TOP SECRET - CEO

SIRC REVIEW 2016-08

IMPACT OF THE *SECURITY OF CANADA INFORMATION SHARING ACT* ON CSIS INFORMATION SHARING

SUMMARY

- On August 1, 2015, the *Security of Canada Information Sharing Act (SCISA)* came into force, which is said to encourage "efficient and responsible" information sharing for national security purposes. As CSIS is a recipient of *SCISA* disclosures, the review sought a preliminary understanding of its impact on CSIS's information sharing with its domestic partners.

- The volume of exchanges under *SCISA* has been modest, with disclosures received by CSIS, primarily from Global Affairs Canada (GAC) and Canada Revenue Agency (CRA). SIRC's review focused on implementation efforts with these partners.

- SIRC found that the initiatives being undertaken by GAC and CSIS to facilitate information sharing are appropriate and in line with the general direction for implementation of *SCISA* given by Public Safety Canada. However, SIRC recommended that CSIS clarify its position, as appropriate, on the issue of when the *Privacy Act* instead of *SCISA* should be cited as the authority and take steps to ensure consistency in the future.

- As a result of the enactment of *SCISA*, the *Income Tax Act (ITA)* was amended, the effect of which was to allow taxpayer information to be shared without a judicially authorized warrant. This is a departure from the past. Moreover, as Canadian courts have ruled that privacy interests attach to taxpayer information, SIRC was particularly alert to how CSIS is operationalizing this change.

- In order to better reflect the requirement "that information be shared in a manner that is consistent with the *Canadian Charter of Rights and Freedoms* and the protection of privacy" as set out in the preamble to *SCISA*, SIRC made a number of recommendations. At a minimum, SIRC recommended that CSIS change the required threshold for requesting taxpayer information . SIRC also recommended that CSIS institute parameters around when it is appropriate to request taxpayer information

- Overall, SIRC concluded that the impact of *SCISA* to date has been modest given the relatively small number of disclosures.

Contents

1 INTRODUCTION

On August 1, 2015, the *Security of Canada Information Sharing Act* (*SCISA*) came into force. This legislation is said to encourage "efficient 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 the *Act*, information may be disclosed if it is "relevant to the recipient institution's jurisdiction or responsibilities under an Act of Parliament 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."

This review sought a preliminary understanding of *SCISA*'s impact on CSIS's information sharing with its domestic partners. The volume of exchanges under *SCISA* has been modest, with [1] disclosures received by CSIS, primarily from Global Affairs Canada (GAC) and Canada Revenue Agency (CRA). SIRC found that CSIS is engaging bilaterally with those government partners identified as priority. Since the vast majority of disclosures have come from GAC and CRA, SIRC focused on discussions and implementation efforts with these government partners.

This review considered whether CSIS's engagements with GAC and CRA have resulted in workable arrangements for operating under this new authority that support efficient and responsible information sharing. SIRC found that CSIS and GAC have made progress toward a framework for information sharing that accommodates for *SCISA*. Nevertheless, SIRC was told that the overall impact to date of *SCISA* on the sharing of consular information has been minimal. At the same time, the review acknowledges the efforts underway by CSIS and GAC to address the challenges associated with sharing consular information. SIRC will assess the results of those efforts in future reviews.

There has been less progress toward instituting a satisfactory arrangement with CRA. A new Memorandum of Understanding (MOU) between CRA and CSIS has not been completed. Moreover, there have been significant delays in CRA responses to CSIS requests for information. This is likely due, in part, to the fact that the situation with respect to CRA has changed significantly, from one in which a warrant was required to obtain taxpayer information to one in which CSIS can obtain taxpayer information without a warrant.

CSIS has put in place a Deputy Director of Operations (DDO) Directive on the collection of taxpayer information without a warrant which provides that all taxpayer information can be obtained for . SIRC found this to be insufficient in view of the privacy rights at stake. Two recommendations were made in this regard: that CSIS change the required threshold for requesting taxpayer information and that a case-by-case analysis of the proportionality of the request be required.

[1] This figure of disclosures made pursuant to *SCISA* includes

2 METHODOLOGY

This review had two main objectives. The first was to make a preliminary assessment of the impact of *SCISA* on CSIS and its ability to conduct its investigations. To that end, SIRC sought to establish the volume of information exchanges under *SCISA*. The second objective was to examine CSIS's engagement with its government partners, as well as its internal policies and procedures with respect to *SCISA*.

The core review period for this study was August 2015, when the legislation came into force, to December 2016, although information falling outside of this period was examined to make a full assessment.

2.1 Review Activity

SIRC met with CSIS representatives to provide context to the issues under review. The discussions included meetings with the group responsible for overseeing the implementation of *SCISA*, the Branch, as well as with operational branches to discuss exchanges of both consular and taxpayer information. SIRC held two meetings with CSIS officials posted in to discuss consular exchanges. SIRC met informally with officials from GAC and CRA, who offered their perspectives. SIRC also examined all corporate documents related to *SCISA*, including the agreement with GAC and all internally-directed documents. Finally, SIRC reviewed the exchanges of information under the authority of *SCISA*.

2.2 Criteria for Assessment

SIRC considers that putting into place arrangements with government partners involved in exchanges of information under *SCISA* to be of central importance in supporting efficient and responsible information sharing. This is consistent with the "Guiding Principles" of *SCISA*, which set out in section 4(c) that "entry into information-sharing arrangements is appropriate when Government of Canada institutions share information regularly." Arrangements should address the finer points of information sharing: what can be shared, how, and what are the safeguards that attach to it.

Similarly, SIRC expects, at a minimum, that CSIS develop guidance or guidelines for its employees with respect to the types of information that can be shared by partners, and solicited by CSIS, and under what circumstances. This is an expectation that SIRC has for all types of information sharing. In this specific context, SIRC expects that guidance material should emphasize that CSIS is responsible under *SCISA* for providing enough information to allow the disclosing department to be satisfied that the information requested is relevant to CSIS's mandate. Finally, it should be underscored that *SCISA* does not alter CSIS's collection threshold, which is that information can only be collected by CSIS to the extent that is "strictly necessary."

3 BACKGROUND

Section 5 of *SCISA* provides that federal government institutions may disclose information to certain recipient federal institutions if the information is assessed to be relevant to "the institution's jurisdiction or responsibilities under an Act of Parliament or another lawful authority in respect of activities that undermine the security of Canada, including in respect of their detection, identification, analysis, investigation or disruption". *SCISA* operates alongside the *Privacy Act*[2] and other authorities that permit disclosure of information under certain specific circumstances. This includes, for example, the *Customs Act*, which contains an exception for disclosing customs-related information for national security purposes. All communications about *SCISA* from Public Safety Canada note that *SCISA* does not override other statutory restrictions on information sharing and that *SCISA* disclosures must respect the *Charter* and the privacy rights of Canadians.

CSIS's efforts are supported by the activities of Public Safety Canada, the government department responsible for leading the implementation of *SCISA*. Among other things, the department has prepared a guidebook, *Security of Canada Information Sharing Act* Deskbook, *A Guide to Responsible Information Sharing.* SIRC is also aware that CSIS has engaged the Office of the Privacy Commissioner on its strategy for implementing *SCISA*.

Prior to the enactment of *SCISA*, CSIS stated publicly that confusion about the patchwork of authorities for information sharing led departments to take a cautious stance toward sharing. SIRC has made comments in past reviews with respect to the flow of consular information between GAC and CSIS.[3] In its 2009 audit, the Auditor General also commented on the challenge faced by government departments when sharing sensitive information.[4]

SIRC was told that CSIS's general approach is to develop tailored proposals for each government partner.[5] This can include putting in place a new formalized arrangement to spell out the process and considerations around information sharing or updating existing arrangements. Initially, GAC, were identified by CSIS as priority partners. This was subsequently expanded to include CRA. From this list, CSIS determined that the immediate requirements were to facilitate the sharing of taxpayer information (CRA) and consular information (GAC). Discussions with

[2] The *Privacy Act* includes a general restriction on disclosing personal information without the consent of the individual. The *Privacy Act* does, however, provide for situations when private information may be shared without the consent of the individual, including, for example, if personal information is disclosed for the same purpose for which the information was collected, or if there is an overriding public interest in its disclosure.

[3] For example, see SIRC STUDY 2013-08, "Review of Stations," June, 2014.

[4] See the 2014 "Fall Report of the Auditor General of Canada, Chapter 2 – Support for Combatting Transnational Crime."

[5] Meeting with , September 27, 2016.

on using *SCISA* as an authority for information sharing, on the other hand, have not progressed and no disclosures have been made by either.

CSIS has designated the , which has a public line, as the recipient unit for potential *SCISA* disclosures. Upon receiving unsolicited information under *SCISA* – similar to a "tip" – a analyst is responsible for assessing the information using CSIS's internally held databases to determine if the disclosure should be further ingested. One such "tip" - - was recorded through CGOC during the reporting

SIRC was told that a specific file has been created for all *SCISA* related activity and, further, that CSIS is determining the best process for systematically tracking *SCISA* disclosures.[6] As will be discussed below, CSIS has experienced some challenges with respect to tracking *SCISA* disclosures.

[6] Meeting with , September 27, 2016.

4 GLOBAL AFFAIRS CANADA

Consular information can be an important source of information about threats to national security that have an overseas nexus. This has been amplified in the context of the foreign fighter investigation.

Previous SIRC reviews have commented on information sharing between GAC and CSIS. Most recently, SIRC's review of CSIS's relationship with GAC in 2014 found that the 2007 Protocol guiding information disclosures between the two departments was not functioning well. Similarly, during recent visits to CSIS stations in SIRC was told by CSIS that information sharing with GAC is an on-going issue. This review offered the opportunity to assess the impact of GAC's information sharing with CSIS pursuant to *SCISA*.

4.1 Operationalizing *SCISA*

4.1.1 Interdepartmental Efforts

Since *SCISA* was enacted, CSIS and GAC have taken a number of initiatives toward a workable framework that satisfies the requirements of both departments and their respective mandates. A policy proposal was developed jointly in October 2015, which was to be an interim measure until such time as a formal arrangement could be negotiated. This was followed in January 2016 by a "tripartite message" to Heads of Missions, Heads of Station and RCMP Liaison Officers. The message underscored that information available at missions that could be relevant to Canada's security or to another federal institution's mandate should be sent in a timely manner for approval to disclose consistent with the new authority under *SCISA*.

In May 2016, GAC and CSIS signed an Information Sharing Arrangement (ISA). The arrangement governs the disclosure of consular information and provides a "non-exhaustive" list of information that may be shared with CSIS, either proactively or following a request. The list includes:

SIRC is aware that the list is the product of extended discussions with respect to what will and will not be shared by GAC, and under what circumstances. For example, the first version of the list included [8]

GAC clarified its perspective that this information and therefore GAC has no authority to disclose it. As will be discussed below, this led to discussions between GAC and
Overall, SIRC is of the view that these discussions contributed to a mutually better understanding of CSIS and GAC's respective mandates and limitations.

SIRC also notes that the arrangement includes attention to issues of use and retention of information, including with respect to third party disclosure. The arrangement stipulates that "the Participants will return and remove from their possession any personal information (as defined in s.3 of the *Privacy Act*) that is disclosed to them which they are not authorized to collect." This inclusion is positive from SIRC's perspective, and should cover information that is disclosed to GAC from CSIS. CSIS is reminded that it should "return and remove" information that is shared that is not "strictly necessary," whether it be personal information or not, as per the *CSIS Act*.

4.2 CSIS Internal Guidance

In September 2016, a DDO Directive was issued "to provide guidance and tools to Service employees for requesting consular information."[9] At the same time, specific internal guidelines were issued on the procedures for requesting information. Both the DDO 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. It is GAC that is ultimately responsible for determining whether the information sought is relevant to CSIS's mandate. CSIS's main responsibility is to provide sufficient information to satisfy GAC in this regard.

SIRC was attentive to the specific parameters around the information being sought by CSIS. As noted, both the DDO Directive and the guidelines indicate that information sought must be relevant to an authorized investigation. SIRC also questioned whether was required prior to making a request for

[7] The agreement also includes a list of information that will not be shared by GAC under this agreement,

[8] 10 21 2015, Draft for Discussion Purposes only, "CSIS-DFATD Consular Information Sharing."
[9] DDO Directive on Consular Information Requests, 2016 09 09.

consular information. CSIS responded that canvassing other government departments for information is permitted with a covering the broad investigation.

CSIS and GAC have worked on developing templates for requesting consular information. These initial templates responded to requirements identified by GAC and had the effect of expediting GAC responses.[10] A more standardized, single template was subsequently developed in September 2016 and disseminated, along with the DDO Directive. SIRC was told that this updated template may not reflect GAC's requirements. SIRC encourages further refinements to the template, if deemed necessary.

4.3 Disclosures to date

Between August 2015, when *SCISA* entered into force, and October 2016, CSIS received consular information from GAC.[11] were disclosed proactively by GAC.[12] The overwhelming majority of disclosure requests from CSIS concerned . Of the total disclosures from GAC to CSIS, SIRC notes were made consistent with the *Privacy Act.* SIRC enquired as to the rationale for citing the *Privacy Act* instead of *SCISA* when making a request of GAC. CSIS responded that it collects information pursuant to the *CSIS Act*, regardless of whether the disclosing institution discloses information pursuant to *SCISA* or the *Privacy Act*. Moreover, CSIS stated that it is the responsibility of the disclosing institution to determine the appropriate authority.[13] SIRC was also told, however, that, when requesting information, CSIS may cite one authority over another depending on whether the request pertains to [14] **SIRC recommends CSIS clarify its position on this issue, as appropriate, and take steps to ensure consistency in the future.**

CSIS reports that GAC has responded to all requests from CSIS for consular information pursuant to *SCISA*.[15] However, CSIS also reports that the amount of information provided per disclosure varies and that several requests may be made on an individual throughout the course of an investigation.[16] This reflects, in part, that specific information is disclosed by GAC if deemed to be relevant to the request rather than a complete accounting of the consular file.

All disclosures from GAC must be processed through its headquarters, which involves GAC's Legal Services.[17] GAC has committed to responding to urgent requests within

[10] Meeting with former CSIS secondee, January 6, 2017.
[11] Response to SIRC memo.
[12] September 2016 memo to CSIS's Assistant Director of Collection (ADC) From DG
[13] Response to SIRC memo. See footnote 18 for further clarification.
[14] Meeting with former secondee, January 6, 2017.
[15] September 2016 memo to CSIS's Assistant Director of Collection (ADC) From DG
[16] Ibid.
[17] In the documentation, SIRC has seen references to GAC's clarification with respect to the different authorities for sharing; in particular, that information may be shared proactively under either s.8 (2)(m)(i) of the *Privacy Act* or

Nevertheless, SIRC has seen some frustration on the part of CSIS on this aspect of the process. In its sample review, SIRC found that CSIS's requests are answered by GAC as quickly as . In other instances, it can take for an answer to be provided. Since *SCISA* was enacted, SIRC has seen refinements to the process of requesting information that should continue to expedite the responses. SIRC expects that, with time and continued use of those tools that have been jointly developed, including the template, there may be further gains in terms of efficiency and timeliness.

4.3.1 Proactive Disclosure

Proactive disclosures of information are viewed by CSIS as essential, as CSIS cannot request information on an individual of which it is unaware. CSIS has cited the example of an individual
Although GAC did disclose the information eventually,

. CSIS felt this information should have been disclosed proactively

[18] In the documents reviewed, there were references to other instances when CSIS felt proactive disclosures should have been made.

SIRC is aware that there are ongoing interdepartmental discussions involving the whole community of implicated departments in connection to concerns about

[19] Moreover, a number of concrete initiatives are taking place

one of the missions most involved in

s.5(1) of *SCISA* or in response to a request under either s.8(2)(e) of the *Privacy Act* or s.5(1) of *SCISA*. Email exchange FW*: SCISA* and consular information sharing.

[18] September 2015 memo to CSIS's Assistant Director of Collection (ADC) From DG

At the same time, training on protocols, thresholds and triggers for disclosures of information is being conducted overseas jointly by GAC and CSIS.[23] The first of such training took place in November 2016 . It involved a number of exercises to sensitize CSIS and GAC to the specific mandates of the two organizations, including to the limitations of those mandates with respect to sharing. This joint training emphasized the threat environment to better enable GAC employees to recognize scenarios that could be triggers for proactive disclosures of information. CBSA also provided a presentation on threat indicators to officials . SIRC is also aware that GAC may be preparing to deliver a presentation to new consular officials to sensitize them to situations that should trigger a proactive disclosure.[24]

SIRC has seen other steps being taken by CSIS and GAC, even before the enactment of *SCISA*, to improve the sharing of consular information. This includes having a CSIS secondee assigned to GAC. Overall, **SIRC found that these initiatives are appropriate and in line with the general direction for implementation of *SCISA* given by the 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.

4.4 Tracking Disclosures

For tracking disclosures, SIRC was told that a specific file has been created for all *SCISA* related activity. Regardless, SIRC observed that it was not always straightforward for CSIS to tabulate GAC disclosures. SIRC is aware that was keeping track of disclosures for CSIS. Though this is positive, it is not a sustainable model . SIRC also noticed that, in some cases where GAC had no information to provide to CSIS, the information exchange was not recorded. **SIRC recommends 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 recommends that a record be kept of exchanges under SCISA for tracking purposes, including NIL responses.**

[23] September 2016 memo to CSIS's Assistant Director of Collection (ADC) From DG
[24] GAC Secondment Report, 2014-2016.

5 CANADA REVENUE AGENCY

The *Income Tax Act* (*ITA*) was amended through the *Anti-Terrorism Act*, 2015, to provide for a broader definition of taxpayer information that is sharable with agencies, such as CSIS, on a "reasonable grounds to suspect" standard than was previously the case.[25] The amended *ITA* 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 Act*."

On the basis of this legislative change, taxpayer information may now be shared by CRA without the requirement of a judicially authorized warrant. This is a departure from the past, 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 is particularly alert to how CSIS is operationalizing this change.

5.1 Operationalizing *SCISA* and the *ITA*

5.1.1 Interdepartmental Efforts

As a first step toward putting in place a framework for operating, the CSIS DDO wrote to the Assistant Commissioner of CRA

A policy document was subsequently drafted by CSIS and CRA as a "precursor" to the revision of a framework MOU. The objective was to establish parameters for the disclosure of taxpayer information under the amended authority of the *ITA*. It provides information on CSIS's mandate and how taxpayer information may contribute to CSIS's investigations. The document includes considerations for when taxpayer information will be sought by CSIS. The document notes that, given the nature of the information involved, privacy considerations have been taken into account.[27] As will be discussed later, SIRC is of the view that this statement, which appears supportive of responsible sharing of information of this nature, is not well reflected in CSIS's current approach to implementing the new authority.

[25] Previously, the *ITA* included that "designated taxpayer information" could be shared without a warrant. "Designated taxpayer information" was limited to information related to registered charities or individuals who had applied to register a charity.

[27] "CSIS-CRA Taxpayer Information Sharing" document.

SIRC was told that a new MOU has been developed and is awaiting finalization. Until then, there is an MOU in place from 1987 between CRA and CSIS that provides some guidance on the release of taxpayer information, but that MOU is grounded in the need for a Federal Court warrant and outlines the procedures in place for executing a warrant. **Considering the priority assigned to obtaining taxpayer information from CRA, SIRC recommends that CSIS prioritize the finalization of the MOU with CRA.** In fact, SIRC commented two years ago in its inquiry into CSIS collection of CRA information without a warrant on the need for a renewed MOU.

5.2 CSIS Internal Guidance

As noted, alongside a formalized arrangement between departments that share regularly, SIRC was also looking for specific direction and guidance to be developed by CSIS to provide a framework for its officials toward the goal of efficient and responsible sharing.

A template was developed by CSIS and CRA to facilitate requests for CRA information under the authority of *SCISA*. The template requires that CSIS provide a description of the threat-related activities of the individual in question, as well as the specifically financial aspect of those activities to further support the disclosure of taxpayer information. As in the case of GAC, SIRC considers the template a useful tool in promoting a standardized approach to information sharing, as well as a means of tracking and reporting on disclosures.

The principal internal direction issued by CSIS has been the DDO Directive on the collection of financial and taxpayer information without a warrant from April 2016. The Directive stipulates that CSIS may request taxpayer information from CRA on an individual

Given the expectation of privacy which has been found to apply to taxpayer information, **SIRC finds that the practice of requesting taxpayer information on the strength of does not reflect the requirement "that information be shared in a manner that is consistent with the *Canadian Charter of Rights and Freedoms* and the protection of privacy" as set out in the preamble to *SCISA*. SIRC recommends that, at a minimum, CSIS change the required threshold for requesting taxpayer information** This would be more consistent with CSIS's practice which, in turn, reflects the principle of proportionality. **Additionally, SIRC further recommends that CSIS consider the appropriateness of soliciting a case-by-case analysis of the proportionality of the request from the Department**

[28] Ibid,

of Justice. This should be reflected in internal CSIS guidance concerning requests to CRA.

In its recent decision concerning an application for warrants reported as 2016 FC 1105, the Federal Court acknowledged[29] that it no longer adjudicated CSIS requests for warrants to obtain information from the CRA. Nevertheless, when warrant powers are being sought against targets who also happen to be the subject of non-warranted CRA information sharing, SIRC's expectation is that CSIS will inform the Court that taxpayer information is being sought and obtained from CRA.

5.3 Disclosures to Date

In 2015,

[30] SIRC asked CSIS about the lack of timely responses from CRA. CSIS reported that the overall process for exchanging information was agreed to early-on by both parties. Based on the record of disclosures to date, it is unclear to SIRC whether that initial agreement has translated into a real understanding between the two departments.

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. SIRC understands that CRA has suggested a CSIS employee be assigned to CRA to, among other things, facilitate the exchange of information. This would bring the situation with CRA more in line with that of GAC, where SIRC has observed the positive impact of the CSIS secondee on exchanges of consular information.

CSIS also attributed delays to the consultation process by which CRA determines whether the information is relevant to CSIS's jurisdiction or responsibilities. CSIS reported that it has met with CRA several times to determine what elements would be required in CSIS requests that would meet CRA's thresholds for sharing information. This is reflected in the operational files, where SIRC saw instances of CRA returning to CSIS for further information to support the disclosure request.

SIRC is of the view that 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.[31] Moreover, consultations between CRA and CSIS further sensitize CSIS to CRA's specific considerations regarding information sharing. Going forward, SIRC expects that these

[29] 2016 FC 1105 at paragraph 46.
[30] Response to SIRC memo #1.
[31] Similarly, when disclosed information under *SCISA*, CSIS met with at least once to determine whether the information in the possession of did in fact meet the threshold of relevance to CSIS's mandate. Following the discussion, it was determined that information on one of the individuals in question – there were four – was not in fact relevant and was not disclosed.

consultations will assist CSIS in providing the information needed to satisfy CRA that the requested information meets the required threshold. This as 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 encourages the two partners to work together to resolve outstanding issues.

Finally, SIRC notes that neither *SCISA* nor the *ITA* 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 *ITA*, CSIS retains the option of producing a warrant. This is also noted in CSIS's legal opinion, to the effect that CSIS can continue to avail itself of warrants in cases of disagreement with CRA. SIRC therefore suggests that CSIS policy and internal procedures reflect that a warrant remains an available option.

5.3.1

[32] Response to SIRC memo.

6 OPERATIONAL IMPACT OF SCISA

SIRC set out to make a preliminary assessment of the impact of *SCISA* on CSIS's information sharing. Overall, with a relatively small number of disclosures, it is possible to conclude that the impact to date has been modest. In fact, in the cases of , partners that had been identified initially as priorities for CSIS, no discernable progress has been made toward instituting a framework for operating under this new authority. SIRC was told that CSIS has held preliminary discussions regarding *SCISA*.

With respect to consular information, CSIS noted that there has been an increase in the number of disclosures, particularly proactive disclosures. Overall, however, the effect of *SCISA* on the volume of sharing is not significant considering that consular information has always been shared. From SIRC's perspective, perhaps the most important impacts of *SCISA* have been at the level of interdepartmental discussion and cooperation. Over time, these have the potential to make improvements in this aspect of the relationship between GAC and CSIS.

SIRC has found that, when disclosures of consular information are difficult to obtain, or no consular information exists, CSIS has engaged its other government contacts to obtain information relevant to CSIS's instigative activities abroad.

With respect to CRA and taxpayer information, CSIS reported that, while taxpayer information is often a small part of an investigation, it has the potential to add to an investigation

In this context, SIRC reiterates that it is important for CSIS and CRA to take what steps are necessary to improve the situation,

7 CONCLUSION

SCISA implicates upward of 100 departments and agencies, all of which now have the authority to share information with the list of 17 designated recipients of *SCISA* disclosures, including CSIS. The foregoing discussion has acknowledged the generally cautious approach that CSIS and its partners have taken to date with respect to implementing *SCISA*. That said, under this authority, the volume of information that could be shared in the future is substantial. Moreover, the potential range of personal information in the possession of the over 100 departments and agencies included in *SCISA* that could be shared about Canadians is also substantial.

CSIS has elected to take a strategic approach to implementing *SCISA*, focusing on putting in place formal frameworks with individual government partners. SIRC found this a necessary, but not necessarily sufficient step towards ensuring responsible sharing of information that ensures that the *Charter* and the privacy rights of Canadians are respected. Going forward, CSIS should consider a process requiring consideration of whether information being sought involves interests protected by the *Charter* or the *Privacy Act* or another statutory restriction. For SIRC, issues of information sharing will continue to be a priority.