact, CSIS has implemented a large percentage of SIRC's recommendations, as noted in SIRC's annual Departmental Performance Reports. Moreover, CSIS has publicly acknowledged that SIRC has made CSIS a better organization over the years.

SIRC annually solicits the Service's formal responses to its recommendations. CSIS is expected to clearly and unambiguously indicate whether it agrees or disagrees with the recommendation, what actions it intends to take in response to the recommendation, and when it intends to take such action. SIRC includes CSIS's responses to the recommendations in the annual report summaries as a means of giving the public better insight into the impact of SIRC's work on security intelligence.

FIND OUT MORE ABOUT SIRC'S EARLIER REVIEWS

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

CSIS describes an insider threat as "any person with authorized access who causes harm, intentionally or otherwise, to the assets of the organization (employee, contractor)."

THEMATIC REVIEWS

SIRC REVIEW: THE "INSIDER THREAT" AND ITS EFFECT ON INFORMATION MANAGEMENT SECTION 54 REPORT

Under section 54(2) of the CSIS Act, SIRC may furnish the Minister with a special report concerning any matter that relates to the performance of its duties and functions.

In the aftermath of high-profile classified documents leaks such as those attributed to WikiLeaks, Edward Snowden and Sub-Lt. Jeffrey Paul Delisle, the "Five Eyes" community has elevated the concern posed by the "insider threat" to a higher level. Intelligence agencies are paying increased attention to the insider threat in order to reduce its potential rate of occurrence and, failing that, to help limit the damage that can be caused by a malicious internal actor.

This review set out to examine the Service's efforts to mitigate insider threats, in particular with respect to information management. SIRC's exploration of the issue began with a survey of policies and procedures guiding access to classified information. SIRC then focused its attention on the components and

operations of CSIS's Internal Security unit, which is responsible for managing the development and implementation of the national security program to protect CSIS, its assets, operations and employees from security threats. Finally, SIRC examined a sample of CSIS's internal investigations regarding suspected security threats and breaches of information.

FINDINGS

Over the past few years, CSIS has internalized a series of principles meant to address potential weaknesses in the storage, transmission and sharing of classified information. Since adopting this new policy regime, SIRC noted that CSIS has supported the needs of Canadian agencies and departments that are not as experienced in security matters, and worked on numerous internal measures aimed at improving the security of Service assets and employees. At the same time, CSIS has worked to fulfil its obligations to allied agencies, particularly with respect to meeting requirements for shared security initiatives. In the end, SIRC found there had been an observable decrease in the number of security violations—especially those concerning information technology—at all of CSIS's facilities.

SIRC also found that CSIS addressed its physical security with the expected level of attention, and reacted appropriately to the violations that take place within its facilities. Of note, during the review period, there was a concerted effort to address some employee concerns regarding the legal foundations of CSIS's search policies. SIRC found that it was reasonable for CSIS employees to expect, and adhere to, a strict regime of physical security.

SIRC also examined CSIS's practices surrounding access lists, the process through which CSIS tracks how sensitive information is accessed and by whom. SIRC found examples of a haphazard application of this process, as well as a lack of documented procedures governing the functioning and maintenance of its access lists. Therefore, **SIRC recommended that CSIS immediately develop robust procedures governing access lists.**

Finally, SIRC examined a sample of CSIS's own internal investigations, which can range from the inadvertent loss of classified information to cases of suspected information leaks. SIRC identified three interrelated issues.

First, SIRC found there was insufficient training, gaps in policy and procedures, and a lack of managerial feedback for employees working on internal investigations. There is a significant difference between the work of an Intelligence Officer, who collects information on national security threats, and that of an Internal Security employee, who conducts internal investigations of former and future colleagues, subordinates and supervisors, all with similar background, training and experience. **SIRC recommended that CSIS create a robust training and mentoring program suited to the unique work of Internal Security employees who are expected to conduct sensitive investigations into suspected violations and/or breaches of security.**

Second, SIRC found there are unsatisfactory thresholds for internal investigations. SIRC noted that the threshold whereby a suspected breach or violation moves from a "fact finding" assignment to an official investigation is unclear and seemingly subjective. Additionally, SIRC noted that policy and procedures governing internal investigations have been unclear and unsystematic; overall, the policy does not provide any practical guidance on what situation warrants the use of a particular investigative tool. **SIRC recommended that CSIS create more detailed policy on the conduct of Internal Security investigations into suspected violations and/or breaches of security.**

Third, SIRC found that CSIS did not maintain proper documentation on decision making surrounding internal investigations. As a result, some files remained incomplete several years after the completion of the investigation, turning any assessment of decision making into a challenging task. **SIRC recommended that CSIS take immediate action to ensure that all decision making pertaining to internal investigations be documented appropriately, in accordance**

with the standard requirements set by Treasury Board guidelines.

SIRC delved into one particular internal investigation as a case study that exemplified the problems cited above. Although a senior executive committee had recommended, in regards to this case, several disciplinary measures and a follow-up investigation, SIRC found the recommendations had not been actioned and saw no documentation to explain the decision making surrounding the case.

After going to great lengths to try to piece together the facts of the case, SIRC found that CSIS had failed to give the case the appropriate level of attention and scrutiny, and to take follow-up action. As a result, **SIRC recommended that CSIS re-examine the original case in its entirety, guided by six specific concerns regarding violations of internal policy and possible information breaches.**

In the end, **the Committee recommended that, in the future, Internal Security should forward final investigation reports to a group outside of its unit for review to help ensure that the investigation is complete, objective and well documented.**

Finally, in light of the serious issues noted, SIRC intends to examine CSIS's internal security activities on a regular basis. The purpose of this undertaking is to evaluate whether internal investigations and other security processes, including the management of sensitive case files, meet with the stringent security practices expected of a modern intelligence agency.

CSIS RESPONSE TO RECOMMENDATIONS:

The Service agreed with SIRC's recommendation to create more detailed policy on the conduct of Internal Security investigations and will undertake a review to clarify definitions, timeliness and techniques. CSIS also agreed to develop clear procedures to ensure that all decision making pertaining to internal investigations is documented appropriately.

CSIS partially agreed with the recommendation pertaining to access lists; while it agreed with the principle of improving the management of access lists, it has a different approach with respect to the implementation. It also partially agreed with the recommendation to create a robust training and mentoring program for Internal Security employees, arguing that while formal Intelligence Officer training is sufficient, there may be an opportunity to review the current informal mentoring process and to develop a guideline document of best practices.

The Service did not agree to re-examine a particular investigation as the Director is satisfied with its outcome and assessed that there were no lingering concerns of an internal security nature. Moreover, CSIS did not agree with the recommendation to forward final investigation reports to a group outside of Internal Security for review due to its belief that third-party review would jeopardize the confidentiality and sensitivity of certain investigations, affect timeliness and objectivity of the investigation, and impede the Director's authority vis-à-vis management of employees.

SIRC REVIEW: CSIS'S INVESTIGATION OF CANADIAN FOREIGN FIGHTERS

In Canada today, as in other allied countries, the threat represented by the foreign fighter phenomenon has risen to the top of the national security agenda. While this has prompted a significant and over-arching government response, CSIS's work and resources have specifically shifted so as to treat this challenge as its top intelligence priority.

The goal of this review was to examine CSIS's investigation of the foreign fighter threat by focusing on targeting, advice to government and information exchanges. The review also examined how CSIS's own strategies, definitions, management processes and governance feed into the whole-of-government approach to the issue. As the review unfolded, however, several significant events occurred that altered the nature and scope of the foreign fighter phenomenon; as a result, this review presents a partial assessment of a broad threat.

The *2014 Public Report on the Terrorist Threat to Canada* placed the travel of Canadian extremists abroad to participate in terrorism-related activities as its first "key terrorism development." Shortly thereafter, the Government indicated it would bring forward "additional measures to strengthen the ability of our security services to monitor aspiring terrorists to, where possible, prevent their return to Canada or to, where that is not possible, give greater tools to be able to charge and prosecute." In 2015, the *Protection of Canada from Terrorists Act* and the *Anti-terrorism Act* (Bills C-44 and C-51) received Royal Assent and became law in Canada.

FINDINGS

The key message that SIRC heard concerning the investigation of foreign fighters was that while the context of this threat is unique—greatly increased volume of potential targets, many more public and partner leads, an almost daily demand for information on the threat—CSIS relied on the same investigative methods, approach and tools as it does for its other investigations.

Still, to better organize and streamline its intelligence collection on this investigation, CSIS undertook an internal realignment. The goal of this initiative was to pool resources, maximize expertise and "burden share" on the broader counter-terrorism file. The Service also outlined new strategic direction, which outlined the range of investigative techniques to be employed, highlighted the need to leverage new foreign partnerships, and stressed the importance of engaging both domestic partners and long-standing foreign allies.

SIRC reviewed a sample of CSIS targets and warrants to better understand the foreign fighter investigation. Indeed, SIRC noted that the Service did not have to "reinvent the wheel" in regards to its methods of collection and investigation. SIRC also found that CSIS implemented targeting authorizations at differing but appropriate times in various investigations and that, overall, CSIS's targeting complied with all relevant legislation, Ministerial Direction and policies. On the issue of warrants, SIRC found that CSIS did not face any specific challenges in obtaining required warrant powers and that it followed internal direction, policies and processes in the application and execution of warrants powers.

SIRC also reviewed CSIS's role within the broader whole-of-government approach to the foreign fighter threat. SIRC noted CSIS's close cooperation with the RCMP, with whom it conducts parallel investigations. SIRC found that CSIS conducts regular and frequent deconfliction meetings with the RCMP on foreign fighter investigations. At the same time, CSIS has engaged in producing a broad range of reports and studies for its partners and clients.

SIRC nonetheless noted challenges that lie ahead for the Service. The most immediate impact of redirecting operational resources to the counter-terrorism threat, and more particularly foreign fighters, is the potential short-term strain on other areas of intelligence collection. While proportionate to government intelligence priorities and direction,

Every year, SIRC reviews one of CSIS's foreign stations. This year, SIRC's foreign station review was not presented as a stand-alone review; rather, the findings fed into two of SIRC's reviews, namely, "CSIS's Investigation of Canadian Foreign Fighters" and "CSIS's Relationship and Exchanges with the Department of Foreign Affairs, Trade and Development."

SIRC heard concerns that this significant operational shift could result in a loss of investigative capacity in counter-intelligence and counter-proliferation areas in the long term.

In relation to the foreign fighter investigation specifically, CSIS continues to seek information to fill intelligence gaps concerning the broad threat. Like its allies, CSIS also continues to debate and assess what category of foreign fighters poses the greater security threat: individuals returning to Canada from active fighting abroad or individuals wishing to travel abroad to engage in terrorist activity but who are denied the means to do so. SIRC found that going forward, CSIS may have to shift its investigative emphasis away from the threat posed by returnees towards the growing number of radicalized Canadians who wish to travel abroad to fight, but are denied the ability to leave the country. In the end, however, the challenges that lie ahead are largely rooted in the need to continually assess the evolving geo-political environment, as well as the nature and scope of the foreign fighter threat.

Consequently, SIRC will need to revisit and review this investigation through several lenses to gain a fuller appreciation of CSIS's work. Next year, SIRC will focus on the overseas facets of CSIS's foreign fighter investigation.

SIRC REVIEW: CSIS'S RELATIONSHIP AND EXCHANGES WITH DFATD SECTION 54 REPORT

SIRC has been examining CSIS's multifaceted relationship with DFATD for years, albeit always within reviews focused on particular CSIS investigations or foreign stations. Indeed, CSIS and DFATD interact on numerous fronts: for example, DFATD facilitates the provision of diplomatic accreditation by host governments for CSIS employees, is consulted by the Service on high-risk operations and foreign arrangements with other security and intelligence services, and is a significant driver and client of CSIS's intelligence products. In sum, DFATD plays an integral role in supporting the Service's security intelligence mandate as it is carried out overseas.

This review examined the recent evolution of CSIS's relationship with DFATD, both overseas and between respective headquarters. One of its key objectives was to confirm whether or not the relationship challenges identified in previous SIRC reviews were isolated. SIRC examined a wide spectrum of CSIS's corporate and operational files, in addition to seeking employee feedback from a survey sent to all of the Service's foreign stations. SIRC also requested that DFATD headquarters provide some perspective on its relationship with CSIS, including the Department's level of satisfaction as a client of CSIS. SIRC is appreciative of DFATD's participation in this voluntary process. The Department's response was of considerable benefit to the review.

In recent foreign station reviews, SIRC has paid close attention to CSIS's cooperation and exchanges of information with DFATD given the importance of this relationship in the context of CSIS's expanding overseas activities. As a number of these reviews noted issues, namely, with respect to potential overlapping initiatives and disclosure commitments, last year, SIRC committed to undertaking a comprehensive examination of this relationship.

FINDINGS

Overall, SIRC found the Service's relationship with DFATD at overseas missions to be positive. Problematic issues have typically been resolved absent the need for high-level managerial involvement. This is a credit to the professionalism exhibited by both CSIS and DFATD employees working abroad who routinely achieve resolutions on what are, in many cases, complex problems. That said, SIRC did identify two key challenges at play in the CSIS-DFATD relationship. In addition, the review identified a possible legal issue concerning some CSIS activities being in contravention of Canadian regulations related to United Nations Security Council (UNSC) resolutions.

In 2007, following a recommendation made by the O'Connor Commission of Inquiry, CSIS and DFATD signed a Protocol concerning cooperation in respect of consular cases involving Canadians detained abroad with national security or terrorism-related implications. The purpose of the Protocol was to help ensure a formalized and systematic approach to information disclosures between DFATD and CSIS.

SIRC found that in some instances, however, disclosures between CSIS and DFATD are not being made in the manner that was intended by the Protocol, owing primarily to divergent legal interpretations regarding the sharing of consular information to assist in national security investigations. SIRC believes that the spectre of the foreign fighter threat requires timely sharing of information between DFATD and CSIS, consistent with the principles outlined in the Protocol. As such, **SIRC recommended that CSIS renegotiate the 2007 Protocol with DFATD in order to reach mutual agreement on issues that have impeded the functionality of the agreement.**

Another issue raised in previous reviews has been the evolving nature of CSIS's relationship with DFATD in light of CSIS's expanding activities abroad. In particular, SIRC noted the tension that has sometimes resulted from DFATD expecting to be forewarned of CSIS's foreign operations versus CSIS's own assessment of how much DFATD needs to know.

Ultimately, SIRC found that there is insufficient operational and/or program deconfliction between the two organizations on certain overseas activities. This situation has developed as the result of the respective foreign activities of CSIS and DFATD gradually outstripping agreement(s) initially designed to help guide the relationship. These agreements help to ensure transparency on activities of mutual interest, so that government priorities are not unintentionally undermined; however, this goal can only be reached if the agreement(s) reflect on-the-ground realities.

As a result of this finding, and especially in light of expanding CSIS's foreign operational footprint, **SIRC recommended the development of clear deconfliction guidelines between CSIS and DFATD where there is the potential for operational and/or program entanglement.** Ideally, this process would first entail high-level discussions between CSIS and DFATD to outline core principles moving forward, and lead to a

The *United Nations Act* (R.S.C., 1985, C. U-2) is a law of the Parliament of Canada that enables the Governor in Council to make such orders and regulations considered necessary to give effect, under Canadian domestic law, to measures that Canada is called upon to apply by the UNSC. The UNSC has over time adopted many resolutions dealing with the threat of terrorism related to Al Qaeda and the Taliban in which it has called on UN member states, such as Canada, to apply measures against these groups. The UNAQTR are Canadian domestic regulations, binding under Canadian law, made pursuant to the *United Nations Act* to give effect to UNSC measures against Al Qaeda and the Taliban.

revamped Memorandum of Understanding that more appropriately addresses the working realities of both organizations.

More importantly, SIRC raised a potential legal concern with respect to CSIS's activities and the *United Nations Al Qaeda and Taliban Regulations* (UNAQTR).

The UNAQTR prohibit specific actions and are explicitly binding on the Crown. Of specific relevance to the review was the prohibition found at section 3 of the UNAQTR governing the provision of funds to prohibited parties, such as persons associated with the Taliban or Al Qaeda. This prohibition is applicable in Canada and to Canadians outside Canada. Therefore, it applies to CSIS, its employees, its human sources in Canada and its Canadian human sources abroad.

In 2013, CSIS raised with DFATD the potential investigative limitations on human source operations stemming from the UNAQTR prohibitions. In its review, SIRC saw no documentation indicating that CSIS had pursued this issue further or that it had reported to the Minister of Public Safety on the possibility of human sources (or CSIS employees) being in contravention of the UNAQTR.

After careful consideration, SIRC made two findings. First, SIRC found that CSIS lacked a procedure to systematically verify whether the human source operations it conducts against Al Qaeda and Taliban threats are in contravention of the UNAQTR. Second, SIRC found that CSIS cannot systematically attest as to whether or not its past human source operations have already violated the UNAQTR. As a result, **SIRC recommended that CSIS put in place formal internal mechanisms to ensure that none of its human source operations are in contravention of the UNAQTR or any similar Canadian statute or regulations.**

Furthermore, SIRC felt that CSIS needed to examine the full scope of potential violations. The Committee, as per paragraph 40(1)(a) of the *CSIS Act*, directed the Service to conduct a review of the specific activities involving compliance with Canadian laws and regulations implementing measures, decisions, resolutions or recommendations of an international organization of states of which Canada is a member. Once completed, the findings of this report should be included within the CSIS Director's annual report to the Minister of Public Safety.

SIRC will examine the methodology and findings of CSIS's review and provide an assessment both to the Minister of Public Safety in its certification process and to Parliament in its subsequent annual report. SIRC will also take whatever follow-up action it deems necessary to ensure satisfactory resolution of this issue.

Paragraph 40 (1)(a) of the *CSIS Act* states that for the purpose of ensuring that the Service's activities are carried out in accordance with the *CSIS Act*, its regulations and Ministerial Direction, and do not involve any unreasonable or unnecessary exercise of the Service's powers, SIRC may direct the Service to conduct a review of specific activities and to provide a report of the review to the Committee. SIRC's last request to CSIS of this nature dates back to the early 1990s.

CSIS RESPONSE TO RECOMMENDATIONS:

The Service partially agreed with the recommendation to renegotiate the 2007 Protocol with DFATD, stating that it regularly engages with DFATD senior management to ensure timely discussions and agreements on information exchanges and emerging issues. CSIS will, nonetheless, discuss the functionality of the Protocol with DFATD. CSIS also partially agreed with the recommendation to develop deconfliction guidelines; it will participate in regular meetings with DFATD at all levels to discuss specific issues where existing deconfliction processes may not be adequate. Finally, the Service agreed to update its human source protocols to include regular verification that human source operations are not in contravention of any Canadian statute or regulation. CSIS will report on the specified section 40 (1)(a) review in the 2015–2016 Director's annual report to the Minister.

PROGRAM/ INVESTIGATION REVIEWS

SIRC REVIEW: A COUNTER-TERRORISM INVESTIGATION

Every year, SIRC carries out a focused review of one of CSIS's investigations. This year, SIRC undertook a comprehensive review of an investigation into a terrorist organization that appears to represent an escalating threat: the review's point of departure was the realignment of CSIS's investigation from one centred on fundraising and propaganda activities in Canada, to one focused increasingly on individuals in Canada with connections to the operational threat posed by this organization.

SIRC sought to assess how the Service had positioned itself to meet this evolving threat, to identify and explore challenges associated with the investigation and its realignment, as well as examine the accompanying increase in information sharing and cooperation with foreign partners. To better understand the nature and scope of the threat, SIRC examined more closely one region's investigative activities. In so doing, SIRC sought to gain greater insight into some of the operational challenges of the investigation from a regional perspective, but also to validate whether CSIS regional offices share those challenges identified from a strategic standpoint.

FINDINGS

Overall, SIRC found the investigation was run soundly and was focused on threats having a nexus to Canada. Moreover, CSIS's operational activities were reasonable and proportional to the threat.

To bridge the knowledge gap created by the realignment, CSIS has worked closely with its foreign partners. SIRC found the information CSIS received from its foreign partners to be of value; this information has proven useful for planning operations as it

Every year, SIRC devotes at least one of its reviews to an in-depth examination of a particular CSIS investigation—whether counter-terrorism, counter-intelligence or counter-proliferation. This kind of review provides SIRC with profound insight into various facets of a single investigation, and also allows for a valuable longitudinal assessment of the investigation.

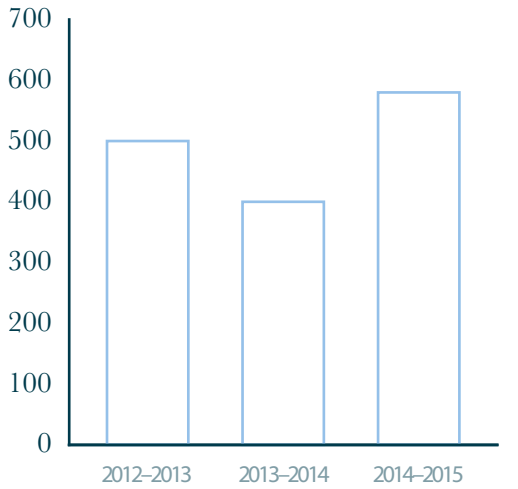
has helped CSIS to mitigate some potential risks, thereby enhancing the safety and security of both sources and handlers. CSIS has also engaged in joint operations with some of these partners. While joint operations have contributed to CSIS's understanding of the threat, they have also come with some challenges. SIRC explored this aspect of the investigation by examining all operational exchanges with one particular foreign partner. SIRC found that the Service exercised due caution when seeking information on individuals who were themselves not directly associated with threat activity.

SIRC also examined human source files from different CSIS regional offices and found that CSIS's activities were authorized, necessary and reasonable. However, in the case of one human source, SIRC noted that a regional desk withheld relevant information from a risk assessment for an operation abroad.

CSIS human sources may travel abroad for varying amounts of time to collect information, and such travel always requires approval. In all the files reviewed by SIRC, CSIS adhered to relevant policies and procedures. In one file, however, SIRC could not understand why the specific advice of an expert

TARGETING

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



group was not heeded in a decision related to source safety.

In response to SIRC's questions, the regional office indicated that it was privy to sensitive operational information that it did not share nor include in the request for approval. The requirement to consult with experts ensures the assessment, and possible mitigation, of operational risks. It is extremely difficult for an expert unit to provide complete and relevant advice if that advice is based on incomplete information. SIRC's initial finding was that the regional office had undermined the integrity of the risk assessment on this operation by withholding information directly relevant to operational security.

SIRC was subsequently informed that consultation had in fact taken place and that, in the end, a compromise had been reached. SIRC believes that recording

the decision making or rationale for choosing not to follow expert advice would be beneficial, both from a case-management perspective and from an internal risk-management perspective. Accordingly, **SIRC recommended that CSIS procedures include a requirement to record the justification(s) for the acceptance or dismissal of internal expert advice acquired through mandatory consultation.**

CSIS RESPONSE TO RECOMMENDATION:

The Service agreed with SIRC's recommendation to record decision making surrounding the acceptance or dismissal of internal expert advice and will update its procedures accordingly.

SIRC REVIEW: CSIS'S SECTION 16 PROGRAM

Under section 16 of the *CSIS Act*, "CSIS may, in relation to the defence of Canada or the conduct of international affairs of Canada, assist the Minister of National Defence or the Minister of Foreign Affairs, within Canada, in the collection of information relating to the capabilities, intentions or activities of any foreign state" – commonly referred to as "foreign intelligence." In past years, SIRC has touched on CSIS's section 16 activities in a few reviews; however, it has been five years since SIRC has taken a comprehensive look at the section 16 program.

This review examined several facets of CSIS's section 16 activities, including government direction, requests for assistance, prioritization, collection, record keeping and dissemination. The review took an in-depth look at a sample of section 16 investigations to assess compliance with the *CSIS Act*, Ministerial Direction and policy. SIRC also assessed the Service's overall management processes and governance of its section 16 program, as well as its advice to government through reporting and feedback from clients.

FINDINGS

In recent years, the Government made several changes to the section 16 process to coordinate and streamline intelligence requirements, priorities and collection. In 2014, CSIS officially changed its section 16 procedures to come into line with those changes. SIRC found the new changes to CSIS's foreign intelligence function have improved not only the process for requesting collection, but also the relevance and utility of the information collected. Overall, SIRC was satisfied with the governance of CSIS's section 16 program.

In recent reviews that have touched on section 16 activities, SIRC commented on what it viewed as an increasing overlap between sections 12 and 16 collection. Specifically, SIRC's analysis was that the lines of distinction between the two distinct legislative mandates were becoming blurred. As a result, SIRC made recommendations to CSIS to further demarcate collection for security intelligence and foreign intelligence. Since that time, the changes CSIS has brought to its section 16 process have resulted in a clearer distinction between sections 12 and 16 collection.

SIRC's examination of a sample of section 16 targets showed that the more centralized process contributed to ensuring that collection was reasonable and efficient. The intelligence collected aligned with, and responded to, the wider government intelligence priorities and requirements, and reflected CSIS's capacity to collect. Overall, SIRC found that the reporting associated with the targets it reviewed complied with collection requirements and the terms of the Federal Court warrants.

SIRC REVIEW: CSIS'S COUNTER-PROLIFERATION STRATEGY

The proliferation and use of weapons of mass destruction (WMD) is an issue of international concern that has received considerable public attention over the past few years. The use of chemical weapons against civilians in Syria and Iran's continued attempts to build a nuclear weapons capacity have dominated press coverage and public discussion on this important issue.

The Government has a policy objective of non-proliferation and the elimination of all nuclear, chemical and biological weapons. To this end, Canada is committed to upholding its obligations under existing multilateral regimes intended to restrict trade in nuclear, chemical and biological weapons and to monitor their civil applications. Through these regimes, member states use cooperative and coercive measures to achieve non-proliferation and counter-procurement objectives, including the enactment of laws and the implementation of procedures to control the export and transport of materials and technology used in the development of WMD. Accordingly, the Government has identified the detection and investigation of proliferation activities with a link to Canada as an intelligence priority.

The objective of this study was to review the Service's investigation of proliferation/procurement attempts by state and non-state actors, its relationships with domestic and foreign partners, and CSIS's advice to government on proliferation and issues relating to chemical, biological, radiological and nuclear weapons.

FINDINGS

In April 2004, the UNSC adopted Resolution 1540 requiring all states to develop and maintain appropriate effective border controls and law enforcement efforts to detect, deter, prevent and combat illicit trafficking and brokering in nuclear, chemical or biological weapons, their means of delivery and related materials. The UNSC then strengthened its call for the implementation of strong export controls in April 2006 with Resolution 1673.

Yet, Canada does not have a national coordinating structure for counter-proliferation efforts. Indeed, the absence of a formal, coordinated structure involving all relevant Canadian government departments and agencies was identified recently by stakeholders as a challenge to implementing the directives enshrined in UNSC Resolutions 1540 and 1673. SIRC believes that a coordinated government strategy on counter-proliferation would be highly beneficial for CSIS and its partners.

SIRC noted that counter-proliferation investigations come with some substantial challenges. SIRC identified two main challenges that influenced how the case studies SIRC examined were carried out: managing joint operations with foreign partners of varying capabilities and priorities; and balancing risk with intelligence benefit.

Overall, SIRC found that CSIS has worked, and continues to work, at maintaining cooperative relationships with domestic and foreign partners on counter-proliferation issues and at finding an acceptable balance between risk and reward in its counter-proliferation investigations. SIRC also found that CSIS followed internal direction, policies and processes in preparing its advice to government, and that the advice represented an accurate reflection of the threat.

BASELINE REVIEW

SIRC REVIEW: CSIS'S USE OF METADATA

The use of metadata by intelligence agencies has received considerable scrutiny following Edward Snowden's revelations. In the United States, engagement on metadata and associated topics has implicated all levels of government, extending all the way to the Presidency. In Canada, public and media reaction has been more muted. Nevertheless, there has been a marked upswing in interest on issues related to metadata, especially among parliamentarians, advocacy groups and scholars.

Although much of the public discussion has focused on Canada's signals intelligence agency's metadata also being used by CSIS, SIRC first had to define the scope of its review in such a way as to be both manageable and meaningful. Accordingly, it chose to define the parameters of its review using CSIS's own definition of metadata, which is "information collected via section 21 warrant that is associated with a communications event in order to identify, describe, manage or route that communication event or the means of its transmission, but excludes any information which could reveal the purport of the communications event, or the whole or any part of its content."

This review marked the Committee's first focused examination into the scope of CSIS's collection and use of metadata, as well as the authorities and accountability structures that exist to guide metadata collection, use and retention. SIRC selected two specific uses of metadata for analysis. In both cases, SIRC sought to determine whether the Service's collection, use and retention of metadata were carried out lawfully and appropriately. SIRC also reviewed discussions between CSIS's legal services and the Federal Court of Canada, and examined warrants and the execution of warrant powers in which metadata was collected.

"Metadata" is a relatively broad term that, in the context of communications, refers to information about a communications "event" that does not include the actual content of the communication. In principle, for virtually every piece of transmitted data, there is an associated "metadata" component.

FINDINGS

The study first examined the use of metadata collected as part of the Service's communications intercepts to support the Service's larger data exploitation program. SIRC paid attention to early Service discussions on whether the standard warrant conditions allowed for the long-term retention and use of metadata. The Service's initial assessment was that, though warrants did not place any restrictions on the Service's ability to retain intercepted communications of targets, warrant conditions required that any communication of a person other than the target(s), collected incidentally, presumably including the metadata, be destroyed.

At the same time, however, warrant conditions allowed for the retention of incidentally collected communications if a determination was made that they "may assist" in the investigation of a threat to the security of Canada. The Service concluded that "may assist" amounted to a low threshold for the retention of communications; accordingly, the metadata of communications intercepts was retained and used.

Eventually, the Service proposed changes to the wording of the warrant conditions to bring the warrant language and its metadata use and retention practices into better alignment; in effect, rendering the warrant conditions silent on questions of metadata use and retention. During a warrant application before the Federal Court in late 2011, when the matter of the wording change was raised, CSIS legal services did make reference to the retention of metadata. However, SIRC was given no indication that the Service was fully transparent with the Federal Court about the nature and scope of its activities with respect to metadata in the context of that discussion. SIRC, on the other hand, was of the view that the Court has a general interest in how the Service uses the intelligence, including metadata, collected under the authority of a warrant.

SIRC's view was informed by the fact that the Service's use of metadata in this context is distinct from how intercept communications are traditionally used to support investigations in a number of specific ways, all strongly suggesting that metadata is deserving of specific mention in warrant applications as a specific "type of information" proposed to be obtained through the warrant power. **SIRC therefore recommended that the Service make the Court aware of the particulars of the Service's retention and use of metadata collected under warrant.**

Second, the review examined a CSIS program that makes use of specialized surveillance technology and associated CSIS tradecraft against targeted individuals. The operational outcome of these surveillance activities can result in the collection of metadata from warranted targets. SIRC was satisfied that the Service has taken an appropriately cautious approach on the use of this technology.

In addition to the legal considerations explored during the review, SIRC also examined the operational utility of this program and found that, overall, CSIS lacked precise data on the program's efficiency and effectiveness. As a result, **SIRC recommended that CSIS further enhance feedback on the utility of these surveillance operations, and based on these findings, that it produce an updated internal assessment to help guide the future direction of this program.**

Finally, this review provided SIRC with an in-depth glimpse into the Service's data exploitation and data acquisition activities—a trend visible across all allied intelligence agencies. For its part, CSIS believes that by harnessing available data through advanced analytics, it will increasingly be able to predict the behaviour of targets, generate new investigative leads, uncover networks, and make more informed decisions regarding the placement of surveillance resources, among other investigative benefits. Given the continuing importance of this subject, the Committee will look more thoroughly at data exploitation and data acquisition in the next research cycle to assess whether collection is done "to the extent that is strictly necessary," as set out in section 12 of the *CSIS Act*.

TABLE 1 WARRANTS

On an annual basis, SIRC selects a sample of CSIS warrants from which to examine the entire warrant process—application, approval and execution—*ex post facto*.

WARRANTS	2012-2013	2013-2014	2014-2015
New warrants	71	85	104
Replaced or supplemental	189	178	181
Total	**260**	**263**	**285**

CSIS RESPONSE TO RECOMMENDATIONS:

The Service did not agree with SIRC's recommendation to advise the Federal Court of activities relating to metadata collected under warrant. CSIS's position is that section 21 of the *CSIS Act* does not confer any general supervisory authority to Federal Court judges, therefore, it believes that SIRC's recommendation was both inappropriate and unwarranted. Moreover, the Service maintains that its position on the issue in question was communicated clearly and transparently to the Federal Court during a warrant application in December 2011. CSIS did agree to enhance feedback on the utility of certain surveillance operations by developing processes and procedures to ensure that they are standardized, comprehensive and value-added.

In its 2013–2014 CSIS foreign station review, SIRC had found that CSIS was not utilizing as many of the available techniques to validate intelligence collected overseas as it could and should, especially when operating in more secure overseas locations. SIRC was pleased to note that, a year later, CSIS had made progress in this regard.

CORE REVIEW

SIRC REVIEW: CSIS'S FOREIGN-BASED HUMAN SOURCES

CSIS operations abroad have become an integral part of its activities, and the recruitment and development of foreign-based human sources is at the leading edge of this work. These human sources often have little or no connection to Canada, but they are nevertheless tasked, managed and paid by CSIS. Indeed, foreign-based human sources are covered by the same policy framework as domestic-based human sources.

The purpose of this study was twofold: first, to undertake a comprehensive assessment of the Service's foreign-based human source program, and second, to develop an appreciation of the program's contribution to the Service's overall intelligence collection and production. To this end, SIRC examined the accountability and policy frameworks in place to guide the management of these sources. In addition, SIRC reviewed a sample of foreign-based human sources to assess CSIS's case and information management; this assessment comprised an examination of the Service's use of validation techniques, risk assessment and compensation, as well as the collection, reporting and dissemination of information obtained from these sources.

FINDINGS

SIRC examined the policies and procedures that apply to the management of CSIS's human source program and their specific application in the context of several different operations. Overall, SIRC found that the Service's accountability framework in the area of human source management was sound. SIRC also concurred with the Service's decision to develop a series of policies and procedures that apply to all human sources, regardless of location. In SIRC's view, these policies and procedures provide employees with clear guidance and establish processes that support CSIS in fulfilling its obligations under the *CSIS Act*, complying with relevant Ministerial Direction and meeting the Government's intelligence priorities.

On the issue of case management, SIRC found the Service had recently implemented a new initiative to increase the use of validation techniques for both foreign and domestic human sources. Furthermore, SIRC found the Service had clear definitions, as well as qualitative and quantitative criteria, to help ensure that a source's relationship with the Service and reporting history were accurately and consistently described throughout CSIS records. Finally, SIRC's review of several individual source operations revealed that, in those cases, CSIS made use of the validation tools available to it and, in particular, in the event that circumstances brought the source's credibility into question.

With respect to other elements of case management, SIRC found that the Service's activities were, on the whole, reasonable and necessary. SIRC did identify an issue with respect to the approval process for an operation involving a human source. On the basis of the risks identified by CSIS, SIRC is of the opinion that this operation posed a risk to life and, therefore, should have been subject to a risk-assessment process as required by their internal process. This would have involved a more detailed evaluation of all the risks associated with the operation, particularly with respect to the risk to the source's personal safety. Ultimately, however, SIRC concurred with the Service's rationale for conducting this operational activity.

SIRC was also concerned about the Service's process for recording contact between CSIS employees and human sources. SIRC believes that this policy is particularly important in operations outside Canada, where there can be an increased risk to life and greater potential for controversy. Although, in most cases, SIRC found documentation showing that CSIS was complying with this policy, in other cases, SIRC could not completely verify adherence to the policy.

SIRC's review also included an examination of CSIS's management of information. This involved a review of the collection, analysis, retention and dissemination of information obtained from the foreign-based human sources in the review sample. With only a few exceptions, SIRC found the information collected pertained to specific government intelligence priorities, the information disseminated was consistent with operational reporting and the source of the information was described in a manner consistent with relevant case-management documentation and the source's access to the information in question.

SIRC'S INQUIRY INTO CSIS'S COLLECTION OF CANADA REVENUE AGENCY INFORMATION REQUEST BY CSIS DIRECTOR

In a letter sent in August 2014, the CSIS Director notified SIRC's Interim Chair of an incident involving a CSIS Intelligence Officer who obtained taxpayer information from the Canada Revenue Agency (CRA) without a Federal Court warrant. Questions regarding the authority under which the taxpayer information was collected were first raised by the Federal Court when the information in question was used in a warrant application. In response, CSIS requested that SIRC review the circumstances surrounding the incident and make recommendations as necessary and appropriate to militate against Service employees obtaining information in this manner in the future.

For the Service to make a request of this nature to SIRC is exceptional. Although there are no provisions in the *CSIS Act* through which the Service can compel SIRC to undertake a review, the Committee agreed to conduct an inquiry into the incident and to issue a report of its findings to the CSIS Director.

SIRC'S INQUIRY

SIRC's examination yielded two principal findings. The first finding was that this was not an isolated incident of a single Intelligence Officer obtaining information improperly from CRA. In fact, SIRC found there were multiple instances of a particular CSIS office obtaining information from CRA absent a

warrant. Secondly, SIRC found that, overall, the management of this incident was not adequate as those charged in CSIS with briefing SIRC, and who were responsible for "coordinating and reviewing" the response, have acknowledged operating under the assumption that this was an isolated event until SIRC apprised them of its findings.

Moreover, following the incident, the Federal Court and the Minister of Public Safety were advised that all of the CRA information obtained absent a warrant had been deleted from the operational database. In fact, most of the information remained within the database until brought to CSIS's attention by SIRC.

These findings suggest numerous internal-to-CSIS issues that SIRC assessed fell outside the scope of its inquiry. At the same time, the Committee strongly felt that CSIS should consider looking carefully at its management of the incident.

To that end, **SIRC made several recommendations, namely, that the CSIS Audit Unit address any substandard managerial and communication practices by the CSIS regional office in question; that CSIS conduct a post-mortem to assess the adequacy of its management of the incident once it became known that the information in the warrant application had been improperly collected; and that CSIS clarify the scope of the incident to the Federal Court and the Minister of Public Safety. Finally, SIRC recommended that CSIS advise the Privacy Commissioner of this incident.**

The Committee determined it was not able to make recommendations aimed at preventing such a future occurrence because SIRC was not provided with any explanation to account for the full scope of the improper collection of taxpayer information. Therefore, though the immediate action taken by the CSIS Executive—to issue a stern reminder to all employees of the need for a warrant to collect taxpayer information—was appropriate in the circumstances, it may not be sufficient. SIRC does suggest that CSIS look carefully at what additional measures could be taken in the training and development of Intelligence Officers to impress upon them the need to be alert to the various activities that require judicial authorization.

Finally, a prudent model moving forward may be for CSIS to conduct an internal review of the flow of information from CRA every five years to ensure proper conduct regarding the sharing of taxpayer information. The Committee considers that, if the sharing of taxpayer information from CRA to CSIS is put on a new footing as a result of the new *Security of Canada Information Sharing Act*, a routine audit of those activities through a renewed memorandum of understanding could be even more important.

CSIS RESPONSE TO RECOMMENDATIONS:

The Service agreed with the spirit of the recommendation to conduct an audit of the CSIS office in question. CSIS believes that the actions it has taken since the discovery of the incident were similar to those that would have been taken during an audit, namely, to ask whether the policies in place at the time were adequate and whether employees followed those policies. CSIS also agreed to conduct a post-mortem of the incident with respect to the issues identified by SIRC, and has provided a copy of the report to the Committee. Along the same lines, CSIS stated that it has taken steps to make its compliance reporting regime more robust so as to advise senior management and appropriate policy centres of any compliance issues in a more timely manner.

The Service also agreed with the recommendation to clarify the scope of the incident to the Federal Court and the Minister of Public Safety; in the interest of full transparency, CSIS will advise the Court of additional details pertaining to the incident to ensure that the Court has a full understanding of the events. Finally, CSIS has advised the Privacy Commissioner of the incident.

INVESTIGATIONS

SIRC's investigations are conducted using a quasi-judicial process. Once SIRC takes jurisdiction over a complaint, the complainant becomes a party to a litigation process in which CSIS, and sometimes the deputy head of a government department, are involved as respondents. Usually, the complainant, his witnesses, as well as government witnesses, will testify and be cross-examined in a hearing presided over by a SIRC Committee Member. Classified documentation and testimony is heard by the presiding Member in the absence of the complainant. An investigation may take up to 30 months.

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

THE INVESTIGATION PROCESS AT SIRC

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

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

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

Pre-hearing conferences are conducted with the parties to establish and agree on preliminary procedural matters, such as the allegations to be investigated, the format of the hearing, the identity and number of witnesses to be

HOW SIRC DETERMINES JURISDICTION OF A COMPLAINT

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

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

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

Under section 42 of the *CSIS Act*, SIRC shall investigate complaints from:

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

These types of complaints must be filed within 30 days of the denial of the security clearance. SIRC may extend this period if valid reasons are presented.

called, the disclosure of documents in advance of the hearing and the date and location of the hearing.

The time to investigate and resolve a complaint will vary in length depending on a number of factors, such as the complexity of the file, the quantity of documents to be examined, the number of hearings days required, the availability of the participants and the various procedural matters raised by the parties.

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

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

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

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

Table 2 provides the status of all complaints directed to SIRC over the past three fiscal years, including complaints that were misdirected to SIRC, deemed to be outside SIRC's jurisdiction, or investigated and resolved without a hearing.

SIRC INVESTIGATION: DENIAL OF A SECURITY CLEARANCE

SIRC investigated a complaint under section 42 of the *CSIS Act* regarding the denial of a top secret security clearance as a result of an assessment by CSIS that brought into question the complainant's loyalty and reliability as it related to loyalty. Prior to making its decision, the Department afforded the complainant the opportunity to provide any additional information relevant to the denial recommendation, but the complainant did not avail himself of this opportunity.

Upon completion of the Department's internal security clearance process, the Deputy Head informed the complainant that he had been denied a security clearance at any level, including a reliability status, based on the findings of the investigation that had identified concerns with the complainant's associations and activities deemed to be incompatible with holding a security clearance; as such, the complainant could not be employed by the Department.

SIRC found that the information with respect to the complainant's loyalty was not supported by the evidence. Furthermore, SIRC was not persuaded that the complainant had been unforthcoming during his interviews with the Service or was lacking candour when he testified before the Committee.

Still, SIRC ultimately found that, based on other evidence before it, the denial of the complainant's security clearance was warranted under the Policy of Government Security and the Personnel Security Standard. SIRC found there were reasonable grounds to question the complainant's reliability as it related to loyalty given his behaviour and features of character, which were incompatible with holding a security

TABLE 2 COMPLAINTS DIRECTED TO SIRC

	2012-2013	2013-2014	2014-2015
Carried over	22	24	20
New	17	9	23
TOTAL	**39**	**33**	**43**
Closed*	15	13	13

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

clearance. As such, SIRC recommended the decision of the Deputy Head to deny the security clearance at any level be upheld.

SIRC also noted there was a recording malfunction during one of the interviews between the Service and the complainant. In this regard, the Committee referred to a recommendation it made in 2012, namely, that CSIS issue a direction to all its regional offices requiring that investigators take recording devices to all immigration interviews and that they ensure that such devices are in working order. SIRC encouraged the Service to do the same in relation to security screening interviews, as was the case here, if it had not already done so.

SIRC INVESTIGATION: DENIAL OF A SECURITY CLEARANCE

SIRC investigated a complaint under section 42 of the *CSIS Act* in which the complainant was denied a security clearance at any level, including reliability status. The Deputy Head's decision was based on investigations carried out both by the Service and the Department, which identified concerns with the complainant's associations with a foreign intelligence service that are not compatible with holding a security clearance.

SIRC found the Deputy Head had reasonable grounds to deny the complainant a security clearance pursuant to section 2.8 of the Personnel Security Standard. Furthermore, SIRC was satisfied the complainant was afforded procedural fairness during both the CSIS screening investigation and the Department's security screening review process as he was informed of the security concerns relating to him and was given an opportunity to respond to the concerns.

SIRC also rejected the complainant's allegation regarding the conduct of the CSIS interviewer during one of the interviews. SIRC's review of the interview tapes found the CSIS interviews to be cordial and the Service interviewer to be professional.

SIRC also noted that security interviews are an important part of the security clearance process. For this reason, it is of the utmost importance that applicants be forthcoming and truthful in their responses since it is their only opportunity to provide clarification on issues of concern to the Service.

Lastly, SIRC was satisfied with the accuracy of the information upon which the Deputy Head relied to make his decision. The complainant's features of character, namely, his lack of candour and honesty, as well as his evasiveness, were incompatible with holding a security clearance under the Policy of Government Security and the Personnel Security Standard. For those reasons, the Committee recommended the decision of the Deputy Head to deny the security clearance at any level be upheld.

SIRC INVESTIGATION: DENIAL OF A SECURITY CLEARANCE

SIRC investigated a complaint under section 42 of the *CSIS Act* regarding the denial of a secret-level security clearance. The complainant, who was working in his position prior to having obtained his secret-level security clearance, was informed by the Deputy Head that his security clearance was denied due to adverse information discovered during the investigation phase. A few days later, the complainant was informed that the denial of the security clearance led to a termination of his functions.

Following its investigation, SIRC found that there were reasonable grounds to question the complainant's reliability as it related to loyalty. In this respect, the complainant could act, or be induced to act, in a way that would constitute a threat to the security of Canada. For these reasons, SIRC found that, in accordance with the Personnel Security Standard and the information at his disposition, the Deputy Head had reasonable grounds to deny the complainant a secret-level security clearance. The decision taken by the Deputy Head was reasonable in the circumstances

and was made in accordance with the Government Security Policy, the Personnel Security Standard and the *CSIS Act*.

Accordingly, the Committee recommended that the denial of the security clearance be maintained. With respect to the fact that the individual had been in his position prior to obtaining the required security clearance, the Committee did not make a recommendation in this regard as it fell outside of its jurisdiction.

SIRC INVESTIGATION: DENIAL OF CSIS SITE ACCESS SECURITY CLEARANCE

SIRC investigated a complaint under section 41 of the *CSIS Act* in which the complainant was denied Site Access Certification at a CSIS location. The CSIS Site Access Certification program, which has been implemented across all CSIS regional offices, is designed for vetting potential contractors or employees of contracted companies who require access to CSIS facilities. The complainant, who possessed a federal government secret-level clearance, had previously been granted access to the CSIS location to conduct contractual work following his initial application, but was denied in the two following years.

SIRC found that CSIS did not consider all relevant information in its holdings in processing the complainant's later Site Access Certification applications. SIRC also found that the complainant should have been granted Site Access Certification. Lastly, SIRC found that the Service did not initially produce all relevant witnesses and information at the outset of the investigation.

SIRC recommended that the complainant's next Site Access Certification application be granted unless any adverse information regarding the complainant came to light. **The Committee also recommended that a new Site Access Certification direction, which was adopted by the CSIS regional office in question, be implemented in all regional offices with the required modifications. Finally, the Committee recommended that the CSIS Site Access Certification program be reviewed in light of the new Treasury Board Secretariat's Standard on Security Screening.**

CSIS RESPONSE TO RECOMMENDATIONS:

The Service agreed to implement the new Site Access Certification direction in all CSIS regional offices and to review the Site Access Certification program in light of the new Standard on Security Screening.

SIRC INVESTIGATION: ALLEGATION OF HARASSMENT, DISCRIMINATION AND PROFILING

SIRC investigated a complaint pursuant to section 41 of the *CSIS Act* in which the complainant alleged that he had been the victim of harassment, discrimination and profiling following three interviews by CSIS agents. In its response to the complainant, the Service indicated that to fulfill its mandate, CSIS regularly meets with members of the public, and that its agents had acted in a professional manner within the authority of their mandate in conducting the three meetings with the complainant.

Following its investigation, the Committee found that the complainant had not been the subject of harassment, discrimination or profiling by CSIS. The Committee concluded that the allegations were without merit and that the CSIS agents had acted in accordance with the *CSIS Act*, Ministerial Direction and relevant CSIS policies.

SIRC AT A GLANCE

COMMITTEE MEMBERSHIP

SIRC is chaired by the Honourable Pierre Blais, P.C. The other Committee Members are the Honourable L. Yves Fortier, P.C., C.C., O.Q., Q.C., the Honourable Gene McLean, P.C., the Honourable Ian Holloway, P.C., C.D., Q.C., and the Honourable Marie-Lucie Morin, P.C.

STAFFING AND ORGANIZATION

SIRC is supported by an Executive Director and an authorized staff complement of 17, located in Ottawa. This includes a Deputy Executive Director, Director of Research, Senior Counsel, Senior 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 SIRC staff also visit CSIS regional offices to understand and assess the day-to-day work of investigators in the field. These visits give SIRC an opportunity to be briefed by regional CSIS staff on local issues, challenges and priorities. They also provide an occasion for SIRC to communicate its focus and concerns.

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

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

TABLE 3 EXPENDITURES

Program	2013-2014 Expenditures	2014-2015 Forecast Spending	2014-2015 Actual Spending	2015-2016 Planned Spending
Reviews	1,053,600	1,362,200	1,296,000	1,325,400
Investigations	513,800	682,900	742,800	771,300
Subtotal	1,567,400	2,045,100	2,038,800	2,096,700
Internal Services*	1,333,900	741,700	941,300	780,700
Total	**2,901,300**	**2,786,800**	**2,980,100**	**2,877,400**

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

SIRC ACTIVITIES

April 2014: The Executive Director gave a presentation to the Armed Forces Communications and Electronics Association "Lunchtime Speaker Series" in Ottawa.

May 2014: The Executive Director and senior staff met with a delegation of senior intelligence officials from an allied country to discuss Canada's model of security intelligence accountability.

May 2014: The Executive Director and senior staff gave a presentation on SIRC's work to a delegation of American Congressional fellows.

June 2014: The Executive Director gave a presentation about SIRC to delegates assembled for the Evanta CISO Conference in Vancouver.

August 2014: The Committee met with a number of CSIS's domestic partners during a visit to CSIS's Atlantic Region office in Halifax.

September 2014: The Executive Director gave a presentation about SIRC to Ryerson University students in the context of the "Career Conversations Talk" series.

October 2014: The Executive Director gave a presentation at the Annual Meeting of the Federal, Provincial and Territorial Privacy and Information Ombudspersons and Commissioners, which was held under the theme "Protect and Promote Canadians' Access and Privacy Rights in the Era of Digital Government."

October 2014: SIRC's Senior Counsel and Director of Research gave a presentation on SIRC's role and activities to a group of Cégep Édouard-Montpetit students participating in their "SPY" project.

December 2014: SIRC's Senior Counsel and Director of Research gave a lecture to a group of students registered in an intelligence course at the Université de Sherbrooke.

December 2014: The Executive Director and senior staff met with the United Kingdom's Independent Reviewer of Terrorism Legislation, Mr. David Andersen, to discuss SIRC's review and investigation activities.

March 2015: The Executive Director appeared before the Standing Senate Committee on National Security and Defence in its study of Bill C-44.

LIST OF SIRC RECOMMENDATIONS

DURING THE 2014–2015 FISCAL YEAR, SIRC MADE THE FOLLOWING RECOMMENDATIONS.

REPORT	RECOMMENDATION
The "Insider Threat" and its Effect on Information Management	SIRC recommended that CSIS immediately develop robust procedures governing access lists. SIRC recommended that CSIS create a robust training and mentoring program suited to the unique work of Internal Security employees who are expected to conduct sensitive investigations into suspected violations and/or breaches of security. SIRC recommended that CSIS create more detailed policy on the conduct of Internal Security investigations into suspected violations and/or breaches of security. SIRC recommended that CSIS take immediate action to ensure that all decision making pertaining to internal investigations be documented appropriately, in accordance with the standard requirements set by Treasury Board guidelines. SIRC recommended that CSIS re-examine an original case in its entirety, guided by six specific concerns regarding violations of internal policy and possible information breaches. SIRC recommended that, in the future, Internal Security should forward final investigation reports to a group outside of its unit for review to help ensure that the investigation is complete, objective and well documented.

CSIS's Relationship and Exchanges with DFATD	SIRC recommended that CSIS renegotiate the 2007 Protocol with DFATD in order to reach mutual agreement on issues that have impeded the functionality of the agreement. SIRC recommended the development of clear deconfliction guidelines between CSIS and DFATD where there is the potential for operational and/or program entanglement. SIRC recommended that CSIS put in place formal internal mechanisms to ensure that none of its human source operations are in contravention of the UNAQTR or any similar Canadian statute or regulations.
A Counter-Terrorism Investigation	SIRC recommended that CSIS procedures include a requirement to record the justification(s) for the acceptance or dismissal of internal expert advice acquired through mandatory consultation.
CSIS's Use of Metadata	SIRC recommended that the Service make the Court aware of the particulars of the Service's retention and use of metadata collected under warrant. SIRC recommended that CSIS further enhance feedback on the utility of specific surveillance operations, and based on these findings, that it produce an updated internal assessment to help guide the future direction of this program.
SIRC's Inquiry into CSIS's Collection of Canada Revenue Agency Information	SIRC recommended that CSIS Audit Unit address any substandard managerial and communication practices by the CSIS regional office in question. SIRC recommended that CSIS conduct a post-mortem to assess the adequacy of its management of the incident once it became known that the information in the warrant application had been improperly collected. SIRC recommended that CSIS clarify the scope of the incident to the Federal Court and the Minister of Public Safety. SIRC recommended that CSIS advise the Privacy Commissioner of this incident.
Denial of CSIS Site Access Security Clearance	SIRC recommended that a new Site Access Certification direction, which was adopted by the CSIS regional office in question, be implemented in all regional offices with the required modifications. SIRC recommended that the CSIS Site Access Certification program be reviewed in light of the new Treasury Board Secretariat's Standard on Security Screening.

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