

TOP SECRET//█//CANADIAN EYES ONLY

National Security and Intelligence
Review Agency



Office de surveillance des activités en matière
de sécurité nationale et de renseignement

TOP SECRET//█//CANADIAN EYES ONLY

**REVIEW OF INFORMATION SHARING
(NSIRA REVIEW 2018-16)**

TOP SECRET//█//CANADIAN EYES ONLY

TABLE OF CONTENT

I	AUTHORITIES.....	3
II	INTRODUCTION	3
III	OBJECTIVES	4
IV	SCOPE AND METHODOLOGY	4
V	CRITERIA	4
VI	BACKGROUND	5
VII	FINDINGS	9
	ANNEX A: Case Studies.....	14

TOP SECRET//█//CANADIAN EYES ONLY

I AUTHORITIES

This review was initially undertaken by the Security Intelligence Review Committee (SIRC) as articulated in section 38(1) of the *Canadian Security Intelligence Service Act*, which stipulates that SIRC is mandated to review CSIS's operations in the performance of its duties and functions.

However, while this review was being prepared, Bill C-59-*An Act respecting national security matters* received Royal Assent on June 21, 2019. Part 1 of the Bill enacts the *National Security and Intelligence Review Agency Act (NSIRA Act)*, which was brought into force through an Order in Council on July 12, 2019. *NSIRA Act* repeals the provisions of the *CSIS Act* establishing the Security Intelligence Review Committee, which was replaced following the establishment of the National Security and Intelligence Review Agency (NSIRA). The *NSIRA Act* sets out the composition, the mandate and the powers of NSIRA, and amends the *CSIS Act* and other Acts to transfer certain powers, duties and functions to NSIRA.

So this review continued as articulated in section 8 (1)(a) and 8 (3) of the *NSIRA Act* and proceeded with the examination of activities performed by CSIS in order to submit findings and formulate appropriate recommendations.

II INTRODUCTION

CSIS considers that information sharing with non-Canadian entities is crucial inasmuch as it enables the Service to carry out its mandate to guard against threats to national security. However, information sharing with non-Canadian entities (or foreign entities) involves a certain level of risk, which means that CSIS has had to develop a series of measures aiming at mitigating that risk. For instance, information sharing must be subject to caveats and assurances, either verbal or written, therefore placing restrictions on methods through which CSIS information may be used or shared.

Numerous SIRC reviews addressed the issue of information sharing with foreign entities. For example, in 2015, SIRC established that CSIS needed to apply DDO's directives more rigorously and more consistently, especially the part that documents the decision-making process.¹ Furthermore, in 2017, SIRC raised concerns about the fact that operations managers would not adequately evaluate or sufficiently document the risks arising from failures to respect caveats and assurances.² In 2018, SIRC found that the post ██████ had not attempted to obtain new assurances or to renew the current ones. More recently, the review of the ██████ post demonstrated—even though SIRC had not raised any concerns about the nature and scope of the information shared with foreign entities—that there was a requirement for using substantive caveats and assurances in order to facilitate information sharing, which includes commenting on the methods used by CSIS to measure the outcomes.

¹ *Review of Ministerial Direction and CSIS Directives on Information Sharing* (SIRC Review 2015-03).

² *Review of CSIS Operations Within Dangerous Environments* (SIRC Review 2017-06).

TOP SECRET//█//CANADIAN EYES ONLY

III OBJECTIVES

The objective set for this review is to determine the degree to which:

1. CSIS sought assurances that would be sufficient to ensure that
 - the Service has the ability to meet its legal obligations and to comply with Ministerial Directions during the information sharing; and,
 - the Service has the ability, where possible, to mitigate the risks posed by the sharing of information with foreign entities;
2. the proposed changes to policies and procedures (to be issued in 2019) will strengthen the regime that governs information exchange with foreign entities.

IV SCOPE AND METHODOLOGY

The scope of this review includes examining the information exchange cycle from entering agreements with foreign entities to managing higher-risk information exchange, including caveats and assurances applying to information exchange with foreign entities whose human rights record remains a concern.

NSIRA selected three (3) case studies based on decisions made by the Information Sharing Evaluation Committee (ISEC or the Committee) in 2018-2019. For those three case studies, NSIRA reviewed the information sharing cycle, from the conclusion of an arrangement to the risks inherent to sharing information with foreign entities. These case studies were not randomly selected, since selection was based on the following parameter: the countries identified for this review were assessed as high risk of human rights violations. There was at least one dissenting vote within ISEC, as per meeting minutes.

For the three case studies, SIRC reviewed all relevant documents, either written or electronic, including records, correspondence and any other legal or regulatory documents applying to information sharing processes and procedures.

V CRITERIA

The performance of CSIS is assessed against provisions set in CSIS governance documents. NSIRA expects that CSIS operate in accordance with the *Canadian Charter of Rights and Freedoms*, the *CSIS Act*, the *Criminal Code of Canada* and the instruction provided by the Minister of Public Safety, but also with applicable policies and procedures.

Here are the ministerial obligations, and CSIS internal policies and procedures that apply to this assessment:

TOP SECRET//[REDACTED]//CANADIAN EYES ONLY

Ministerial Obligations

- *Ministerial Direction to the Canadian Security Intelligence Service: Accountability*, July 31, 2015; and,
- *Ministerial Direction to the Canadian Security Intelligence Service: Avoiding Complicity in Mistreatment by Foreign Entities*, September 25, 2017.

Policies and Procedures

- *DDO Directive on Information Sharing with Foreign Entities* (2017);
- *Procedures: Requesting and Modifying Foreign Arrangements*;
- *CSIS Procedure: Caveats and Assurances*;
- *OPS-601 – Authorized Disclosure of Information and Intelligence – General*;
- *OPS-602 – Disclosure of Security Information or Intelligence*; and,
- Memorandum from the ADO [REDACTED] – Reminder concerning assurances from foreign entities (previous and/or continued respect for human rights), dated December 19, 2018.

VI BACKGROUND

In May 2019, CSIS had signed 313 arrangements with foreign entities spread out across more than 150 countries and territories.³ Since April 2018, [REDACTED] of those arrangements are considered active, although subject to restrictions.⁴

Section 17 of the *CSIS Act*

In order to meet the requirements of its mandate to investigate threats to the national security of Canada, CSIS ought to share information with foreign entities. Under section 17 of the *CSIS Act*, the Service may, with the approval of the Minister after consultation by the Minister of Public Safety with the Minister of Foreign Affairs, enter into an arrangement or otherwise cooperate with a foreign entity. This section aimed to codify a practice long established within RCMP's Security Service consisting of the conclusion of information sharing arrangements among jurisdictions.

Any new arrangement must be considered beneficial to CSIS operational priorities, namely that it must directly meet government of Canada and CSIS requirements for intelligence.⁵ In this case, the Foreign Relations Branch (FRB) is responsible for managing and assessing such arrangement with foreign entities. Following a CSIS enquiry concerning a possible arrangement with a foreign entity, the Branch starts a discussion with Global Affairs Canada (GAC). Meanwhile, the Director of CSIS submits to the Minister of Public Safety a request to authorize the conclusion of

³ CSIS Foreign Arrangements and Information Sharing, Briefing to NSIRA, May 21, 2019.

⁴ Memo from the ADP, Compliance with the *Ministerial Direction on Avoiding Complicity in Mistreatment by Foreign Entities: Restricting Foreign Arrangements*, April 23, 2018.

⁵ Requirements ought to be level [REDACTED]

TOP SECRET//█//CANADIAN EYES ONLY

an arrangement with the said foreign entity. After a consultation with both ministers, the Minister of Public Safety indicates to the Director of CSIS whether the arrangement is authorized or not.

FRB must also consistently monitor and assess foreign entity's human rights record, and register this information within each arrangement profile that is available for each foreign entity. The Branch creates an arrangement profile, which can be shared with other Canadian agencies or departments upon request.

Ministerial Directions

The most recent ministerial directions relating to arrangements with foreign entities date back to 2015 and 2017. The *Ministerial Direction for Operations and Accountability* was published on July 31, 2015. Annex A indicates that CSIS is the lead agency for liaising and cooperating with foreign entities in relation to threats to the security of Canada, and to security assessments under the *CSIS Act*. Annex A also provides guidelines for the conclusion of any such arrangement.

Ministerial Directions (MD) have been issued in relation to human rights. The Minister decided to revise the 2011 ministerial direction on information sharing with foreign entities.⁶ In the *Ministerial Direction: Avoiding Complicity in Mistreatment by Foreign Entities*, published on September 25, 2017, the Minister sent instructions to CSIS stating that the Service is to strongly oppose the infliction of mistreatment regardless of the motives.

The new MD sets out specific prohibitions for the disclosure, requesting and use of information. It clearly prohibits disclosing or requesting information where doing so would result in substantial risk of mistreatment. Moreover, it is forbidden to use information likely obtained through mistreatment. However, there is one exception:

Such information can only be used to deprive a person of their rights or freedoms in exceptional cases – to prevent loss of life or serious personal injury – with the approval of the Deputy Head [Director of CSIS].⁷

MD also requires that reports be submitted to the government⁸ for transparency and greater accountability.⁹ Thus, the Minister, the National Security and Intelligence Committee of Parliamentarians and NSIRA will be kept informed of all cases referred to the Deputy Head (i.e., the Director of CSIS).

Evaluation process – Information Sharing with or Request to Foreign Entities

A few days after the publication of the MD *Avoiding Complicity in Mistreatment by Foreign Entities*, the Deputy Director of Operations (DDO) issued a directive instructing CSIS employees to comply with new requirements. Dated September 28, 2017, the Directive from the DDO intended to provide CSIS employees with tools that would allow them to comply with Canadian

⁶ *Ministerial Direction to the Canadian Security Intelligence Service on Information Sharing with Foreign Entities*, July 2011.

⁷ www.canada.ca/en/public-safety-canada/news/2017/09/ministerial-directionsonavoidingcomplicityinmistreatmentbyforeign.html

⁸ "CSIS is directed to produce a classified annual report to the Minister regarding the application of this Direction." "The Minister will provide CSIS [sic] with this report." "The Minister will provide the National Security and Intelligence Committee of Parliamentarians with as much information from the report as the Committee is authorized to receive by law." Paragraphs 24, 25 and 26 of the 2017 Ministerial Direction.

⁹ Deputy Ministers National Security Committee, PCO, January 25, 2018.

TOP SECRET//█//CANADIAN EYES ONLY

and international law. The Directive emphasized the importance of obtaining the appropriate level of approval for any sharing of information with foreign entities, adding that the said level ought to be proportional to the risk that the information might have been obtained through mistreatment or might be the cause of mistreatment.

The decision-making process that leads to a decision with respect to information sharing with foreign entities must analyze and take into account important considerations to insure the information is accurate and reliable, and to guarantee that the said information has not been obtained through mistreatment. When using information acquired from a foreign entity, CSIS must determine whether:

- the information was obtained while a detainee was being interrogated outside of Canada;
- the information was obtained through incriminating admission; and,
- there are other indicators of potential mistreatment (including, but not limited to poor human rights record; unusual extradition practice, e.g., transferring suspects from one State to another without regard to the law; etc.).

When information sharing with a foreign entity is required, CSIS must base its assessment on three criteria:

- is the information about a person detained outside of Canada?
- would the information potentially lead to adverse actions against a person (detained or other)? and,
- are there other indicators pointing to a risk of mistreatment if information is shared or requested?¹⁰

When at least one criteria applies to the information (either received or to be provided), CSIS cannot use nor share this information, and a review must be conducted by the Deputy Director General Operations (DDG OPS). If the DDG considers that a risk of mistreatment exists and that the caveats and assurances would not help mitigate the said risk, the case is referred to ISEC for assessment and decision.

The information received can be used once the Committee has assessed that it had not been obtained through mistreatment. If the Committee finds it was likely obtained through mistreatment, the information received cannot be used. In rare exceptions where CSIS's posture would require the sharing of information likely obtained through mistreatment (following a rigorous case analysis) – for instance, when there is a serious or imminent threat –, the Director is responsible for making a decision.¹¹ This provision is included in the MD (2017 version).¹²

¹⁰ Directive from the Deputy Director of Operations, Avoiding Complicity in Mistreatment by Foreign Entities – Annex 2.

¹¹ Annex C of the 2017 MD.

¹² Of note, the 2011 version of the Ministerial Directions indicates “[t]he Director may refer the decision whether or not to share information with the foreign entity to the Minister of Public Safety, in which case the Minister will be provided with the information described above. The Director or Minister of Public Safety shall authorize the sharing of information with the foreign entity only in accordance with this Direction and with Canada’s legal obligations.” One could therefore imply that the 2011

TOP SECRET//█//CANADIAN EYES ONLY

With respect to the information shared with or requested from foreign entities, the Committee must refer the case to the Director for decision if:

- the Committee determines there is a risk of mistreatment and this risk cannot be mitigated, while there is a serious threat of injury or loss of life; or
- the Committee is not able to determine whether a substantial risk of mistreatment can be mitigated with the use of caveats or assurances.

Finally, if the substantial risk cannot be mitigated, information will neither be requested from nor be shared with the foreign entity.

Until recently, the Committee required a quorum of six (6) persons, and decisions were based on a majority vote. Since the spring of 2019, decisions are made by consensus.

Update – New Procedural Restrictions

In April 2018, FRB recommended restricting an additional number of arrangements, which would allow CSIS to fully comply with the MD *Avoiding Complicity in Mistreatment*. CSIS adopted a new model whose purpose is to restrict arrangements with foreign entities based on three levels of restriction that apply in accordance with specific circumstances. In a letter to the Minister of Public Safety, the Director explains that this new approach aligns with the following three objectives:

1. ensure CSIS engagement with a foreign entity does not pose a substantial risk of mistreatment;
2. allow information sharing that is not likely to pose a risk of mistreatment, thus promoting a certain level of continued engagement; and,
3. ensure full compliance with the new MD.¹³

At the same time, CSIS informed NSIRA that a new mechanism had been put in place; it also indicated which foreign entities were involved, including the ones that are subject to restrictions.

Risk Mitigation Measures

Caveats and assurances from countries with a human rights record that is questionable or that raises concerns present a considerable challenge for CSIS. In fact, according to several experts and civil society organizations like *Human Rights Watch*, *Civil Liberties Union*, and *Amnesty International Canada*, sharing information with certain countries raises numerous issues considering the substantial risk of mistreatment this practice may entail and the possibility that risk mitigation may not be possible.¹⁴

version of the Ministerial Directions would allow the Director to exercise discretion when determining whether a request to share information with a foreign entity should be submitted to the Minister.

¹³ Memorandum to Minister – Restrictions imposed on *CSIS Act*, section 17(1) (b) Foreign Arrangements, dated April 3, 2018 (CCM#29891).

¹⁴ In this regard, the expert Alex Neve draws attention to the fact that information sharing with non-traditional partners could lead to abuse, since many of them have a poor human rights record.

⁵ DDO, New Procedures and Training Regarding Caveats, June 18, 2019.

TOP SECRET//█//CANADIAN EYES ONLY

The MD to CSIS on avoiding complicity in mistreatment by foreign entities clearly sets out the parameters to consider when sharing information with countries known to have a poor human rights record. In 2009, CSIS implemented a procedure to obtain, from foreign entities, assurances that would be more global. This procedure was under review in the spring of 2019. NSIRA was advised that procedures relating to caveats and assurances would soon be replaced.

Caveats

CSIS caveats provide the recipient with instructions on information handling in order to avoid misclassification or dissemination that would be potentially prejudicial to CSIS.¹⁵

As of July 8, 2019, new procedures to apply to Canadian and foreign recipients came into effect. These procedures now come with tools that help identify the caveat to be used or provide a new function that automatically inserts, when required, a caveat into an operational report. This function can even validate the selected caveat.

Assurances

FRB is currently preparing procedures that align with human rights assurances required from foreign entities. CSIS needs to apply such measures to mitigate risks when information sharing takes place. These measures are to be used together with appropriate caveats during the sharing process. They should become effective subsequently.

Decision-Making Process

At the end of 2018, CSIS reviewed decision-making procedures. The new measures were announced in May 2019 and will come into force within the next months. NSIRA was informed¹⁶ that from now on, ISEC was to make decisions based on consensus instead of a majority. Moreover, the Legal Services representative (Department of Justice) is no longer a voting member, but acts as a legal advisor to ISEC. Lastly, OPS EXEC team will be informed on a regular basis with regard to tendencies and disputes about ISEC decision-making process. Once management is informed, a discussion will take place. Then, a recommendation will be made to solve the issue and/or the issue will be brought to CSIS Director's attention.

VII FINDINGS

Finding 1: Taking ██████████ into Account

NSIRA finds that two of the cases examined by ISEC should have been transferred to the Director, for it is the Director, not the Committee, who is responsible for making a final decision in compliance with MD: *Avoiding Complicity in the Mistreatment by Foreign Entities*.

¹⁵ DDO, New Procedures and Training Regarding Caveats, June 18, 2019.

¹⁶ Meeting with DDO Secretariat, June 2019.

TOP SECRET//█//CANADIAN EYES ONLY

[REDACTED]

CSIS received information [REDACTED]
[REDACTED] This case was referred to ISEC since some indicators pointed to [REDACTED] poor human rights record. It was referred to the Committee on November 9, 2018.

[REDACTED]

ISEC concluded that exchanging this information would pose substantial mistreatment risk, even with [REDACTED]. However, ISEC also considered that the risk could be mitigated by using proper caveats and seeking assurances from [REDACTED]

Meanwhile, [REDACTED] also considered that sharing information with [REDACTED]
[REDACTED] In this case, the meeting minutes do not contain any additional information regarding the verbally expressed [REDACTED]

On November 9, 2011, the Deputy Director Intelligence (DDI) approved the majority decision by agreeing that there was a substantial risk of mistreatment, but that the said risk could be mitigated and the information could therefore be shared, as long as appropriate caveats and existing assurances are applied.

[REDACTED]

In this case, the information sharing with [REDACTED] pertained to [REDACTED]
[REDACTED]
The information relating to [REDACTED]
[REDACTED]
[REDACTED] The case was referred to ISEC on October 4, 2018.



[REDACTED]

The Committee established there was a substantial risk of mistreatment [REDACTED]
[REDACTED]


[REDACTED]

TOP SECRET////CANADIAN EYES ONLY



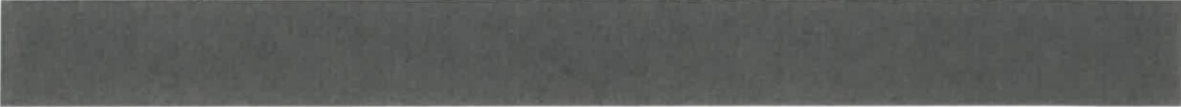

Nevertheless, two Committee members (the Committee has five [5] voting members) expressed their disagreement:  






  





On October 30, 2018, despite the substantial risk of mistreatment, the DDI considered that the risk could indeed be mitigated through caveats and  assurances, and therefore gave its approval to the majority decision.

Comments


The assessment of mitigation measures and their impact is not only a legal issue; it must also be considered in light of established facts. CSIS remains responsible for decisions made within ISEC.






When a decision needs to be made, the Service is not obligated to  . Other ISEC members, for instance other CSIS branches and GAC, express their viewpoint when assessing substantial risk of mistreatment is required. All the same, according to NSIRA, the Director must be advised when the  believes that the proposed action is not permitted .

Lastly, NSIRA notes that majority-based decision process was not advisable, since the majority of members are from CSIS.¹⁸   
 With the consensus-based decision-making process that was recently adopted by CSIS, particularly contentious cases will be escalated to a higher level, namely the Director of CSIS.

Recommendation 1

NSIRA recommends, when  consider that substantial risk of mistreatment cannot be mitigated, that the case be automatically referred to the Director for a final decision.

Finding 2: Lack of  regarding 

After reviewing information, NSIRA finds that no written  had been obtained to validate or invalidate the  notice orally communicated to ISEC regarding the use of  as a mitigation measure during information sharing.

¹⁸ One of ISEC members represents Global Affairs Canada.

TOP SECRET//█//CANADIAN EYES ONLY

CSIS is currently reviewing ways to mitigate risk that would permit information sharing when there are human rights concerns are raised toward a foreign entity. One of the ways considered by CSIS would be [REDACTED]

[REDACTED]

[REDACTED]

In the second case regarding [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] the case was referred to ISEC on May [REDACTED].

ISEC concluded there was a substantial risk of mistreatment [REDACTED]
[REDACTED] Maintaining there was no appropriate mitigation measures in place, the Committee concluded that the risk could not be mitigated. Therefore, the case was escalated to the acting director, [REDACTED]

[REDACTED]

The Committee Chair indicated that all members agreed there was a substantial risk of mistreatment and that ISEC members should understand how [REDACTED] works before being satisfied that it would constitute an appropriate mitigation measure.

ISEC requested [REDACTED] to explore other options that would mitigate the risk of mistreatment. Before making a decision, the Director of CSIS also requested more information regarding [REDACTED]
[REDACTED] The Branch ultimately withdrew its request, for the information discussed [REDACTED] no longer needed to be shared, [REDACTED]²⁰

NSIRA submitted a request to CSIS asking whether a written legal opinion had been provided to CSIS regarding [REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
²⁰ In a memo dated [REDACTED] the Director of CSIS informed the Minister of this case, although it was not required by the MDs, since information was never shared with [REDACTED]
Memorandum to the Minister: Rescinding of request to share [REDACTED]
[REDACTED]

TOP SECRET//~~SI~~//CANADIAN EYES ONLY

Comments

For the two case scenarios relating to [REDACTED] CSIS tried to [REDACTED]
[REDACTED]. In both cases, [REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED] ISEC's decision-making process cannot always provide sufficient time to thoroughly analyze case facts. Specifically, the process is not always propitious for considering additional legal aspects and factors. However, a formal legal notice would allow CSIS to determine the possible validity of [REDACTED] mitigation measures.

In this case, the information held by CSIS regarding the threat was subject to a specific timeframe; it has not been possible to share the information [REDACTED]. It would be helpful if CSIS received a formal legal opinion in order to prevent this kind of result that could have serious repercussions in the future.

Recommendation 2

NSIRA recommends that CSIS request a formal legal opinion before determining whether [REDACTED] could be used in the future as mitigation measures for information sharing with a foreign entity.

TOP SECRET////CANADIAN EYES ONLY

[REDACTED] AFC noted that information sharing [REDACTED] carried substantial risk of mistreatment and that the said risk could not be mitigated.

On November 9, 2018, [REDACTED] an update regarding qualification of the information source (*qualification de la source de l'information*).

On the same day, ADI gave its approval to the majority decision. ADI recognized there was a substantial risk of mistreatment, but also indicated that the said risk could be mitigated and that the information could therefore be shared with the proper caveats and existing assurances.

Second Case Study – [REDACTED] The case was submitted to ISEC on May 29, 2018.

Summary

[REDACTED]
[REDACTED]

Decision

- In accordance with *DDO Directive on Information Sharing with Foreign Entities* (2017), the Committee notes that information sharing with [REDACTED] poses substantial risk of mistreatment, but there are no adequate mitigation measures in place, which makes it impossible to mitigate the risk. Therefore, the case must be escalated to the acting Director, while [REDACTED] will explore other mitigation options involving [REDACTED]²⁴

On May 29, 2018, ADP approved the Committee's recommendation.

On the same day, before making a decision in this matter, the acting Director of CSIS requests additional information from [REDACTED] regarding [REDACTED]

On August 1, 2018, [REDACTED]

On November 1, 2018, [REDACTED] withdrew the request previously submitted to ISEC, for the information discussed on [REDACTED] no longer needed to be sent [REDACTED]

Identified Risk

Given [REDACTED] human rights record, there is still a possibility that detained persons be mistreated because CSIS offers to share information containing [REDACTED]

²⁴ [REDACTED] considered possible mitigation measures for CSIS. [REDACTED]
[REDACTED]
[REDACTED]

TOP SECRET//CANADIAN EYES ONLY

Minutes

- The Chair informs the members that this instance of information sharing with [REDACTED] is the first to be brought to ISEC's attention and the first case where there is a risk that [REDACTED] information be shared with an entity [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
- [REDACTED] highlights the fact that information sharing [REDACTED] remains the issue to consider based on [REDACTED] risk of mistreatment as well as the stipulations included in the MD and the Charter. [REDACTED] asked whether the decision in the matter would be referred to the Director.
- The Chair declares that all members agree to the fact that there is a substantial risk of mistreatment and that [REDACTED] must be understood before ISEC is satisfied that it represents an adequate mitigation measure.

[REDACTED]

[REDACTED] the relation [REDACTED] dates [REDACTED]
[REDACTED] In [REDACTED] CSIS submitted to Solicitor General Canada a request to obtain an [REDACTED]
[REDACTED] in order to cover [REDACTED]
provisions [REDACTED] [REDACTED] [REDACTED]
[REDACTED] CSIS had also informed Solicitor [REDACTED]
General that relations with [REDACTED]
[REDACTED]²⁵

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

²⁵ Email from [REDACTED] to [REDACTED] in reference to cooperation with [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

TOP SECRET////CANADIAN EYES ONLY

Third Case Study [REDACTED]

The proposed information sharing with [REDACTED] pertained to [REDACTED]

The file was submitted to ISEC on [REDACTED]

Information related to the [REDACTED]
[REDACTED]
[REDACTED]

During their briefing, [REDACTED] also provided [REDACTED] for sharing information. The objective was to communicate information [REDACTED]
[REDACTED] In addition, the Branch wanted [REDACTED] to provide information [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

Committee's Decision

In keeping with the *DDO Directive on Information Sharing with Foreign Entities* (2017), the Committee notes that information sharing with [REDACTED] poses substantial risk of mistreatment [REDACTED]
[REDACTED] The Committee considers that the risk can be mitigated with caveats and [REDACTED] assurances.

Nevertheless, [REDACTED] Committee members, [REDACTED]
[REDACTED] expressed their disagreement. [REDACTED]

[REDACTED]

TOP SECRET//█//CANADIAN EYES ONLY

[REDACTED]

[REDACTED]

[REDACTED]