ACCELERATING ACCOUNTABILITY

ANNUAL REPORT 2016–2017

SECURITY INTELLIGENCE
REVIEW COMMITTEE

Canada

Security Intelligence Review Committee

P.O. Box 2430, Station D Ottawa ON K1P 5W5

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

Catalogue No. PS105E-PDF

ISSN 1921-0566

Security Intelligence Review Committee

Comité de surveillance des activités de renseignement de sécurité

September 18, 2017

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

Dear Minister Goodale:

We are pleased to present you with the annual report of the Security Intelligence Review Committee for fiscal year 2016–2017, 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., C.M.
Appointed May 1, 2015

ABOUT SIRC

The Security Intelligence Review Committee (SIRC) is an external independent review body that reports to the Parliament of Canada on the operations of the Canadian Security Intelligence Service (CSIS). 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 activities; and conducting investigations into complaints.

SIRC has the absolute authority to examine all information under CSIS's control, no matter the classification or sensitivity, except Cabinet confidences. A summary of SIRC's work for the year, edited to protect national security and privacy, is presented in an annual report to Parliament and made available to the public.

SIRC exists to provide assurance to Parliament and to all citizens of Canada that CSIS 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 THE COMMITTEE

The members of the Security Intelligence Review Committee are 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.; the Honourable Marie-Lucie Morin, P.C., C.M.; and the Honourable Pierre Blais, P.C., who chairs the Committee.

The Committee is supported by an Executive Director and an authorized staff complement of 31, 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 members, in consultation with SIRC staff, approve direction on research and other activities that are identified as a priority for the year. Management of day-to-day operations is delegated — with direction, when necessary — to the Executive Director by the Chair, who serves as Chief Executive Officer.

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 and foreign stations 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.

TABLE OF CONTENTS

MESSAGE FROM THE COMMITTEE

A broad range of CSIS activities received SIRC's scrutiny this year, including security screening, foreign fighters (also known as extremist travellers), information sharing, and CSIS's foreign arrangements and activities abroad. SIRC examined activities in every CSIS domestic regional office, and visited three foreign posts. We completed the certification of the CSIS Director's report to the Minister of Public Safety and Emergency Preparedness and made multiple recommendations pertaining to CSIS policies, procedures and operations.

Our annual report, and our message, traditionally serves as a platform for commenting on the activities of CSIS in the previous fiscal year, in particular, what we examined, what we found and what we recommended. While this report will summarize the year's reviews and investigations of complaints, this year's message also discusses what is to come.

One aspect of the effectiveness of review as an instrument of accountability is timeliness. Our mandate involves determining whether CSIS respected the law and the rights of Canadians and informing all citizens of Canada about our work. While it is SIRC's experience that CSIS generally acts quickly to address our recommendations, the sooner we publish our findings, the sooner the public dimension of accountability can be engaged.

In January 2016, after reading SIRC's annual report, the Federal Court of Canada called on CSIS to explain the metadata activities of its Operational Data Analysis Centre. As a result, the Federal Court ruled that both collection and retention of metadata must pass the test — set out in section 12 of the *CSIS Act* — of being "strictly necessary." This decision confirmed SIRC's already long-standing practice of examining CSIS activities through the lens of section 12. SIRC has always been — and will continue to be — vigilant in its assessment of the lawfulness of CSIS activities, including in how CSIS applies the "strictly necessary" threshold to its collection and retention of information.

In response to the Court's ruling, the Minister of Public Safety and Emergency Preparedness invoked section 54 of the *CSIS Act* to formally request that SIRC review CSIS's response to the Federal Court. SIRC agreed. We are examining CSIS's response in terms of its treatment of the illegally retained data and its construction of a new compliance system for warrants and third-party/non–threat-related information. We are also examining CSIS's data set holdings to determine their relevance and necessity. SIRC will report its findings at the earliest opportunity to best serve accountability and transparency.

In supporting accountability for CSIS activities, SIRC promotes CSIS efforts to develop and effectively apply measures to encourage compliance and safeguard the rights of Canadians. Our value to the security and intelligence community goes much deeper, however, as we dedicate ourselves to encouraging the development of effective institutions to protect our country and our democracy.

As such, SIRC is anticipating the shift in the accountability landscape as Bill C-59 — which establishes both the National Security and Intelligence Review Agency to review all national security and intelligence activities and an Intelligence Commissioner to oversee, among other things, use and retention of datasets — makes its way through the House. These proposed legislative changes will serve to eliminate the current restrictions and silos in Canada's accountability structure. These changes reflect the need to take a horizontal approach to effectively review integrated security and intelligence activities, something SIRC has been commenting on for many years. For the time being, we continue to review new and emerging areas — such as cyber security (see p. 26) and terrorist financing (see p. 11), as well as the impact on CSIS of the *Security of Canada Information Sharing Act* (see p. 21). SIRC's accumulated experience and established independence mean we are well positioned to assist in the success of the new review agency and we look forward to contributing, publicly and in Parliament, to the discussion on Bill C-59.

From left to right: Ms. Marie-Lucie Morin, Mr. Pierre Blais, Mr. Gene McLean, Mr. Yves Fortier, Dr. Ian Holloway. © 2016 BalfourPhoto

MESSAGE FROM THE EXECUTIVE DIRECTOR

SIRC is pleased to present this annual report for 2016–2017, a year of new challenges and opportunities. In terms of outcomes, we have delivered in a number of important areas:

- we formalized risk-based planning for review;
- we completed an ambitious research plan, delivering 12 reviews — more than in any other year in our history;
- we visited and reviewed three foreign posts and dealt directly with all CSIS regional offices; and
- we, once again, comprehensively reviewed CSIS's threat reduction measures, which have been a subject of considerable debate.

SIRC's risk-based planning for reviews and our updated business plan mean that we are cognizant of the level and extent of coverage that we can provide on CSIS's activities. The increase in our capacity funding — first for one year, then extended for three additional years until 2020 — means that SIRC is operating at capacity with a significant complement of employees with broad and varied experience in national security and intelligence.

The professionalism of the staff at SIRC, our independence, and our role as a valued member of the security and intelligence community in Canada have been demonstrated time and again this year in our outreach and engagement with universities, practitioners and foreign partners. As we boost our efforts in these activities, we will continue to contribute to discussion and debate on issues dealing with accountability for security and intelligence. SIRC is also poised to work with the proposed committee of parliamentarians to ensure greater accountability and meaningful engagement. We look to next year with optimism and ambition.

CERTIFICATION OF THE CSIS DIRECTOR'S ANNUAL REPORT TO THE MINISTER

Pursuant to subsection 38(2) of the *Canadian Security Intelligence Service Act (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 annual report to the Minister;
- whether the operational activities described in the Director's report contravened the *CSIS Act* or ministerial directions; and
- whether the activities described in the report involved any unreasonable or unnecessary use of CSIS's powers.

This certificate therefore provides an important high-level assessment of the legality, reasonableness and necessity of CSIS's operational activities.

To fulfill its responsibility for the certification process, SIRC relies on a carefully designed and rigorous research methodology. To that end, SIRC conducts an extensive review of CSIS information holdings and requests briefings with CSIS officials to ensure that the information in the Director's report is placed in its proper context. SIRC grounds its assessment in reviews of several specific operations and activities referred to in the Director's report.

SIRC's ongoing baseline and thematic review work, which yields important findings and recommendations, directly supports the certification process. In addition, SIRC conducts three core reviews — human sources, targeting and warrant execution — to support the certification process. Those reviews include examining samples of each core function based on the investigations covered in the Director's annual report. SIRC assesses all its reviews against CSIS's compliance with the *CSIS Act* and ministerial direction in order to determine whether SIRC considers any use by CSIS of its powers to be unreasonable or unnecessary.

SATISFACTION WITH THE DIRECTOR'S ANNUAL REPORT

The Director's annual report for 2015–2016 was issued in December 2016, which SIRC does not consider to be timely. SIRC's ability to provide a meaningful assessment of the Director's annual report is contingent on its submission as soon as possible after fiscal year-end (March 31 of each year), so that SIRC may plan and devote adequate resources to thoroughly assess the activities described in the report in a manner that best serves accountability. SIRC is committed to

completing the certification process prior to the end of the fiscal year in which it receives the report. The purpose for this is twofold: first, to provide the most timely and relevant high-level assessment of the compliance of CSIS's operational activities and, second, to allow us to report to Parliament, and by extension to all Canadians, at the soonest opportunity through the SIRC annual report.

SIRC's satisfaction with the Director's report is based on its assessment of the extent to which the report provides information to assist the Minister in exercising ministerial responsibility for CSIS. SIRC used several criteria to make this assessment, including: whether the report met the ministerial reporting requirements set out in the 2015 ministerial direction, whether the report put the information in its proper context, and whether the report was factually accurate. This year, however, SIRC cannot ignore the issue of timeliness, which, in addition to the requirements identified above, is also clearly articulated in the ministerial direction. Although SIRC found that the information was placed in its proper context and was factually accurate, SIRC expressed concern about the delayed release of the Director's 2015–2016 report.

COMPLIANCE WITH THE *CSIS ACT* AND MINISTERIAL DIRECTIONS AND 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 the *CSIS Act* or ministerial directions, and whether the activities involved any unreasonable or unnecessary use of CSIS's powers. To make this assessment, SIRC reviewed ministerial direction to CSIS, including an examination of ministerial direction for operations and accountability and on intelligence priorities, as well as the Ministerial Direction on Information Sharing with Foreign Entities. SIRC also reviewed several specific operations and activities referred to in the Director's report, as well as a sample of the core CSIS activities that support the operations described in the report.

This year's report was somewhat of a transitional document that dealt with how CSIS was implementing the ministerial direction that came out in July 2015, halfway through the reporting period. SIRC noted that the Director's report did not mention several cases of non-compliance with the new ministerial direction that were subsequently brought into compliance. While SIRC understands the challenges around bringing existing operations into compliance with a direction issued mid-year, SIRC believes that the cases should have been included in the report: not only were they non-compliant, but they also represented an illustration of the scale and scope of operations that needed to be brought into compliance with the new ministerial direction. Overall, SIRC found that, with some minor exceptions, CSIS was in compliance with the *CSIS Act*, ministerial direction and operational policy.

THE DIRECTOR'S ANNUAL REPORT AS A MECHANISM OF MINISTERIAL ACCOUNTABILITY

Over the past four years, SIRC has commented on the content and structure of the Director's annual report in order to further refine its utility as a mechanism of ministerial accountability. In addition, SIRC has made recommendations in several reviews in recent years calling for more frequent and timely communication with the Minister on issues of significance or sensitivity. SIRC is aware that this communication has increased and notes that CSIS provided oral

and written briefings to the Minister throughout the period. These briefings form part of the supporting documentation of the Director's report and should therefore be included in SIRC's certification process.

As such, SIRC should be receiving copies of these reports and information on the oral briefings in order to fulfill its certification obligation. SIRC expects to receive copies of ministerial briefing notes, in addition to the Director's annual report, so that it can assess satisfaction and compliance on all reporting to the Minister for the purposes of ministerial accountability.

GOVERNANCE

The Director's annual report covered a number of governance issues including policy, accountability and partnerships — both foreign and domestic — in order to show how CSIS supports the "responsible exercise of authorities in accordance with the *CSIS Act*." SIRC examined the relevant documentation and received briefings on several aspects of CSIS governance.

Specifically, SIRC reviewed CSIS's foreign arrangements and met with CSIS personnel to discuss the foreign arrangements process. SIRC observed the lengthy time from application to approval of new foreign arrangements during the period covered by the annual report. SIRC notes that with the *Protection of Canada from Terrorists Act*, CSIS has explicit authority under subsection 12(2) of the *CSIS Act* to operate abroad. However, the length of time required to establish a foreign arrangement can be significant. The timeliness of the process by which CSIS establishes foreign arrangements may need to be reconsidered in light of increased operational activity abroad, including perhaps a distinction between foreign arrangements for liaison and those for operational theatres.

SIRC also examined the update of the One Vision, a framework for cooperation between CSIS and the Royal Canadian Mounted Police (RCMP), and received briefings covering the ongoing policy revisions and updates to bring it in line with strengthened risk assessment and accountability. SIRC was also briefed by CSIS on the new compliance-reporting regime that CSIS is in the process of implementing. SIRC will continue to assess these developments through its reviews.

THREAT REDUCTION MEASURES

CSIS is required to report on its threat reduction measures in the Director's annual report. SIRC is also obligated to review threat reduction measures on an annual basis, which it does through an annual stand-alone review (see p. 25). For 2015–2016, SIRC found that all measures that CSIS had approved or considered during that period complied with the *CSIS Act*, ministerial direction and operational policies. At that time, SIRC recommended that CSIS prioritize the development of formal mechanisms for consultation with relevant Government of Canada departments and agencies and for tracking best practices and/or lessons learned.

CONCLUSION

SIRC will continue to fulfill its statutory requirement to certify the Director's annual report to the Minister. However, next year, SIRC expects to receive the Director's report earlier and to be able to carry out its responsibility with more insight into the operational information provided to the Minister in the form of oral and written briefings.

EFFECTING CHANGE THROUGH REVIEW

As Public Safety Canada stated, Bill C-59 "responds to recommendations raised in recent reviews by the Security Intelligence Review Committee." Specifically, the proposed changes address SIRC's recommendation that CSIS put in place formal internal mechanisms to ensure that none of its human source operations are in contravention of the *United Nations Al-Qaida and Taliban Regulations* or any similar Canadian statute or regulations.

The bill also proposes to create not only a National Security and Intelligence Review Agency, but also an Intelligence Commissioner to authorize certain intelligence and cyber security activities prior to their conduct. These include the Minister's decisions regarding classes of Canadian data sets that CSIS could collect and the retention of foreign data sets.

These proposed changes are responses to the following recommendations that SIRC has made in the last three years regarding data sets and metadata:

- SIRC recommended that CSIS make the Court aware of the particulars of CSIS's retention and use of metadata collected under warrant;
- SIRC recommended that CSIS re-evaluate all referential bulk data sets to ensure that they should continue to be considered referential, and those that do not should be assessed against the "strictly necessary" threshold;
- SIRC recommended that CSIS undertake a formal and documented assessment for each of its existing non-referential data sets to ensure the information was collected only to the extent that was "strictly necessary"; and
- SIRC recommended that CSIS halt its acquisition of bulk data sets until it has implemented a formal process of assessment to confirm that the bulk data sets meet the collection threshold.

REVIEWS

THE REVIEW PROCESS AT SIRC

SIRC's reviews are designed to provide Parliament and Canadians with an assessment of whether CSIS performs its duties and functions appropriately, proportionally, effectively and in accordance with the law. SIRC reviews cover all of CSIS's key activities, including targeting, warrants and human sources, and CSIS's program areas, including counter-terrorism, counter-intelligence, counter-proliferation and security screening. Besides examining CSIS's arrangements for cooperating and exchanging information with foreign agencies and domestic organizations, SIRC examines the advice CSIS provides to the Government of Canada.

A typical review requires hundreds of staff hours and is completed over a period of several months. As part of this process, SIRC researchers consult multiple information sources to examine specific aspects of CSIS'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 CSIS. 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 members for approval. Once the Committee has approved the reviews, SIRC sends them to the Minister of Public Safety and Emergency Preparedness and to the CSIS Director.

Each review is also included — after being edited for national security and privacy considerations — in the annual report tabled in Parliament.

With the exception of Cabinet confidences, CSIS cannot withhold any information from SIRC, on any grounds.

SIRC'S METHODOLOGY

To provide comprehensive and meaningful review of CSIS's activities, SIRC relies on risk-based planning. This method allows SIRC to identify all areas of CSIS activity and rank them annually in terms of risk, which contributes to the focus and coverage of reviews. Given that it is impractical for an organization as small as SIRC to examine all of CSIS's duties and functions annually, risk-based planning also allows SIRC to ensure that all CSIS activities are reviewed regularly and systematically.

SIRC assesses CSIS's activities as effectively as possible through a carefully selected combination of review methods. Each review that SIRC produces falls into one of the following categories.

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

Investigation/program reviews: these reviews examine a particular CSIS investigation or area. They are valuable in that they allow SIRC to maintain knowledge of priority investigations on 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 — that is, targeting, warrants and the use of human sources — through a larger sample analysis. These reviews provide an opportunity for SIRC to drill down more deeply into a specific type of activity.

THE YEAR AHEAD

In 2017–2018, SIRC will be reviewing a broad range of CSIS activities, including reviews of CSIS's efforts to comply with the Federal Court decision on the retention of metadata; threat reduction measures; right-wing extremism; and CSIS's approach to targets and sources with mental health issues. SIRC will continue to examine CSIS's activities abroad, including a review of operational activities in combat zones and reviews of three foreign stations.

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* — for example, reasonableness, proportionality and strict necessity — as well as principles of good governance, such as compliance with ministerial direction and CSIS's policy framework.

RECOMMENDATIONS

SIRC reviews include findings and, when appropriate, recommendations. The guidelines for SIRC's recommendations ensure that they are practical, constructive, and focused on tangible actions and results.

SIRC actively solicits a formal response from CSIS to its recommendations. CSIS is expected to clearly and unambiguously indicate whether it agrees or disagrees with each recommendation, what actions it intends to take in response to the recommendation, and when it intends to take such action. Including those declassified responses in the review summaries of this report provides greater transparency and gives the public better insight into the impact of SIRC's work on security intelligence.

REVIEW SUMMARIES

CSIS'S INVESTIGATION OF TERRORIST FINANCING

Terrorist financing involves the raising, moving, using and storing of funds for terrorism-related purposes. In this review, SIRC examined how CSIS investigates terrorists' use of financial mechanisms to fund threat-related activities and sought to provide a general overview of financial intelligence, including CSIS's governance structure, CSIS's cooperation with domestic partners, CSIS's strategic initiatives with the financial sector, and a case study. Because CSIS's collection methods underlie these issues, they were also examined.

FINDINGS

Overall, SIRC found that CSIS's investigation into threat financing activities complied with the *CSIS Act* and ministerial direction. One particular case, however, raised concerns about whether information that CSIS received and retained met the "strictly necessary" legal threshold for retention. SIRC also noted that CSIS should strengthen the governance framework around these disclosures.

CSIS uses financial intelligence to identify the financial means and methods used to facilitate threats, and to understand the intentions, capabilities, and activities of individuals or groups of concern. According to CSIS, financial intelligence can aid in determining whether a group is well funded and organized, from what countries or regions it draws its support, and how its financial profile is changing over time.

In one particular instance, SIRC believed that CSIS did not abide by the "strictly necessary" principle when it incorporated financial information into its operational database.

SIRC found that obtaining this type of information requires additional direction. **SIRC made two recommendations, one concerning CSIS's work in this area and one related to the clarity of retention thresholds in policy**.

Given the importance of the relationship between CSIS and the Financial Transactions and Reports Analysis Centre (FINTRAC), SIRC reviewed all information sharing between the two organizations during the period under review. Overall, SIRC found that information exchanges between CSIS and FINTRAC complied with the *CSIS Act* and CSIS policies and procedures.

CSIS RESPONSE

CSIS agreed with one recommendation and partially agreed with the other, noting that the retention thresholds were being considered within a broader effort already underway within CSIS.

A TYPE OF WARRANTED TECHNICAL COLLECTION

Last year, SIRC reviewed a large number of CSIS operations executed under a warrant. This review continued this examination of CSIS's warranted operations, focusing broadly on how CSIS ensures compliance with the terms and conditions of warrants in three contexts.

FINDINGS

The first was a specific type of technical collection that is used to support investigations. SIRC looked at how CSIS executes this type of technical operation. SIRC noted that a number of significant changes in technology have combined to create challenges in the execution of this type of collection with respect to the privacy of persons not named in the authorizing warrant.

With that in mind, SIRC examined the documentation for seeking approval for the execution of a warrant power. SIRC observed that for most of the period under review, certain information was not always included in the approval documentation. SIRC found not having a policy requiring this information created a risk of non-compliance with the warrant. Notwithstanding that, SIRC found that CSIS made good faith efforts to comply with the terms and conditions of the warrants. Moreover, by the end of the period under review, CSIS had established a new process that better reflected the need to include all relevant information.

SIRC also considered the implications of the significant changes in technology for the execution of the warrants. In SIRC's view, the warrants invoked during the initial period under review did not contemplate the eventual change in the nature of the operation. A new type of warrant created toward the end of the period under review better accommodates this type of operation. However, SIRC believes that earlier consultations with the Department of Justice could have mitigated any risk that the specifics of the operation might exceed what was allowable under the warrant authority. Certain changes have taken place internally to encourage the solicitation of legal advice as necessary. Alongside this, SIRC believes that there should be an ongoing flow of information between the Department of Justice and CSIS on the technical details related to the execution of warrant powers.

The second area of focus involved a series of warrant non-compliance incidents that have occurred intermittently since March 2012. Given the seriousness of the issue, CSIS working groups were established to complete a full analysis of the scope and impact of this discovery, and external stakeholders were also informed — including the Minister of Public Safety and Emergency Preparedness, the Federal Court and SIRC.

The crux of the problem involved both computer errors and human errors, resulting in information being retained within CSIS's databases that should have been deleted. Despite the seriousness of the errors, CSIS assessed that the actual impact on the privacy of individuals was minimal, given that the retained data was not used for operational reporting purposes. Given that the data was supposed to be deleted — and CSIS had believed it had been deleted — there was no reason for the information to be used for operational reporting purposes.

SIRC closely reviewed efforts by CSIS to delete all of the improperly retained information and, as of June 6, 2016, CSIS confirmed that it had all been deleted. CSIS has since introduced additional computer improvements and human auditing processes to reduce similar occurrences.

Irrespective of these improvements, SIRC believes that one reason these retention errors continued unnoticed for so long was that those employees with expert knowledge of intercept technologies and CSIS databases had incomplete knowledge of warrants, while those employees who knew about the importance of warrant precepts had incomplete knowledge about the technologies used for collection and retention. As such, SIRC found that a gap has slowly developed between CSIS's use of technology and the management of critical compliance functions.

The appropriate retention of information by CSIS, and the technical and human processes used to make such determinations, remains an issue beyond the scope of this particular review. As such, SIRC will be following up on this topic in next year's review cycle.

Finally, SIRC examined a specific intercept operation that occurred without legal authority. This non-compliance, which was brought to SIRC's attention by CSIS, occurred in a specific technical operation conducted for the first time in a particular region. In its review, SIRC saw that there were discussions with respect to whether the operation was compliant with the language of the existing warrant before the execution of the warrant power. Ultimately, CSIS decided that the proposed operation could proceed.

However, several months later, the same operation was proposed in a different region. In contrast to the first region, this region consulted with the office of the Deputy Director Operations on whether the operation could take place within existing warrant conditions. Eventually, the Department of Justice was consulted as well and it was determined that the operation was not permitted within the warrant language. The first region was informed of the legal interpretation and those technical operations were immediately terminated.

Soon after the operations were halted, CSIS instituted a number of practices to raise visibility for this type of warrant execution and the Minister of Public Safety and Emergency Preparedness was informed of the incident in the Director's 2014–2015 annual report. Concern over a repeat of this error was rendered moot following changes to the warrant templates to permit this type of activity.

This incident highlights an inconsistency in how warrants are interpreted, as well as in the hiring and warrant training for key employees across job functions. This is problematic given that those employees are responsible for ensuring that they understand warrant powers and conditions in the context of warrant executions.

SIRC also enquired if CSIS had informed the Federal Court of the incident. CSIS responded that it had not done so prior to the Court granting these new powers, although the matter was reported to the Minister of Public Safety and Emergency Preparedness in the Director's annual report. The Federal Court has since been advised of the matter.

CSIS's warrant activities must conform to what was initially prescribed by the Federal Court and, in cases where it failed to do so, it is SIRC's opinion that the Court would benefit from this knowledge so as to prescribe whatever the Court deems appropriate in that circumstance. It is therefore a positive development that the Department of Justice and CSIS are jointly working on a series of measures aimed at reinforcing the capacities of both organizations to discharge their obligation to the Federal Court. SIRC believes this may result in additional measures that will further enhance accountability.

To address internal changes needed at CSIS, **SIRC recommended that**:

- **all employees with warrant-related responsibilities receive standardized and comprehensive training on an ongoing basis, and that those responsible for providing legal advice have up-to-date knowledge about technical operations;**
- **roles and responsibilities be clearly defined and standardized across the regions; and**

- **CSIS create a warrant policy centre devoted to the execution of warrants.**

CSIS RESPONSE

CSIS agreed with all of the recommendations, noting that it was already in the process of initiating a number of interrelated activities to enhance the training and awareness of employees with warrant-related responsibilities and is also providing technical briefings to CSIS legal counsel, as well as the Federal Court. Furthermore, CSIS is in the process of implementing a new governance framework for warranted activities, including clarifying the role of the policy centre and defining and standardizing warrant-related roles and responsibilities.

SECURITY SCREENING

The mandate of the security screening program is to prevent individuals of security concern from gaining access to sensitive Canadian information, assets, sites or events, and to prevent entry to or the acquisition of status in Canada by non-Canadians who pose a security threat. To this end, CSIS provides security assessments to other government departments and security advice to Immigration, Refugees and Citizenship Canada and the Canada Border Services Agency under the authorities of sections 13 and 14 of the *CSIS Act*, respectively. Security screening is one of CSIS's two major operational programs. SIRC examines the security screening process on a continual basis as part of its complaints function and on a biennial basis through its review activity.

FINDINGS

The present review included a follow-up to CSIS's response to SIRC's 2013 recommendation to consult with the Office of the Privacy Commissioner of Canada about a change SIRC believed possibly violated the *Privacy Act*. At the time of this review, these consultations were still ongoing; nevertheless, SIRC expects CSIS to abide by any recommendations or decisions made by the Office of the Privacy Commissioner of Canada.

SIRC also examined the technological changes put in place by CSIS to increase the effectiveness and efficiency of the Security Screening Branch (SSB). Since SIRC's last screening review, the SSB has benefited from significant advances in technology: technology has changed not only how the SSB performs its duties on a daily basis, but also how the SSB collaborates with its partners. To understand this evolution, SIRC looked at the role of two specific advances used by the SSB, as well as two case studies looking at how technology has furthered security screening. SIRC found that technological advances have resulted in CSIS being better equipped to manage its regular screening responsibilities, as well as any emerging issues or special events that may arise. In the review of one of the case studies, however, SIRC found that CSIS had unnecessarily shared information about Canadians with a Five Eyes partner.

SIRC then turned its focus to what tools and methods CSIS used to conduct its security screening investigations and whether or not they comply with the *CSIS Act* and internal policy. SIRC looked at three tools/procedures used in security screening investigations. SIRC found that in two instances, the use of these tools/procedures in screening investigations conformed to policy, although

SIRC recommended that internal procedures be updated. However, when examining how CSIS collects information during the course of a security screening investigation from an employer, SIRC was concerned that CSIS had issued a memo allowing investigators to obtain information without properly considering the implications of the expectation of privacy.

In view of recent case law regarding section 8 of the *Canadian Charter of Rights and Freedoms* (the Charter), SIRC was concerned about information CSIS obtained from employers for a limited number of security screening investigations. SIRC found that obtaining particular information without a warrant for security screening investigations creates a situation through which CSIS could obtain information for section 12 purposes without a warrant. **SIRC recommended that a review of these particular cases be conducted in conjunction with the Department of Justice and that, if it is determined that *Charter* rights were infringed, the information be purged from CSIS's holdings. Going forward, SIRC recommended that CSIS follow the same procedures for security screening investigations as are applicable to its other investigations, including seeking a warrant from the Federal Court in appropriate cases**.

Overall, the security screening program has evolved to become more efficient and effective at providing its clients with required information in a timely manner. Nonetheless, SIRC expects all security screening investigations to be conducted according to the principles of necessity and proportionality. This includes infringing on the privacy of individuals only when there are valid reasons to do so and only to the extent that is necessary.

CSIS RESPONSE

CSIS agreed with all of the recommendations. CSIS noted that the referenced investigative practices were developed pursuant to legal advice that set out the criteria under which this information could be obtained without a warrant. CSIS agreed to ask the Department of Justice to review all the cases highlighted by SIRC, and that if it was determined that the reasonable expectation of privacy was not properly considered, to destroy the information in question. SIRC will also be advised of the outcome of the review.

EVOLVING PLATFORMS ABROAD

In recent years, CSIS has developed a new foreign collection platform model to refine and enhance its collection capacity abroad to better meet intelligence requirements. In late 2014, CSIS decided to pilot this concept at a station, given the station's geopolitical and strategic importance in the ongoing investigation against Daesh and Canadian foreign fighters.

The new collection platform deploys additional staff with diverse skill sets, is led by a senior executive, and has enhanced communication connectivity and operational resources. Under this platform, the station was expected to respond more nimbly to intelligence requirements while covering a larger investigative area.

SIRC assessed the new model's initial rationale and current functionality. SIRC aimed to gain a thorough understanding of the initiative, as well as to better understand CSIS's vision for

In the 2016 *Public Report on the Terrorist Threat to Canada*, the Minister of Public Safety and Emergency Preparedness observed that: "It is a serious and unfortunate reality that terrorist groups, most notably the so-called Islamic State of Iraq and the Levant (ISIL), use violent extremist propaganda to encourage individuals to support their cause. This group is neither Islamic nor a state, and so will be referred to as Daesh (its Arabic acronym) in this Report."

its foreign collection activities going forward. In addition to extensive document review and briefings with representatives from CSIS Headquarters, SIRC conducted an on-site visit to this foreign station in mid-October 2016. SIRC examined not only the activities of CSIS personnel at the station, but also the station's operations in support of a particular investigation. While at the station, SIRC's Executive Director and accompanying staff held several meetings with CSIS personnel, as well as with other pertinent Government of Canada officials in the region.

FINDINGS

Overall, CSIS has methodically tracked the progress of this pilot initiative and identified areas requiring further attention to help meet operational objectives. The functionality of the concept was initially hindered by limited work stations for the additional staff, connectivity and technical issues, and the need to divert the station's resources to assist with a particular investigation.

A key success thus far has been greater engagement with foreign regional partners, as well as the development of new foreign partnerships to help collect intelligence related to Daesh and foreign fighters. The overall impression was that CSIS is regarded as a valuable team player among Government of Canada counterparts.

At the heart of this transition is the relationship between CSIS Headquarters and the station, as well as the issue of delegated authorities to managers deployed overseas. The nature and extent of support provided by CSIS Headquarters remains to be determined, on both the operational and the administrative front. While the delegation issue proved challenging to implement, it will be crucial to the success of the platform. All stakeholders appear committed to making the pilot work. On the ground, certainly, SIRC heard that the model is the right one to support CSIS with its overseas collection mandate.

SIRC expected CSIS to apply the lessons learned from its experience in various dangerous operating environments for activities in support of the operation under review. However, CSIS has not created any formal process for discussing, evaluating, assessing and documenting what would constitute necessary and reasonable standard operating procedures

for operations within specific dangerous operating environments. **SIRC recommended that CSIS develop standard operating procedures derived from lessons learned from operating in dangerous operating environments**.

CSIS's collection efforts within a specific dangerous operating environment did not produce significant intelligence to address a key intelligence requirement. In addition, SIRC heard that in certain cases, collecting intelligence on specific CSIS targets in the region can be challenging, if not dangerous. **SIRC recommended that CSIS create clear operational objectives to assist the station in addressing key intelligence requirements, including further assessment of the resource allotment to ensure that CSIS can sufficiently meet Government of Canada intelligence needs. In addition, SIRC recommended that CSIS create, on a priority basis and in consultation with the Department of Justice, policy and procedures regarding the use of information sharing in dangerous environments**.

One of the final objectives of the review was to follow up on observations from last year's review of CSIS's investigation of Canadian foreign fighters. At that time, SIRC 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 Headquarters take on a more decisive leading role in certain activities when necessary. These recommendations are still being implemented. Further, CSIS is still undergoing changes in the scope and sophistication of its operations abroad and other operational enhancements. Nonetheless, SIRC believes that CSIS is gradually embracing a more strategic approach to undertaking overseas collection.

CSIS RESPONSE

CSIS agreed with all of the recommendations, noting that work has already commenced to develop standard operating procedures for dangerous operating environments to supplement the tools and mechanisms that already exist. CSIS agreed that clear objectives are necessary to ensure the success of CSIS contributions to Government of Canada efforts and provides these to its overseas stations via the collection requirements that are disseminated in several types of documents. Additionally, CSIS works with its Government of Canada clients to ensure it is meeting their requirements and updates the operational objectives accordingly. In conjunction with these efforts, CSIS actively assesses staffing requirements on an ongoing basis. With respect to information sharing in dangerous operating environments, CSIS has prepared instructions in consultation with the Department of Justice and new procedures are expected to be published in the fall of 2017.

INFORMATION TECHNOLOGY ACCESS CONTROLS

CSIS operates a complex information management and technology environment that is subject to pressures from deliberate threats within Canada and abroad. Although information is the currency of CSIS, the organization must balance the imperative for collaboration and sharing, while restricting access to sensitive intelligence and protecting the privacy of individuals.

The objective of this review was to evaluate the appropriateness of security access control measures as a means of safeguarding sensitive information within CSIS. Although the focus of the review was information technology access control, SIRC also sought to address the general security and privacy controls or mechanisms that determine access.

The core principle in determining the sufficiency of access controls was to first verify if they comply with policy, standards or guidelines and, second, to ensure they were appropriately aligned to address the level of risk.

FINDINGS

Overall, SIRC reviewed CSIS's security policies, procedures and directives for completeness against government and departmental policy and standards, and found that they met or exceeded requirements established by the Government of Canada.

CSIS has a clear roadmap and executive commitment toward information technology security. It is articulated as a strategic organizational priority. In this regard, SIRC found that CSIS demonstrated a high level of maturity in information management, security and privacy by design, and that personnel showed exemplary understanding of corporate systems, security, information and technology.

SIRC was able to identify with rigour and confidence all system components, security access controls and safeguards. Moreover, SIRC reviewed procedural and technical documentation, and threat and risk assessments, as well as independent certification evidence, privacy impact assessments, and third-party security testing. SIRC received briefings from business units and conducted thorough interviews of experts within CSIS.

Over the past few years, CSIS has deployed security controls to address potential weaknesses in the storage, transmission and sharing of classified information as part of its Information Technology Security Roadmap. Based on its review of the roadmap and supporting evidence, SIRC agrees with the requirements and recommendations for security controls. **SIRC recommended that CSIS implement those findings on an accelerated timeline and extend the initiative across its system**.

On the matter of access control, **SIRC recommended that CSIS develop policy, guidance and procedures that define separation of duties and its implementation across all branches. Based on best practices, these policy instruments could require the user to authenticate using multiple factors**.

Finally, SIRC found that CSIS is fully compliant in the manner in which it is managing risk in the control of access to sensitive information, but noted that the risk assessment does not appear to have explicitly benefited from the full strength of in-house expertise. Thus, **SIRC recommended that CSIS's risk management process integrate operational threat intelligence with the objective of achieving best security practices across the organization**.

CSIS RESPONSE

CSIS agreed with all of the recommendations.

BUSINESS MODERNIZATION

Beginning in 2010, CSIS undertook several corporate initiatives that identified a number of deficiencies in its operational model. In response, CSIS launched a plan in 2012 to modernize its business. This important operational initiative is intended not only to change how CSIS approaches its operations, but also to transform the roles and responsibilities of its staff. The new business model focuses on streamlining operational functions, with greater emphasis on collaboration and integrated approaches to managing investigations. First piloted in two regional offices, the initiative is still ongoing as significant changes are rolled out both at Headquarters and in the regions.

Guided by three objectives, SIRC established this baseline review to gain a deeper understanding of the model. First, SIRC examined the purpose and

rationale behind the initiative — the need for the transformation and the key components. Second, SIRC looked at how CSIS implemented the initiative, by focusing both on the regions and desks first involved in the initiative, and on Headquarters' expectations. This included an examination of how the plan is actually functioning in the regions and any adjustments the regions made to reflect the reality of the operational environment or the requirements of the desks. Finally, SIRC focused on the implications and operational impact of the initiative from both a Headquarters and regional perspective.

SIRC consulted with all of the regions and examined documentation related to working groups and employee feedback on the initiative.

FINDINGS

Overall, SIRC found that although the model is predicated on a consistent approach to operations, flexibility exists for the regions/desks to adjust the model to meet the realities of individual operating environments.

One of the primary goals of the initiative was to create an operational environment that can be proactive, flexible and forward looking. To achieve these goals, the model clearly delineated and defined positions, which cover the spectrum of CSIS activity and provide for clear case management. However, in setting out these roles, Headquarters did not dictate how they were to be established or implemented. What Headquarters did specify were the principles behind the transition to make clear to the regions what the outcomes should be. The model also reinforces a team-based approach to operations and investigations.

Based on the pilot in the regions, CSIS held formalized feedback sessions with regional staff and prepared a final report. With this feedback, Headquarters issued a document that clarified the various roles and their interactions in order to provide more structure and reduce some of the challenges that had resulted from the ambiguity. From there, CSIS rolled out the model nationally to all regional offices and formed a regional working group of representatives from each region to share lessons learned and exchange information and experiences.

The model delivered benefits such as the furthering of investigations and the increased inclusion of other areas of operational support. The team-based approach for tackling leads, gaps and investigations resulted in integrating roles that had traditionally been viewed as "support" functions so that they now play a larger role in day-to-day regional work. SIRC noted the increased collaborative atmosphere in the regions and CSIS staff reported, universally, that this has been a positive development.

CSIS identified a number of challenges stemming from the model, such as negative preconceptions about the new positions. Regions were given the latitude to decide how to place staff. This was not an easy exercise and there were definite growing pains during the rollout.

The smallest region had the fewest resources and, therefore, found it the most difficult to adapt to a model based on defined roles. Nonetheless, it was able to find a suitable working solution. The region is currently considering a test case for a slightly modified model. Overall, the model's consistent approach to operations still allows flexibility for the regions/desks to adjust the model to the realities of individual operating environments.

While the national rollout is still in its early phase, a few consistent messages emerged. First, the cultural shift, growing pains and change fatigue did not diminish the value or perceived value of the model overall. The collaborative team approach provides a better understanding of various roles and allows more direct input from a diverse number of people working on the file.

All regions, however, noted one drawback: resources. Many regions do not always have enough personnel to fill all of the roles identified under the model. And even when those roles are filled, the model is more acutely affected by vacancies and staff absences, particularly in the smaller offices, where a single absence can make a big difference.

All regions also commented on communication as key to the success of the model — both between the various roles at the working level and between the working level and management. The regions, whether formally or informally, have developed methods for mitigating this through a variety of communication methods (e.g., bi-weekly meetings, informal newsletters, brainstorming sessions). Overall, SIRC found that communication will continue to be an essential element of this transformation — even after it has been firmly established as part of the operational culture of CSIS.

Further changes are to come. The goal at Headquarters is to clarify the roles and functions between Headquarters and the regions, and to provide streamlined and coordinated functions. Overall, the implementation was carefully considered and rolled out in a manner that provided flexibility for the regions to address and adapt the initiative to operational realities. Given the magnitude of the cultural change, the transition will take time. SIRC recognizes that the initiative is ongoing and that there are lessons still to be learned and best practices to be shared. SIRC will have the opportunity to examine the impact of this new model and its implementation at Headquarters in the context of its ongoing reviews.

FOREIGN FIGHTERS

Canadian foreign fighters are the Government of Canada's top intelligence priority, making their investigation by CSIS the topic of reviews in SIRC's last two research cycles. In 2014, SIRC undertook a baseline study to examine CSIS's investigation of the foreign fighter threat by focusing on domestic investigative efforts, as well as how CSIS's own strategies, definitions, management processes and governance feed into the whole-of-government approach to this issue. Last year, SIRC looked at CSIS's evolving foreign fighter strategy abroad, focusing on the use of a particular human source outside Canada. This current review provides an update on the domestic front, especially recent trends and challenges.

The ability for Sunni Islamist extremist organizations like Daesh or Jabhat al-Nusra to lure foreigners to combine their anti-Syrian regime fight with current and future planned attacks on Western countries has translated into a complex and challenging investigation that goes beyond extremist travel into one that seeks to understand the intentions and capabilities of individuals who have travelled abroad, stay in conflict zones, or have returned for a variety of reasons.

Through this review, SIRC examined how CSIS tracks, analyzes and provides indicators on foreign fighters to its executive and key Government of Canada clients. SIRC also reviewed CSIS's approach to a dynamic threat environment, with a particular focus on how CSIS deals with increasingly younger targets and sources. Finally, to examine the front-line operations related to the foreign fighters investigation, SIRC reviewed one region and its approach to a specific target.

FINDINGS

Within the Government of Canada, the issue of foreign fighters involves a number of departments and agencies. CSIS works closely with all its domestic partners in an effort to minimize duplication and enhance understanding of the foreign fighter problem. In light of the importance attached to the foreign fighter issue, CSIS received a significant increase in resources in the 2015 federal budget.

The influence and threat posed by Canadian foreign fighters goes beyond the numbers, and is of particular concern domestically for a number of reasons. Canadian extremists who remain abroad do more than pose a threat to stabilization efforts in foreign countries and to local populations, Canadian interests abroad, and Canadian Armed Forces operating in conflict zones. These individuals may also use social media to "reach back" to Canada to influence others to follow their radical path.

SIRC's first review on foreign fighters noted the potential challenges with returnees versus those who were denied travel, explaining that "going forward, CSIS may continue to face the challenge of shifting its investigative emphasis away from the threat posed by returnees toward the growing number of radicalized Canadians who seek to travel for the purposes of engaging in terrorist activity abroad, but are denied the ability to leave Canada."

The current review underscored this dilemma: extremists who have travelled to conflict areas may indeed be well trained or battle-hardened and potentially return to Canada in order to carry out attacks at home. And while considered unlikely in the near term, this possibility can no longer be treated as a hypothetical — especially in light of the recent attacks in Paris and Brussels. Another problem is that returnees use the knowledge they gained abroad to act as facilitators for the movement of travellers and/or funds to conflict zones. While some returnees might come back disillusioned (or "scared straight") following their experiences abroad, others continue to hold extremist beliefs with a continued desire to travel abroad.

SIRC examined one investigation in detail that highlighted the challenges associated with running a parallel investigation with the RCMP. SIRC found that CSIS managed the investigation appropriately. SIRC also examined, as part of its sample, cases where the targets were minors. Minors as foreign fighters present several challenges for CSIS going forward. It is well recognized in Canadian and international law that youth are entitled to different fundamental rights because of their legal status. Accordingly, ministerial direction and CSIS policy and procedures indicate that a higher level of approval is required for targeting minors than for adults. However, this protection is not explicitly extended to the disclosure of information on a minor target to foreign intelligence agencies.

SIRC examined all disclosures to foreign intelligence agencies for several targets that were minors. SIRC found that CSIS carried out its investigation of these targets in compliance with existing policies and procedures. However, as foreign intelligence agencies may operate with a different understanding of the rights of minors, **SIRC recommended that an additional caveat be applied to all disclosures to foreign intelligence agencies where the target is a minor**.

CSIS RESPONSE

CSIS agreed with the recommendation, adding that a new policy will be drafted to supplement those already in place, with specific reference to CSIS activities involving minors, including information disclosures.

THE *SECURITY OF CANADA INFORMATION SHARING ACT*

The Security of Canada Information Sharing Act (SCISA) came into force on August 1, 2015. SCISA is said to encourage "effective and responsible" information sharing for national security purposes by establishing a single authority for federal institutions to share information with designated recipient institutions, including CSIS. Under SCISA, information may be disclosed if it is "relevant to the recipient institution's jurisdiction or responsibilities under an Act of Parliament

THREATS TO THE SECURITY OF CANADA MEANS:

(a) espionage or sabotage that is against Canada or is detrimental to the interests of Canada or activities directed toward or in support of such espionage or sabotage,

(b) foreign influenced activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person,

(c) activities within or relating to Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political, religious or ideological objective within Canada or a foreign state, and

(d) activities directed toward undermining by covert unlawful acts, or directed toward or intended ultimately to lead to the destruction or overthrow by violence of, the constitutionally established system of government in Canada,

but does not include lawful advocacy, protest or dissent, unless carried on in conjunction with any of the activities referred to in paragraphs (a) to (d).

Source: Section 2 of the CSIS Act.

or another lawful authority in respect of activities that undermine the security of Canada, including in respect of their detection, identification, analysis, prevention, investigation or disruption."

SIRC sought a preliminary understanding of SCISA's impact on CSIS's information sharing with its domestic partners. SIRC noted that the volume of exchanges under SCISA has been modest, primarily from Global Affairs Canada (GAC) and the Canada Revenue Agency (CRA). SIRC thus focused on implementation efforts with these partners.

FINDINGS: GLOBAL AFFAIRS CANADA

SIRC found that CSIS and GAC have made progress toward a framework for information sharing that accommodates for SCISA. In May 2016, GAC and CSIS signed an information-sharing arrangement to govern the disclosure of consular information, including by providing a "non-exhaustive" list of information that may be shared with CSIS, either proactively or following a request.

In September 2016, CSIS issued a directive to provide guidance and tools to its employees for requesting consular information. At the same time, specific internal guidelines were issued on the procedures for requesting information. Both the directive and the guidelines state that exchanges with GAC should be done in a consistent manner and that they be recorded for tracking purposes. Both also include information on the threshold for disclosure, specifically, that the threshold will be met if the information is relevant to CSIS's mandate and that there is a rational link between activities that undermine the security of Canada and the *CSIS Act* definition of threats to the security of Canada. Nevertheless, it is GAC that is ultimately responsible for determining whether the information sought is relevant to CSIS's mandate. SIRC focused on CSIS's main responsibility to provide sufficient information to satisfy GAC in this regard.

CSIS views proactive disclosures of information as essential since CSIS cannot request information on an individual of whom it is unaware. In the documents reviewed, SIRC saw references to instances when CSIS felt GAC should have made proactive disclosures. CSIS and GAC are conducting ongoing interdepartmental discussions on this issue, as well as establishing joint training on protocols, thresholds and triggers for disclosures of information.

CSIS and GAC had already taken other steps before the enactment of SCISA to improve the sharing of consular information. Overall, SIRC found that these initiatives are appropriate and in line with the general direction for implementation of SCISA given by Public Safety Canada. Specifically, departments are being encouraged to provide training of this kind to promote an understanding of the types of information that are relevant to the designated government institutions.

Finally, a small number of disclosures of consular information were cited as having been made pursuant to the *Privacy Act*. It was not always clear why the *Privacy Act* was cited, however, and **SIRC recommended that steps be taken, as appropriate, to clarify disclosures under the *Privacy Act* to ensure consistency in the future**.

In relation to recording disclosures of consular information and in general, **SIRC recommended that CSIS put in place a system to ensure accurate tracking of SCISA disclosures that is consistent for information exchanges across all departments. SIRC further recommended that a record be kept of exchanges under SCISA for tracking purposes, including NIL responses**.

FINDINGS: CANADA REVENUE AGENCY

As a result of the enactment of SCISA, the *Income Tax Act* was amended to broaden the definition of taxpayer information that is sharable with agencies, such as CSIS, on a "reasonable grounds to suspect" standard. The amended *Income Tax Act* threshold provides that "taxpayer information" may be shared if "there are reasonable grounds to suspect that the information would be relevant to (i) an investigation of whether the activity of any person may constitute threats to the security of Canada as defined in section 2 of the *Canadian Security Intelligence Service Act*."

On the basis of this legislative change, CRA may now share taxpayer information without a judicially authorized warrant. This is a departure, when a warrant was required before seeking taxpayer information. At the same time, however, Canadian courts have ruled that privacy interests attach to taxpayer information. Accordingly, SIRC was particularly alert to how CSIS put this change into practice.

Unlike with GAC, no memorandum of understanding was in place at the time of writing to formalize sharing of taxpayer information, although there has been communication at a high level between the two organizations.

A policy document establishing some parameters for the disclosure of taxpayer information has been drafted by CSIS and CRA as a "precursor" to the revision of a framework memorandum of understanding that has yet to occur. **SIRC recommended that CSIS prioritize the finalization of the memorandum of understanding with CRA**.

Within CSIS, the principal internal direction has been the Deputy Director Operations directive, issued in April 2016, on the collection of financial and taxpayer information without a warrant. The directive stipulates the specific internal authority required before CSIS may request taxpayer information from CRA. Given the type of constitutional protections that have been found to apply to taxpayer information, **SIRC recommended that CSIS increase the required threshold for receiving taxpayer information from CRA. SIRC further recommended that CSIS consider the appropriateness of seeking a Department of Justice case-by-case analysis of the proportionality of each request**. Finally, although a warrant is no longer required, SIRC's expectation is that CSIS will inform the Court when relevant taxpayer information is being sought and obtained from CRA when a warrant is being sought against the same individual.

SIRC is aware that CSIS has engaged CRA to discuss challenges it may be encountering in processing the requests. SIRC was told that CRA is facing resource constraints that have adversely impacted the processing of requests for information. SIRC is also aware that CRA has instituted a new process for responding to CSIS's non-warranted requests for taxpayer information. CSIS also attributed the delays to CRA's consultation process for determining whether the information is relevant to CSIS's jurisdiction or responsibilities. This is reflected in the operational files, where SIRC saw instances of CRA returning to CSIS for further information to support the disclosure request.

Exchanges between CRA and CSIS on individual requests, though they may lengthen the overall response time, appear to lead to more focused, and thus more relevant, CRA information being provided to CSIS. Moreover, consultations between CRA and CSIS further sensitize CSIS to CRA's specific considerations regarding information sharing. Going forward, SIRC expects that these consultations will assist CSIS in providing the information needed to satisfy CRA that the requested information meets the required threshold. This is a crucial part of CSIS's responsibilities as a recipient of this information. That said, SIRC expects that this initial period will eventually lead to sharing in a more timely manner. SIRC encouraged the two partners to work together to resolve outstanding issues.

Neither SCISA nor the *Income Tax Act* creates an obligation on government departments to disclose information. The guidance document prepared jointly by CSIS and CRA states that, should CRA decline to disclose information pursuant to the *Income Tax Act*, CSIS retains the option of producing a warrant. SIRC therefore suggested that CSIS policy and internal procedures reflect that a warrant remains an available option.

CSIS RESPONSE

CSIS agreed to review its existing guidance and provide additional clarification with respect to the *Privacy Act* and SCISA and also agreed to expand the existing tracking mechanism for SCISA disclosures. CSIS agreed to prioritize the finalization of the memorandum of understanding with CRA, which has already been drafted and disseminated. Lastly, CSIS agreed to increase the required threshold for requesting taxpayer information from CRA. However, CSIS did not agree to seek a case-by-case analysis from the Department of Justice for each request, as CSIS believes that raising the threshold of such requests (as agreed to in the

previous recommendation) better addresses the issue of proportionality from a CSIS perspective. CSIS is authorized to request taxpayer information from CRA and CRA is responsible for determining whether it can lawfully respond to a CSIS request under SCISA.

THREAT REDUCTION MEASURES

The enactment of the *Anti-Terrorism Act* in July 2015 resulted in changes to Canada's national security apparatus, including to the *CSIS Act*. These amendments provide CSIS with additional powers to reduce threats to the security of Canada, within or outside Canada. These powers are found in section 12.1 of the *CSIS Act*.

For SIRC, the amendments created a new requirement to review, each fiscal year, "at least one aspect of the Service's performance in taking measures to reduce threats to the security of Canada" as set out in subsection 38(1.1). Last year was the first such review, which examined all threat reduction measures that CSIS had approved or considered to that point, approximately two dozen. SIRC found that they complied with the *CSIS Act*, ministerial direction and operational policy.

During the period under review, CSIS had approved fewer than a dozen threat reduction measures, which were executed in full or in part by CSIS. SIRC looked at all threat reduction measures conducted by CSIS during the period under review.

FINDINGS

SIRC examined the process put in place by CSIS to determine the reasonableness and proportionality of each measure. In particular, CSIS has developed, in consultation with the Department of Justice, a "minimal impairment and balancing test" that addresses whether the measure proposed is the least intrusive possible and whether alternative means are available to reduce the threat. For each proposed measure, the Department of Justice provides a legal risk assessment to determine if the proposed measure is compliant with the *CSIS Act*. As part of its review, SIRC examined all the legal risk assessments. In only one instance did the Department of Justice assess the legal risk at medium, that is, there is an evenly balanced probability that an adverse outcome may or may not materialize for CSIS. Overall, SIRC found that the measures examined complied with the *CSIS Act*, ministerial direction and operational policies.

SIRC also examined the governance structures and processes put in place by CSIS to operationalize its new mandate for threat reduction. In last year's review of threat reduction measures, SIRC paid particular attention to the approval process for each new measure. This year, SIRC focused on how CSIS is assessing and reporting on the outcomes of the measures.

The approval process requires CSIS to identify immediate and intermediate outcomes for each measure. The immediate outcome describes the immediate impact of the measure. This could include CSIS's disclosure of information to an establishment or organization, that is, the immediate outcome is that information has been shared. The intermediate outcome typically is the response to the execution of the measure. CSIS was able to measure and report on the immediate and intermediate outcomes for almost all of the cases.

Strategic outcomes are distinct from the other outcomes in that they are more broadly construed and are meant to assess how successful the measure was in reducing the specific threat. The measuring and reporting on strategic outcomes was more problematic; CSIS reported on the achievement of strategic outcomes in only a few cases. For some of the more moderate measures taken, it seemed unlikely that CSIS could meet the far-reaching strategic outcomes identified.

Of all the measures executed to date, only four strategic outcome assessments have been conducted. SIRC questioned why so few have been prepared. CSIS indicated that strategic outcomes will vary depending on the nature of the measure, and that some measures may not in fact warrant such an overarching strategic outcome assessment. SIRC was also told that CSIS may be more circumspect in its identification of the strategic outcomes identified in the approval documents.

Of course, a certain amount of time must elapse before such a broad assessment of impact could be done. SIRC is also aware that guidance materials on how to prepare the immediate, intermediate and strategic outcomes documents have been prepared. SIRC found the development of guidance documents to support the reporting of threat reduction measure outcomes is a necessary step toward consistency in reporting.

Nevertheless, CSIS's process for developing and reporting on the impacts of the measures lacked some of the thoroughness found in the approval and consultation process. **SIRC therefore recommended that, when CSIS is developing strategic outcomes during the approval process, CSIS consider the realistic prospects of both measuring and achieving the strategic outcomes. SIRC also recommended that CSIS continue to refine those aspects of its governance of threat reduction measures that pertain to outcomes**.

CSIS RESPONSE

CSIS agreed with the recommendations and is actively working to ensure threat reduction outcomes are more quantifiable.

CYBER THREATS

One of the Government of Canada's top intelligence priorities is cyber threats, which are defined as "the unintentional or unauthorized access, use, manipulation, interruption or destruction (via electronic means) of electronic information and/or the electronic and physical infrastructure used to process, communicate and/or store that information." The potential impact of cyber activities was illustrated over the past year, as state-sponsored actors conducted attacks on critical infrastructure in the Ukraine, an international banking network (the Society for Worldwide Interbank Financial Telecommunication), as well as against political actors in the United States.

Along with the Communications Security Establishment (CSE), the Canadian Cyber Incident Response Centre (located within Public Safety Canada) and the RCMP, CSIS plays an important role in collecting intelligence on this key threat and protecting Canadian infrastructure. Given that cyber power is one tool among many available to threat actors, CSIS investigations of cyber threats often intersect with more traditional counter-intelligence, counter-proliferation and counter-terrorism activities.

FINDINGS

SIRC examined the history, strategic orientation and future vision of the area within CSIS responsible for investigating cyber threats, which includes the collection and analysis of cyber intelligence in response to cyber attacks, as well as coordinating responses. A CSIS investigation into a specific foreign state-sponsored attack was selected in order to further understand the capabilities of, and challenges faced by, this program.

CSIS could benefit from more rigorous strategic planning, additional resources and a sustainable growth plan in order to ensure that its area

responsible for the investigation of cyber threats is well positioned to meet the increasing demands in this area.

CSIS is being pressured to evolve the cyber program to take on a broader scope and foreign reach. This is analogous to the evolution of CSIS's foreign collection program. That said, the cyber program will have to compete for resources and much will depend on how jurisdictional lines with other Government of Canada partner agencies solidify.

A case study of a CSIS cyber investigation provided some insight into such challenges. This case revealed a potential disconnect between CSIS and CSE on their respective cyber roles. CSE's mandate under the *National Defence Act* authorizes it "to provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada." That said, there is significant overlap between this and CSIS's mandate to collect and analyze intelligence. To help ensure better coordination of investigation and mitigation in these cases, **SIRC recommended that CSIS seek additional clarity on the roles and responsibilities of CSE and CSIS when it comes to cyber threats, as well as develop a joint protocol with CSE to allow both agencies to exercise their respective mandates following identification of a cyber incident**.

Although SIRC was satisfied with the propensity to seek legal advice that was demonstrated by the area within CSIS responsible for investigating cyber threats, the fact remains that data science and information technology have outpaced legal frameworks. CSIS can expect to be forced to operate in increasingly grey areas for which there is no legal precedence or clarity. For this reason, legal advice should be sought in proactively addressing future cyber intelligence methodologies.

Looking forward, CSIS's cyber program faces a number of operational challenges. As this program matures, it will need to develop new product lines, performance metrics and collaborative arrangements, as well as new ways of integrating legal, cyber and traditional investigative perspectives in order to remain ahead of emerging threats.

To help achieve some of these objectives over the short term, **SIRC recommended that CSIS designate a CSIS executive to be a cyber champion; create a strategic plan for the area within CSIS responsible for investigating cyber threats; allocate regional resources for cyber collection; formulate performance metrics; and enhance cyber intelligence production, including client feedback mechanisms**.

CSIS RESPONSE

CSIS agreed with all of the recommendations. In response to an internal evaluation of the cyber program earlier this year, a "Team Canada" deconfliction model has already been implemented so that all agencies are in a position to exercise their respective mandates within reasonable timelines. This work will feed into broader Government of Canada cyber security efforts underway, which will address any gaps in community governance and outline roles and responsibilities. As CSIS's cyber program evolves within this context, a strategic plan will be developed and championed at the executive level. Work is already underway to develop performance measures and client feedback mechanisms in conjunction with efforts to implement the recommendations of the internal evaluation of the program earlier this year. With respect to regional resourcing, CSIS is in the process of seeking additional resources and will also examine internal reallocation based on intelligence priorities.

FOREIGN POSTS

Every year SIRC travels to a foreign station to undertake an in-depth examination of CSIS's work overseas in order to better appreciate the nature, scope and complexity of its activities abroad. This year, SIRC elected to visit two stations that have cooperated on a number of files and share similar collection requirements. Although this represents SIRC's first on-site visit to either station, SIRC has previously examined activities undertaken at these two stations in the context of other reviews.

SIRC had three broad objectives consistent with its traditional foreign station reviews. The first objective was to gain a deeper understanding of the nature and extent of operational activities at these stations, including any challenges related to the local environment. The second objective was to understand CSIS's relationships with its domestic and foreign partners by examining liaison activities, as well as operational cooperation and information exchanges carried out by the stations. Finally, SIRC examined site-specific developments, conditions, pressures and emerging issues that occurred during the period under review. For example, one station experienced two major crises that diverted resources from the usual interests and priorities.

FINDINGS

SIRC examined CSIS's relationships by meeting with the relevant domestic partners at both stations and reviewing a number of documents, including operational exchanges with partners. Overall, SIRC found that the stations have maintained positive relationships with all of their partners and CSIS's presence is appreciated by its domestic partners at mission. In addition, SIRC found that, during the period under review, all policies and directives on information exchanges were followed and that CSIS responded swiftly and appropriately to an allegation of abuse against one of its regional partners. In another case, however, **SIRC recommended that the foreign arrangement profile be updated to reflect a serious case of corruption**.

CSIS RESPONSE

CSIS agreed with the recommendation and has already updated the referenced foreign arrangement profile.

RESEARCH BRIEF ON NUTTALL AND KORODY

John Stuart Nuttall and Amanda Marie Korody were arrested on July 1, 2013, in Victoria, B.C., while placing pressure cooker bombs near the B.C. Legislature. Their arrests were the result of a months-long RCMP undercover operation. Nuttall and Korody were charged with four counts of terrorism-related offences, one count of which a judge later dismissed. They were found guilty of the three charges in June 2015, but the convictions were not entered, as their lawyers had requested an opportunity to argue that they had been entrapped by police. On July 29, 2016, B.C. Supreme Court Justice Catherine Bruce stayed the charges, stating that Nuttall and Korody had been entrapped by the RCMP undercover operation.

During the process to determine entrapment, the Court requested all documentation and disclosure between CSIS and the RCMP concerning Nuttall and Korody, essentially confirming that their activities had been under investigation by CSIS. Therefore, in order to determine CSIS's involvement in this case, SIRC requested research into the nature and scope of the CSIS investigation, and the nature and scope of CSIS's cooperation and information sharing with the RCMP. SIRC examined all relevant documentation in CSIS holdings.

RISK-BASED PLANNING

The underlying goal of SIRC's formal risk-based planning process is to have confidence that it is focusing resources on the right areas, and to the right extent. An annual research plan is presented to the Committee members for approval. The research plan guides the strategic allocation of resources to areas of CSIS activity assessed as being of highest risk, as well as those that may be of lower risk, but that require regular review to provide comprehensive coverage. A number of factors inform the identification and ranking of risk. For example, SIRC considers:

- whether an activity may affect the well-being of a Canadian or impact on her or his privacy or other rights;
- changes in law, ministerial direction, and CSIS operational policies and procedures;
- issues identified in the course of SIRC reviews and complaint investigations;
- the government's intelligence priorities and CSIS's own plans and priorities; and
- an environmental scan of events or developments that could impact on threats to the security of Canada or on risk.

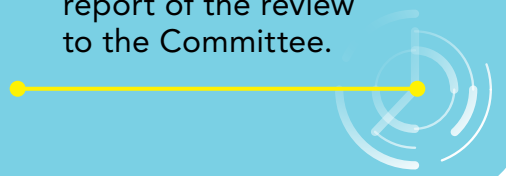
FINDINGS

In examining the documentation, SIRC found that CSIS's coordination with, and disclosure to, the RCMP were appropriate. Overall, CSIS followed policy and procedures and adhered to its mandate.

SECTION 40 UPDATE: ASSESSING HUMAN SOURCES POTENTIALLY INVOLVED IN UNLAWFUL ACTIVITIES

In a 2014 review of CSIS's relationship with the (then) Department of Foreign Affairs, Trade and Development, SIRC raised potential legal concerns with respect to CSIS's activities and the *United Nations Al-Qaida and Taliban Regulations* (UNAQTR). To acquire intelligence, CSIS officials,

Paragraph 40(1)*(a)* of the *CSIS Act* states that for the purpose of ensuring that CSIS's activities are carried out in accordance with the *CSIS Act*, its regulations and ministerial direction, and do not involve any unreasonable or unnecessary exercise of CSIS's powers, SIRC may direct CSIS to conduct a review of specific activities and to provide a report of the review to the Committee.



or those acting at its direction, could be accessing individuals (human sources) involved in a range of potentially unlawful activities.

Although CSIS was aware of the legal implications of the UNAQTR, SIRC found no evidence that CSIS had pursued this issue further, or had reported to the Minister of Public Safety and Emergency Preparedness on the possibility of human sources (or CSIS employees) being in contravention of the regulations.

As a result, SIRC recommended that CSIS put in place formal internal mechanisms to ensure that none of its human source operations were in contravention of the UNAQTR or any similar Canadian statute or regulations.

SIRC also directed CSIS — as per paragraph 40(1)(*a*) of the *CSIS Act* — to conduct a review of activities that may have been in contravention of the UNAQTR or Canadian laws and regulations.

The following year, as a follow-up in its Foreign Fighters review, 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 with regard to the terrorism-related offences within Canada's *Criminal Code*.

CSIS conducted a section 40 review and provided its findings to the Minister of Public Safety and Emergency Preparedness in the Director's 2015–2016 annual report to the Minister. Moreover, the Committee members were provided with a detailed briefing on the findings of the section 40 review in January 2017.

Ultimately, SIRC's identification of the UNAQTR and Crown immunity issues resulted in proposed legislative changes in Bill C-59 to establish in law an authorization regime for otherwise unlawful activities. In the interim, SIRC will continue to track CSIS's efforts to mitigate legal risks associated with collection operations — both for human sources and CSIS employees.

3 COMPLAINT INVESTIGATIONS

Under the *CSIS Act*, one of SIRC's core functions is to investigate complaints in the following instances:

- with respect to **any act or thing** done by CSIS (section 41 of the *CSIS Act*); and
- with respect to the denial or revocation of a security clearance necessary to obtain or keep federal government employment or contracts (section 42 of the *CSIS Act*).

SIRC also has the mandate to conduct investigations into reports made to it pursuant to section 19 of the *Citizenship Act*, and into matters referred pursuant to section 45 of the *Canadian Human Rights Act*.

THE COMPLAINT PROCESS AT SIRC

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

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

If jurisdiction is established, complaints are investigated through a quasi-judicial hearing presided over by a Committee member. They are assisted by staff and SIRC's legal team, which provide 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 hearing days required, the availability of the participants and the various procedural matters raised by the parties.

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

HOW SIRC DETERMINES JURISDICTION OF A COMPLAINT...

...under section 41 of the *CSIS Act*,

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

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

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

...under section 42 of the *CSIS Act*,

SIRC shall investigate complaints from:

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

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

A party may request an *ex parte* hearing (in the absence of the other parties) to present evidence that, 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 Committee member with the most complete and accurate factual information relating to the complaint.

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

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

Note that, whenever appropriate, SIRC encourages the parties to explore informal resolution talks, either through the complaint resolution process set out in SIRC's Rules of Procedure or in some other forum acceptable to the parties. Of the files resolved in this manner this year, one was an investigation into a security clearance denial that was closed after a settlement was reached between the complainant and the relevant deputy head.

COMPLAINT INVESTIGATION SUMMARIES

CSIS INTERVIEW: COMPLAINT PURSUANT TO SECTION 41 OF THE *CSIS ACT*

SIRC investigated a complaint under section 41 of the *CSIS Act* that addressed the following issues: (1) whether the visit by CSIS employees to the complainant's home was justified under the mandate of CSIS; (2) whether the visit caused a considerable amount of anxiety; and (3) whether the visit had an intended purpose, outside the mandate of CSIS, to intimidate the complainant and his family members from exercising their *Charter* rights to freedom of expression and association, and to take part in the Canadian political process, which includes criticism of the policies of the federal government.

Concerns arose in this investigation related to the issue of the voluntary nature of interviews; the loss of operational notes; and a response letter sent by CSIS to the individual. SIRC found that asking an individual if he or she wishes to speak to a CSIS employee is not an approach that sufficiently emphasizes the voluntary nature of such discussions. **SIRC recommended that CSIS review its policy to make clear the responsibilities of CSIS employees with respect to clarifying the voluntary nature of interviews.**

SIRC also found that CSIS lost the operational notes of one CSIS employee, and a second CSIS employee failed to take operational notes, contrary to the requirements set out in CSIS policy. In addition, a response letter sent by CSIS to the complainant stated that appropriate internal inquiries were made, and asserted that CSIS officials acted professionally and entirely within CSIS's legislated mandate. However, based on the evidence heard, SIRC found that CSIS misrepresented to the complainant that appropriate inquiries were made.

With respect to the content of the complaint itself, SIRC found that the complainant's allegations were unsupported. Specifically, while acknowledging the complainant's perception of the events, SIRC found that CSIS acted pursuant to its mandate and its operational focus was not to attempt to intimidate the complainant or prevent him from the exercise of lawful activities, such as expressing public opinions. Finally, SIRC found that a reasonable person with the complainant's knowledge and experience would not suffer considerable anxiety to the extent alleged solely as a result of the visit by CSIS employees.

CSIS RESPONSE

CSIS agreed with the recommendation and has since amended its policies and procedures. Acknowledging that the nature and type of CSIS interactions with the public vary considerably depending on the circumstances, the particular mandate and the security environment, CSIS employees must comport themselves in a way that ensures members of the public know that their interaction with CSIS is voluntary.

DENIAL OF SECURITY CLEARANCE: COMPLAINT PURSUANT TO SECTION 42 OF THE *CSIS ACT*

SIRC investigated a complaint under section 42 of the *CSIS Act* made by a Government of Canada employee who was denied a Secret security clearance. In this case, although the Deputy Head denied the complainant a security clearance, the complainant's reliability status was not revoked.

SIRC found that, based on the assessment provided to the Deputy Head through an independent evaluation, the Deputy Head's decision to deny the complainant a security clearance was reasonable in the circumstances and in compliance with the Policy on Government Security, the Personnel Security Standard, and the *CSIS Act*. That being said, SIRC found that the Deputy Head was not in possession of all relevant information to make an informed decision regarding the granting or refusal of the complainant's security clearance. SIRC deemed unfounded the conclusion that the complainant may engage in activities that would constitute a threat to the security of Canada within the meaning of the *CSIS Act*. SIRC also found that the evidence did not support, with regard to the complainant's reliability as it relates to loyalty, that the complainant may act or may be induced to act in a way that constitutes a threat to the security of Canada; or that the complainant may disclose, may be induced to disclose, or may cause to be disclosed in an unauthorized way, classified

information. In light of the above, SIRC found that in relation to section 2.8 of the Personnel Security Standard, there did not exist reasonable grounds to doubt the complainant's loyalty or reliability as it relates to loyalty. For these reasons, **SIRC recommended that the Deputy Head grant a Secret security clearance to the complainant**.

DENIAL OF ACCESS TO SERVICES: COMPLAINT PURSUANT TO SECTION 45 OF THE *CANADIAN HUMAN RIGHTS ACT*

SIRC investigated a complaint pursuant to paragraph 45(2)(*b*) of the *Canadian Human Rights Act*. The complainant alleged that CSIS discriminated against him because of his national or ethnic origin, race, or religion by denying him access to services customarily available to the general public, and did so on a prohibited ground, contrary to subsection 5(*a*) of the *Canadian Human Rights Act*. SIRC's statutory mandate arises from the *Canadian Human Rights Act*, in conjunction with the *CSIS Act*. Section 45 of the *Canadian Human Rights Act* provides that if a minister of the Crown notifies the Canadian Human Rights Commission that a discrimination complaint under investigation pertains to a practice that was based on considerations relating to national security, it must either dismiss the complaint, or refer the matter to SIRC. In this case, the Canadian Human Rights Commission elected to refer the matter to SIRC for investigation.

SIRC found that this complaint was without foundation. CSIS did not engage in a discriminatory practice against the complainant on the basis of prohibited grounds, and the interview conducted by CSIS agents was appropriate and necessary to resolve any national security concerns. SIRC also concluded that there was no evidence that CSIS acted unlawfully or as a result of any prohibited ground of discrimination. Any practices that may or may not have been taken by CSIS involved considerations relating to the security of Canada. For these reasons, **SIRC recommended that the Canadian Human Rights Commission not investigate this complaint in accordance with subsection 46(2) of the *Canadian Human Rights Act*.**

RECOMMENDATIONS

Review	SIRC recommended that ...	CSIS response
Review of CSIS's Investigation of Terrorist Financing	• CSIS make changes concerning CSIS's work in this area • the clarity of retention thresholds in policy be improved	CSIS agreed with one recommendation and partially agreed with the other, noting that the retention thresholds were being considered within a broader effort already underway within CSIS.
Review of a Type of Warranted Technical Collection	• all employees with warrant-related responsibilities receive standardized and comprehensive training on an ongoing basis, and that those responsible for providing legal advice have up-to-date knowledge about technical operations • roles and responsibilities be clearly defined and standardized across the regions • CSIS create a warrant policy centre devoted to the execution of warrants	CSIS agreed with all of the recommendations, noting that it was already in the process of initiating a number of interrelated activities to enhance the training and awareness of employees with warrant-related responsibilities and is also providing technical briefings to CSIS legal counsel, as well as the Federal Court. Furthermore, CSIS is in the process of implementing a new governance framework for warranted activities, including clarifying the role of the policy centre and defining and standardizing warrant-related roles and responsibilities.
Security Screening	• internal procedures be updated • a review of these particular cases be conducted in conjunction with the Department of Justice and that, if it is determined that *Charter* rights were infringed, the information be purged from its holdings • CSIS follow the same procedures for security screening investigations as are applicable to its other investigations, including seeking a warrant from the Federal Court in appropriate cases	CSIS agreed with all of the recommendations. CSIS noted that the referenced investigative practices were developed pursuant to legal advice that set out the criteria under which this information could be obtained without a warrant. CSIS agreed to ask the Department of Justice to review all the cases highlighted by SIRC, and that if it was determined that the reasonable expectation of privacy was not properly considered, to destroy the information in question. SIRC will also be advised of the outcome of the review.

Review	SIRC recommended that ...	CSIS response
Evolving Platforms Abroad	• CSIS develop standard operating procedures derived from lessons learned from operating in dangerous operating environments • CSIS create clear operational objectives to assist the station in addressing key intelligence requirements, including further assessment of the resource allotment to ensure that CSIS can sufficiently meet Government of Canada intelligence needs • CSIS create, on a priority basis and in consultation with the Department of Justice, policy and procedures regarding the use of information sharing in dangerous environments	CSIS agreed with all of the recommendations, noting that work has already commenced to develop standard operating procedures for dangerous operating environments to supplement the tools and mechanisms that already exist. CSIS agreed that clear objectives are necessary to ensure the success of CSIS contributions to Government of Canada efforts and provides these to its overseas stations via the collection requirements that are disseminated in several types of documents. Additionally, CSIS works with its Government of Canada clients to ensure it is meeting their requirements and updates the operational objectives accordingly. In conjunction with these efforts, CSIS actively assesses staffing requirements on an ongoing basis. With respect to information sharing in dangerous operating environments, CSIS has prepared instructions in consultation with the Department of Justice and new procedures are expected to be published in the fall of 2017.
Information Technology Access Controls	• CSIS implement security control findings on an accelerated timeline and extend the initiative across its system • CSIS develop policy, guidance and procedures that define separation of duties and its implementation across all branches • CSIS's risk management process integrate operational threat intelligence with the objective of achieving best security practices across the organization	CSIS agreed with all of the recommendations.
Foreign Fighters	• an additional caveat be applied to all disclosures to foreign intelligence agencies where the target is a minor	CSIS agreed with the recommendation, adding that a new policy will be drafted to supplement those already in place, with specific reference to CSIS activities involving minors, including information disclosures.

Review	SIRC recommended that ...	CSIS response
The *Security of Canada Information Sharing Act*	**Global Affairs Canada** • steps be taken, as appropriate, to clarify disclosures under the *Privacy Act* to ensure consistency in the future • CSIS put in place a system to ensure accurate tracking of SCISA disclosures that is consistent for information exchanges across all departments • a record be kept of exchanges under SCISA for tracking purposes, including NIL responses **Canada Revenue Agency** • CSIS prioritize the finalization of the memorandum of understanding with CRA • CSIS increase the required threshold for receiving taxpayer information from CRA • CSIS consider the appropriateness of seeking a Department of Justice case-by-case analysis of the proportionality of each request	CSIS agreed to review its existing guidance and provide additional clarification with respect to the *Privacy Act* and SCISA and also agreed to expand the existing tracking mechanism for SCISA disclosures. CSIS agreed to prioritize the finalization of the memorandum of understanding with CRA which has already been drafted and disseminated. Lastly, CSIS agreed to increase the required threshold for requesting taxpayer information from CRA. However, CSIS did not agree to seek a case-by-case analysis from the Department of Justice for each request as CSIS believes that raising the threshold of such requests (as agreed to in the previous recommendation) better addresses the issue of proportionality from a CSIS perspective. CSIS is authorized to request taxpayer information from CRA and CRA is responsible for determining whether it can lawfully respond to a CSIS request under SCISA.
Threat Reduction Measures	• when CSIS is developing strategic outcomes during the approval process, CSIS consider the realistic prospects of both measuring and achieving the strategic outcomes • CSIS continue to refine those aspects of its governance of threat reduction measures that pertain to outcomes	CSIS agreed with the recommendations and is actively working to ensure threat reduction outcomes are more quantifiable.

Review	SIRC recommended that ...	CSIS response
Cyber Threats	• CSIS seek additional clarity on the roles and responsibilities of CSE and CSIS when it comes to cyber threats, as well as develop a joint protocol with CSE to allow both agencies to exercise their respective mandates following identification of a cyber incident • CSIS designate a CSIS executive to be a cyber champion • CSIS create a strategic plan for the area within CSIS responsible for investigating cyber threats • CSIS allocate regional resources for cyber collection • CSIS formulate performance metrics • CSIS enhance cyber intelligence production, including client feedback mechanisms	CSIS agreed with all of the recommendations. In response to an internal evaluation of the cyber program earlier this year, a "Team Canada" deconfliction model has already been implemented so that all agencies are in a position to exercise their respective mandates within reasonable timelines. This work will feed into broader Government of Canada cyber security efforts underway, which will address any gaps in community governance and outline roles and responsibilities. As CSIS's cyber program evolves within this context, a strategic plan will be developed and championed at the executive level. Work is already underway to develop performance measures and client feedback mechanisms in conjunction with efforts to implement the recommendations of the internal evaluation of the program earlier this year. With respect to regional resourcing, CSIS is in the process of seeking additional resources and will also examine internal reallocation based on intelligence priorities.
Foreign Posts	• the foreign arrangement profile be updated to reflect a serious case of corruption	CSIS agreed with the recommendation and has already updated the referenced foreign arrangement profile.

Complaint	SIRC recommended that ...	CSIS response
CSIS Interview (section 41 of the *CSIS Act*)	• CSIS review its policy to make clear the responsibilities of CSIS employees with respect to clarifying the voluntary nature of interviews	CSIS agreed with the recommendation and has since amended its policies and procedures. Acknowledging that the nature and type of CSIS interactions with the public vary considerably depending on the circumstances, the particular mandate and the security environment, CSIS employees must comport themselves in a way that ensures members of the public know that their interaction with CSIS is voluntary.
Denial of Security Clearance (section 42 of the *CSIS Act*)	• the Deputy Head grant a Secret security clearance to the complainant	
Denial of Access to Services (section 45 of the *Canadian Human Rights Act*)	• the Canadian Human Rights Commission not investigate this complaint in accordance with subsection 46(2) of the *Canadian Human Rights Act*	

CORPORATE OPERATIONS

TABLE 1: EXPENDITURES

Program	2015–2016 Expenditures	2016–2017 Planned Spending	2016–2017 Actual Spending	2017–2018 Planned Spending
Reviews	1,185,800	2,222,300	1,670,700	2,344,000
Legal Services	639,300	1,694,800	980,500	1,429,600
Subtotal	**1,825,100**	**3,917,100**	**2,651,200**	**3,773,600**
Internal Services*	1,044,300	3,187,700*	1,823,500	1,247,700*
Total	**2,869,400**	**7,104,800**	**4,474,700**	**5,021,300**

**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 and access to information and privacy). 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 information technology 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.*

OUTREACH

SIRC participated in a number of outreach activities, including presentations at universities and conferences. The Chair of SIRC and the Executive Director appeared several times at parliamentary committees to discuss SIRC's work and its role within the wider accountability structure. In addition, SIRC staff participated in academic panel discussions and briefed new CSIS employees on SIRC's role.

ANNEX

TABLE 2: TARGETING

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

	2014–2015	2015–2016	2016–2017
Targets	590	550	560

TABLE 3: WARRANTS

Historically, SIRC has provided statistics on the total number of warrants granted by the Federal Court during a fiscal year. In such instances, a single warrant may be directed toward numerous individuals. Similarly, many warrants provide for a multitude of powers, whereas others are singular in nature. Moreover, not all individuals are subject to the same number of warrants. The warrant statistics found here represent the total number of warrant applications submitted to the Federal Court, independent of the actual number of warrants granted in each application or the number of individuals who were the subject of warrants.

	2014–2015	2015–2016	2016–2017
New	13	14	11
Replacement or Supplemental	25	22	18
Total	38	36	29

TABLE 4: COMPLAINTS

Program	2016–2017
Intakes	90
Complaints Carried over from Previous Fiscal Year	15
New Complaints	19
Total	34
Files Closed	18
Files Carried Forward	16