TOP SECRET – CANADIAN EYES ONLY

SIRC REVIEW 2015-03

REVIEW OF MINISTERIAL DIRECTION AND CSIS DIRECTIVES ON INFORMATION SHARING

SUMMARY

- The purpose of this study was to evaluate CSIS's compliance with the MD by examining the information-sharing framework that it has put in place, namely through the 2011 Deputy Director of Operations (DDO) Directive on Information Sharing with Foreign Entities.
- SIRC assessed a sample of information-sharing cases against the benchmarks set out in the MD and in CSIS's DDO Directive, which require CSIS to assess and mitigate the potential risks of sharing information and to identify information that is likely to have been derived from mistreatment.
- Overall, SIRC found that CSIS acted quickly to implement a sound information-sharing framework.
- However, SIRC found that the framework could be strengthened through a more rigorous and consistent application of the DDO Directive and recording of the decision-making process, especially at the level. In SIRC's opinion, these gaps led CSIS to take contradictory decisions on at least two cases.
- As a result, SIRC made three recommendations aimed at improving CSIS's recording of decision-making surrounding information sharing with foreign entities.

File No. 2800-197 (TD R553)

Table of Contents

1 INTRODUCTION

In 2006, Justice Dennis O'Connor, who led the commission of inquiry into the actions of Canadian officials in relation to Maher Arar, recommended that CSIS policies include specific directions "aimed at eliminating any possible Canadian complicity in torture, avoiding the risk of other human rights abuses and ensuring accountability." Since then, two Ministerial Directions (MD) on Information Sharing with Foreign Entities have been promulgated, one in 2009 and another in 2011. The 2011 MD, while condemning the use of torture in responding to terrorism, established a process for determining when it may be permissible to exchange information even when it may not be possible to mitigate a substantial risk of mistreatment. Although a number of recent SIRC reviews have examined CSIS's information-sharing practices,[1] this is the first review focused on CSIS's response to the 2011 MD.

The purpose of this study was to evaluate CSIS's compliance with the MD by examining the information-sharing framework that it has put in place, namely through the 2011 Deputy Director of Operations (DDO) Directive on Information Sharing with Foreign Entities. SIRC assessed a sample of information-sharing cases against the benchmarks set out in the MD and in CSIS's DDO Directive, which require CSIS to assess and mitigate the potential risks of sharing information and to identify information that is likely to have been derived from mistreatment.

Overall, SIRC found that CSIS acted quickly to implement a sound information-sharing framework. However, SIRC found that the framework could be strengthened through a more rigorous and consistent application of the DDO Directive and recording of the decision-making process, especially at the level. In SIRC's opinion, these gaps led CSIS to take contradictory decisions on at least two cases. As a result, SIRC made three recommendations aimed at improving CSIS's recording of decision-making surrounding information sharing with foreign entities.

[1] See for example: Review of CSIS's role in interviewing Afghan detainees (SIRC Study 2010-01. File No: 2800-153), Review of CSIS's relationship with Partners (SIRC Study 2011-08. File No.: 2800-167), Review of the role of CSIS in the matter of Abousofian Abdelrazik (SIRC Study 2011-04, File No: 2800-163).

2 METHODOLOGY

The objective of this study was to assess CSIS's response to the 2011 MD. SIRC reviewed corporate and operational documentation related to the cases that were discussed at the Information Sharing Evaluation Committee (ISEC), a senior executive level committee that meets as needed, on specific cases, to assess whether to proceed with sharing information where there may be a risk of mistreatment.[2] SIRC also reviewed operational documentation for over 300 decisions taken including closer examination of over a dozen of these decisions. To ensure that the review sample was representative of the overall information-sharing process, SIRC chose cases consisting of information received from foreign entities, as well as information sent and/or solicited from foreign entities.

The core review period for this study was from August 1, 2011 to December 31, 2014, but to make a complete assessment of relevant issues, SIRC requested information that fell outside this period.

2.1 Review Activity and Criteria

According to the DDO Directive on Information Sharing with Foreign Entities, all deliberations resulting from the assessment process must be documented and saved in the appropriate files.[4] A reference to the decision (ISEC or the Director) must also be indicated in the relevant operational report(s). SIRC examined these files and relevant operational reporting to ensure compliance to this procedure. SIRC also attended a briefing with CSIS to discuss the implementation of the MD.

[2] See ISEC structure and guidelines in Annex C.

[4] i.e. the operational file as well as the Information Sharing Evaluation Committee File. DDO Directive on Information Sharing with Foreign Entities. August 24th, 2011.

3 BACKGROUND

3.1 Ministerial Direction: 2009 vs. 2011

In May 2009, a Ministerial Direction (MD) on Information Sharing was issued, stipulating that information-sharing was a vital component of safeguarding Canada's national security, as well as an obligation of all states engaged in the struggle against terrorism.[5] The MD authorized CSIS to enter into formal information-sharing arrangements with foreign agencies, including those that are "generally recognized as having poor human right records." At the same time, it also directed CSIS to not knowingly rely upon information which is derived from the use of torture, and to have in place reasonable and appropriate measures to identify any questionable information. In addition, CSIS was asked to take all other reasonable measures to reduce the risk that any action taken by CSIS might promote or condone, or be seen to promote or condone the use of torture, including when appropriate, seeking assurances from the foreign agencies.

In July 2011, this direction was replaced by a new Ministerial Direction on Information Sharing with Foreign Entities. The 2011 MD reiterated the Government of Canada's opposition to the mistreatment of any individual by any foreign entity for any purpose; by the same stroke, the MD established a decision-making process for determining when it may be permissible to share or receive information despite a substantial risk of mistreatment that cannot be mitigated through the use of caveats or assurances. These cases must be referred to the Director, who must consider the following in his decision: the threat to Canada's national security, the importance of sharing the information, the status of the relationship with the foreign entity, the rationale for believing that there is a substantial risk of mistreatment, the proposed measures to mitigate the risks, the views of the Department of Foreign Affairs, Trade and Development (DFATD) and of other departments as appropriate. When deemed necessary, the Director may also refer the decision to the Minister of Public Safety.

Additionally, the MD directed CSIS to adhere to the following information-sharing principles:

- CSIS must act in a manner that complies with Canada's laws and legal obligations;
- CSIS must assess the accuracy and reliability of information received, and properly characterize it in any further dissemination. It must have in place reasonable and appropriate measures to identify information that is likely to have been derived from mistreatment;
- The approval level that CSIS requires in order to share information must be proportionate to the risk of mistreatment that may result; and,
- CSIS must keep the Minister of Public Safety generally informed about its

[5] Ministerial Direction to the Director of the Canadian Security Intelligence Service: Information Sharing with Foreign Entities, May 2009.

information-sharing practices.

According to CSIS, the involvement of the Minister is guided by both the Ministerial Direction on Information Sharing with Foreign Entities as well as the Ministerial Direction for Operations and Accountability.[6] As of today, the principles and processes outlined in these MDs are those to which the Service must continue to adhere.

3.2 Review process at the level

Through the DDO Directive, CSIS has implemented a set of assessment criteria to be used by CSIS employees when considering whether to use information received from a foreign entity (see Annex E), or to send information to / solicit information from a foreign entity (see Annex F) where there may be a risk of mistreatment. The processes described below will be engaged only if the information is required for a specific action.[7] When a CSIS employee wishes to use information received from a foreign entity, he or she must assess the information against three criteria: 1- Does the information come from a detention interview conducted abroad? 2- Does the information come from a self-incrimination confession? 3- Is there any other information indicating a potential mistreatment (such as, but not limited to: poor human rights records, practice of extraordinary rendition, i.e. transfers of suspects from one state to another outside the law, etc)? If any of these criteria are met, an must evaluate the information and make one of three decisions:

- If there is no potential mistreatment, the information can be used as usual;
- If there is a potential mistreatment, but the information does not need to be included in the action, namely that the action could be undertaken by leaving out the problematic information without affecting the action, the information will not be used in the action;
- If there is a potential mistreatment and the information needs to be actioned, the case must be referred to the Information Sharing Evaluation Committee (ISEC).

The process for sending or soliciting information from foreign entities is similar. The CSIS employee must apply three assessment criteria: 1- Does the information pertain to an individual in detention abroad? 2- Could the information result in a negative action against an individual (detention or other)? 3- Is there any other information indicating a potential mistreatment if the information is sent / solicited? If one of these assessment criteria is met, the can make one of the following decisions:

---

[6] According to the Ministerial Direction for Operations and Accountability, the Director will advise the Minister of issues on a case-by-case basis as necessary.

(Ministerial Direction for Operations and Accountability. July 31, 2015).

[7] There are instances when information received from a foreign entity resides in CSIS holdings without being assessed. (Preliminary Briefing with June 11, 2015).

- If there is no potential mistreatment, the information can be sent or solicited, with appropriate caveats and/or assurances if required;
- If there is a potential for mistreatment and caveats and/or assurances would likely mitigate the risks, the information will be sent / solicited with appropriate caveats and/or assurances;
- If there is a potential for mistreatment, and the information needs to be sent or solicited and caveats and/or assurances would likely not mitigate the risks, the case must be referred to the Information Sharing Evaluation Committee.

3.3 Review process at the Information Sharing Evaluation Committee

When an refers a decision to the ISEC, the Committee must assess the information and make a decision. If the Committee determines that the information received from a foreign entity is likely not derived from mistreatment, the information can be used in an action without further consultation. However, if the Committee determines that the information is likely derived from mistreatment, but there is not a serious threat of loss of life, injury, or substantial damage or destruction of property, the information cannot be used in a specific action. Finally, if the Committee determines that the information is likely derived from mistreatment, and there is a serious threat of loss of life, injury, or substantial damage or destruction of property, the decision will be referred to the Director.

With regard to information sent to or solicited from foreign entities, if the Committee determines that there is no substantial risk of mistreatment, the information will be sent / solicited with appropriate caveats / assurances. Yet, if the Committee determines that there is substantial risk of mistreatment, but there is not a serious threat of loss of life, injury, or substantial damage or destruction of property, the information will not be sent / solicited. Finally, if the Committee determines that there is substantial risk of mistreatment and there is a serious threat of loss of life, injury, or substantial damage or destruction of property, the decision will be referred to the Director.

It is worth noting that the 2011 MD provides a definition for the terms "mistreatment" and "substantial risk"[8] to help guide the decision-making process. The ISEC also has guidelines that outline, for example, how it can request additional checks/actions to be carried out for re-evaluation purposes[9] and a list of sources[10] that Committee members

[8] "Mistreatment" means torture or other cruel, inhuman, or degrading treatment or punishment. "Substantial risk" is a personal, present, and foreseeable risk of mistreatment. In order to be "substantial", the risk must be real and must be based on something more than theory or speculation. In most cases, the test of a substantial risk of mistreatment will be satisfied when it is more likely than not that there will be mistreatment. However, the "more likely than not" test should not be applied rigidly because in some cases, particularly when the risk is of severe harm, the "substantial risk" standard may be satisfied at a lower level of probability. (Ministerial Direction to the Canadian Security Intelligence Service: Information Sharing with Foreign Entities. July 28, 2011).

[9] For example, carry out a specific interview, request assurances from the foreign entity (new or additional), ask the foreign entity for details regarding how the information was obtained. (Information Sharing Evaluation Committee.

can consult to help them in their decision-making. Overall, CSIS elaborated a clear course of action for determining when it may be permissible to exchange information even when it may not be possible to mitigate a substantial risk of mistreatment.

Appendix 3, August 2011).

[10] Such as CSIS databases, CSIS Arrangements with Foreign Governments and Institutions, assurances received from the Foreign Entity in question, Country Human Rights Reports from DFAIT, Reporting from organisations such as Amnesty International, Human Rights Watch, US State Department, relevant open source information, and private databases. (Information Sharing Evaluation Committee. Appendix 3, August 2011).

4 LEVEL PROCESS

4.1 Recording of deliberations and resulting decisions

SIRC examined all operational reporting reflecting the over 300 decisions on information exchanges taken at the level during the review period. The approval section of each operational report generally indicated the various actions that were taken as part of the assessment process, including the following: a review of existing CSIS arrangements with the foreign entity, discussion related to assurances with this foreign entity, a review of available open information on the respective country's human rights record and of recent exchanges with the entity.

SIRC selected a sample of sixteen cases for in-depth review; for each case, CSIS was asked to provide a summary of the assessment process, as well as a copy of the documents examined by the In the cases reviewed, **SIRC found that while CSIS had a record of decision-making, it had no record of the deliberations surrounding assessments, as required in the DDO Directive.** The DDO Directive states that: "All deliberations coming from assessments requested in this directive as well as the resulting decisions must be documented and saved in the appropriate files (…)."[11] Given this absence of documentation, SIRC found it difficult to make a complete assessment of the decisions taken at the level.

SIRC has previously raised concerns with the absence of records surrounding CSIS's decision-making process. As noted in two recent reviews,[12] SIRC believes that CSIS must take its obligations to maintain records of its decision-making very seriously, so as to ensure that it is in compliance with standard requirements set by Treasury Board. Accordingly, **SIRC recommends that CSIS's Executive prioritize the development of an action plan to address this issue within this fiscal year.**

4.2 Cases of inconsistencies in the application of the DDO Directive

In the review of operational reporting, **SIRC found inconsistencies in the application of the DDO Directive and in the decision-making process at the level.** SIRC found cases where the DDO Directive was not well understood by the responsible for assessing the information and making a decision. In one case, for

[11] DDO Directive on Information Sharing with Foreign Entities. August 24th, 2011.

[12] In the review of CSIS Operational Support and its Use Overseas (SIRC Study 2013-07), SIRC recommended that CSIS take immediate and appropriate steps to impress the importance of maintaining records of discussions and decisions to ensure proper accountability. Additionally, in the review of the Insider Threat and its Effect on Information Management (SIRC review 2013-06), SIRC recommended that CSIS take immediate action to ensure that all decision-making pertaining to internal investigations be documented within the appropriate case file, in accordance with the standard requirements set by Treasury Board.

example, when analyzing information received from a indicated being confident that the issue of assurances did not apply to an interview conducted by the CSIS acknowledged that this was an instance of misinterpretation of the Directive in response, CSIS indicated that the issue had been clarified by way of FAQs with respect to information sharing with foreign entities. SIRC encourages to ensure that employees understand that the DDO Directive applies to all foreign agencies, without any exception.

In another case, CSIS had to decide whether to share information obtained from In a DFATD report, the had noted concerns about isolated reports of abuse of detainees in this country, but nothing specific to the foreign entity who had sent the information to CSIS. According to the DDO Directive, the had to decide if there was potential mistreatment, and if so, whether caveats and/or assurances would mitigate the risks. However, the did not address the criteria of "potential mistreatment", focusing instead on the criteria of "serious threat of loss of life, injury, or substantial damage of property."[16] This criteria, however, is to be used when the case is referred for decision to the senior-executive level. SIRC followed-up with CSIS on this case, asking the to confirm if there was potential mistreatment. CSIS responded that the report indicated the issue had been assessed very thoroughly by the and that CSIS had no concerns regarding human rights as torture has been designated as a crime in Still, SIRC believes that the record of decision-making should have included an assessment of the proper criteria.

4.3 The criteria of potential mistreatment

The assessment process at the level is largely based on the criteria of "potential mistreatment". In SIRC's view, the DDO Directive does not provide guidance to the on how to assess the "potential of mistreatment", nor does it define what "potential of mistreatment" means and how it differs from a "substantial risk of mistreatment". In response to SIRC's queries, CSIS recognized that "potential mistreatment" was not specifically defined in the DDO Directive. In an effort to provide further clarification, CSIS explained that "potential mistreatment" was "the criteria used to determine whether the Information Sharing Evaluation Committee (ISEC) is required to assess whether a "substantial risk of mistreatment" exists. As such, "potential

---

[16] See The notes that: "l'information peut être communiquée À la lumière des vecteurs de menaces existants dans la région et de leur imminence, le Service se doit de poursuivre toute piste crédible afin d'essayer de prévenir d'autres attaques similaires".

mistreatment" is considered a lower threshold aimed at ensuring that the ISEC can conduct a thorough assessment of all such potential mistreatment." SIRC believes that
having a defined criteria could help to ensure a more consistent understanding and application of the information-sharing process.

4.4 Use of Arrangement Profiles

In support of their decision to share information, often quoted from the arrangement profile[19] of the foreign entity in question. As part of its sample review, SIRC examined all arrangements profiles cited in the approval section of the operational reports. In at least three cases, the used the arrangement profile to note that the foreign entity had never been the focus of human rights concerns or complaints. While accurate, these statements did not include any mention of the fact that the foreign entity does not usually possess the authority to arrest or detain persons and that it must act in concert with a law enforcement agency, such as the national or local police, to affect an arrest.

In their response, CSIS also indicated that "potential mistreatment applies to situations in which CSIS is assessing whether mistreatment has already occurred as well as whether mistreat may occur. "Substantial risk of mistreatment" applies exclusively to a situation where CSIS is assessing whether mistreatment may occur.

[19] The arrangement profile provides a snapshot of the current status of the section 17 arrangement with the agency in question, and the reliability ratings of the latter. According to section 17 of the CSIS Act, for the purpose of performing its duties and functions under this Act, the Service may, with the approval of the Minister after consultation by the Minister with the Minister of Foreign Affairs, enter into an arrangement or otherwise cooperation with the government of a foreign state or an institution thereof or an international organization of states or an institution thereof.

[21] CSIS Act s.17(1)(b) Arrangement Profile (2012) with the
Last updated on: 2012 05 01. File # :

In light of these findings, **SIRC recommends that CSIS ensure that all deliberations at the as well as any concerns raised in the arrangement profiles or in CSIS internal documentation about respect of human rights of detainees, be mentioned in the record of decision-making.**

[25] CSIS Act s.17(1)(b) Arrangement Profile with File #: Last updated on: 2012 01 01.

5 SENIOR EXECUTIVE LEVEL PROCESS

Overall, SIRC found that all cases that were referred to ISEC were managed appropriately at the senior executive level. The range of participants around the table fostered substantive discussion and provided for a rigorous decision-making process. SIRC inquired more closely into three cases, described below, that were discussed at the ISEC level.

5.1 The case of

In April 2013, ISEC met to discuss

5.2 The case of

In November 2014, ISEC met to assess the risk

5.3 Allegations of mistreatment

According to 2011 MD, CSIS must keep the Minister of Public Safety generally informed about its information-sharing practices: the greater the risk, the more senior the level of approval required. SIRC examined a case where this requirement was put into practice.

Page

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information Act

de la Loi sur l'accès à l'information

6 RISK MITIGATION AND CSIS RELIANCE ON ASSURANCES

When disseminating information, CSIS uses two risk mitigation methods: caveats and assurances. At the level, in cases where there was a risk of potential mistreatment regarding information sent to or solicited from foreign entities, approximately 90 percent relied on the use of assurances as a means to mitigate that risk. In other cases, CSIS used the caveat that any risk of potential mistreatment would likely be mitigated by the adherence of foreign entities to international law, including the United Nations Convention against Torture and Other Cruel, Inhuman, or Degrading Treatment or Punishment.[45] At the ISEC level, in the committee asked for assurances as a condition to proceed with the action.

In a previous review,[46] SIRC had noted the lack of specific guidelines, whether in a directive, policy or other document, outlining the circumstances or conditions that would trigger the seeking of assurances or the process to be followed in these exceptional cases. As a result, SIRC noted a lack of clear understanding as to what assurances actually were, when they were to be used or how they should be recorded on file. In light of this, SIRC had recommended that CSIS develop direction and then policy on the practical application of assurances, such as when and how they should be sought, under whose authority, and how this process should be documented in operational reporting.

In August 2015, CSIS introduced a policy[47] to provide direction concerning the use of caveats and assurances when disseminating information or intelligence to any department, agency or organization outside of CSIS. This policy refers back to the DDO Directive to determine instances when there is a need to request assurances; CSIS employees are directed to consult the criteria listed in the directive, which include the capacity of the foreign entity to fulfil the proposed assurance. Given CSIS's reliance on assurances as a risk mitigation tool, **SIRC recommends that CSIS make explicit in the record of decision-making its assessment of the capacity of the foreign entity to fulfill the proposed assurance.**

[45] See for example
[46] Review of CSIS's relationship with Partners. SIRC Study 2011-08. File No.: 2800-167.
[47] Governing Policy:

7 CONCLUSION

Overall, SIRC found that CSIS has implemented a sound framework for sharing information with foreign entities where there may be a risk of mistreatment. SIRC cautioned CSIS to keep in mind that risk mitigation techniques, like caveats and assurances, have their limitations, especially when dealing with countries with poor human rights records. CSIS's information-sharing policies and practices will continue to be an integral component of SIRC's annual reviews and certification process.

ANNEX A

SUMMARY OF FINDINGS

- Overall, SIRC found that CSIS acted quickly to implement a sound information-sharing framework. However, SIRC found that the framework could be strengthened through a more rigorous and consistent application of the DDO Directive and recording of the decision-making process, especially at the level.

- In the cases reviewed, SIRC found that while CSIS had a record of decision-making, it had no record of the deliberations surrounding assessments, as required in the DDO Directive.

- SIRC found inconsistencies in the application of the DDO Directive and in the decision-making process at the level.

- SIRC found that all cases that were referred to ISEC were managed appropriately at the senior executive level.

- In the case of

- In the case of

- SIRC found that in the case of allegations of mistreatment

ANNEX B

SUMMARY OF RECOMMENDATIONS

- SIRC recommends that CSIS's Executive prioritize the development of an action plan to address the issue of maintaining records of decision-making within this fiscal year.

- SIRC recommends that CSIS ensure that all deliberations at the level, as well as any concerns raised in the arrangement profiles or in CSIS internal documentation about respect of human rights of detainees, be mentioned in the record of decision-making.

- SIRC recommends that CSIS make explicit in the record of decision-making its assessment of the capacity of the foreign entity to fulfill the proposed assurance.

ANNEX C

INFORMATION SHARING EVALUATION COMMITTEE (ISEC)

STRUCTURE AND GUIDELINES

MEMBERS

Note: The quorum consists of the above-mentioned positions. The powers and responsibilities inherent in the above-mentioned positions or titles are delegated to any employee performing the duties of the position or title in an acting capacity.

COORDINATION

Coordinator and Secretary:

The coordinator is responsible for convening the committee members, further to a request

The coordinator is responsible to update these guidelines.

GUIDELINES

GENERAL

- Before making a decision, the Committee can request that additional checks/actions be carried out for re-evaluation purposes. For example:
  - Carry out a specific interview
  - Request assurances from the foreign entity (new or additional).
  - Ask the foreign entity for details regarding how the information was obtained.

- In the event of an imminent threat, the decisions of the Evaluation Committee and/or the Director can be made verbally. However, a report must be prepared as soon as possible afterwards.

- The decision and the justification that led to the decision from the Director and/or the Committee must be recorded in a report and saved in the appropriate files, i.e: the operational file as well as the Information Sharing Evaluation Committee File,

- The concerned with the specific information and who participates in the Information Sharing Evaluation Committee, must ensure that the decision from the Committee and/or the Director be indicated in the relevant report(s).

EXAMPLES OF SOURCES TO CONSULT

- CSIS databases.
- "CSIS Arrangements with Foreign Governments and Institutions"

- Assurances received from the Foreign Entity in question.
- Country Human Rights reports from DFAIT.
- Reporting from organisations such as Amnesty International, Human Rights Watch, US State Department.
- Relevant open source information.
- Private databases, such as Maplecroft.

EXAMPLES OF POINTS AND QUESTIONS TO CONSIDER

- The threat to Canada's national security or other interests, and the nature and imminence of that threat;
- The importance of sharing the information, having regard to Canada's national security or other interests;
- The status of the relationship with the foreign entity with which the information is to be shared, and an assessment of the human rights record of the foreign entity;
- The rationale for believing that there is a substantial risk that sharing the information would lead to the mistreatment of an individual;
- The proposed measures to mitigate the risk, and the likelihood that these measures will be successful (including, for example, the foreign entity's record in complying with past assurances, and the capacity of those government officials to fulfil the proposed assurance);
- The views of DFAIT;
- The views of other departments and agencies, as appropriate, as well as any other relevant facts that may arise in the circumstances;
- The likelihood that the information could be acted upon by a foreign entity;
- The pertinent Country legislation;
- CSIS S.17 arrangement with the Foreign Entity:
    - Scope of exchanges
    - Restrictions (if any)
    - Status
    - Reliability
- Assurances:
    - the foreign entity's record in complying with past assurances

- the capacity of foreign entity to fulfil the proposed assurance
- The Human Rights assessment - Does the country and the Foreign Entity:
  - systematically violate human rights of detainees or engage in torture?
  - have safeguards in place to protect against torture?
  - signed and ratified the *Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment*?
  - prosecute officials who are alleged to have engaged in torture?
  - adhere to the precepts of customary international law?
  - adhere to the Non-Refoulment principle (removal to a country where an individual would be at risk of persecution for reasons of race, religion, nationality, membership in a particular social group or political opinion or at risk of torture or cruel and unusual treatment or punishment)?
  -
  - timely reports to organizations such as Amnesty International?
  - participate in rendition or has the country been a party to rendition in the past?
  - have an effective complaint mechanism for victims?
  - have preventive safeguards such as notification and detention records?
- If applicable, was the detention lawful under local and international law ?
  - "Incommunicado detention" (denial of access to family or legal representation)?
  - Has the detainee been given the reasons for his arrest?
  - Has the detainee been brought before a judge?
  - Can the detainee challenge the lawfulness of his detention?
  - Has the detainee received a fair trial?
- Has the individual been subject of rendition (transfer of an individual from one jurisdiction (usually country) to another or removal of an individual to another place without any legal proceeding)?

EXAMPLES OF ASPECTS TO CONSIDER

- Persons most targeted by torture are political detainees and perceived terrorists (various interpretations of the *Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment*).

- The more self-inculpatory the nature of the information provided by an individual, the less likely the information was voluntarily provided by this individual, particularly where it could support a prosecution leading to conviction, the imposition of a lengthy prison term, hard labour, or the death penalty. The question to consider is whether it is plausible that a person would have provided that information voluntarily (various interpretations of the *Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment*).

- Corroborated intelligence does not mean that it had not been derived from torture. The level of detail or the reliability of the information are not, on their own, useful factors in assessing whether there are reasonable grounds to believe that information was obtained by torture. A person who was tortured could tell the truth or not, and therefore that torture could produce either reliable or unreliable results. The issue is therefore not to determine whether the information is true or false, whether it is corroborated or not, but whether it is obtained

through torture or not (Justice Blanchard - In relation to Mahjoub's Security Certificate, June 2010 and various interpretations of the *Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment*).

- There is Federal Court jurisprudence that indicates that in the event the decision maker disagrees with the conclusions reached by credible human rights reports such as Amnesty International, the decision maker is required to state why s/he found the report to be unpersuasive (Memo from General Counsel Immigration Law Divison dated 2010 09 22 citing Thang v. Canada (Solicitor General) (2004) and Kazi v. Canada (Minister of Citizenship and Immigration) (2002)).

- It is widely accepted that reports from Amnesty International, Human Rights Watch and the UN Committee against Torture represent the best evidence available since there is very little direct evidence of torture (Justice Blanchard - In relation to Mahjoub's Security Certificate, June 2010).

- The Service cannot simply rely upon anecdotal information or personal relationships that may exist between special liaison officers and security officials in foreign countries. The Service must always ask what the motivation is of the person who is providing the information. This is particularly the case when countries have poor human rights records, and may be more interested in maintaining a relationship with the Service than actually providing truthful information as to the human rights conditions in that country (Justice Blanchard - In relation to Mahjoub's Security Certificate, June 2010).

- To establish that information was obtained by the use of torture required more than simply pointing to the poor human rights records of a given country (Justice Blanchard - In relation to Mahjoub's Security Certificate, June 2010).

- There are no reasonable grounds to believe that all unsourced information was obtained by torture (Justice Blanchard - In relation to Mahjoub's Security Certificate, June 2010).

DECISIONS FROM THE COMMITTEE

Following an assessment, the Committee must make one of the following decision:

Information received from a Foreign Entity

a) The information is likely not derived from mistreatment:

- The information can be used for a specific action without further consultation

b) The information is likely derived from mistreatment:

- If there is no serious threat of loss of life, injury, or substantial damage or destruction of property: The information cannot be used for a specific action.

- If there is a serious threat of loss of life, injury, or substantial damage or destruction of property: The report from the Committee must be sent to the Director via appropriate chain of command and the final decision is to be made by the Director.

Information to be sent to /solicited from a Foreign Entity

a) There is no Substantial Risk of mistreatment in sharing information:

- The information can be sent/solicited with appropriate caveats / assurances.

b) There is a Substantial Risk of mistreatment in sharing information:

- If there is no serious threat of loss of life, injury, or substantial damage or destruction of property: The information cannot be sent/solicited.
- If there is a serious threat of loss of life, injury, or substantial damage or destruction of property: The report from the Committee must be sent to the Director via appropriate chain of command and the final decision is to be made by the Director.

TERMINOLOGY

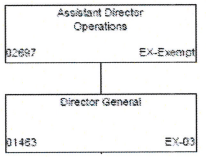
Mistreatment: Torture or other cruel, inhuman, or degrading treatment or punishment, as defined in the *Convention Against Torture and Other Cruel, Inhuman, or Degrading Treatment or Punishment (CAT)* and the *Criminal Code of Canada.*

Likely Derived: Means that it is more probable than not, that it is a real possibility.

Substantial Risk: In order to be "substantial," the risk must be real and must be based on something more than mere theory or speculation. In most cases, the test of a substantial risk of mistreatment will be satisfied when it is more likely than not that there will be mistreatment. However, the "more likely than not" test should not be applied rigidly because in some cases, particularly where the risk is of severe harm, the "substantial risk" standard may be satisfied at a lower level of probabili

ANNEX D

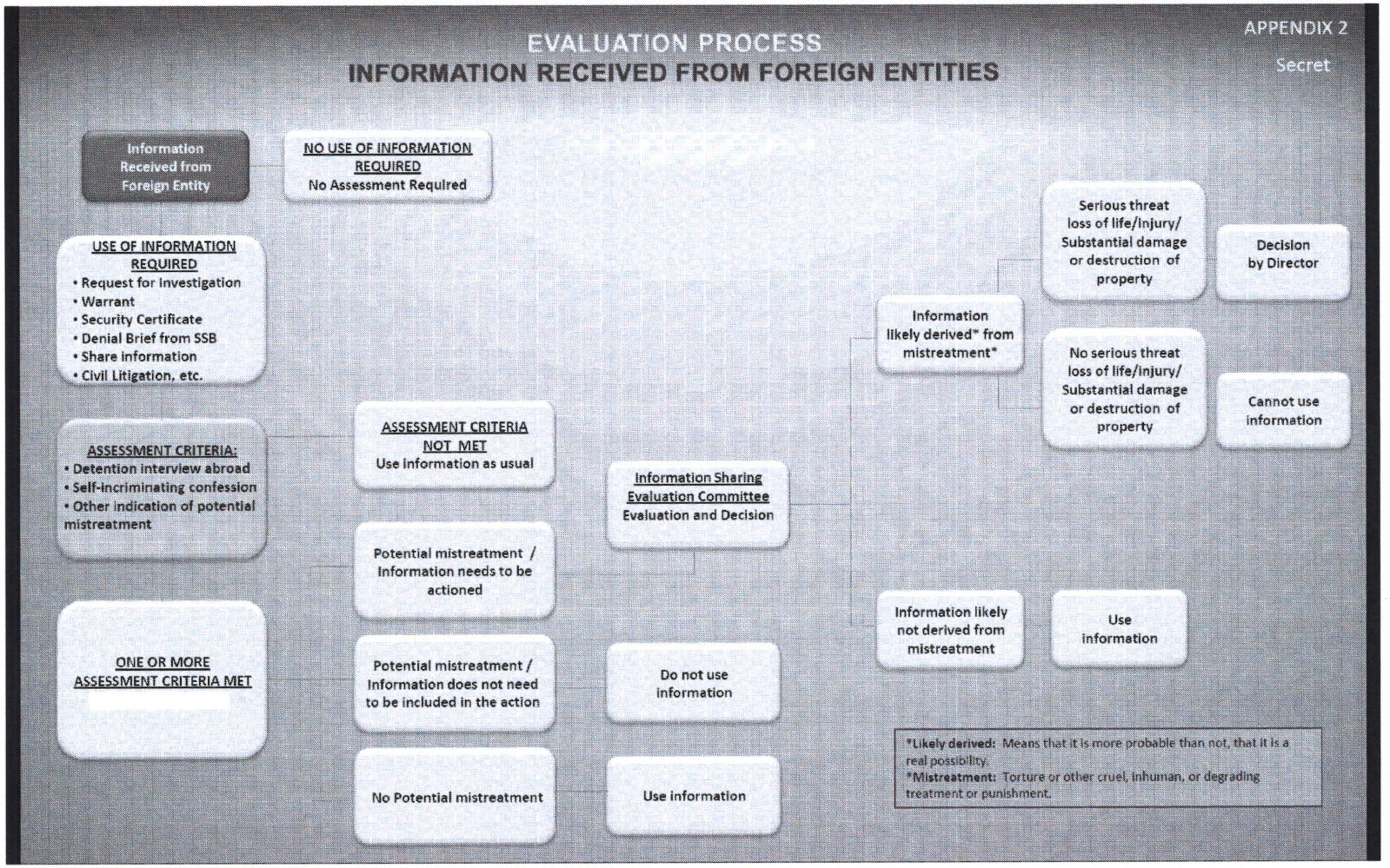
CANADIAN SECURITY INTELLIGENCE SERVICE



Date Approved

Assistant Director, Human Resources

ANNEX E



ANNEX F