

Security Intelligence  
Review Committee



Comité de surveillance des activités  
de renseignement de sécurité

Office of the Chairman

Bureau du président

**TOP SECRET//CEO**

File No. 2800-220

January 17, 2018

The Honourable Ralph Goodale, P.C.  
Minister of Public Safety and Emergency Preparedness  
269 Laurier Avenue West  
Ottawa, Ontario K1A 0P8

Dear Mr. Goodale,

**Re: SIRC Review of Case Studies Regarding CSIS Information Sharing with Foreign Entities (SIRC Study 2017-01)**

This letter summarizes the results of a Security Intelligence Review Committee (SIRC) study of four cases of information sharing where a potential risk of mistreatment existed. Two cases involved information exchanges with CSIS the other two involved CSIS information exchanges with CSIS

SIRC examined material for indications that CSIS used information obtained by, or provided information that may have been used in, detention and/or mistreatment; and whether CSIS complied with the 2011 Ministerial Direction on Information Sharing with Foreign Entities in its information exchanges. In doing so, SIRC examined intelligence reporting, corporate documents, ministerial direction, and related CSIS policies and procedures. SIRC also received a number of briefings from CSIS with respect to the details of cases and decision-making processes. SIRC last examined information sharing with foreign entities in 2015 (Study 2015-03). Annex A provides further detail on the cases examined and criteria used.

In the information examined, SIRC found no evidence that CSIS used information obtained by torture and other cruel, inhuman, or degrading treatment, nor directly contributed to human rights abuses when it shared information in these cases. However, SIRC was not satisfied that CSIS adequately assessed and mitigated the potential risks of information sharing, as required by the 2011 Ministerial Direction.

**SIRC recommends that CSIS prioritize the development of guidelines on assessing and documenting the risk of mistreatment, as well as the risks to the assurances and caveats being respected. Such assessments should take into account the most recent and relevant information, including operational reporting.**

**SIRC also recommends that when there is a substantial risk of mistreatment that needs to be mitigated in sharing or requesting information, the decision to share should be referred to the Director through the Information Sharing Evaluation Committee, rather than an operational manager.**

First, SIRC found in the cases reviewed that the risks of sharing or soliciting information, as well as the risk that caveats and assurances would not be respected, were not appropriately assessed or documented. The corporate documentation available to operational managers generally lacked the information necessary to make an assessment regarding mitigation.

Second, SIRC found that CSIS shared and requested information with respect to a Canadian detained \_\_\_\_\_ without the approval of the Information Sharing Evaluation Committee, despite evidence casting doubt on \_\_\_\_\_ adherence to the caveats and assurances it provided regarding mistreatment. In this case, CSIS continued to rely on assurances from five years prior, despite having committed to you to seek updated assurances due to credible allegations of torture.

Finally, at the strategic level, SIRC found that CSIS did not have any documented criteria or threshold that would trigger a re-evaluation of the relationships with \_\_\_\_\_ CSIS had intelligence suggesting that assurances were not being adhered to, but any re-examination was *ad hoc* and it was unclear to SIRC under what circumstances it would be required.

SIRC will continue to monitor CSIS's activities with respect to information sharing with foreign entities as its policy and processes in this area evolve, in particular, with respect to its application of the most recent information sharing ministerial direction released in September.

Sincerely,



Pierre Blais, P.C.  
Chair

c.c.:

David Vigneault, Director of CSIS  
Director General,

**ATIP version**

JUN 08 2019

dated: \_\_\_\_\_

**TOP SECRET // CEO**

- 1 -

## **Annex A**

### **What SIRC Reviewed**

This Security Intelligence Review Committee (SIRC) review covered four cases concerning information sharing where a substantial risk of mistreatment existed. Two cases involved information sharing by the Canadian Security Intelligence Service (CSIS) while the other two cases involved CSIS information sharing with

SIRC's last review on the implementation of the Ministerial Direction on Information Sharing with Foreign Entities occurred in 2015 (2015-03), and found problems with respect to the consistency and documentation of decisions made by CSIS operational managers in cases where potential for mistreatment existed. This review follows up by examining four cases that were identified as potentially problematic.

### **Scope and Methodology**

The core review period was from January 2008 to September 2017.

SIRC considered all information relating to the four investigations, including operational reports, corporate documentation, and Federal Court transcripts. SIRC also received a number of briefings in order to clarify questions with respect to foreign arrangements and the decisions to share information.

SIRC approached the review of the cases through the lens of the 2011 Ministerial Direction on Information Sharing with Foreign Entities. SIRC looked at the following criteria:

- CSIS did not use information obtained by torture and other cruel, inhuman, or degrading treatment, nor directly contributed to human rights abuses through information it shared with partners.
- The risks associated with sharing or requesting information were appropriately documented; that is, that information provided in records of decision on the risks of the proposed instances of information sharing was accurate, up-to-date, and consistent.
- If mitigation measures were used, such as assurances and caveats, the risk that they would not be adhered to was appropriately assessed and documented.
- Cases where it was unclear whether the risk could be mitigated through the use of caveats or assurances were referred to the Director for decision, through the Information Sharing Evaluation Committee (ISEC).

**ATIP version**

JUN 08 2019

dated: \_\_\_\_\_

**TOP SECRET // CEO**

- 2 -

With respect to assurances, their reliability in mitigating the risk of torture or mistreatment depends on a number of contextual factors. The Supreme Court of Canada has highlighted a number of factors to consider,<sup>1</sup> of which the following are relevant in this context:

1. The human rights record of the state
2. Whether the assurances are specific or general
3. Who has given the assurances and whether that person can bind the other state
4. Whether the assurances concern treatment that is legal or illegal in the state in question
5. The length and strength of bilateral relations between the two states, including the other state's record in abiding by similar assurances
6. Whether compliance with assurances can be objectively verified
7. Whether there is an effective system of protection against torture in the other state

### **Background**

---

<sup>1</sup> See *India v. Badesha*, 2017

**ATIP version**

**JUN 08 2019**

**dated: \_\_\_\_\_**

TOP SECRET // CEO

- 3 -

### Rationale for Findings

**Finding #1: SIRC found in the cases reviewed that the risks of sharing or soliciting information, as well as the risk that caveats and assurances would not be respected, were not appropriately assessed or documented by operational managers.**

In these four cases during most of the period covered by the review, with the exception of one case that went to the ISEC, documentation regarding the rationale for sharing information with foreign agencies where a potential for mistreatment existed was provided in a paragraph at the end of an operational report. The purpose of this paragraph was to explain whether there was a substantial risk of mistreatment and whether the risk could be mitigated through assurances and caveats.

SIRC observed that these paragraphs did not provide reasonable assessments of the risk to the individual concerned. In the cases examined, the information contained in the paragraphs generally included: 1) an acknowledgment that a risk existed, 2) a reference to the arrangement profile having been consulted and 3) an assertion that assurances and caveats would mitigate the risk. In cases reviewed \_\_\_\_\_ rationales given with respect to the risk of caveats and assurances not being respected were inconsistent and the criteria on which the decisions were based were not clear.<sup>11</sup> Given the issues with respect to \_\_\_\_\_ after March 2015 described under

---

**ATIP version**

JUN 08 2019

dated: \_\_\_\_\_

TOP SECRET // CEO

- 4 -

findings 2 and 3, SIRC considers that a rationale demonstrating why CSIS believed that it was clear that caveats and assurances would mitigate was needed.<sup>12</sup>

Given the reliance on arrangement profiles in the documentation, SIRC examined the relevant versions. SIRC noted a disconnect between the information contained in the profiles and the assessments in the documentation of decisions for sharing information. While the arrangement profiles contained adequate summaries of the overall human rights situation in those countries, there was insufficient information by which to assess the risk that assurances would not be followed.

In particular, key pieces of intelligence suggesting [redacted] was not respecting caveats or assurances were not included within the arrangement profile [redacted] were not featured in the decision for sharing information.

Although it was explained to SIRC that arrangement profiles were "evergreen documents" used to help inform operational managers when making decisions regarding sharing,<sup>18</sup> this pertinent information was not included in the arrangement profile.

In August 2017, CSIS introduced a template for documenting the rationale for information sharing, in response to SIRC's previous recommendation in Study 2015-03. Following a meeting with both operational managers and [redacted] it was clear that the new process neither satisfied workflow nor compliance requirements.<sup>19</sup> In particular, SIRC noted that there were no guidelines for operational managers to follow in assessing the risk that caveats and assurances would not be respected. With respect to the ISEC process, SIRC noted that the information provided to ISEC was not only inconsistent with

---

<sup>12</sup> The Ministerial Direction on Information Sharing indicated that if "it is unclear whether that risk can be mitigated through the use of caveats or assurances, the matter will be referred to the Director for decision."

<sup>18</sup> Meetings with [redacted] Unit, July 19, 2017 and CTD, September 7, 2017.

<sup>19</sup> Refer to SIRC meetings with [redacted] and [redacted] November 6, 2017; as well as record of decision for [redacted]

**ATIP version**

**JUN 08 2019**

**dated:** \_\_\_\_\_

**TOP SECRET // CEO**

- 5 -

that considered by operational managers in their decision-making, but also between ISEC meetings on the same country within a short time span.<sup>20</sup>

**Finding #2: SIRC found that CSIS shared and requested information with respect to a Canadian without the approval of the Information Sharing Evaluation Committee (ISEC), despite evidence of a risk that the caveats and assurances would not be respected.**

---

<sup>20</sup> ISEC minutes

**ATIP version**

**dated: JUN 08 2019**

**TOP SECRET // CEO**

- 6 -

---

**ATIP version**

dated: JUN 0 8 2019



**TOP SECRET // CEO**

- 7 -

**Finding #3: SIRC found that CSIS did not have any documented criteria or threshold that would trigger a re-evaluation of the relationships in response to intelligence suggesting that assurances were not being adhered to.**

In their dealings  
to human rights,

had serious concerns with respect

<sup>33</sup> CSIS acknowledged these concerns in their s.17 arrangement profiles.<sup>34</sup>

In the two cases reviewed

specific assurances were obtained

CSIS indicated that it  
believed these assurances to be reliable, given the significant relationship built with  
In addition, efforts were made  
to include provisions for accountability,

SIRC noted that, in  
addition to obtaining assurances, CSIS remained cautious in terms of the information  
exchanged due to concerns over human rights abuses.

---

<sup>34</sup> 17(1)

2014-06-18

**ATIP version**

JUN 08 2019

dated: \_\_\_\_\_

TOP SECRET // CEO

- 8 -

verbal assurances with respect to mistreatment were obtained and were not reviewed or discussed again, despite the decline in CSIS's relationship with

As described above with respect to the case, in

Head of Station expressed concerns regarding the Third Party Rule and recommended a number of follow-up actions.<sup>40</sup> However, no action was taken, nor was used in later cases to evaluate the risk that assurances would not be followed.

This sequence of events should have resulted in CSIS re-evaluating its posture with respect to information sharing

the events described above with respect to case occurred. The information available at the time should be sufficient for CSIS to re-evaluate its relationship with the risk that assurances and caveats would not be honoured.

### **Recommendations**

**SIRC recommends that CSIS prioritize the development of guidelines on assessing and documenting the risk of mistreatment, as well as the risks to the assurances and caveats being respected. Such assessments should take into account the most recent and relevant information, including operational reporting.**

**SIRC also recommends that when there is a substantial risk of mistreatment that needs to be mitigated in sharing or requesting information, the decision to share should be referred to the Director through the Information Sharing Evaluation Committee, rather than an operational manager.**

---

40

**ATIP version**

JUN 08 2019

**dated:** \_\_\_\_\_

**TOP SECRET // CEO**

- 9 -

**ATIP version**

**dated: JUN 0 8 2019**

TOP SECRET // CEO

- 10 -

**ATIP version**

**JUN 0 8 2019**

**dated: \_\_\_\_\_**