ANNUAL REPORT
2015-2016

maintaining MOMENTUM

SECURITY INTELLIGENCE
REVIEW COMMITTEE

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. PS105E-PDF
ISSN 1912-1598

SECURITY INTELLIGENCE
REVIEW COMMITTEE

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

September 19, 2016

Dear Minister Goodale:

We are pleased to present you with the annual report of the Security Intelligence Review Committee for the fiscal year 2015-2016, 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

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

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

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

Table of Contents

I	II	III	IV	V
CERTIFICATE Page 11	REVIEWS Page 13	INVESTIGATIONS Page 35	LIST OF RECOMMENDATIONS Page 39	HIGHLIGHTS Page 42

INTRODUCTION – pg. 05
MESSAGE FROM THE COMMITTEE – pg. 07
MESSAGE FROM THE EXECUTIVE DIRECTOR – pg. 10
SECTION 1: CERTIFICATE – pg. 11
SECTION 2: REVIEWS – pg. 13
- Review of CSIS's Threat Reduction Activities – pg. 16
- Review of CSIS's Investigation of Canadian Foreign Fighters – pg. 18
- Review of CSIS's Warranted Collection of Information – pg. 21
- Review of CSIS's Data Management and Exploitation Activities – pg. 23
- Review of Ministerial Direction and CSIS Directives on Information Sharing – pg. 26
- Review of CSIS's Collection of Economic Intelligence – pg. 28
- Review of CSIS's Traditional and Non-Traditional Foreign Partners – pg. 30
- Review of a CSIS Foreign Station – pg. 31
- Review of CSIS's Relationship with the Canada Border Services Agency (CBSA) – pg. 32

SECTION 3: INVESTIGATIONS – pg. 35
SECTION 4: LIST OF RECOMMENDATIONS – pg. 39
SECTION 5: HIGHLIGHTS – pg. 42
- Expenditures – pg. 42
- Outreach Activities – pg. 42

INTRODUCTION

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"). CSIS investigates and 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.

SIRC has three core functions: certifying the CSIS Director's annual report to the Minister of Public Safety and Emergency Preparedness, carrying out in-depth reviews of CSIS's activities, and conducting investigations into complaints.

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. A summary of its work, edited to protect national security and privacy, is presented 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 law and the rights of Canadians. Visit **www.sirc-csars.gc.ca** for more information.

ABOUT SIRC

The Security Intelligence Review Committee is composed of the Honourable L. Yves Fortier, P.C., C.C., O.Q., Q.C., the Honourable Ian Holloway, P.C., C.D., Q.C., the Honourable Gene McLean, P.C., and the Honourable Marie-Lucie Morin, P.C., and is chaired by the Honourable Pierre Blais, P.C.

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 SIRC 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, who serves as Chief Executive Officer.

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

As part of their ongoing work, the Committee Members and senior staff participate in regular discussions with the executive and staff of CSIS and other members of the national security 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 visit CSIS regional offices to understand and assess – for the purposes of review – 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 while allowing SIRC to communicate its focus and concerns.

Message from the Committee

Accountability is crucial to building public trust, especially in the realm of secretive intelligence work. For more than 30 years, SIRC's mandate has been to hold Canada's security intelligence service accountable by providing assurance to Parliament – and by extension all Canadians – that CSIS respects both the law and Canadians' rights and freedoms in carrying out its mandate to investigate threats to national security. This annual report provides a window into our assessment of CSIS's activities, as seen through our three core functions: certification, reviews and investigations.

While SIRC's fundamental mandate has not changed, the nature and scope of our work have evolved in recent years to keep up with the important changes that have taken place in the national security and intelligence fields. And while the emphasis is still on ensuring strategic and comprehensive coverage of Canada's increasingly complex security intelligence activities both at home and abroad, we have had to re-think the approach to our work to follow the expansion of CSIS's activities.

OUR ASSESSMENT

In response to comments we made last year regarding our certification of the CSIS Director's report, the Minister of Public Safety and Emergency Preparedness issued new direction to CSIS concerning the format and structure of the report. We are satisfied that the latest Director's report fulfilled the Ministerial reporting requirements.

SIRC completed nine reviews this past year, seven of which focused on information sharing, operations abroad, and technology. The recently-enacted *Security of Canada Information Sharing Act* provides a new framework for the sharing of information – one of the cornerstones of contemporary intelligence work – between departments and agencies with a national security nexus. Therefore this year, the Committee made recommendations aimed at ensuring that all of CSIS's exchanges of information with domestic and foreign partners are appropriately recorded for future reference, and that CSIS uses consistent language in its advice to government.

Operations abroad were considered in light of new legislation that strengthens and

SIRC has been providing impartial and objective retrospective reviews of CSIS's activities for more than 30 years. The information garnered from these reviews not only informs ongoing discussions, in many cases it can impact current and future operations.

expands CSIS' ability to conduct international activities; specifically, examining CSIS's investigations of Canadians who aspire – or have gone – to fight abroad (foreign fighters), reviewing its operational activities at a foreign station, and examining its relationships with both traditional and non-traditional foreign partners. Accordingly, we made a number of recommendations which we believe will ultimately strengthen CSIS's decision-making processes and accountability for its overseas operations.

A recurring theme for our reviews involved ensuring CSIS's activities remain within the scope of its legislated mandate in light of enhanced operational and analytical capabilities afforded by technology. In our review of CSIS's data management and exploitation activities, we recommended that CSIS prioritize the establishment of a governance framework guiding the collection, retention and use of bulk datasets to set clear parameters around the acquisition of such information. We also recommended an immediate halt to its acquisition of bulk datasets until it had implemented a formal process of assessment to confirm that the bulk datasets met the "strictly necessary" collection threshold set out in the *CSIS Act*.

The *Anti-Terrorism Act*, *2015* broadened CSIS's mandate by authorizing it to take measures, within or outside Canada, to reduce threats to the security of Canada. In our first review of CSIS's new threat reduction mandate, we examined the governance structure CSIS has put in place to frame and guide these activities. We found that CSIS has developed a sound governance framework, however this is still a work in progress.

Lastly, we continued to streamline our processes in an effort to make our complaints procedure more efficient, accessible and transparent.

SIRC AND THE PROPOSED COMMITTEE OF PARLIAMENTARIANS

In 2006, the O'Connor commission highlighted the need to strengthen Canada's national security accountability structure. Three years later, Parliament reiterated that "without an integrated structure for the full review of national security issues, the government cannot effectively and efficiently protect Canadians from violations of their civil rights and freedoms."

Proper accountability of Canada's security intelligence activities is crucial, and our model of independent expert review serves an important purpose. At the same time, it has been our position publicly for many years that Canada's accountability framework requires updating to keep pace with contemporary intelligence work.

Currently, Members of Parliament are not authorized to receive classified information. While SIRC has been able to fulfill its role of providing expert review of CSIS's activities, the extent to which we are able to disclose classified information to Parliament is limited by the legal constraints under which

we operate. In June 2016, the government tabled Bill C-22, the *National Security and Intelligence Committee of Parliamentarians Act*, which aims to create a committee of Parliamentarians who will have access to classified information from all departments and agencies that have national security responsibilities.

SIRC has built a solid reputation of thoroughness and relevance, and we believe that a new committee of Parliamentarians could draw upon our insight and expertise to broaden its understanding of Canada's security intelligence activities and to enhance its own overarching view of our country's national security activities.

MAINTAINING MOMENTUM

The Committee views SIRC's relationship with Parliament as an important component of its mandate. For this reason, we believe that the success of Canada's national security accountability depends on all organizations that have a national security nexus – including the bodies that review them – working in a complementary manner.

A decade after Justice O'Connor's remarks, SIRC continues to look forward to being part of this integrated effort to strengthen accountability and public confidence in Canada's national security organizations.

© 2016 BalfourPhoto
L-R: Ms. Marie-Lucie Morin, Mr. Pierre Blais, Mr. Gene McLean, Mr. Yves Fortier, Dr. Ian Holloway.

Message from the Executive Director

The fundamental benefit of providing comprehensive review is that it allows us to take a look at what was done in the past with both a critical eye and a view to making recommendations for necessary adjustments. With this in mind, I am pleased to report that as the 2015-2016 fiscal year draws to a close, our reviews have been timely and relevant to the ongoing discussion of national security.

Our ability to assess CSIS's activities has increased, allowing us to provide much more timely information and feedback. This has been made possible by the dedication and professionalism of our staff, the streamlining of our processes and, I believe most importantly, our outreach efforts, that have led to greater collaboration with members of Canada's national security community without compromising our independence.

On the topic of accountability, I am looking forward to the prospect of a committee of Parliamentarians to provide broad oversight of government departments and agencies with national security responsibilities. I believe SIRC could complement the work of this committee as it could provide a forum for us to engage Parliament on intelligence matters in a more meaningful manner. Similarly, I feel SIRC is very well placed to provide sound advice to the committee, who will no doubt draw upon our vast experience in the area of security intelligence accountability.

In my last message, I mentioned that our organization has begun transforming to meet additional review responsibilities. In particular, we have been modernizing our practices, which has allowed us faster access to CSIS's electronic information.

Along with accountability and transparency, adequate resourcing is essential. Therefore, a priority for the coming year will be to secure the additional funding commitment outlined in the 2015 federal budget on a permanent basis, since SIRC's funding has not kept pace with an increased workload. In order to be able to conduct comprehensive and effective reviews of CSIS's evolving operational realities, we must be assured sufficient resources.

I anticipate that this coming year will be one of change for the national security community, and SIRC is prepared to contribute positively to the discussion. Our dedicated research and legal staff have developed extensive expertise in reviewing even the most sensitive national security issues. This expertise, coupled with our obligation to keep abreast of the operating environment and organizational changes at CSIS, ensure that we remain well positioned to provide sound and timely advice. I look forward to sharing with you some of our contributions in next year's annual report.

1

CERTIFICATION OF THE CSIS DIRECTOR'S ANNUAL REPORT TO THE MINISTER OF PUBLIC SAFETY AND EMERGENCY PREPAREDNESS

Pursuant to subsection 38(2) of the *CSIS Act*, SIRC is required to submit to the Minister of Public Safety and Emergency Preparedness 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 described in the report involved any unreasonable or unnecessary use of CSIS's powers. SIRC's certificate, therefore, provides an important high-level assessment of the compliance of CSIS's operational activities.

In order to be able to certify the CSIS Director's report, SIRC relies on a carefully designed and rigorous research methodology to conduct an extensive review of CSIS's information holdings. We also request briefings with CSIS officials to ensure that the information in the Director's report is provided in its proper context. We review several of the operations and activities referred to in the Director's report, as well as a sample of core CSIS activities and then assess these against CSIS's compliance with the CSIS Act and Ministerial Direction in order to determine whether we consider any use by CSIS of its powers to be unreasonable or unnecessary. In addition, SIRC uses its reviews to support the certification process.

SATISFACTION WITH THE CSIS DIRECTOR'S ANNUAL REPORT

SIRC's approach to the certification process has evolved since it was given this function. Last year, as CSIS was undergoing a period of change with the expansion of its mandate, the Committee undertook to study the question of whether the Director's report was adequately meeting the requirements of Ministerial responsibility. Of particular concern to the Committee was whether the report remained true to its original intent, which is to make available to the Minister important information as to the functioning of CSIS. The Committee believed the proper flow of information to the Minister to be especially important in the current context.

Given the length and amount of details contained in the Director's report, the Committee questioned its effectiveness in ensuring Ministerial accountability. To address this, SIRC recommended that the Minister provide the new *Ministerial Direction on Responsibility and Accountability* to the Service containing more specific instructions with respect to the format, structure, and timing of the Director's report.

SIRC's observations and recommendation were well received. In July 2015, the Minister issued Ministerial Direction that provided new and more

explicit direction to the Director with respect to his annual report. We believe that the new format for the report adopted by CSIS more effectively supports the Minister in his responsibility for the activities undertaken by CSIS, and that the report is more concise and focused on issues of ministerial concern. SIRC acknowledges CSIS's work toward revising the format of the report to better support these requirements.

SIRC was satisfied with the Director's report, finding that it fulfilled Ministerial reporting requirements, that information was placed in its proper context, and that it was factually accurate.

COMPLIANCE WITH THE *CSIS ACT* AND MINISTERIAL DIRECTIVES AND THE EXERCISE OF CSIS'S POWER

The *CSIS Act* also requires SIRC to state whether, in its opinion, the operational activities described in the Director's report contravened either the *CSIS Act* or Ministerial Direction, and whether the activities involved any unreasonable or unnecessary use of the Service's powers. To make this assessment, SIRC reviewed a number of specific operations and activities, as well as a sample of CSIS's core activities. We also reviewed the *Ministerial Direction on Information Sharing with Foreign Entities*, which is addressed separately in this report.

SIRC's assessment of compliance is informed by its review work. Two instances of non-compliance are discussed in more detail later in this report. The first, examined in the review of CSIS's warranted collection of information, involved non-compliance with respect to a warranted collection activity. A second incident was explored in SIRC's review of CSIS's foreign fighter investigation, in which SIRC found that CSIS did not comply with Ministerial Direction to notify the Minister in certain specific circumstances.

Finally, there were incidents of CSIS obtaining taxpayer information from the Canada Revenue Agency without a warrant. Though this was already reported in SIRC's 2014-2015 annual report, the incidents themselves occurred during the fiscal year under review for this certificate, and thus are considered in this year's assessment of compliance. All of these incidents were reported by the CSIS Director to the Minister in his report.

CONCLUSION

SIRC is of the opinion that, notwithstanding the exceptions identified above, the activities described in the Director's report, and those assessed as part of SIRC's review activities, complied with the *CSIS Act* and Ministerial Direction and did not constitute an unreasonable or unnecessary exercise of CSIS's powers.

SIRC also expressed to the Minister that it would welcome the opportunity to be consulted in light of the important changes that are occurring in the national security environment. SIRC has developed substantial knowledge and expertise over more than 30 years of reviewing security intelligence activities, and our unique position allows us to provide information and objective advice – in addition to assurances to Parliament and to the Canadian public – regarding the activities of Canada's security intelligence service.

II

REVIEWS

One of SIRC's most important functions is to conduct in-depth reviews into CSIS's activities and operations. SIRC's reviews provide "snapshots" of CSIS's work which, when viewed together and over time, provide a broad picture of Canada's security intelligence landscape.

THE REVIEW PROCESS

SIRC's reviews provide a retrospective examination and assessment of a representative sample of CSIS's investigations and activities. With the exception of Cabinet confidences, SIRC has, in law, the absolute authority to examine any information under the control of CSIS, regardless of sensitivity or level of classification. This access gives us a very good understanding of CSIS's actions in a specific case while allowing us to manage the inherent risk of being able to review only a fraction of the Service's activities.

At the outset of each fiscal year, SIRC's dedicated staff of researchers 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;
- The potential for particular activities to infringe upon individual rights and freedoms;
- The priorities and concerns for Parliament and the Canadian people;
- The CSIS Director's annual report to the Minister of Public Safety and Emergency Preparedness on operational activities; and,
- The importance of regularly reviewing each of the Service's major programs and activities.

SIRC's reviews cover all of CSIS's key activities – including targeting, warrants, and human sources – and program areas: counter-terrorism, counter-intelligence, counter-proliferation and security screening. SIRC also examines CSIS's arrangements to cooperate and exchange information with both foreign agencies and domestic organizations. And we examine 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.

In every review, the examination of documentation generates follow-up exchanges with the Service. For this reason, SIRC researchers often conduct meetings and briefings with CSIS personnel to seek clarification and to ensure an in-depth understanding. The reviews are then presented to the Committee for approval. Once the Committee has approved the reviews, SIRC sends them to the CSIS Director and to the Department of Public Safety and Emergency Preparedness. The reviews are then edited for national security and privacy considerations before being collated into the annual report, which is tabled in Parliament.

SIRC'S METHODOLOGY

For a number of years, SIRC has used a carefully selected combination of review methods in order to assess CSIS's activities as effectively as possible.

Thematic reviews: these horizontal reviews are designed to give a broad view of a particular issue or theme that cuts across CSIS's programs or investigations. These reviews often provide us with our 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 a regular basis.

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

Core reviews: these reviews offer insight into CSIS's main activities – such as targeting, warrants, and the use of human sources – through a larger sample analysis. These reviews 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 widen the lens on CSIS's expanding activities. At the same time, these horizontal reviews are designed to cover more ground at a higher level, therefore they cannot replace the "drilling down" that comes from more focused reviews. Finding the right mix of review types to satisfy our review mandate remains an ongoing challenge.

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

The Year Ahead

Over the past several years, SIRC has increasingly examined CSIS's activities abroad. In keeping with this, SIRC will be undertaking two foreign station reviews this year to better understand CSIS's evolving collection platforms abroad. We will also continue our examination of CSIS's investigation into the warranted operations of threats posed by "foreign fighters," which includes individuals returning to Canada from active fighting abroad, as well as individuals wishing to travel abroad to engage in terrorist activity. We will also examine its information sharing practices in light of changes brought about by the enactment of the *Security of Canada Information Sharing Act*. Finally, we have committed to reviewing CSIS's security screening activities, a significant organizational initiative, as well as its role in countering terrorist financing and cyber threats.

RECOMMENDATIONS

SIRC's reviews include findings and, where appropriate, recommendations. We have developed guidelines regarding our recommendations to ensure that they are practical, constructive, and focus on tangible actions and results.

SIRC actively solicits the Service's formal responses to its recommendations for inclusion in the annual report summaries as a means of providing greater transparency and of giving the public better insight into the impact of our work on security intelligence. 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.

And although our recommendations are non-binding, CSIS has implemented a large percentage of them – as noted in our annual Departmental Performance Reports – and has publicly acknowledged that over the years it has become a better organization because of SIRC.

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.

REVIEW OF CSIS'S THREAT REDUCTION ACTIVITIES

The enactment of the *Anti-Terrorism Act, 2015* in July 2015 ushered in a number of changes to Canada's national security landscape, including significant changes to the *CSIS Act*. Under the new legislation, CSIS was provided with additional powers to take measures to reduce threats to the security of Canada, within or outside of Canada. By the same stroke, the legislation requires SIRC to each year "review at least one aspect of the Service's performance in taking measures to reduce threats to the security of Canada," and to specify in the SIRC annual report "the number of warrants issued under section 21.1 in the fiscal year and the number of applications for warrants made under that section that were refused in that year."

The *CSIS Act* does not define a "threat reduction measure." Accordingly, CSIS has developed its own definition, guided by Ministerial Direction and based on the threat-related activities defined in section 2 of the *CSIS Act*. The intent of a threat reduction measure is not to collect information, but to reduce a threat to the security of Canada. Accordingly, the threshold required for CSIS to undertake a threat reduction measure is based on *reasonable grounds to believe* that the activity constitutes a threat, as opposed to its collection mandate, which requires *reasonable grounds to suspect* that an activity constitutes a threat.

Moreover, the legislation states that the threat reduction measure "shall be reasonable and

In 2010, SIRC examined CSIS's use of disruption measures against a suspected threat. Although the review stated that countering or disrupting was part of the continuum of investigating threats to national security, the review raised a number of important issues, such as the appropriateness of giving a civilian intelligence agency the authority to take measures to disrupt threats.

In response to SIRC's study, CSIS undertook an internal examination to assist in the eventual preparation of a Ministerial Directive or other guidance that would define the limits of CSIS's authority on this matter. Ultimately, CSIS's own examination made a recommendation similar to SIRC's, namely that Ministerial Direction be sought with respect to disruption activities.

In December 2010, CSIS issued a directive outlining that "disruption activities" did not fall within its mandate, and therefore, employees were directed not to engage in such activities. The directive specified that although disruption could potentially occur as a secondary effect of its mandated collection activities, disruption was not to be the intended outcome.

In the aftermath of the October 2014 events in Ottawa and Saint-Jean-sur-Richelieu, the discussion surrounding CSIS's ability to conduct disruption activities was re-ignited with the tabling of legislation.

CSIS's new threat reduction powers are found in section 12.1 of the *CSIS Act*, which reads:

> (1) If there are reasonable grounds to believe that a particular activity constitutes a threat to the security of Canada, the Service may take measures, within or outside Canada, to reduce the threat;
>
> (2) The measures shall be reasonable and proportional in the circumstances, having regard to the nature of the threat, the nature of the measures and the reasonable availability of other means to reduce the threat;
>
> (3) The Service shall not take measures to reduce a threat to the security of Canada if those measures will contravene a right or freedom guaranteed by the *Canadian Charter of Rights and Freedoms* or will be contrary to other Canadian law, unless the Service is authorised to take them by a warrant issued under section 21.1;
>
> (4) For greater certainty, nothing in subsection (1) confers on the Service any law enforcement power.

Section 12.2 of the *CSIS Act* further reads:

> (1) In taking measures to reduce a threat to the security of Canada, the Service shall not:
>
> a) cause, intentionally or by criminal negligence, death or bodily harm to an individual;
>
> b) wilfully attempt in any manner to obstruct, pervert or defeat the course of justice; or
>
> c) violate the sexual integrity of an individual.
>
> (2) In subsection (1), "bodily harm" has the same meaning as in section 2 of the *Criminal Code*.

proportional in the circumstances, having regard to the nature of the threat, the nature of the measures and the reasonable availability of other means to reduce the threat." CSIS must therefore demonstrate the proportionality and reasonableness of any measure in the context where it is proposed to be taken.

This study marked SIRC's first legislated review of CSIS's new threat reduction activities. In it, SIRC sought to understand the evolution in thinking on threat reduction activity within CSIS, particularly following SIRC's 2010 study regarding CSIS's use of disruption to counter national security threats. SIRC then examined how CSIS has operationalized its new threat reduction powers by looking at the governance structure it has put into place to frame and guide these activities. Finally, SIRC reviewed all threat reduction activities that had been conducted to date to assess for CSIS's compliance with *CSIS Act*, Ministerial Direction and its own operational policies.

To allow for a full and thorough understanding of CSIS's threat reduction activities, SIRC's review was not limited to a defined review period; rather, SIRC examined all relevant and up-to-date information as it became available.

FINDINGS

SIRC found that CSIS has developed a sound governance framework, including policies and procedures, to help guide the approval and conduct of threat reduction activities. Moreover, CSIS has created a responsibility centre to manage all matters related to these

activities, and has put in place mandatory training for CSIS employees.

Ministerial Direction requires that CSIS assess the risks associated with threat reduction activities, including operational, political, foreign policy and legal risks. This process relies on specific consultation with the RCMP and Global Affairs Canada, as well as other federal departments/agencies when required. SIRC found that this consultation process is positive, but there is a need to further outline how formal consultation on threat reduction activities will occur with these other federal departments/agencies. **SIRC recommended that CSIS prioritize the development of formal mechanisms for consultation on threat reduction activities with relevant Government of Canada departments and agencies.**

In this first review of CSIS's threat reduction activities, SIRC examined all measures that CSIS had approved or considered to date, approximately two dozen. SIRC found that the threat reduction activity cases examined all complied with the *CSIS Act*, Ministerial Direction and operational policies. Pursuant to subsection 53(2) of the *CSIS Act*, SIRC reported that there were no warrants issued under section 21.1 this fiscal year, nor was any application for warrant refused.

Looking ahead, SIRC noted that there was no process for tracking best practices on threat reduction measures. **SIRC recommended that CSIS create a mechanism for tracking best practices and/or lessons learned for all threat reduction activities.**

At the review's conclusion, SIRC was satisfied with the governance framework that CSIS had put in place, namely the policies and procedures used to guide threat reduction activities, and the training afforded to employees.

CSIS Response: CSIS agreed to prioritize the development of formal mechanisms on threat reduction activity consultation with other government departments and agencies, noting that it has already made the development of framework agreements to guide consultation a priority. CSIS has recently finalized a third consultation framework and is working on a fourth. In response to the recommendation that CSIS create a mechanism for tracking threat reduction activity best practices, CSIS agreed and noted that it has already implemented initial mechanisms.

REVIEW OF CSIS'S INVESTIGATION OF CANADIAN FOREIGN FIGHTERS

Last year, SIRC undertook its first review of CSIS's investigation of the foreign fighter threat by examining domestic investigative efforts. This year, SIRC examined the initiatives and challenges related to CSIS's overseas collection activities in an effort to better understand how overseas conflicts, particularly those in Iraq and Syria, have shaped the nature and complexity of the terrorist threat to Canada.

In order to examine this subject in detail, a three-tiered approach was adopted. First,

SIRC sought a broad perspective on CSIS's evolving foreign fighter strategy, including how resources have been redirected and/or redeployed to address what the CSIS Director has described as "an absolute top priority." Second, the review looked at CSIS's inventory of human sources outside Canada, with an emphasis on the adequacy of direction and on CSIS's interpretation and implementation of governing legal thresholds applicable to such activities. Finally, a case study was devoted to a CSIS overseas operation which encapsulated many of the challenges common to activities against terrorist entities.

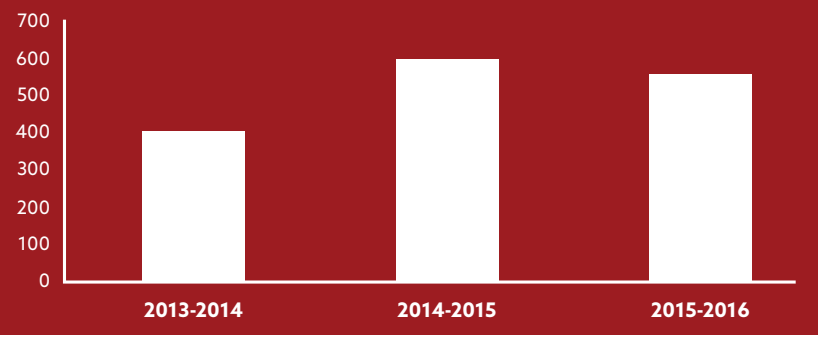
FINDINGS

Over the course of the review, it became evident that not all of CSIS's policies, procedures, operational approvals and disclosure practices were sufficiently robust to address certain overseas scenarios. In one case, for example, Global Affairs Canada authorities, who rely on CSIS for advice on security and intelligence issues, were insufficiently briefed on a particular matter. Moreover, CSIS did not create a timely strategic plan, nor did it seek advice from the National Security Litigation and Advisory Group at the Department of Justice, which could have outlined clearer parameters for engaging in this particular type of overseas collection. Consequently, SIRC found that CSIS needs to strengthen its strategic overseas planning to assess for operational, political, foreign policy and legal risks.

SIRC also observed that CSIS did not inform the Minister of Public Safety and Emergency Preparedness about an incident which, SIRC believes, met the threshold for ministerial notification. SIRC therefore found that CSIS did not comply with Ministerial Direction

FIGURE 1 – TARGETS

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



requiring it to notify the Minister in certain specific circumstances.

In order to address the various issues identified, we believe that CSIS needs to emphasize strategic planning for foreign operations. For example, CSIS should ensure its employees fully understand the extent to which certain activities present legal risks. To this end, **SIRC recommended that CSIS seek legal clarification on whether CSIS employees and CSIS human sources are afforded protection under the Common Law rule of Crown Immunity in regards to the terrorism-related offences of the *Criminal Code of Canada*.**

SIRC also recommended that CSIS conduct an assessment of additional measures for increasing operational support to intelligence officers working overseas, produce country-specific strategies where considerable operational activity transpires, and related to this, that CSIS HQ take on a more decisive leading role in certain foreign activities when necessary.

Lastly, SIRC recommended that CSIS create, on a priority basis, a risk analysis framework to operationalize new Ministerial Direction, which requires it to consider operational, political, foreign policy, and legal factors when assessing risk.

Ultimately, this review underscored the need for CSIS to address lingering challenges associated with overseas operations. As the government demand for intelligence on threats to the security of Canada from within conflict zones grows, CSIS can expect these challenges to increase in parallel. Experience gleaned from CSIS's time in Afghanistan will be put to the test, as will requirements for novel approaches to problems particular to these new collection theaters.

CSIS Response: CSIS agreed to seek clarification on the issue of Crown Immunity and will focus first on clarifying the application of the Criminal Code and Canadian sanctions to its operational activities. With respect to increasing operational support, CSIS has already conducted an assessment of additional measures and has focused on identifying and implementing solutions to the most urgent issues. CSIS agreed in principle to create country-specific strategies where considerable operational activity transpires, noting that it develops instead engagement strategies for areas of increased operational activity. Further to Ministerial Direction, CSIS is also developing an enhanced process to assess foreign policy risk in consultation with Global Affairs Canada. CSIS also agreed in principle to HQ taking on a more decisive role in certain foreign operations; it is considering the best way to address these concerns in conjunction with two ongoing initiatives to be concluded during the fiscal year. Finally, CSIS agreed to create a risk analysis framework to operationalize Ministerial Direction and is updating operational policy to set out clear processes and lines of responsibility for identifying and assessing risks; this will be completed within the fiscal year.

CSIS'S WARRANTED COLLECTION OF INFORMATION

CSIS collects information on targets using various investigative methods, including human sources, interactions with foreign and domestic partners, and physical surveillance. For some of its targets, CSIS also uses more intrusive collection techniques that require the issuance of a warrant by the Federal Court of Canada.

This review examined a large number of CSIS's warranted operations across Canada, paying particular attention to the limitations and conditions set out in Federal Court warrants. In addition, the review considered employee staffing and training issues, as well as ongoing efforts by CSIS to develop quality control and performance standardization.

FINDINGS

Overall, SIRC found that, with one exception, CSIS complied with the applicable warrants, the *CSIS Act*, Ministerial Direction and operational policies when carrying out its warranted activities.

The noted exception involved a warranted collection activity where CSIS did not abide by the applicable warrant. SIRC found no evidence to suggest that any CSIS employee involved in the incident deliberately acted in violation of the Federal Court's warrants. Rather, a number of related factors resulted in the failure to follow the warrant. SIRC confirmed that none of the information collected was retained within CSIS's database. Therefore, in addition to efforts by CSIS to clarify procedures and improve the knowledge of employees about specific warrant parameters, **SIRC recommended that CSIS implement changes to the way in which approval is given for specific operational activities.**

In relation to the above incident, SIRC also noted that CSIS lacked a formal process for scenarios in which a CSIS employee may have acted unlawfully. Although the CSIS Director sent a report about this incident to the Minister of Public Safety and Emergency Preparedness, pursuant to section 20 of the *CSIS Act*, SIRC found there was confusion and disagreement among CSIS stakeholders about how this process should have unfolded. Although the CSIS Director must have the discretion to determine when an action by an employee constitutes an illegal act, his ability to make sound decisions on such important matters is predicated upon clear procedures for how such cases are to proceed *before* they reach the Director's desk. To avoid confusion in future cases, **SIRC recommended that CSIS create a formal and more robust internal process to assist the Director in determining when an action by an employee may have been unlawful.**

SIRC also observed that there was no clear process within CSIS for accessing legal opinions and/or advice issued by the Department of Justice's National Security Litigation and Advisory Group. The inability for CSIS managers to fully access legal opinions can create scenarios where legal clarity on certain matters is jeopardized. For example,

In accordance with subsection 20(2) of the CSIS Act, "If the Director is of the opinion that an employee may, on a particular occasion, have acted unlawfully in the purported performance of the duties and functions of the Service under this Act, the Director shall cause to be submitted a report in respect thereof to the Minister." The Act further states that the Minister shall provide a copy of the report to the Attorney General of Canada, together with any comment that he considers appropriate in the circumstances. A copy of this information is also to be provided to SIRC.

technologies developed for one purpose can quickly evolve, and accordingly, CSIS managers must have assurance that their decisions are consistent with the latest legal precepts. Therefore, **SIRC recommended that CSIS implement a process to ensure that relevant CSIS stakeholders have knowledge of, and access to, legal opinions and/or advice.**

During the review, SIRC also noted that CSIS lacked a defined category within policy for individuals who assist CSIS with warranted operations. Given the importance of these human assets, **SIRC recommended that CSIS improve the policy used to manage individuals who assist CSIS with warranted operations.**

Finally, SIRC observed that while CSIS HQ has attracted and maintained employees with considerable knowledge about these specialized warranted operations, CSIS regional offices have not fared as well due to retirements and rotational transfers. This has resulted in a knowledge gap within some regional offices that could affect operational performance. SIRC's assessment was tempered by CSIS initiatives that occurred outside of the review period, aimed at improving the training offered to employees. These efforts notwithstanding, **SIRC recommended that CSIS develop other standardized processes to guide the future of warranted operations.** These processes include a hiring methodology to help maintain personnel consistency between regional offices, the provision of timely training to employees, the provision of more elaborate operational manuals to enhance 'on-the-job' training, and detailed succession planning.

SIRC committed to continuing its in-depth review of CSIS's warranted operations during next year's review cycle, with particular attention to another category of warranted operations that span across all of CSIS's regional offices.

CSIS Response: In response to the recommendation to implement changes to the way in which approval is given for specific operational activities, CSIS agreed, but added that operational circumstances mean this is not always possible. Nonetheless, CSIS will review relevant procedures, as well as options available, associated costs and considerations. CSIS also agreed to create a formal process for suspected section 20 incidents, and to introduce an enhanced operational compliance process. With respect to implementing a process that would ensure access to legal opinions and/or advice, CSIS responded that it has already undertaken an exercise to collate and make available to employees legal opinions relating to warrant acquisition and the conduct of operations. CSIS also agreed to amend the policy used to manage individuals who assist CSIS with warranted operations. Finally, in relation to warranted operations, CSIS agreed to develop a new policy suite that will provide the framework for standardized processes and to revamp its training program, including the development of standard operating procedures.

REVIEW OF CSIS'S DATA MANAGEMENT AND EXPLOITATION ACTIVITIES

This review marked SIRC's first examination into CSIS's data acquisition program. SIRC's review examined the list of bulk datasets in the program's holdings, which are broken down into two broad types. The first type is "referential," meaning that the information is used primarily to facilitate identity verification. Referential datasets contain information on a large number of people and locations. CSIS also has "non-referential" datasets which contain bulk information on a wide variety of individuals; however these can only be retained if they are assessed as being relevant to an ongoing, mandated investigation.

FINDINGS

SIRC noted that CSIS uses bulk datasets in multiple ways. They can be used to conduct indices checks by taking information already connected to a potential threat – such as an address, phone number or citizen identification number – and using it to search for "hits" in the data. Datasets can also be used to enhance knowledge of a target by searching the data

Table 1 - Warrants Issued

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*.

	2013-2014	2014-2015	2015-2016
New	85	104	129
Replacement or Supplemental	178	181	161
Total	**263**	**285**	**290**

for previously undetected trends, links or patterns between and among data points. And data is used to support more focused inquiries, such as "data mining" to identifying leads. Finally, SIRC was told that the data can be used to try to identify previously unknown individuals of interest by linking together types of information which have mirrored threat behaviour. Overall, the addition of more datasets is expected to enrich CSIS's analytical capacity and enhance its ability to provide support for CSIS investigations.

CSIS's data acquisition program has developed a procedure to address the handover of the data from its source to the point that the data is ready for exploitation by analysts; however, beyond the more technical aspects of ingestion, SIRC found that there is no comprehensive governance framework guiding the collection, retention and use of bulk datasets. This was the case despite the fact that SIRC saw references in earlier CSIS documentation to the need to validate the authority to collect and manage the risk of over-collection by confining collection to that which is "strictly necessary." To that end, SIRC was told that a governance framework was drafted two years ago, but that it had not yet been finalized.

SIRC recommended that CSIS finalize and implement the governance framework for dataset acquisition no later than February 1, 2016. According to SIRC, this framework should, among other objectives, set parameters around collection based on the statutory requirement that it be limited to that which is "strictly necessary." Ongoing dataset management issues would need to be addressed as well, to ensure that the datasets being used continue to be relevant and those that are no longer used are deleted.

According to CSIS, because referential datasets are openly sourced and publicly available, they are not "collected" under the authority of section 12 of the *CSIS Act*. SIRC agrees with the principle that there are instances when the acquisition of purely referential datasets would not constitute "collection" per se; the phonebook was given as an example of this type of bulk dataset. However, SIRC reviewed the full list of referential datasets and found instances where we felt the criteria for inclusion in the "referential" category – data that is publicly available and openly sourced – were not met. **SIRC recommended that CSIS re-evaluate all referential bulk datasets against its criteria to ensure that they should continue to be considered referential; those that do not should be assessed against the "strictly necessary" threshold.**

The non-referential datasets, by contrast, are considered by CSIS as having been "collected" under the authority of the *CSIS Act*, and so must meet the collection threshold of "strictly necessary." Despite this, SIRC found no evidence to indicate that CSIS had appropriately considered the threshold as required in the *CSIS Act*. **SIRC therefore recommended that CSIS undertake a formal and documented assessment for each of its existing non-referential datasets to ensure the information**

was collected only to the extent that was "strictly necessary."

To assist in that task, SIRC developed the following guidelines, each of which is meant to promote conformity to the threshold of "strictly necessary." First, for any bulk information, a clear connection to a threat to the security of Canada as defined in section 2 of the *CSIS Act* must be established. Second, it must be established that less intrusive means that would satisfy the intelligence requirements are not available as an alternative to bulk collection, consistent with the principle of proportionality. Third, if there is no reasonable alternative to bulk collection, CSIS needs to provide an objective assessment of how closely connected the bulk information is to intelligence of value; the broader the intended collection, the more strictly CSIS must establish the connection between the bulk information and threat-related intelligence.

Ultimately, **SIRC recommended that CSIS halt its acquisition of bulk datasets until it has implemented a formal process of assessment to confirm that the bulk datasets meet the collection threshold.**

CSIS Response: CSIS agreed to prioritize the finalization and implementation of a governance framework for bulk data acquisition. The framework was approved and is being operationalized, and the CSIS Director has requested that an audit of the implementation of these new procedures be undertaken in one year. CSIS also agreed to re-evaluate all referential bulk datasets and has initiated the process to ensure that these datasets meet the criteria set out in the governance framework. It will also undertake a formal assessment of existing non-referential bulk datasets, a process that began upon approval of the governance framework. Finally, CSIS agreed to halt ingesting bulk datasets pending the implementation of the governance framework. CSIS also provided additional direction to employees to remind them of the requirement that all collection undertaken by CSIS pursuant to section 12 be done only to the extent that is strictly necessary.

REVIEW OF MINISTERIAL DIRECTION AND CSIS DIRECTIVES ON INFORMATION SHARING

In 2006, Justice Dennis O'Connor, who led the commission of inquiry into the actions of Canadian officials in relation to Maher Arar, recommended that CSIS amend its policies to include specific directions "aimed at eliminating any possible Canadian complicity in torture, avoiding the risk of other human rights abuses and ensuring accountability." Since then, two *Ministerial Directions on Information Sharing with Foreign Entities* have been issued, one in 2009 and another in 2011. The latter direction, while condemning the use of torture in responding to terrorism, established a process for determining when it may be permissible to exchange information even when it may not be possible to mitigate a substantial risk of mistreatment.

Although SIRC has regularly examined CSIS's information sharing practices, this was its first review to evaluate CSIS's compliance with and response to the latest Ministerial Direction. This was achieved by examining the information sharing framework that it has put in place, namely an internal directive on information sharing with foreign entities. SIRC examined a number of information sharing cases against the benchmarks set out in the Ministerial Direction and in CSIS's internal directive, which require it to assess and mitigate the potential risks of sharing information and to identify information that is likely to have been derived from mistreatment. In particular, SIRC reviewed all cases that were discussed at a CSIS executive-level committee that meets as needed, on specific cases, to assess whether to proceed with using and/or sharing information where there may be a risk of mistreatment. SIRC also reviewed a large number of decisions taken at the management level with respect to assessments of potential mistreatment.

FINDINGS

Overall, SIRC found that CSIS acted quickly to implement a sound information sharing framework. Moreover, it found that all cases that were referred to CSIS's executive-level committee were managed appropriately; the range of participants around the table fostered substantive discussion and provided for a rigorous decision-making process.

SIRC did find, however, that the framework could be strengthened through a more rigorous and consistent application of the internal directive and recording of the decision-making process, especially at the management level. In SIRC's opinion, these gaps led CSIS to take contradictory decisions in at least two cases.

Through an internal directive, CSIS has implemented a set of assessment criteria to be used by its employees when considering whether to use information received from a foreign entity, or to send information to / solicit information from a foreign entity where there may be a risk of mistreatment. Overall, CSIS elaborated a clear course of action for determining when it may be permissible to exchange information, even when it may not be possible to mitigate a substantial risk of mistreatment.

In the cases reviewed, SIRC found that while CSIS had a record of decisions made, it had no record of the deliberations surrounding the managerial assessments, as required in the internal directive. Given this absence of documentation, SIRC found it difficult to make a complete assessment of the decisions taken at the management level. Accordingly, **SIRC recommended that CSIS's executive prioritize the development of an action plan to address the issue of proper record-keeping within this fiscal year.**

In the review of operational reporting, SIRC also found inconsistencies in the application of the directive and in the decision-making process at the management level. SIRC found two cases where the directive was not well understood by the managers responsible for assessing the information and making a decision. In SIRC's view, the directive does not provide guidance to the managers on how to assess one of the assessment criteria. SIRC believes that having a defined criteria could help to ensure a more consistent understanding and application of the information sharing process. **SIRC therefore recommended that CSIS ensure that all deliberations at the management level, as well as all information related to the assessment criteria in question, be mentioned in the record of decisions.**

Finally, SIRC examined the issue of risk mitigation. When disseminating information, CSIS uses two risk mitigation methods: caveats and assurances. In a previous review, SIRC noted the lack of specific guidelines, whether in a directive, policy or other document, outlining the circumstances or conditions that would trigger the seeking of assurances or the process to be followed in these exceptional cases. In light of this, SIRC had recommended that CSIS develop direction and then policy on the practical application of assurances, such as when and how they should be sought, under whose authority, and how this process should be documented in operational reporting.

In August 2015, CSIS introduced a policy to provide direction concerning the use of caveats and assurances when disseminating information or intelligence to any outside department, agency or organization. This policy refers back to the internal directive to determine instances when there is a need to request assurances; CSIS employees are directed to consult the criteria listed in the directive, which include an assessment of the foreign entity. Given CSIS's reliance on assurances as a risk mitigation tool, **SIRC recommended that CSIS make explicit in the record of decision-making its assessment of the foreign entity fulfilling the proposed assurance.**

CSIS Response: CSIS agreed in principle to prioritize proper record-keeping of decisions. Although CSIS will not develop an action plan, this issue has been raised at senior levels within CSIS, relevant communications with employees are ongoing and robust record-keeping requirements are being added in the course of ongoing revision of operational policies. CSIS agreed to clearly record the outcome and nature of deliberations at the management level in a standardized format to help ensure consistency and completeness. Finally, CSIS agreed in principle to make explicit its assessment regarding the foreign entity fulfilling the proposed assurance. CSIS is issuing direction to ensure the process for seeking, obtaining and documenting assurances is systematic and standardized; it is raising the matter during meetings with foreign counterparts; and it is enhancing internal documents used in managing relationships with foreign partners.

REVIEW OF CSIS'S COLLECTION OF ECONOMIC INTELLIGENCE

CSIS collects information and intelligence regarding threats to the security of Canada as defined under section 2 of the *CSIS Act*. Increasingly, some of those threats are related to economic matters, particularly when they fall under espionage or foreign-influenced activities. This review undertook an examination of CSIS's collection of economic security intelligence and its role and participation in the *Investment Canada Act* process.

FINDINGS

Overall, SIRC found that CSIS operated within its mandate in collecting economic security intelligence. However, SIRC believes that more clarity around the language used in the advice provided to Government under the *Investment Canada Act* would aid in ensuring a consistent approach.

As stated by Industry Canada, "the *Investment Canada Act* is the primary mechanism for reviewing foreign investments in Canada. Its purpose is twofold: to review significant foreign investments to determine if they are likely to be of economic benefit to Canada, and to review investments that could be injurious to national security." It is for the latter purpose that CSIS participates in the process. Similar legislation governing foreign investment exists among Canada's allies.

In Canada, an investment is reviewable if the Minister of Industry (now the Minister of Innovation, Science, and Economic Development of Canada), after consultation with the Minister of Public Safety and Emergency Preparedness, considers that the investment could be injurious to national security. If the Minister is satisfied, based on the advice he receives, that the investment would be injurious to national security, or if he is not able to make that determination based on the information available, he shall refer the investment under review to the Governor in Council, together with a report of his/her findings and recommendations on the review. The triggers for such a review, while provided to

the departments and agencies involved in the process, are not shared with either the potential investor nor with the public.

Under the authority of the *Investment Canada Act*, CSIS "is required to evaluate foreign investments in Canada for potential national security concerns" once they are referred for review by the Minister of Industry. Ultimately, the outcome of CSIS's advice under this process is to assist in determining whether or not a transaction is referred for further consideration by the Governor in Council owing to national security concerns. SIRC examined a sample of transactions referred for review together with the advice provided by CSIS.

In two cases, SIRC found that there was a lack of clarity and that, from one case to the other, no legal opinions were sought nor were lessons learned or concerns recorded as to the appropriateness of the request. Therefore, **SIRC recommended that CSIS seek clarification on that type of activity when its assistance is requested through *Investment Canada Act* channels.**

SIRC found there was a lack of clear criteria in one case to move from the threshold of "*could be* injurious to national security" to "*would be* injurious to national security," thresholds which the Minister, in consultation with the Minister of Public Safety and Emergency Preparedness, must be satisfied have been met. SIRC also found a lack of consistency in the language used in CSIS's *Investment Canada Act* assessments in general to express whether or not CSIS considered the investment of concern. Therefore, **SIRC recommended that CSIS use consistent language in the advice it provides through the *Investment Canada Act* process: there either is or is not a national security concern, or there is not enough information to determine whether there is a national security concern.**

CSIS Response: CSIS disagreed with the recommendation to seek clarification on this activity on the basis that they were providing national security advice under sections 12 and 19 of the *CSIS Act*. CSIS disagreed with the second recommendation, stating that the threshold language that guides CSIS's assessments is defined in the *Investment Canada Act*, but did commit to ensuring that the terms are used in a consistent manner.

REVIEW OF CSIS'S TRADITIONAL AND NON-TRADITIONAL FOREIGN PARTNERS

Cooperation between and among foreign intelligence agencies is by no means new. Some of the most important examples of foreign cooperation and liaison relationships are those that developed among the "Five Eyes" partners, a multilateral alliance between the United States, the United Kingdom, Australia, Canada, and New Zealand. Although CSIS has decades of experience cooperating with foreign partners, the changing threat environment is requiring more frequent and substantial collaboration with non-traditional partners.

In this review, SIRC examined how CSIS has prepared itself to achieve its collection requirements in an increasingly complex and dynamic threat environment, through policy, internal consultation and guidance, and by actively seeking out engagement with non-traditional partners. More broadly, this review provided SIRC with insight into the nature and scope of CSIS's evolving relationships with foreign partners through the lens of joint operations and operational support.

FINDINGS

Overall, SIRC found that the policies and procedures in place were sound, and that the investigations reviewed were clearly related to CSIS's mandate and collection requirements. There were two recommendations stemming from this review that concern CSIS's arrangements with foreign agencies.

CSIS's foreign arrangements and cooperation are governed by section 17(1)(b) of the CSIS Act, *Ministerial Direction, and internal operational policies. New arrangements must be approved by the Minister of Public Safety and Emergency Preparedness, after consultation with the Minister of Foreign Affairs.*

In the course of its review, SIRC found that, in some cases, CSIS showed prudence in establishing foreign arrangements with smaller units within foreign agencies in countries with human rights concerns. In others, however, CSIS began cooperation with a broad arrangement. Going forward, **SIRC recommended that CSIS, if faced with the necessity to cooperate with partners in countries with human rights concerns, begin with an arrangement with one (or more) narrowly defined unit(s) within the foreign agency before considering expanding the arrangement more broadly.**

SIRC understands that there are circumstances which may require CSIS to engage or cooperate with foreign organizations without an arrangement. However, there is a process in place that allows CSIS to cooperate in the absence of an arrangement. SIRC found that in two instances, CSIS approved leveraging an existing foreign arrangement to cooperate with a foreign agency with which it did not have either a separate and distinct arrangement, or Ministerial approval. In these two cases, SIRC did not find that CSIS was in violation of the *CSIS Act*, as these operations

did not progress to the point of execution. Still, **SIRC recommended that CSIS seek Ministerial approval as per the *CSIS Act*, or follow Ministerial Direction if exigent circumstances apply, when cooperating with a foreign agency with which it does not have a foreign arrangement.**

More broadly, SIRC assessed CSIS's approach to, and management of, joint operations and cooperation by focusing on the governance framework surrounding these activities and compliance with the *CSIS Act* and Ministerial Direction. Overall, SIRC found that the procedures in place around joint operations are clear and detailed, with room for discussion between CSIS HQ and regional offices, reflecting the value of both the strategic and tactical aspects of operational planning.

CSIS Response: CSIS agreed to, when possible, engage in more narrowly-defined foreign arrangements and to focus on CSIS's specific requirements. CSIS also agreed to seek Ministerial approval or to follow Ministerial Direction when exigent circumstances apply, emphasizing that it cannot use existing foreign arrangements to cooperate with, obtain operational assistance from or undertake joint activity with third parties with whom it does not have an established foreign arrangement unless it follows established procedures.

During its on-site foreign station visits, SIRC meets with CSIS personnel to discuss an array of issues and to gain a better understanding of the working environment at station. As in every foreign station review, SIRC also has meetings with the Canadian Head of Mission, as well as representatives of other Canadian departments and agencies. These meetings allow for open and honest discussion on a number of timely and relevant matters.

REVIEW OF A CSIS FOREIGN STATION

For a number of years, SIRC has been reviewing CSIS's expanding footprint abroad, which has resulted in the growth of operational activities and personnel outside Canada. Against the backdrop of this new operational reality, SIRC has sought ways to use the information gleaned from its foreign station visits to feed its broader view of CSIS's activities abroad.

This was SIRC's first examination of this particular foreign station. SIRC's on-site visit provided perspective on an evolving threat situation that has led to a change in CSIS's role in this part of the world. SIRC also gained perspective on the work undertaken in hostile, dangerous and difficult environments. Finally, the review provided insight into new relationships that are being forged and tested to support CSIS's increased foreign operational presence.

FINDINGS

Overall, SIRC found that CSIS's presence in this part of the world was seen as both welcome and necessary. The relationships that CSIS has developed with Canadian domestic partners appear to be of mutual benefit, and relationships with foreign partners are also productive. This study demonstrated the added benefit and need for CSIS to operate in various parts of the world in fulfilling its mandate on behalf of the Government of Canada.

SIRC noted that the workload at this foreign station was continuously heavy. On occasion, temporary analytical officers had been deployed for short-term assignments, which allowed for an enhanced quality of intelligence products and more focused intelligence collection efforts. Accordingly, SIRC saw the benefit of CSIS considering the addition of permanent analytical support at this station.

SIRC also noted that CSIS had put in place a new communications system at the station, which has helped to overcome issues that were noted in previous SIRC foreign station reviews. Still, some challenges exist. As this new communications system is implemented more widely, SIRC found that it would be prudent for CSIS HQ to place additional pressure on the responsible Government of Canada service providers to ensure that CSIS is given the appropriate technical infrastructure to accomplish its work abroad.

In meetings with SIRC, CSIS indicated that its priority at the station was Canadian targets, as well as broader strategic threat-related information pertaining to Canadian interests abroad. To meet these objectives, the station has been involved in some innovative operational activities aimed at addressing a number of Government of Canada intelligence requirements. In relation to these initiatives, SIRC found that all operational authorities were up-to-date, in order, and appropriately documented.

This review provided SIRC with a number of avenues to consider for future reviews.

REVIEW OF CSIS'S RELATIONSHIP WITH THE CANADA BORDER SERVICES AGENCY (CBSA)

Every year, SIRC undertakes a closer examination of one of CSIS's domestic partnerships. This year, SIRC elected to examine CSIS's relationship with the Canada Border Services Agency (CBSA) by looking at the mechanisms that are in place for exchanging information between the two organizations. SIRC also looked at the relationship through the lens of some of the larger-scale programs and initiatives by focusing on the more routine forms of cooperation and exchanges managed by a dedicated unit within CSIS. SIRC's objective was to gain insight into the nature of CSIS's interactions with the CBSA and to identify any issues or areas for follow-up in future SIRC reviews.

FINDINGS

In light of its role in the national security community, the CBSA is one of CSIS's most important domestic partners. CSIS and the

CBSA work together closely, particularly with regard to border and immigration screening, and matters related to threats to national security. Cooperation between CSIS and the CBSA takes place through a number of specific initiatives, some directly related to the CBSA's mandate to ensure that individuals entering Canada do not pose a threat, and others related to CSIS's mandate to investigate threats to the security of Canada. The mandates of both organizations allow for broad information sharing on issues of mutual concern, but over the past few years, collaboration between CSIS and the CBSA has become more formalized and complex.

In the spring of 2015, CSIS and the CBSA signed an overarching framework Memorandum of Understanding (MoU). The annexes accompanying the MoU are still in early stages of development; therefore, it would be premature for SIRC to comment on the MoU's impact. **SIRC recommended that CSIS work closely with the CBSA to expedite the finalization of the annexes underpinning the 2015 MoU.**

SIRC took an in-depth look at two information sharing mechanisms between CSIS and the CBSA. The first is an initiative designed to have CSIS proactively share information with the CBSA on cases where there is a serious national security concern. This initiative is modeled on an established information sharing process guiding CSIS-RCMP cooperation. At the time of the review, two test cases had gone through the process. Yet, SIRC found no documentation at the conclusion of these pilot cases. Moreover, SIRC found that despite engagement on the initiative, there was no clear center of responsibility managing the process within CSIS. Going forward, CSIS should strive to provide formal management and guidance with respect to this process.

The second mechanism for information sharing focused on a letter of agreement signed between CSIS and the CBSA in 2013 that governs the disclosure of a specific type of personal information. Two conditions were of interest to SIRC: the first condition specifies that this particular information can only be shared by the CBSA on a case-by-case basis in the context of an active CSIS investigation. The second condition specifies that the recipient of the information, in this case CSIS, must be subject to "oversight by an independent public authority." SIRC requested that, in the future, it be informed of instances when CSIS's collaborative endeavors or information sharing practices rely upon SIRC as a mechanism of accountability.

The volume of exchanges of information between CSIS and the CBSA during the review period suggests a high level of cooperation between both organizations on several fronts. A large proportion of these exchanges are centrally managed at CSIS through a dedicated unit, whose primary role is to contribute to Canada's border security through enhanced cooperation with the CBSA and other agencies or departments with related concerns.

SIRC examined three programs under the purview of this unit and found the policies and

procedures governing these three programs to be sound. In addition, SIRC found that having a unit dedicated to managing the bulk of the CBSA's exchanges is of benefit to CSIS both in terms of quality control and managing the relationship.

SIRC noted that CSIS's relationship with the CBSA is an important one, with each organization providing the other with important operational information and assistance. SIRC will continue to examine different facets of this relationship in the course of its ongoing reviews, and it will also continue to monitor how CSIS leverages information received from other government agencies and departments, particularly in light of the enactment of the *Security of Canada Information Sharing Act*.

CSIS Response: CSIS agreed to expedite the finalization of the annexes underpinning the MoU. Discussions with CBSA are ongoing with regard to the requirement for, and value of, the annexes to the MoU.

III

INVESTIGATIONS

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 COMPLAINT INVESTIGATION PROCESS

Once SIRC receives a complaint, it must first determine whether it is related to its mandate. If so, SIRC will open an intake file and the SIRC Registrar will determine whether the intake file is complete and contains all of the appropriate forms, properly filled out as per the publicly available *Rules of Procedure*, and that no information is missing. If the file is incomplete or missing documentation, SIRC will contact the complainant to advise him or her of this.

Once the intake file has fulfilled the requirements of SIRC's *Rules and Procedures*, a formal complaint file is opened and SIRC conducts a preliminary review. If SIRC determines that the complaint does not fall within its jurisdiction under the *CSIS Act*, it will not investigate the complaint.

In September 2015, SIRC implemented changes to improve efficiency and make access to its process easier for members of the public.

If the complaint falls within SIRC's jurisdiction, it will be investigated through a quasi-judicial hearing presided over by a Committee Member assisted by SIRC's staff and legal team, who provide support and legal advice on procedural and substantive matters.

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

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

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 either not received a response within a reasonable period of time, or been dissatisfied with the response; and

2. SIRC must be satisfied that the complaint is not trivial, frivolous, vexatious or made in bad faith.

It is important to note that 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.

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, but no one is entitled as of right to be present during, to have access to, or to comment on, representations made to SIRC by any other person.

A party may request an *ex parte* hearing (in the absence of the other parties) to present evidence which, for reasons of national security or other reasons considered valid by SIRC, cannot be disclosed to the other party or their counsel. During such hearings, SIRC's legal team will cross-examine the witnesses to ensure that the evidence is appropriately

tested and reliable. This provides the presiding Member with the most complete and accurate factual information relating to the complaint.

Once the *ex parte* portion of the hearing is complete, 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 Emergency Preparedness 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 active SIRC complaints for the past fiscal year. The files closed encompass all completed investigations, complaints deemed to be outside SIRC's jurisdiction and those resolved without a hearing.

Table 2 - Complaints

PROGRAM	2015-2016
Intakes *	54
Complaints Carried Over From Previous Fiscal Year	30
New Complaints	26
TOTAL	56
Files Closed	41
Files Carried Forward	15

**Reflects changes implemented in September 2015.*

INVESTIGATION OF "AN ACT OR THING DONE BY CSIS"

The Committee investigated a complaint under section 41 of the *CSIS Act* in which it addressed the following issues: (a) whether CSIS illegally targeted and marginalized the complainant based on racial and religious profiling; (b) whether CSIS shared information with foreign states and if so, did it do so inappropriately or in contravention of the *CSIS Act* and applicable policies; (c) whether CSIS requested, directly or indirectly, the arrest, detention or denial of entry of the complainant into foreign countries; and (d) whether CSIS inappropriately interfered with the complainant's ability to leave Canada. The complainant also raised issues under the *Canadian Charter of Rights and Freedoms* (the Charter).

Based on the entirety of the evidence, the presiding member of the Committee found that CSIS's actions did not constitute racial profiling and did not breach the *CSIS Act* and applicable policies. Consequently, CSIS did not breach the complainant's rights under the Charter. The presiding member found that there was no evidence implicating CSIS in either the complainant's denial of entry into a foreign country or his deportation from another foreign country. Furthermore, the evidence demonstrated that CSIS had not interfered with the complainant's ability to leave Canada.

During the testimony of one of the witnesses, an issue arose as to whether a security screening assessment process was a "proceeding" under section 51 of the *CSIS Act*. Section 51 of the *CSIS Act* provides that, except for an offence under section 133 of the *Criminal Code*, no statement made during a testimony before the Committee can be admissible in another "proceeding". The witness in question was currently seeking a security clearance, and did not want any information that he would disclose during his testimony to be shared with the individuals responsible for his security screening assessment. In the end, the witness decided to testify, and the presiding member did not need to decide the issue.

Nonetheless, the presiding member stated that, if he had had to decide the issue, he would have found that a security screening assessment process is not a "proceeding" as understood under section 51 of the *CSIS Act*. The member noted that while the purpose of section 51 of the *CSIS Act* is to promote frank and full disclosure, it aims at ensuring that the information disclosed by witnesses will not be held against them in substantive legal proceedings where their rights, such as liberty, are at stake.

A security clearance is not of the same nature, as it provides an individual access to special information, and it is a privilege that can only be obtained following appropriate investigation of the individual's loyalty and reliability. Depending on whether the security screening assessment process were interpreted as a "proceeding" or not would determine whether CSIS could rely on that information in assessing an individual's loyalty and reliability.

IV

LIST OF RECOMMENDATIONS

REPORT	RECOMMENDATIONS
In its review of CSIS's Threat Reduction Activities, SIRC recommended that CSIS:	• Prioritize the development of formal mechanisms for consultation on threat reduction activities with relevant Government of Canada departments and agencies; and • Create a mechanism for tracking best practices and/or lessons learned for all threat reduction activities.
In its review of CSIS's Investigation of Canadian Foreign Fighters, SIRC recommended that CSIS:	• Seek legal clarification on whether CSIS employees and CSIS human sources are afforded protection under the Common Law rule of Crown Immunity in regards to the terrorism-related offences of the *Criminal Code of Canada*; • Conduct an assessment of additional measures for increasing operational support to intelligence officers working overseas, produce country-specific strategies where considerable operational activity transpires, and related to this, that CSIS HQ take on a more decisive leading role in certain foreign activities when necessary; and • Create, on a priority basis, a risk analysis framework to operationalize new Ministerial Direction, which requires it to consider operational, political, foreign policy, and legal factors when assessing risk.
In its review of CSIS's Warranted Collection of Information, SIRC recommended that CSIS:	• Implement changes to the way in which approval is given for specific operational activities;

- Create a formal and more robust internal process to assist the Director in determining when an action by an employee may have been unlawful;
- Implement a process to ensure that relevant CSIS stakeholders have knowledge of, and access to, legal opinions and/or advice;
- Improve the policy used to manage individuals who assist CSIS with warranted operations; and
- Develop other standardized processes to guide the future of warranted operations.

In its review of CSIS's Data Management and Exploitation Activities, SIRC recommended that CSIS:

- Finalize and implement the governance framework for dataset acquisition no later than February 1, 2016;
- Re-evaluate all referential bulk datasets against its criteria to ensure that they should continue to be considered referential and that those that are not should be assessed against the "strictly necessary" threshold;
- Undertake a formal and documented assessment for each of its existing non-referential datasets to ensure the information was collected only to the extent that was "strictly necessary;" and
- Halt its acquisition of bulk datasets until it has implemented a formal process of assessment to confirm that the bulk datasets meet the collection threshold.

In its review of Ministerial Direction and CSIS Directives on Information Sharing, SIRC recommended:

- That CSIS's executive prioritize the development of an action plan to address the issue of proper record-keeping within this fiscal year;
- That CSIS ensure that all deliberations at the management level, as well as all information related to the assessment criteria in question, be mentioned in the record of decisions; and

	• That CSIS make explicit in the record of decision-making its assessment of the foreign entity fulfilling the proposed assurance.
In its review of CSIS's Collection of Economic Intelligence, SIRC recommended that CSIS:	• Seek clarification on that type of activity when its assistance is requested through *Investment Canada Act* channels; and • Use consistent language in the advice it provides through the *Investment Canada Act* process: there either is or is not a national security concern, or there is not enough information to determine whether there is a national security concern.
In its review of CSIS's Traditional and Non-traditional Foreign Partners, SIRC recommended that CSIS:	• Begin with an arrangement with one (or more) narrowly defined unit(s) within the foreign agency before considering expanding the arrangement more broadly when faced with the necessity to cooperate with partners in countries with human rights concerns; and • Seek Ministerial approval as per the *CSIS Act*, or follow Ministerial Direction if exigent circumstances apply, when cooperating with a foreign agency with which it does not have a foreign arrangement.
In its review of CSIS's Relationship with the Canada Border Services Agency (CBSA), SIRC recommended that CSIS:	• Work closely with the CBSA to expedite the finalization of the annexes underpinning the 2015 Memorandum of Understanding.

V

HIGHLIGHTS

SIRC's Departmental Performance Reports and Reports on Plans and Priorities, which contain all of SIRC's publicly available financial information, are available on our website.

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	2014-2015 Expenditures	2015-2016 Planned Spending	2015-2016 Actual Spending	2016-2017 Planned Spending
Reviews	1,296,000	1,325,400	1,185,800	2,222,300
Legal Services	742,800	771,300	639,300	1,694,800
Subtotal	**2,038,800**	**2,096,700**	**1,825,100**	**3,917,100**
Internal Services*	941,300	780,700	1,044,300	3,187,700*
TOTAL	**2,980,100**	**2,877,400**	**2,869,400**	**7,104,800**

**Internal Services are groups of related activities and resources that are administered to support the needs of programs and other corporate obligations of an organization (i.e. human resources management, financial management, information management, information technology, ATIP). In 2016-2017, SIRC will be moving to new offices as our current office building will be disposed of by the owner. In addition to the costs for the relocation, SIRC will use this opportunity to upgrade its aging IT infrastructure and modernize its records management practices, including scanning and digitizing paper records. These initiatives will not only increase efficiencies but they will also ensure resources are spent prudently and in ways that maximize return on investment.*

HIGHLIGHTS OF SIRC'S OUTREACH ACTIVITIES THIS YEAR

APRIL 2015

Our Executive Director appeared before the Standing Senate Committee on National Security and Defence to discuss what Bill C-51 would mean for SIRC and for national security accountability in Canada.

MAY 2015

Our Director of Research and counsel put together a one-day discussion addressing the topic of intelligence accountability, entitled "Renseignement : perspective et analyse," to a class offered by the Université de Sherbrooke.

Our Executive Director and Deputy Executive Director gave an overview of SIRC and its role, as well as accountability in Canada, to a delegation of United States Congressional Fellows.

Our Executive Director appeared before the Standing Senate Committee on National Security and Defence to discuss Bill C-51 and the announced increase in SIRC's budget.

Our Executive Director and Deputy Executive Director presented at a conference hosted by the Philippe Kirsch Institute on the role of SIRC and the impact of new proposed legislation, particularly Bills C-44 and C-51.

JUNE 2015

Our Executive Director gave a presentation on our role, history and mandate at a federal/provincial/territorial meeting in the city of Québec.

OCTOBER 2015

Our research team gave a presentation on our structure and mandate to an undergraduate class at Carleton University studying the Canadian intelligence community.

Our Executive Director gave a presentation on intelligence oversight and review to the Canadian Military Intelligence Association (CMIA)'s third annual Canadian Intelligence Conference (CANIC 2015).

NOVEMBER 2015

Our Executive Director gave a presentation to a class of undergraduates at Ryerson University on SIRC and accountability in intelligence. This is the second year he has spoken to Ryerson students.

Our Deputy Executive Director and Director of Research gave a presentation during the "Intelligence and International Relations" conference at the University of Ottawa.

Our Director of Research and counsel gave a presentation to a University of Ottawa national security law class.

Our Executive Director participated in a panel and gave a presentation at the "Privacy and Access 20/20: The Future of Privacy" conference in Vancouver, B.C., hosted by the Information and Privacy Commissioner for British Columbia. The panel discussed *Anti-Terrorism Act, 2015*, national security and surveillance.

SIRC met with a representative of the Norwegian Parliamentary Intelligence Oversight Committee (the EOS Committee) in order to develop and maintain relationships with foreign review bodies.

FEBRUARY 2016

Our Chair and Executive Director appeared before the Standing Senate Committee on National Security and Defence to discuss the 2014-2015 annual report.

MARCH 2016

Our Deputy Executive Director provided an overview of our mandate and work to a University of Ottawa law class on national security.