

**Pages 1 to / à 13  
are not relevant  
sont non pertinentes**

## DesRochers, Patrick

---

**From:** Hirsch, Darryl  
**Sent:** Tuesday, September 18, 2012 2:38 PM  
**To:** DesRochers, Patrick  
**Subject:** FW: CBSA's policy on implementing the MD on information sharing  
**Attachments:** DRAFT Policy on MD 04SEP2012.docx  
  
**Categories:** Red Category

dfh

**From:** Brin, Jean-Guy [<mailto:Jean-Guy.Brin@cbsa-asfc.gc.ca>]  
**Sent:** September-06-12 4:37 PM  
**To:** Amy JOHNSON; Hirsch, Darryl; Banerjee, Ritu  
**Cc:** Peters, Adam; Klos, Roland  
**Subject:** CBSA's policy on implementing the MD on information sharing

Colleagues,

Last fall, following the receipt of the Ministerial Directive, the CBSA implemented an interim policy to operationalize it for our staff. In recent weeks, we've taken steps to make this policy permanent. I thought I would share with you our final draft which will be going for final approval next week. I would ask that if you have any feedback, please forward it to Adam Peters (with a c.c. to me).

Amy: if you are aware of any policy documents that you might be able to share with us (either in whole or in part) that would help inform our policy, that would also be greatly appreciated.

Darryl/Ritu: I'm still trying to find an appropriate contact at the RCMP now that Rosemary has moved on. Any ideas?

Thanks to all.

Jean-Guy Brin  
A/Director, Program, Planning and Legislation Division / Directeur p.i., Division du programme, de la planification et de la législation  
Planning & Performance Management Directorate | Direction de la planification et de la gestion du rendement  
Programmes Branch / Direction générale des programmes  
Canada Border Services Agency / Agence des services frontaliers du Canada  
191 Laurier Avenue West Ottawa ON K1A 0L8 / 191 avenue Laurier Ouest Ottawa Ontario K1A 0L8  
**Tel: (613) 954-6319**  
[jean-guy.brin@cbsa-asfc.gc.ca](mailto:jean-guy.brin@cbsa-asfc.gc.ca)

## **Policy on Implementing the Ministerial Direction to the CBSA on Information Sharing with Foreign Entities**

### **Background and Scope**

In September of 2011, the Minister of Public Safety issued a ministerial direction (MD) to the CBSA in regards to information sharing with foreign entities wherein the information in question may be linked to a substantial risk of mistreatment, or in other words, human rights abuses. The purpose of this Policy is to implement the 2011 MD, and replace the October 2011 Interim Policy.

The procedures in this Policy are subject to all applicable legislation governing the use and sharing of information and must be read in conjunction other CBSA and Government of Canada policies on information collection, use and disclosure. These procedures and the MD do not change existing legal authorities for sharing information with foreign entities.

### **Definitions**

1. "Mistreatment" means torture or other cruel, inhuman, or degrading treatment or punishment.
2. "Link to mistreatment" means that mistreatment may be associated with the production, disclosure, request, or use of the information.
3. "Substantial risk" is a personal, present, and foreseeable risk of mistreatment.
  - a) In order to be "substantial," the risk must be real and must be based on something more than mere theory or speculation.
  - b) 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 probability.

The following definitions are intended for these procedures only:

4. "Foreign entity" refers primarily to foreign government agencies and militaries, and it may also refer to military coalitions, alliances, and international organizations.
5. "Use" refers to the treatment of information as a resource and includes sharing information.

6. "Sharing" refers to both the collection and disclosure of information.
7. "Information" is intended to refer primarily to personal information, but may refer to other types of information associated with a substantial risk of mistreatment.
8. "Officer" is intended to refer generally but not exclusively to Liaison Officers, Intelligence Officers and Inland Enforcement Officers.
9. "CBSA headquarters" refers to the Unit or Division within headquarters that provides operational or program guidance for a particular officer's line of business.

### **Policy Statement**

10. The CBSA must assess the accuracy and reliability of information being shared with foreign entities, and properly characterize this information in any further use. It will take reasonable and appropriate measures to identify information that is likely to result in mistreatment and in normal circumstances not disclose such information with the foreign entity in question.
11. In exceptional circumstances, when there is a serious threat of loss of life, injury, or substantial damage or destruction of property, the CBSA will make the protection of life and property its priority. If, in these exceptional circumstances, the CBSA needs to share information with appropriate foreign authorities in order to mitigate a serious threat, and that information is linked to a substantial risk of mistreatment, the matter will be referred to the President for decision, which shall be made only in accordance with the MD and with Canada's legal obligations.
12. The CBSA must also take all reasonable measures to eliminate the risk that any action on its part might promote or condone the use of mistreatment. Measures must be taken to ensure that the information which may have been derived through mistreatment is accurately described, its reliability is properly characterized, and in normal circumstances, not used to administer or enforce program legislation, or as evidence in legal proceedings.
13. Caveats should be imposed on information shared with both domestic and foreign recipients to restrict their use of information, as appropriate. Standard caveats can be found at the end of the CBSA Enforcement Manual Part 7, Chapter 3: Information Sharing Policy for the Enforcement Manual.

### **Characterizing information**

14. Information must be evaluated to ensure to the point of due diligence that information shared with foreign governments, institutions or agencies is not obtained through the mistreatment of individuals or other criminal/illegal acts.

15. Where it is known that information if disclosed, or requested, may result in the substantial risk of mistreatment, this knowledge should be attached to the information, or put towards ensuring to the point of due diligence that disclosures of or requests for such information are not made. The attachment should precede the information, and be highly conspicuous manner, such as a coversheet or bolded designation similar to a security clearance.

### **Identifying Substantial Risk of Mistreatment Prior to Sharing Information**

16. When an officer, in the course of regular duties, forms an opinion that there may be a substantial risk of mistreatment associated with an information sharing activity, no sharing should occur until the following procedures have been applied.

17. The officer should endeavour to provide a clear and complete articulation of the substantial risk of mistreatment and discuss next steps with their immediate manager or supervisor prior to any referral of the matter to headquarters. The following elements should be considered:

- a) the rationale for believing that there is a substantial risk that sharing the information would lead to the mistreatment of an individual, or that the information about to be shared may have been obtained through the mistreatment of an individual.
- b) any 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 officials to fulfil the proposed assurance, or evidence to support that substantial risk of mistreatment was more likely not to have occurred);

18. If after an assessment of the above, local management is of the opinion that:

- a) a substantial risk of mistreatment is present; and
- b) the benefits of the information sharing activity can be clearly demonstrated to outweigh the substantial risk of mistreatment in terms of a serious threat
  - 1) against life or
  - 2) of serious injury or
  - 3) of substantial damage to property or
  - 4) of substantial destruction of property, then

local management shall route the matter up through their management structure to CBSA headquarters.

19. CBSA headquarters will consider the following;

- a) The risk and mitigation assessment made by the officer and local management or supervisors.
  - b) The necessity of consultations with other headquarters areas such as Legal Services, Information Sharing, International and Partnerships, and any Programs Branch or Operations Branch counterparts as applicable.
  - c) the threat to Canada's national security or other interests, and the nature and imminence of that threat;
  - d) the importance of sharing the information, having regard to Canada's national security or other interests;
  - e) 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;
  - f) the views of the Department of Foreign Affairs and International Trade (DFAIT); and
  - g) the views of other departments and agencies, as appropriate, as well as any other relevant facts that may arise in the circumstances.
20. CBSA headquarters should ensure that all the data elements and any additional relevant information are presented objectively and completely in a format suitable for referring to the President.
21. CBSA headquarters should consider any possible jeopardy to any current or future investigative or judicial proceedings by the use of information associated with mistreatment.
22. CBSA headquarters may present options and make recommendations to the President regarding the sharing of the information, or may recommend referral to the minister for decision. All options and recommendations made must be in accordance with Canada's legal and international obligations and in accordance with the MD to which this policy refers.

### **Identifying Substantial Risk of Mistreatment during Information Sharing.**

23. When a substantial risk of mistreatment or actual mistreatment is identified during the collection or disclosure of information, the collection or disclosure must cease as soon as practicable.
24. If further information would have been shared notwithstanding the cessation, the procedures in this policy under "Identifying Substantial Risk of Mistreatment Prior to Sharing Information" should be followed.

25. Any information already shared should be dealt with according to the procedures in this policy under "Identifying Substantial Risk of Mistreatment after Sharing Information."

### **Identifying Substantial Risk of Mistreatment after Sharing Information.**

#### *Collection*

26. If, after collecting information an officer becomes concerned that the information is linked to a substantial risk of mistreatment, the link must be clearly articulated and kept with the information. Further, the information should be kept in a special file that will clearly identify it as linked with substantial risk of mistreatment. Local management or supervisors should then be informed.
27. The information should neither be used nor shared unless the procedures under "Identifying Substantial Risk of Mistreatment Prior to Sharing Information" are followed.

#### *Disclosure*

28. If, after disclosing information, an officer becomes concerned that the information is linked to a substantial risk of mistreatment, the officer should immediately attempt to halt the use and further disclosure of that information at the earliest opportunity. Local management and CBSA headquarters should be informed as soon as possible.
29. CBSA headquarters, in conjunction with local management, should employ as many mitigating actions as possible and consider obtaining the assistance of other government departments. Every effort should be made to obtain assurances from the recipients of such information that the information will not be further used or disclosed, and the information be destroyed or returned to the discloser to be dealt with in accordance with policy and legal obligations.

### **Use of Information Linked to a Substantial Risk of Mistreatment**

30. If, due to a serious threat, the President of the CBSA or the Minister of Public Safety allow the use of information that may have been obtained through, or may result in mistreatment, the following applies.
31. A clear rationale for and record of the decision should be kept by all parties to the sharing, indicating the decision is made only in accordance with the MD, and with Canada's legal obligations.
32. The CBSA will subsequently take all reasonable measures to reduce the risk that any use of information on its part might promote, condone the use of, or result in mistreatment. Such measures may include but are not limited to:

- a) sanitizing the information;
- b) progressive sharing over time;
- c) limitation of recipients;
- d) using more secure media;
- e) using one-time procedures;
- f) monitoring use of information;
- g) use of caveats; or
- h) obtaining or securing assurances through DFAIT.

### **Proactive Disclosure to Prevent Mistreatment**

33. Where an area of the CBSA is in control of information that is likely to prevent mistreatment if disclosed or requested, it shall endeavour to disclose or request such information as soon as possible and within the confines of policy and law, and also inform via the appropriate channels the Vice President of the Branch under which that particular area's management structure resides.



**Des Rochers, Patrick**

**From:** Hirsch, Darryl  
**Sent:** Wednesday, December 05, 2012 12:19 PM  
**To:** Des Rochers, Patrick  
**Subject:** FW: policy  
**Follow Up Flag:** Follow up  
**Flag Status:** Completed  
**Attachments:** info sharing policy in response to MD.doc

**Classification: CONFIDENTIAL**



**From:** Drodge, Edward [mailto:edrodge@rcmp-grc.gc.ca]  
**Sent:** Wednesday, December 05, 2012 9:57 AM  
**To:** Hirsch, Darryl  
**Subject:** policy

**Classification: CONFIDENTIAL**

Good morning Darryl,  
Here is the policy as requested. My DG has requested that you not disseminate this very widely at all, please. It is currently with our Policies & Publications Branch being edited and translated. While the MD itself and its implications were disseminated widely to our NSCI personnel last year when it was issued, the ensuing policy (in its draft form) has had limited circulation internally to this point in time. I should also point out that the policy builds upon existing policy; it is not a stand-alone document, rather the current Chapter 12 (section 3) of our Operational Manual (a massive document) has been amended.

Regards,  
Ed

### 12.3. Sharing Information in the National Security Context

1. Definitions
2. General
3. Meetings and Briefings
4. Sharing Information with Foreign Entities
5. Foreign Entities with Questionable Human Rights Records
6. Information Sharing with Foreign Entities when there is a Substantial Risk of Mistreatment
7. Approval Levels
8. Mutual Legal Assistance Treaty
9. Sharing Information with Domestic Departments/Agencies
10. Caveats

#### 1. **Definitions:**

“Sharing” encompasses provision, receipt and use of information.

“Foreign entity” refers primarily to foreign government agencies, which include law enforcement and intelligence agencies, militaries, coalitions, alliances and international organizations, as outlined in the Ministerial Direction on Information Sharing with Foreign Entities ([link](#)).;

“Mistreatment” means torture or other cruel, inhumane or degrading treatment or punishment.

“Need-to-know” means the need for someone to access and know information in order to perform his/her duties. See Government Security Policy.

“Right to know” means the legal authority, including the appropriate security clearance, to access classified information.

“Substantial risk” is a personal, present and foreseeable risk of mistreatment. The risk must be real and must be based on something more than mere theory or speculation.

## **2. General**

2. 1. For sharing of classified/designated information, see AM XI.1.N.
2. 2. For release of criminal record information, see I.3.L.
2. 3. For information sharing with RCMP liaison officers, see ch. 12.7.
2. 4. In accordance with sec. 7 and 8, Privacy Act, classified/designated national security information may be shared with an appropriate department/agency based on the “need-to know” and the “right-to-know”.
2. 5. A written record will be maintained of all national security-related information transmitted to and received from a domestic department/agency or foreign entity.
2. 6. Prior to dissemination, all information that describes facts, individuals or events must be assessed for reliability, relevance and accuracy by:

2. 6. 1. assessing the reliability of the information including an assessment of the information source as outlined in ch. 31.5.;
2. 6. 2. considering why another department/agency/ foreign entity is requesting the information (need-to-know), the nature of the request, how the information might be used.
- 2.7. Prior to dissemination, the department/agency/foreign entity's record in complying with caveats or assurances and the possibility that the information will lead to the mistreatment of an individual must be assessed (see sec. 5.7).
2. 8. All information must be assessed for compliance with applicable laws relating to the disclosure of personal information.
2. 9. Any doubt concerning the reliability or accuracy of the source or the information must be clearly communicated to the recipient.
2. 10. All information received from another department/agency/ foreign entity will remain the property of the originator and cannot be reclassified or disseminated without the documented authorization of the originator.
  - 2.10.1. If authorization to reclassify or disseminate is granted, any subsequent sharing of the information will remain subject to the new classification and dissemination caveats in effect.
2. 11. All sensitive or potentially injurious information related to national security will be classified Confidential, Secret or Top Secret. See AM XI.1.J., K. and App. XI-1-3.

2. 11. 1. An investigator's notebook containing sensitive or potentially injurious information will be stored and classified equivalent to the highest protected information contained in the notebook. See also ch. 25.2.

2. 12. All classified information must be stored as outlined in AM XI.3.H.

2. 13. For marking and transmittal of classified documents by mail, see AM XI.1.L. and App. XI-1-4.

2. 14. For electronic transmission of classified information, see AM XI.4. and AM XI.5.

### **3. Meetings and Briefings**

3. 1. Any operational meeting or briefing with a domestic department/agency or foreign entity, including a law enforcement, security or intelligence department/agency, must be documented in writing and filed as per IM IV.1. The documentation will include the names of the participants and highlight decisions that were made.

### **4. Sharing Information with Foreign Entities**

4. 1. National Security Criminal Operations (NSCO) at RCMP National Headquarters (NHQ) is responsible for the exchange of information with a foreign entity.

4. 2. NSCO at NHQ must immediately be informed of all requests for assistance and/or information from foreign entities related to national security criminal investigations.

4.3 For information sharing protocol with a foreign entity, see also ch. 12.9.

- 4.4. Information sharing with foreign entities must be conducted in a manner that complies with Canada's laws and legal obligations, including international agreements and the *Canadian Charter of Rights and Freedoms*, and in accordance with the Ministerial Direction on Information Sharing with Foreign Entities as outlined in App. 12 -General-4.
- 4.5. Before dissemination, all correspondence to be released to a foreign entity by an Integrated National Security Enforcement Team (INSET)/National Security Enforcement Section (NSES) must be reviewed by the Criminal Operations Officer (Cr. Ops. Officer) and forwarded to National Headquarters, ATTN: DG Federal Policing Criminal Operations for approval and dissemination.
- 4.6. The RCMP may, with the Minister's prior approval, enter into a written or verbal arrangement or co-operate with a foreign security or intelligence department/agency.
  - 4.6.1. A written arrangement with a foreign security or intelligence department/agency will be in accordance with the Ministerial Direction National Security Related Arrangements and Cooperation as outlined in App. 12-General-2.
  - 4.6.2. National Security Criminal Investigations and Protective Policing (NSCI & PP) will retain copies of any arrangement between the RCMP National Security Criminal Investigation program and a foreign security or intelligence department/agency, including documentation of the terms and understanding of verbal arrangements.
- 4.7. When entering into arrangements with a foreign security or intelligence department/agency, the country's respect for democratic or human rights must be taken into consideration, as determined in consultation with the Department of Foreign Affairs and International Trade (DFAIT). [See sec. 5]
- 4.8. When requesting or receiving information from a foreign entity, ensure the request includes:

4. 8. 1. the name of the department/agency or appropriate authority;
  4. 8. 2. the subject or nature of the investigation/request;
  4. 8. 3. a description of the type of information or cooperation being sought; and
  4. 8. 4. the purpose or intended use of the information being requested, e.g. investigation, judicial proceedings.
4. 9. Information received from a foreign entity must be assessed for reliability, relevance and the likelihood that the information may have been derived from mistreatment or torture. The findings must be documented on the file. (See sec. 2.6.)
  - 4.10. In exigent circumstances (subject to policy sections 6 through 8 below) NSCO (NHQ) may exchange information verbally with a foreign entity. The interaction must be documented in writing.

## **5. Foreign Entities with Questionable Human Rights Records**

- 5.1. Information sharing with foreign entities with questionable human rights records is conducted on a case-by-case basis and should be proportionate to the importance of sharing the information, having regard to Canada's national security or other interests.
- 5.2. In assessing the human rights record of a foreign entity with which the RCMP intends to share information, the DFAIT annual reports assessing the human rights record of that country must be consulted.

- 5.3. The DFAIT will be consulted regarding decisions to interact with a foreign entity with a questionable human rights record.
- 5.4. All decisions to interact with a foreign entity with a questionable human rights record will be documented, including the importance of receiving such information and the implications of doing so for Canada's human rights obligations. NSCI & PP at NHQ is responsible for interdepartmental coordination.
- 5.5. Information received must be assessed for reliability, i.e. the risk that the country may provide misinformation or false confessions induced by torture, violence or threats, and documented.
- 5.6. In assessing the implications of sharing information with a foreign entity with a questionable human rights record, steps must be taken to ensure the information will be protected from improper disclosure, that there is no implicit support for torture or other abuse of human rights, and that the foreign entity is governed by sanctioned institutional controls (e.g., the rule of law).
- 5.7. Such a risk assessment must be documented in writing and must include:
  - 5.7.1. the particular context for sharing (e.g., specific threat or imminence of threat);
  - 5.7.2. its investigational value/importance;
  - 5.7.3. outcome of consultations with DFAIT;
  - 5.7.4. a summary of pertinent information from country reports issued by the DFAIT, RCMP, CSIS, US State Department;



- 5.7.5. the likelihood of caveats being respected and the bases for that determination;
- 5.7.6. past relations with the agency/department (including information-sharing relations);
- 5.7.7. relevant intelligence reports (both classified and open source);
- 5.7.8. whether the foreign entity promotes or condones the use of torture or other abuses of human rights.
- 5.8. For the approval level required in order to share information with a foreign entity having a questionable human rights record, see sec. 7.
- 5.9. When it is determined that a Canadian is being detained abroad in connection with a national security-related investigation, National Security Criminal Operations (at NHQ) will immediately notify the DFAIT.

## **6. Information Sharing with Foreign Entities when there is a Substantial Risk of Mistreatment**

- 6.1 When there is a substantial risk that sending information to, or soliciting information from, a foreign entity would result in the mistreatment of an individual (i.e., a known individual), and it is unclear whether that risk can be mitigated through the use of caveats or assurances, the matter will adhere to the Ministerial Direction to the RCMP: Information Sharing With Foreign Entities [App. 12-General-4].

## **7. Approval Levels**

- 7.1. The approval level required for information sharing (receiving, sending and using) with a foreign entity with a questionable human rights record is proportionate to the risk of mistreatment that may result. The greater the risk, the more senior the level of approval required.
- 7.2 If the DG Federal Policing Criminal Operations (FPCO) has concerns about information sharing with a foreign entity after considering the key criteria for substantial risk (see sec. 5.7), the request will be forwarded to the Assistant Commissioner, National Security Criminal Investigations and Protective Policing (NSCI &PP) for his/her review. The request must be forwarded in writing with a report of the risk assessment.
- 7.3 If the Assistant Commissioner NSCI & PP is uncertain whether the substantial risk threshold has been met, or that the risks can be adequately mitigated, the Deputy Commissioner, Federal Policing will be contacted for his/her review. Again, the request for review must be in writing and must be supported by the risk assessment.
- 7.4 If the Deputy Commissioner, Federal Policing believes there are substantial risks of mistreatment and that risks cannot be adequately mitigated, a request for a decision is sent to the Commissioner, in writing and supported by the risk assessment.
- 7.5 The Commissioner has the authority to decide whether or not to share information. He/she may refer the decision to the Minister of Public Safety [App. 12 – General -4].
- 7.6 RCMP Legal Services may be consulted at any point in the approval process noted above.

## **8. Mutual Legal Assistance Treaty**

8. 1. All incoming and outgoing Mutual Legal Assistance Treaty requests must be channeled through NSCI & PP (at NHQ).

8. 2. When receiving a Mutual Legal Assistance Treaty request, NSCO (at NHQ) will task the INSET/NSES as appropriate.

8. 2. 1. A Mutual Legal Assistance Treaty request to a foreign department/agency must be forwarded to National Headquarters, ATTN: DG Federal Policing Criminal Operations for his/her review and final approval.

8. 3. A Mutual Legal Assistance Treaty request must be consistent with the directives outlined in II.1.M.

## **9. Sharing Information with Domestic Departments/Agencies**

9. 1. The INSET/NSES commander is responsible for the exchange of information with a domestic law enforcement department/agency in ensuring compliance with sec. 7 and 8, *Privacy Act*.

9. 2. The Cr. Ops. Officer will approve the dissemination of information for a request from a domestic non-law enforcement department/agency, i.e. municipal, provincial, private sector.

9. 3. NSCO will approve and disseminate the information or a request from a non-law enforcement federal department/agency, e.g. Canadian Security Intelligence Service, Department of National Defence, DFAIT, Health Canada.

## **10. Caveats**

10. 1. Caveats must be included on all national security-related information shared within and outside the RCMP.

10. 2. All outgoing classified or national security-related information that is shared with a foreign entity must include the following caveat:

10. 2. 1. *This document is the property of the Royal Canadian Mounted Police (RCMP), National Security Program. It is loaned specifically to your department/agency in confidence and for internal use only. This document is not to be reclassified, copied, reproduced, used or further disseminated, in whole or part, without the consent of the originator. It is not to be used in affidavits, court proceedings or subpoenas or for any other legal or judicial purpose without the consent of the originator. If you are subject to freedom of information or other domestic laws which do not allow you to protect this information from disclosure, notify the RCMP National Security Program immediately and return the document. This caveat is an integral part of this document and must accompany any extracted information. Should the recipient wish to modify these terms, contact the Director General, Federal Policing Criminal Operations, RCMP.*

10.3. All classified and national security-related information that is shared with a domestic department/agency must include the following caveat:

10. 3. 1. *This document is the property of the Royal Canadian Mounted Police (RCMP), National Security Program. It is loaned specifically to your department/agency in confidence and for internal use only, and it is not to be reclassified, copied, reproduced, used or further disseminated, in whole or in part, without the consent of the originator. It is not to be used in affidavits, court proceedings, subpoenas or any other legal or judicial purpose without the consent of the originator. The handling and storing of this document must comply with handling and storage guidelines established by the Government of Canada for classified information. If your department/agency cannot apply these guidelines, please read and destroy this document. This caveat is an integral part of this document and must accompany any extracted information. For any enquiries concerning the information or the caveat, please contact the Officer in Charge (OIC), National Security Criminal Operations, RCMP.*

10. 4. All information and criminal intelligence that was collected from sensitive sources or where further disclosure may reveal RCMP sources, operational methodology or investigative techniques, and thereby potentially engage the provisions of the *Security of*

*Information Act and/or the Canada Evidence Act designed to prevent or deter injury to national security as the result of the disclosure of special operational information, must include the following caveat in addition to the caveat stated in sec. 10.3.:*

10. 4. 1. *This document may be subject to mandatory exemption under the Access to Information and Privacy Acts. If access is requested under this legislation, the decision to disclose will not be made without prior consultation with the Departmental Privacy Coordinator of the Royal Canadian Mounted Police (RCMP). This document may constitute "special operational information" as defined in the Security of Information Act. This information may also be protected by the provisions of the Canada Evidence Act (CEA). The RCMP National Security Program may take all steps pursuant to the CEA or any other legislation to protect this information from production or disclosure, including the filing of any necessary notices with the Attorney General of Canada.*

10 5. All internal correspondence that contains national security-related information must include the following caveat:

10. 5. 1. *This document is the property of the Royal Canadian Mounted Police (RCMP), National Security Program. It is provided to your section/unit and should not be disseminated, in whole or in part, without the prior consent of the originator. This document will not be declassified without the written consent of the originator. This document may constitute "special operational information" as defined in the Security of Information Act. The handling and storing of this document must comply with handling and storage guidelines established by the Government of Canada for classified information. If you cannot apply these guidelines, please read and destroy this document. Failure to comply with this caveat will constitute a breach of RCMP policy and federal legislation. For any enquiries concerning the information, please contact the originator of the document.*

SECRET

2011-08-24

---

# MEMORANDUM

**TO:** HQ and Regional  
Directors General

**CLASSIFICATION:** SECRET  
**FILES:** 280-39 / 370-692

**c.c.** Executive members

**FROM:** DDO

**DATE:** August 24<sup>th</sup>, 2011

**SUBJECT: DDO DIRECTIVE ON INFORMATION SHARING WITH FOREIGN ENTITIES**

In the current threat environment, terrorism is the top national security priority of the Government of Canada. In this context, it is essential that the Service be able to maintain strong relationships with foreign entities, and share information with them on both a routine and an urgent basis.

The Government of Canada opposes in the strongest possible terms the mistreatment of any individual by any foreign entity for any purpose. The Government of Canada does not condone the use of torture or other unlawful methods in responding to terrorism and other threats to national security. Canada is a party to a number of international agreements that prohibit torture and other forms of cruel, inhuman, or degrading treatment or punishment and torture is a criminal offence in Canada which has an extraterritorial application.

The objective of this Directive is to provide a tool to the Service's employees to ensure that they comply with international and Canadian Legislation and that decisions to proceed or not with the use of a specific piece of information or with an information exchange, are made at a level commensurate with the possibility that:

- the information to be used may have been obtained through the mistreatment of individuals; or
- the exchange may result, directly or indirectly, in the mistreatment of individuals.

This DDO Directive applies to the sharing of information with all foreign entities, is guided by the Ministerial Direction on Information Sharing with Foreign Entities approved by the Minister on July 28<sup>th</sup>, 2011 and received by the Service on August 23<sup>rd</sup>, 2011 (Please see Appendix 1) and must be interpreted in a manner consistent with this Ministerial Direction.

000034

Charts illustrating the information provided in this Directive are included in Appendix 2.

### **INFORMATION EXCHANGE WITH FOREIGN ENTITIES - GENERAL**

In the context of this Directive "mistreatment" means 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* and the *Criminal Code* of Canada.

The following other two definitions also apply to this Directive:

- 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 probability.

Employees must inform in writing their line manager of instances where they know or suspect a foreign entity to have engaged in mistreatment, as well as instances where Service information may have been misused or our caveats not respected.

All information exchanges with foreign entities must:

- provide balanced information with properly described context;
- describe threats and individuals in a manner that is properly qualified (proper use of terms such as suspected/believed/confirmed/extremists/terrorists);
- bear the appropriate caveat; and,
- be documented.

At any time, employees and managers may consult upward for direction on the advisability of a particular information exchange or use of information.

All deliberations coming from assessments requested in this directive as well as the resulting decisions must be documented and saved in the appropriate files, i.e: the operational file as well as the Information Sharing Evaluation Committee File, # 370-692.

A reference to the decision (from the [REDACTED] the Information Sharing Evaluation Committee or the Director) must also be indicated in the relevant [REDACTED] report(s).

### **USE OF INFORMATION RECEIVED FROM FOREIGN ENTITIES**

When considering using information received from a foreign entity (examples: request for investigation, security certificate, etc), the following assessment criteria must be taken into consideration:

SECRET

- Does the Information come from a detention interview conducted abroad?
- Does the Information come from self-incriminating confession?
- Is there any other information indicating a potential mistreatment (such as, but not limited to: poor human rights records, practice of extraordinary rendition, ie transfers of suspects from one state to another outside the law, etc)?

If none of the assessment criteria are met, then the information can be used.

If one or more of the assessment criteria are met, the information must be reviewed by an [REDACTED] via appropriate channels. The [REDACTED] must assess the information and make a decision. In his decision-making process, the [REDACTED] can take into account some of the criteria that must be considered by the Information Sharing Evaluation Committee (Please see [Appendix 3](#)):

- 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.

When an [REDACTED] refers a decision to the Information Sharing Evaluation Committee via a [REDACTED] the Committee must assess the information and make a decision (Please see [Appendix 3](#)):

- If the Committee determines that the information is likely not derived from mistreatment, the information can be used in an action without further consultation.
- 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.
- 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 via appropriate channels.

#### **INFORMATION TO SEND TO / SOLICIT FROM FOREIGN ENTITIES**

When considering sending information to / soliciting information from a foreign entity, the following assessment criteria must be taken into consideration:

- Does the Information pertain to an individual in detention abroad?
- Could the Information result in a negative action against an individual (detention or other)?
- Is there any other information indicating a potential mistreatment if the information is sent / solicited (such as, but not limited to: poor human rights records, practice of extraordinary rendition, ie transfers of suspects from one state to another outside the



SECRET

law, etc)?

If none of the assessment criteria are met, then the information can be sent or solicited.

If one or more of the assessment criteria are met, the information must be reviewed by an [REDACTED] via appropriate channels. The [REDACTED] must assess the information and make a decision. In his decision-making process, the [REDACTED] can take into account some of the criteria that must be considered by the Information Sharing Evaluation Committee (Please see [Appendix 3](#)):

- 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 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 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.

When an [REDACTED] refers a decision to the Information Sharing Evaluation Committee via a [REDACTED] the Committee must assess the information and make a decision (Please see [Appendix 3](#)):

- If the Committee determines that there is no substantial risk of mistreatment, the information will be sent / solicited with appropriate caveats / assurances.
- If the Committee determines that there is a 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.
- If the Committee determines that there is a 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 via appropriate channels.

In conclusion, I wish to reiterate the need to foster an effective dialogue on this issue and for all operational managers to encourage consultation. Although balancing these responsibilities with our mandate to protect Canadians will, at times, pose difficult challenges, we need to remain sensitive to our responsibilities in protecting individuals from mistreatment which could result from our action, or inaction.

New policy and procedures regarding this subject will be developed.

Michel Coulombe  
Deputy Director Operations

**SECRET**

Top

2011-08-24

**SECRET**



**SECRET**

- 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, # 370-692.
- The [REDACTED] 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 [REDACTED] report(s).

### EXAMPLES OF SOURCES TO CONSULT

- CSIS databases.
- "CSIS Arrangements with Foreign Governments and Institutions" ([REDACTED])
- 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:

SECRET

- 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-Refoulement 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)?
  - permit monitoring of returnees by reputable non governmental organizations?
  - 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

000041

SECRET

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 Division 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

SECRET

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 probability.

Top

2011-08

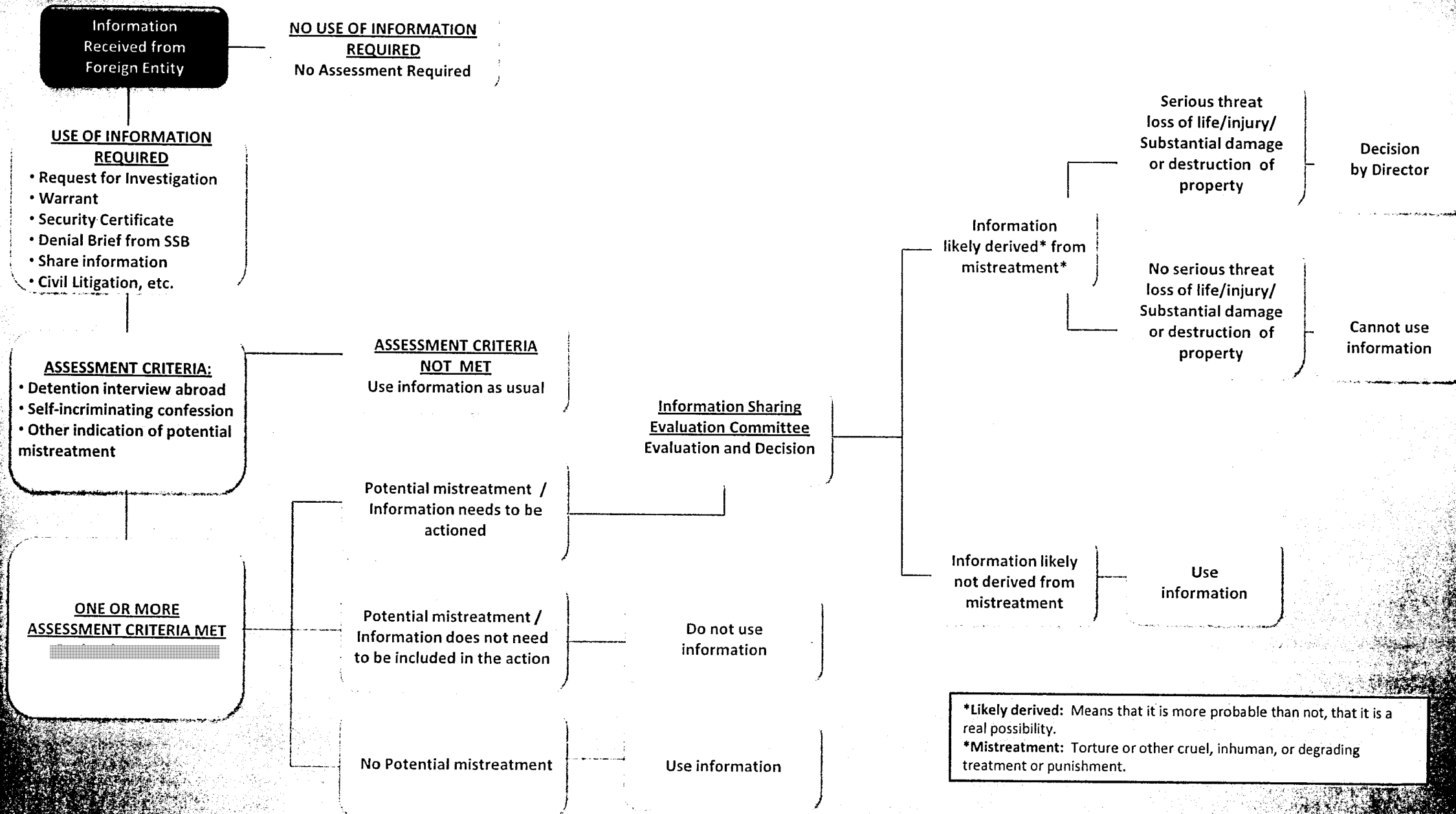
SECRET

# EVALUATION PROCESS

APPENDIX 2

## INFORMATION RECEIVED FROM FOREIGN ENTITIES

Secret



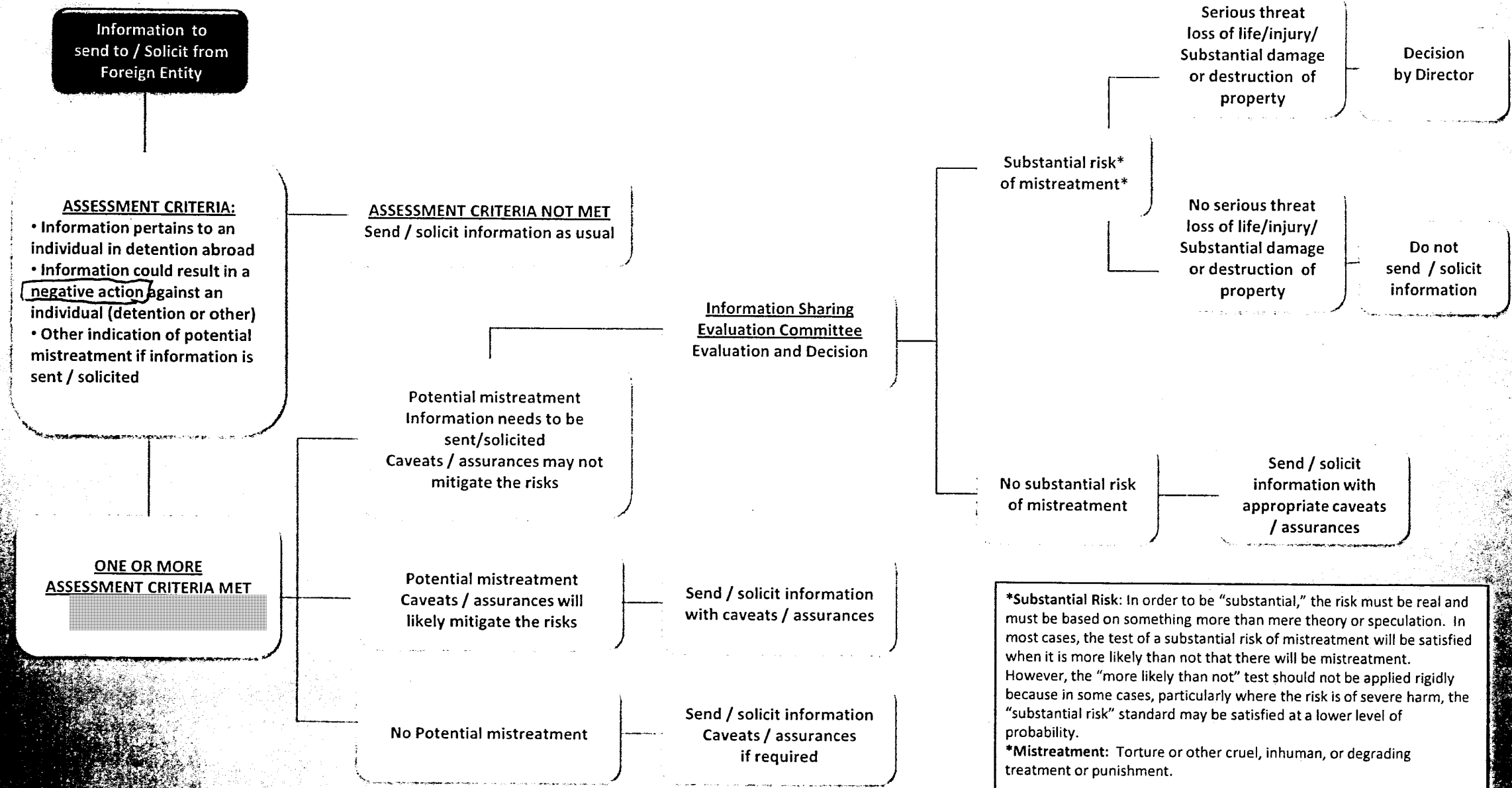
\*Likely derived: Means that it is more probable than not, that it is a real possibility.  
 \*Mistreatment: Torture or other cruel, inhuman, or degrading treatment or punishment.



# EVALUATION PROCESS

## INFORMATION TO SEND TO / SOLICIT FROM FOREIGN ENTITIES

Secret



**\*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 probability.

**\*Mistreatment:** Torture or other cruel, inhuman, or degrading treatment or punishment.

UNCLASSIFIED

**Ministerial Direction to the Canadian Security Intelligence Service:  
Information Sharing With Foreign Entities**<sup>1</sup>

In the current threat environment, terrorism is the top national security priority of the Government of Canada. In this context, it is essential that the Canadian Security Intelligence Service (CSIS) is able to maintain strong relationships with foreign entities, and can share information with them on both a routine and an urgent basis. CSIS must also be able to quickly share information with other key domestic stakeholders, including federal departments and agencies that have the mandate and responsibility to respond to serious threats before they materialize.

The following Ministerial Direction provides guidance to the Director of CSIS, pursuant to section 6(2) of the *CSIS Act*, on information sharing with foreign entities.

**1. Canada's Legal Obligations**

Sharing information with foreign entities is an integral part of CSIS' mandate. It is also a formal obligation pursuant to Canada's adoption of various international resolutions and agreements.

The Government of Canada opposes in the strongest possible terms the mistreatment of any individual by any foreign entity for any purpose. The Government also has a duty to its own citizens and to its allies to prevent individuals engaging in threat related activities from causing harm, whether in Canada or in a foreign country.

The Government of Canada does not condone the use of torture or other unlawful methods in responding to terrorism and other threats to national security. The Government is committed to pursuing a principled and proportionate response to these threats, while promoting and upholding the values Canada seeks to protect.

Canada is a party to a number of international agreements that prohibit torture and other forms of cruel, inhuman, or degrading treatment or punishment. These include the *International Covenant on Civil and Political Rights* and the *Convention Against Torture and Other Cruel, Inhumane, or Degrading Treatment or Punishment (CAT)*. The *CAT* requires state parties to criminalize all instances of torture, and to take effective measures to prevent torture and other cruel, inhuman, or degrading treatment or punishment in any territory under their jurisdiction.

Torture is a criminal offence in Canada that has extraterritorial application. The *Criminal Code*'s provisions governing secondary liability also prohibit aiding and abetting the commission of torture, counselling the commission of torture whether or not the torture is committed, conspiracy to commit torture, attempting to commit torture, and being an accessory after the fact to torture.

---

<sup>1</sup> This Direction would not change existing legal authorities for sharing information with foreign entities. Although the term, foreign entity, has not been formally defined, it primarily refers to foreign government agencies and militaries. The term may also refer to military coalitions, alliances, and international organizations.

UNCLASSIFIED

More broadly, section 7 of the *Canadian Charter of Rights and Freedoms* guarantees that “everyone has the right to life, liberty, and security of the person.” Section 12 of the *Charter* prohibits “any cruel and unusual treatment or punishment,” which Canadian courts have described as behaviour “so excessive as to outrage the standards of decency.” This behaviour includes torture and other cruel, inhuman, or degrading treatment or punishment.

## **2. Definitions**

“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 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 probability.

## **3. Information Sharing Principles**

Sharing information with foreign entities is an integral part of CSIS’ mandate. It is also a formal obligation pursuant to Canada’s adoption of various international resolutions and agreements.

In sharing information, CSIS must act in a manner that complies with Canada’s laws and legal obligations. It is to avoid any complicity in mistreatment by foreign entities.

CSIS must assess and mitigate potential risks of sharing information in ways that are consistent with its unique role and responsibilities.

CSIS must also assess the accuracy and reliability of information received, and properly characterize this information 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: the greater the risk, the more senior the level of approval required.

CSIS also has a responsibility to keep the Minister of Public Safety generally informed about its information sharing practices.

UNCLASSIFIED

#### **4. Decision Making Process When There Is A Substantial Risk of Mistreatment In Sharing Information**

Except when there is a substantial risk, CSIS is responsible for establishing approval levels that are proportionate to the risks in sharing information with foreign entities. The following decision making process applies when there is a substantial risk of mistreatment of an individual.

When there is a substantial risk that sending information to, or soliciting information from, a foreign entity would result in the mistreatment of an individual, and 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.

In making his or her decision, the Director will normally consider the following information, all of which must be properly characterized in terms of its accuracy and reliability:

- 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 the Department of Foreign Affairs and International Trade (DFAIT); and
- the views of other departments and agencies, as appropriate, as well as any other relevant facts that may arise in the circumstances.

The 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.

#### **5. Use Of Information That May Have Been Derived Through Mistreatment By Foreign Entities**

As a general rule, CSIS is directed to not knowingly rely upon information derived through mistreatment by foreign entities.

UNCLASSIFIED

In exceptional circumstances, CSIS may need to share the most complete information in its possession, including information from foreign entities that was likely derived through mistreatment, in order to mitigate a serious threat of loss of life, injury, or substantial damage or destruction of property before it materializes. In such rare circumstances, ignoring such information solely because of its source would represent an unacceptable risk to public safety.

When there is a serious risk of loss of life, injury, or substantial damage or destruction of property, CSIS will make the protection of life and property its priority. If CSIS needs to share information that was likely derived through mistreatment with appropriate authorities in order to mitigate a serious threat, the matter will be referred to the Director. All decisions shall be made only in accordance with this Direction and with Canada's legal obligations.

CSIS will take all reasonable measures to reduce the risk that any action on its part might promote or condone the use of mistreatment. Measures will also be taken to ensure that the information which may have been derived through mistreatment is accurately described, and that its reliability is properly characterized. Caveats will be imposed on information shared with both domestic and foreign recipients to restrict their use of information, as appropriate.

## **6. Support**

To help ensure a consistent understanding of the risks of sharing information with foreign entities, DFAIT will continue to make its country human rights reports available to the intelligence and law enforcement community.

**Pages 50 to / à 60  
are withheld pursuant to section  
sont retenues en vertu de l'article**

**23**

**of the Access to Information  
de la Loi sur l'accès à l'information**

**Pages 61 to / à 70  
are not relevant  
sont non pertinentes**

**2012-2013 Supplementary Estimates (C) / 2013-2014 Main Estimates**

**MINISTERIAL DIRECTION ON  
“INFORMATION SHARING WITH FOREIGN ENTITIES”**

**PROPOSED RESPONSE:**

- **The Ministerial Direction (MD) on “Information Sharing with Foreign Entities” was issued to CSIS, RCMP, and CBSA in 2011.**
- **The Direction sets out a coherent approach regarding information sharing where there may be a risk of mistreatment.**
- **All decisions to share information with a foreign agency must be “in accordance with this Direction and with Canada’s legal obligations.”**
- **The Government opposes in the strongest possible terms the mistreatment of any individual by any foreign state or agency for any purpose.**
- **This MD ensures that Canada pursues a principled and proportionate response to terrorism and other threats to national security. It is consistent with Canada’s international human rights obligations.**



**QUESTIONS AND ANSWERS:**

**Q1 What guidance does the Government provide in establishing foreign arrangements and sharing information with foreign agencies?**

**A2** In 2011, the Minister of Public Safety issued guidance to CSIS, RCMP and CBSA on sharing information with foreign agencies through a comprehensive MD on "Information Sharing with Foreign Entities." It describes Canada's legal obligations with respect to sharing information. The MD identifies the principles that must be followed in sharing information with foreign agencies. It requires the involvement of senior officials in making decisions about whether to share information as the risk of mistreatment increases, and whether to use information that may have been derived through mistreatment. All decisions to share information with a foreign agency must be "in accordance with this Direction and with Canada's legal obligations."

Additionally, the Minister of Public Safety approves all CSIS foreign arrangements in consultation with the Minister of Foreign Affairs. The Ministerial Direction (MD) on "Operations" contains an annex providing CSIS with guidelines on the establishment and maintenance of foreign arrangements (note: details are classified). While there is no legislation for RCMP foreign arrangements, there is an MD on "National Security Related Arrangements and Cooperation" establishing the process for entering into arrangements with foreign security or intelligence organizations. These foreign arrangements require the Minister of Public Safety's prior approval. They must be compatible with Canada's foreign policy, be in the interest of Canada, and respect all applicable laws.

**Q2 Apart from the MD on "Information Sharing with Foreign Entities," has the present or any former Minister of Public Safety issued other Direction to CBSA, CSIS, and the RCMP?**

**A2** Yes. The MD on "Operations" is the principal means by which the Minister of Public Safety communicates guidelines on the conduct and management of CSIS operations. The most recent MD on "Operations" came into effect in 2008, and establishes the following fundamental principles for CSIS: the rule of law must be observed; the investigative means must be proportional to the gravity and imminence of the threat; and the greater the risk associated with a particular activity, the higher the authority required for approval. Each year, the Minister of Public Safety also issues a classified MD to CSIS on "Intelligence Priorities." This MD helps guide intelligence collection, and informs the assessment and analysis of intelligence to ensure it is aligned with broader government objectives. CSIS has also been provided with a MD on "Responsibility and Accountability." This MD, among other things, sets out the sections of the *CSIS Act* for which Ministerial authorization is required, and identifies the broad responsibilities of the Director of CSIS.

MDs have also been issued to the RCMP on "National Security Investigations in Sensitive Sectors," which provides guidance on investigations as they may relate to, for example, post-secondary institutions, and on "Responsibility and Accountability."

To date, the CBSA has only been issued MD on "Information Sharing with Foreign Entities."

**Q3 Does the MD on "Information Sharing with Foreign Entities" violate any of Canada's international obligations?**

**A3** No. Canada is a party to a number of international agreements proscribing torture and other cruel, inhuman, or degrading treatment, including the *Convention Against Torture* and the *International Covenant on Civil and Political Rights*. These agreements are described in the MD on "Information Sharing with Foreign Entities." As the MD states, if there is a substantial risk that sharing information with a foreign agency would result in the mistreatment of an individual and it is unclear whether that risk can be mitigated, the matter will be referred to the Director or the Minister for decision. All decisions to share information with a foreign agency must be "in accordance...with Canada's legal obligations." The MD is consistent with Canada's international human rights obligations.

<b>CONTACTS:</b>			
Prepared by	Tel. no.	Approved by	Tel. no.
Patrick DesRochers Policy Analyst	990-2626	John Davies Director General National Security Policy	991-1970



Public Safety    Sécurité publique  
Canada            Canada

Ottawa, Canada  
K1A 0P8

**UNCLASSIFIED**

DATE: **APR 30 2012**

File No.: 6210-P2 // 21725 // 387220

**MEMORANDUM FOR THE SENIOR ASSISTANT DEPUTY MINISTER**

**RESPONSE TO CONCERNS ABOUT MINISTERIAL DIRECTION TO  
THE CANADIAN SECURITY INTELLIGENCE SERVICE (CSIS)**

(Decision Sought)

**ISSUE**

In February 2012, the Organization for Security and Cooperation in Europe (OSCE) wrote to Canada's Ambassador, raising concerns about the Minister of Public Safety's 2010 letter to CSIS providing additional guidance on the use of information that may have been derived through torture (**Tab A**). The Department of Foreign Affairs and International Trade (DFAIT) would like to provide a formal response to the OSCE by the end of April 2012.

In preparing a letter responding to the OSCE's concerns (**Tab B**), we have consulted DFAIT, as well as the Canadian Security Intelligence Service, the Royal Canadian Mounted Police, and the Canada Border Services Agency.

**BLANK PAGE / PAGE  
BLANCHE**

**UNCLASSIFIED**

**RECOMMENDATION**

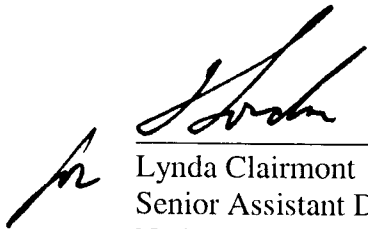
We recommend that you approve the draft response to the OSCE. We will then send the response to DFAIT for transmittal to the OSCE.



John Davies

Enclosures: (2)

I approve:



Lynda Clairmont 20120430.  
Lynda Clairmont  
Senior Assistant Deputy Minister  
National Security

Prepared by: Darryl Hirsch



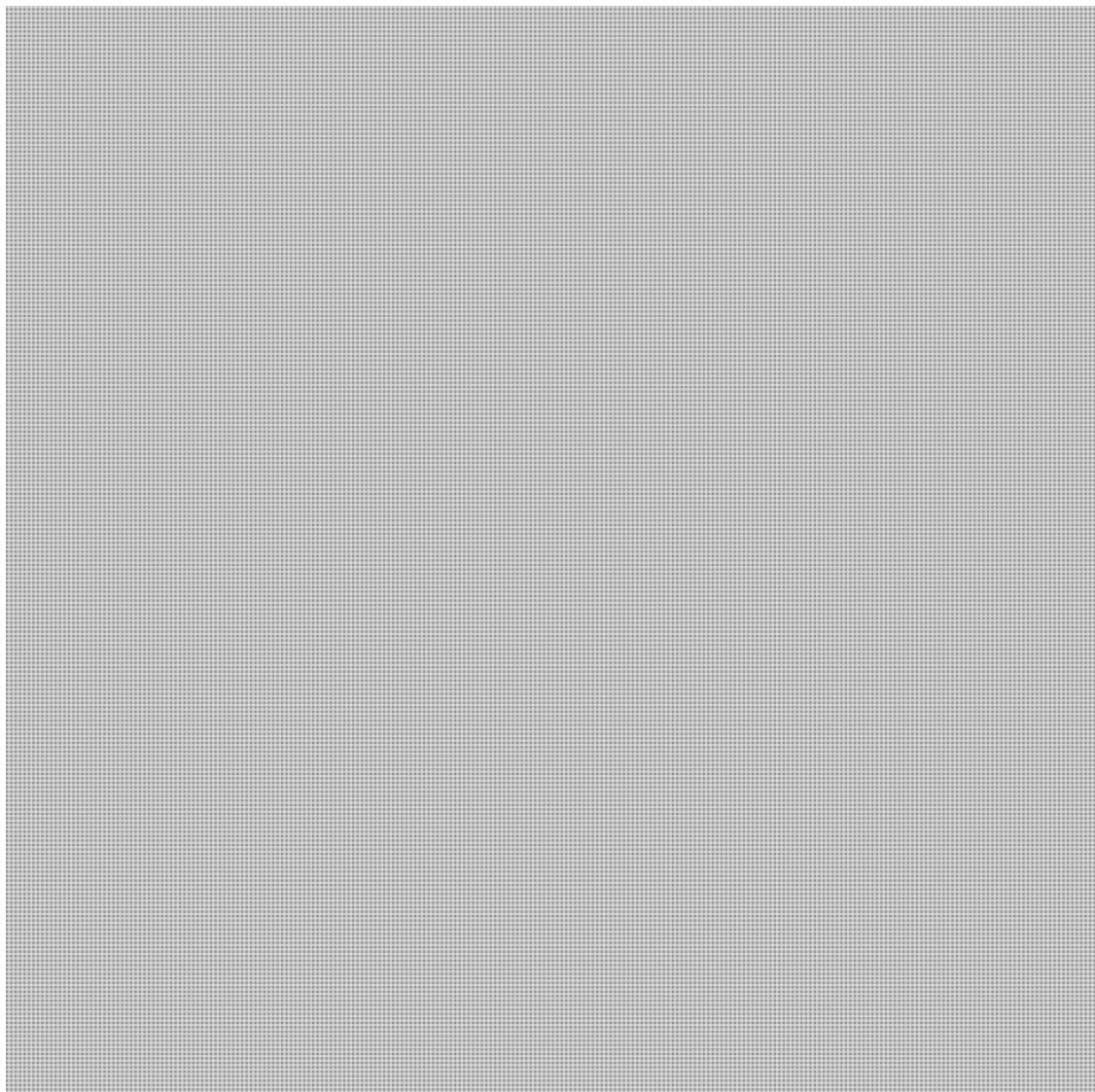
**Organization for Security and Co-operation in Europe  
Office for Democratic Institutions and Human Rights**

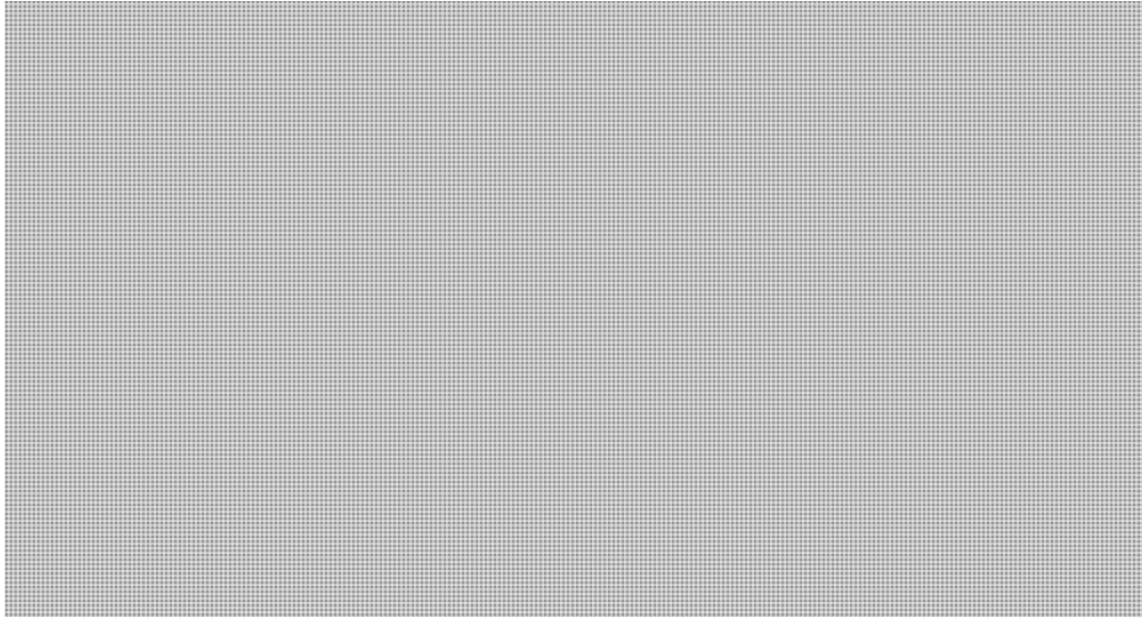
The Director

Warsaw, 16 February 2012

H.E. Ambassador Fredericka Gregory  
Permanent Representative of Canada to the OSCE  
Vienna

Dear Ambassador,





Yours sincerely,

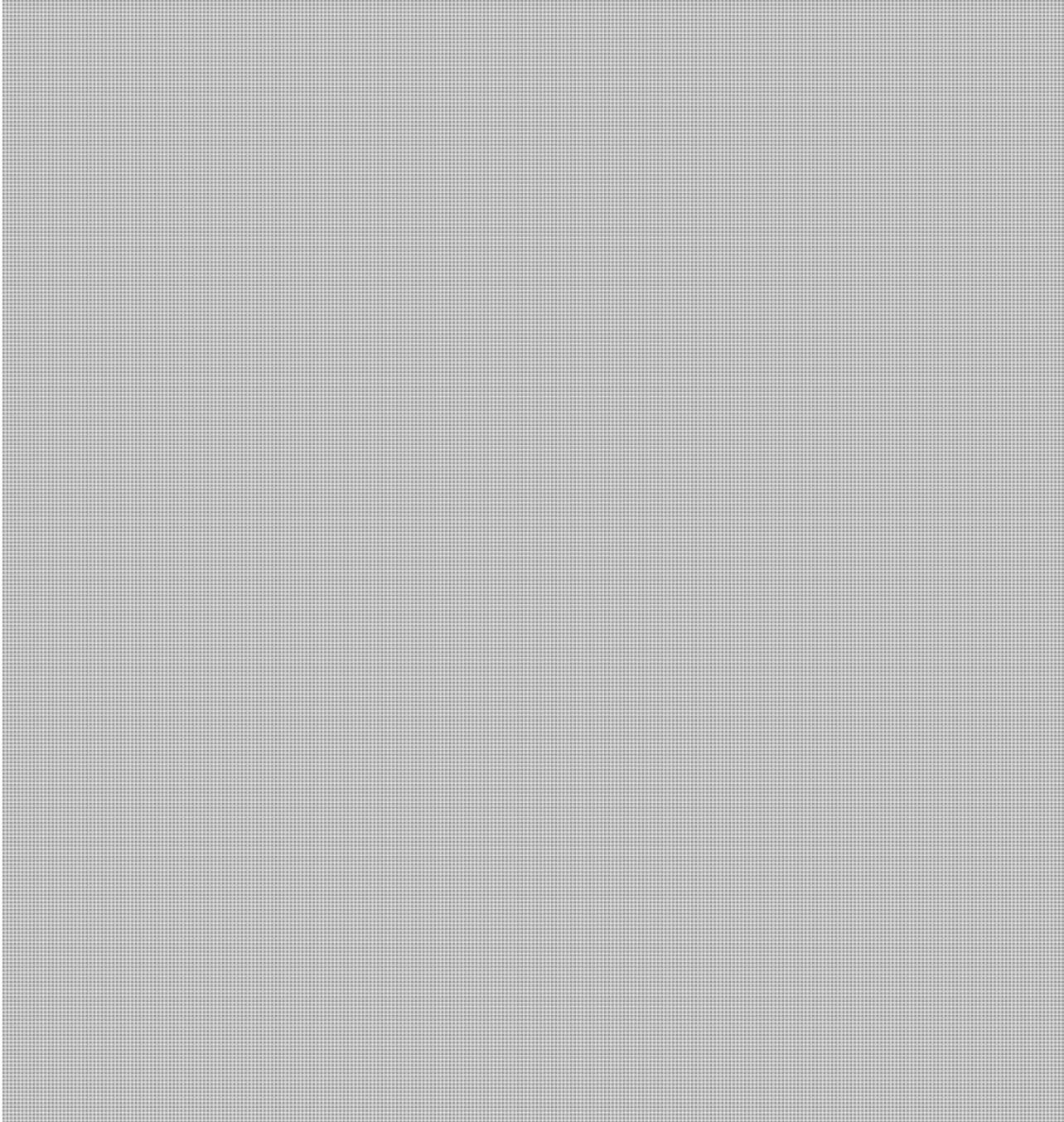
  
Janez Lenarčič  
Ambassador

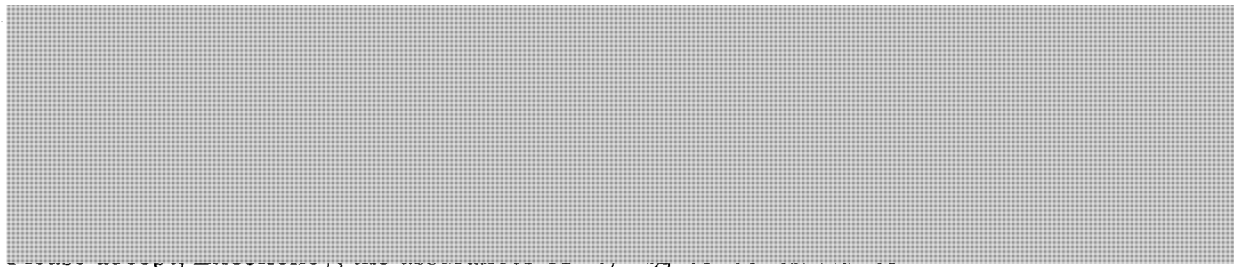
Cc:  
H.E. Ambassador Eoin O'Leary, Chairperson of the OSCE Permanent Council

s.15(1) - Int'l

H.E. Ambassador Janez Lenarčič  
Director of the Office for Democratic Institutions and Human Rights  
Organization for Security and Cooperation in Europe (OSCE)  
Vienna, Austria

Excellency,





Sincerely,

H. E. Ambassador Fredericka Gregory  
Permanent Representative of Canada to the OSCE  
Vienna, Austria



**UNCLASSIFIED**

**Specific Issue: MINISTERIAL DIRECTIVE ON INFORMATION SHARING,  
BOTH RECEIPT AND SENDING OF INFORMATION/  
INTELLIGENCE**  
**(Includes agreements with foreign states for the sharing  
of information)**  
*(Brief is new except where marked; DG approval pending)*

## **MAIN MESSAGES**

- One of the key priorities and duties of any government is ensuring the safety and security of its citizens. As outlined in Canada's recently-released *Counter Terrorism Strategy*, the terrorist threats we face have both domestic and international dimensions, with major threats to Canadian security often originating from abroad. Canada's law enforcement and intelligence agencies must therefore work with foreign partners to keep Canadians safe, including by sharing and receiving intelligence information.
- At the same time, consistent with Canadian democratic values, counter-terrorism activities must be guided by the principles of respect for human rights and the rule of law, proportionality, and adaptability.
- These principles are reflected in the 2011 Ministerial Direction to the Canadian Security Intelligence Service (CSIS) on "Information-Sharing With Foreign Entities." The Direction states that "the Government of Canada opposes in the strongest possible terms the mistreatment of any individual by any state or agency for any purpose." The Direction reiterates that the Government of Canada does not condone the use of torture and specifically references Canada's obligations under the Convention.
- The Ministerial Direction also reiterates that torture is a criminal offence in Canada that has extraterritorial application and that the *Criminal Code* also prohibits aiding and abetting the commission of torture, counselling the commission of torture whether or not the torture is committed, conspiracy to commit torture, attempting to commit torture and being an accessory after the fact. CSIS officials must and do comply with all of Canada's legal obligations. (*Citing MD*)
- The Ministerial Direction requires CSIS approval levels to be proportionate to the potential risks of sharing information: the greater the risk, the higher the level of approval required. In the most serious cases, the matter must be referred to the Director of CSIS or the Minister of Public Safety. While the decision maker will consider a broad range of factors, in all cases he or she "shall authorize the

000080

sharing of information...only in accordance with Canada's legal obligations.”

- Further, the Ministerial Direction establishes important procedural safeguards for the sharing and use of information. CSIS officials must assess and mitigate potential risks of sharing information with their counterparts; for example, through the use of caveats. They must also have in place reasonable and appropriate measures to identify information that is likely to have been derived from mistreatment, and must properly characterize this information in any further dissemination of it.
- As recommended by the O'Connor Inquiry, the Ministerial Direction notes that the Department of Foreign Affairs provides support to CSIS to help ensure a consistent understanding across government of the risks of sharing information with foreign entities, including by making its country human rights reports available to the intelligence and law enforcement community. (*citing M.D.*)
- In Canada's view, the Direction is consistent with Canada's international human rights obligations. The Ministerial Direction ensures that Canada pursues a principled and proportionate response to terrorism and other threats to national security, while continuing to upholding the values it seeks to protect. (*from M.D.*)

#### **SUPPLEMENTARY MESSAGES (arrangements with foreign agencies)**

- As of March 31, 2010, CSIS had 280 arrangements with foreign agencies in 148 countries. All foreign arrangements are reviewed and approved by the Minister of Public Safety following consultation with the Minister of Foreign Affairs. The Minister of Public Safety has also issued Direction to CSIS providing more specific guidance on the establishment of foreign arrangements.
- The Security Intelligence Review Committee (SIRC) is a review body at arm's length from Government. SIRC has access to all CSIS information (except Cabinet Confidences). It regularly reviews CSIS information-sharing with domestic and foreign agencies to ensure compliance with the law and Ministerial Direction.

**SUPPLEMENTARY MESSAGES** (responsive only – in relation to portion of the Direction dealing with situations of high risk of mistreatment flowing from Canadian information-sharing or reliance on information from foreign entities in operational situations)

- Justice/HRLS strongly suggests that PS prepare lines that would allow the delegation to respond at least generally to the very likely questions from the Committee as to what the Directives actually say about exceptional circumstances in which Canada may either share information with foreign agencies or rely on it for operational purposes. We understand that lines are being prepared for a response to Parliamentary Question 591 from MP Cotler that could be helpful in this regard.

## **BACKGROUND INFORMATION**

### **International law and commentary**

Art. 2 of the CAT obliges states to “take effective legislative, administrative, judicial or other measures to prevent acts of torture in any territory under its jurisdiction” and states that “no exceptional circumstances... may be invoked as a justification of torture”.

Art. 4 of the CAT obliges states to criminalize torture as defined in the CAT, as well as any act which “constitutes complicity or participation in torture”. Canada has implemented this obligation through s. 269.1 of the Criminal Code, and through relevant provisions on aiding and abetting, etc.

Art. 15 of the CAT prohibits the reliance on any statement made as a result of torture as evidence “in any proceedings”. This does not extend, however, to information shared for intelligence purposes.

While there is no CAT article that deals explicitly with information-sharing that may lead to a substantial risk of torture, there is considerable commentary by international experts and bodies on the issue of both the use of information obtained through torture and the sharing of information to a risk of torture by intelligence agencies as potential “complicity” in torture. For example, the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, stated in his 2009 report to the tenth session of the Human Rights Council dealing with intelligence cooperation, that : “States ...are responsible where they knowingly engage in, render aid to or assist in the commission of internationally wrongful acts, including violations of human rights” . “Grave human rights violations by States such as torture”, Scheinin continues, “should place serious constraints on policies of cooperation by States, including by their intelligence agencies, with States that are known to violate human rights”... “States must not aid or assist in the commission of acts of torture, or recognize such practices as lawful, including by relying on intelligence information obtained through torture. Furthermore, the Special Rapporteur is of the view that: the active participation [in interrogation] through the sending of interrogators or questions, or even the mere presence of intelligence personnel at an interview with a person who is being held in places

where his rights are violated, can be reasonably understood as implicitly condoning such practices .

According to the Special Rapporteur: "the active or passive participation by States in the interrogation of persons held by another State constitutes an internationally wrongful act if the State knew or ought to have known that the person was facing a real risk of torture or other prohibited treatment..." A State that takes advantage of a coercive environment, when it knows or ought to have known that torture or other prohibited treatment occurred, even if it does not actively participate in the interrogations, violates human rights law. This may include creating a demand for intelligence obtained from torture or other prohibited treatment. States that rely on information obtained through such prohibited means "are complicit in the commission of internationally wrongful acts" according to Scheinin. The Special Rapporteur also expressed his concern with regards to information sharing with foreign governments without adequate safeguards.

In July 2009, the UK Human Rights Joint Committee released its Report on "Allegations of UK Complicity in Torture". The Report includes an attempt to define what "complicity" means at international law based primarily on international and academic commentary. Among other conclusions, the Committee stated:

We are in no doubt that requests to foreign agencies to arrest and detain an individual, the provision of information enabling their arrest, the provision of questions for their interrogation, the sending of interrogators to question a suspect who is being tortured and of observers to sit in on interrogations, are all forms of assistance and facilitation capable of amounting to complicity in torture by the State concerned when those things are done in the knowledge that the person concerned is being, has been or will be tortured by the State which is detaining him, or where that ought to be obvious to the State providing the assistance.

The International Commission of Jurists report entitled "Assessing Damage, Urging Action" has the following to say about complicity in the intelligence context:

This cooperation [between intelligence services of different States] often involves working with States that have insufficient domestic human rights safeguards, or, worse still, with intelligence agencies with a long history of systematic involvement in human rights violations. The Panel believes that such cooperation is necessary. However, if States are to avoid the charge of complicity, and avoid their agents being pursued in subsequent legal actions, a clear legal framework for intelligence cooperation, and safeguards to ensure compliance with human rights law, are essential.

[...]

If intelligence or other State agencies are systematically sharing information with countries and agencies with a known record of human

rights violations, it is difficult to resist the argument that States are complicit, wittingly or unwittingly, in the serious human rights violations committed by their partners in counter-terrorism.

[...]

In particular, information should never be provided to a foreign country where there is a credible risk that the information will cause or contribute to serious human rights violations (emphasis added) .

Courts in the U.K. have drawn distinctions between permissible and impermissible uses of tainted information. For example, judicial statements in the United Kingdom support the view that the executive is entitled to rely on tainted information for operational purposes. In *A v. Home Secretary (No 2)*, [2005] UKHL 71 (BailII), the House of Lords unanimously refused to admit, in immigration proceedings, evidence that may have been procured by torture. Some of the judges went further, however, and commented on "the executive's ability to take into account information procured by torture." Lord Nicholls wrote, at 68-9:

The intuitive response to these questions is that if use of such information might save lives it would be absurd to reject it. If the police were to learn of the whereabouts of a ticking bomb it would be ludicrous for them to disregard this information if it had been procured by torture. No one suggests the police should act in this way. Similarly, if tainted information points a finger of suspicion at a particular individual: depending on the circumstances, this information is a matter the police may properly take into account when considering, for example, whether to make an arrest.

In both these instances the executive arm of the state is open to the charge that it is condoning the use of torture. So, in a sense, it is. The government is using information obtained by torture. But in cases such as these the government cannot be expected to close its eyes to this information at the price of endangering the lives of its own citizens. Moral repugnance to torture does not require this.

Several members of the court drew a distinction, in passing, between the rule against admissibility of tainted information in judicial proceedings and lawful reliance by the executive on tainted information for the protection of the public and the security of the state. Per Lord Brown:

Generally speaking it is accepted that the executive may make use of all information it acquires: both coerced statements and whatever fruits they are found to bear. Not merely, indeed, is the executive entitled to make use of this information; to my mind it is bound to do so. It has a prime responsibility to safeguard the security of the state and would be failing in its duty if it ignores whatever it may learn or fails to follow it up. Of course it must do nothing to promote torture. It must not enlist torturers to its aid (rendition being perhaps the most extreme example of this). But nor need

it sever relations even with those states whose interrogation practices are of most concern.

Recently, in *Ahmed & Anor v R*, [2011] EWCA Crim 184 (BailII), two individuals accused of terrorism offences argued that their trial amounted to an abuse of process due to the alleged complicity of British authorities in their mistreatment while in the custody of foreign authorities. The England and Wales Court of Appeal rejected this argument and restated the principle above:

... the Home Secretary is entitled to rely on material gathered from a foreign source, with which information and intelligence is shared, even if such material might be the product of torture. Likewise, the security services or the police are not required to close their eyes to information which helps to protect the public's safety, such as for example by identifying persons presenting a threat of terrorism, or places where bombs are being made, even if that information comes to them from a foreign source which has used torture. ...

The Court commented that some of the wider concepts of complicity in torture advanced by the UN Special Rapporteur are not based on customary or treaty law, and do not represent general principles of law recognised by civilised nations. As noted by Lord Brown in *A v. Home Secretary (No 2)*, while relationships with foreign entities known to engage in mistreatment is not prohibited, a state must "do nothing to promote torture" or to "enlist torturers to its aid".

### **Canadian approach**

On a periodic basis, the Minister of Public Safety issues Ministerial Direction (MDs) on the conduct and management of CSIS operations. In 2011, the Minister of Public Safety issued a comprehensive MD on "Information Sharing with Foreign Entities." It replaces guidance on information sharing provided by the previous and current Minister in 2009 and 2010, respectively. (*CAT written response*)

The 2011 MD describes Canada's legal obligations with respect to sharing information, reiterating that the Government of Canada does not condone the use of torture and specifically referencing Canada's obligations under the Convention. Within that context, the MD identifies the principles, or procedural safeguards, that CSIS must follow: assessment and mitigation of potential risks in sharing information with foreign agencies; assessment of the accuracy and reliability of information received from foreign agencies; and proper characterization of foreign agency information in any further dissemination of it. (*new and CAT written response*)

Apart from the 2011 MD on "Information Sharing with Foreign Entities," CSIS is subject to an MD on "Operations." It establishes the following overarching

principles for CSIS: the rule of law must be observed; the investigative means must be proportional to the gravity and imminence of the threat; the greater the risk associated with a particular activity, the higher the authority required for approval; and the use of intrusive investigative techniques must be weighed against possible damage to civil liberties, and the least intrusive techniques must be used first. In addition, the MD on "Operations" provides guidance issues such as the management of domestic and foreign arrangements.

### **Shadow reports**

Of note, in its recent "shadow" report to the UN Committee Against Torture relevant to Canada's appearance, Amnesty International Canada raised its concern that Canadian law enforcement and security agencies may rely upon information that may have been obtained under torture in other circumstances, in particular in the course of intelligence activities. Amnesty calls on Canada to establish a clear policy banning CSIS and other Canadian law enforcement and security agencies from using information received from other domestic or international law enforcement or security agencies when there is a real risk that it was obtained as the result of torture or other prohibited treatment. Amnesty has also written directly to the Minister of Public Safety on this issue. (*citing Amnesty International shadow report*).

#### **PREPARED BY:**

PS/NSI/Darryl Hirsch

#### **APPROVED BY: (pending)**

PS/NS/John Davies

#### **DEPARTMENTAL COORDINATION CONTACT:**

Tracy Wilcox, PS International Affairs Division, 613-990-9651

#### **MEDIA RELATIONS CONTACTS:**

PS Media Relations, 613-991-0657

*RDIMS 597634*



# INQUIRY OF MINISTRY DEMANDE DE RENSEIGNEMENT AU GOUVERNEMENT

PREPARE IN ENGLISH AND FRENCH MARKING "ORIGINAL TEXT" OR "TRANSLATION"  
PRÉPARER EN ANGLAIS ET EN FRANÇAIS EN INDIQUANT "TEXTE ORIGINAL" OU "TRADUCTION"

QUESTION NO./N° DE LA QUESTION Q-591	BY / DE Mr. Cotler (Mount Royal)	DATE April 4, 2012
---	-------------------------------------	-----------------------

REPLY BY THE MINISTER OF PUBLIC SAFETY  
RÉPONSE DU MINISTRE DE LA SÉCURITÉ PUBLIQUE

Signed by the Honourable Vic Toews

PRINT NAME OF SIGNATORY  
INSCRIRE LE NOM DU SIGNATAIRE

SIGNATURE  
MINISTER OR PARLIAMENTARY SECRETARY  
MINISTRE OU SECRÉTAIRE PARLEMENTAIRE

QUESTION

With regard to the current Canadian policy on providing information to foreign agencies and using information from foreign agencies for the combating of terrorism and the protection of public safety:

(a) what is the current policy on providing information to foreign agencies when there is a substantial risk this may lead to acts of torture and other cruel, inhuman or degrading treatment or punishment; (b) which departments contributed to the formation of the policy referred to in (a); (c) how long has the policy referred to in (a) been in place; (d) which external experts, including academics, representatives of non-governmental organizations (NGO), private sector representatives, were consulted in the formation of the policy referred to in (a); (e) what was the role of the Minister of Public Safety in the formation of the policy referred to in (a); (f) what was the role of the Minister of Foreign Affairs in the formation of the policy referred to in (a); (g) which official is ultimately responsible for determining whether "substantial risk" exists, in reference to (a); (h) who is responsible for deciding to which foreign agencies Canada will provide information, and what are the substantive criteria behind such a decision; (i) when deliberating the decision referred to in (h), are the "concluding observations" of United Nations Committee Against Torture reports consulted; (j) what sources are used by the Canadian Security Intelligence Service (CSIS), the RCMP or government officials in considering the human rights records of foreign agencies concerning domestic and international activities, including the treatment and interrogation of detainees; (k) what follow-up procedures are used to verify that information transferred from Canada to foreign agencies does not lead to the commission of acts of torture and other cruel, inhuman or degrading treatment or punishment; (l) what is the current policy on the use of information obtained by CSIS from foreign agencies when there are suspicions such information was obtained using acts of torture and other cruel, inhuman or degrading treatment or punishment; (m) which departments contributed to the formation of the current policy referred to in (l); (n) how long has the policy referred to in (l) been in place; (o) which external experts, including academics, NGO representatives, private sector representatives, were consulted in the formation of the policy referred to in (l); and (p) what was the role of the Minister of Public Safety in the formation of the policy referred to in (l)?

REPLY / RÉPONSE

ORIGINAL TEXT  
TEXTE ORIGINAL

TRANSLATION  
TRADUCTION



**With regard to the current Canadian policy on providing information to foreign agencies and using information from foreign agencies for the combating of terrorism and the protection of public safety: (a) what is the current policy on providing information to foreign agencies when there is a substantial risk this may lead to acts of torture and other cruel, inhuman or degrading treatment or punishment;**

Departments and agencies have a suite of directives and policies that govern their information sharing practices. They have reviewed and revised these policies over the years, most recently after the release of Commissioner O'Connor's and Commissioner Iacobucci's reports.

In 2011, the Government of Canada established a coherent and consistent policy for decisions about whether or not to share information with a foreign entity when there may be a substantial risk of mistreatment. The policy is as follows.

- In all situations, departments and agencies must comply with Canada's laws and legal obligations in sharing information with foreign entities. They must avoid any complicity in mistreatment by foreign entities.
- Departments and agencies must assess and mitigate potential risks of sharing information with foreign entities.
- Departments and agencies must have in place reasonable and appropriate measures to identify foreign entity information likely derived from mistreatment. They must assess the accuracy and reliability of information received, and properly characterize this information in any further dissemination of it.
- The approval level to share information with foreign agencies must be proportionate to the risk of mistreatment that may result. Except when the risk may be substantial, departments and agencies are individually responsible for establishing appropriate approval levels.
- When there is a substantial risk that sharing information with a foreign entity would result in the mistreatment of an individual, and it is unclear whether that risk can be mitigated through the use of caveats or assurances, the matter must be referred to the responsible Deputy Head or equivalent (for the Canada Border Services Agency (CBSA), the Communications Security Establishment Canada (CSEC), the Canadian Security Intelligence Service (CSIS), the Department of National Defence / Canadian Forces (DND/CF), and the Royal Canadian Mounted Police (RCMP)) for decision. The Deputy Head may in turn decide to refer the matter to his or her Minister. In both cases, the decision maker will normally consider: the threat, the importance of sharing the information; the intended purpose of the information requested by the foreign entity; 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; the proposed measures to mitigate the risk, and the likelihood that these measures will be successful; and the views of the Department of Foreign Affairs and International Trade (DFAIT) plus other departments and agencies as appropriate. The decision maker shall only authorize the sharing of information with a foreign entity in accordance with Canada's legal obligations.

**(b) which departments contributed to the formation of the policy referred to in (a);**

CBSA, CSEC, CSIS, DFAIT, DND/CF, the Department of Justice (DoJ), the Privy Council Office, Public Safety Canada (PS), and the RCMP contributed to the formation of the policy.

**(c) how long has the policy referred to in (a) been in place;**

The Government introduced the policy in 2011.

**(d) which external experts, including academics, representatives of non-governmental**

**organizations (NGO), private sector representatives, were consulted in the formation of the policy referred to in (a);**

While external experts were not consulted in person, a wide range of documents informed the development of the policy. The documents included findings and recommendations from independent inquiries such as: Commissioner O'Connor's *Report of the Events Relating to Maher Arar*; Commissioner Iacobucci's *Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati, and Muayyed Nureddin*; the full, classified version of the Security Intelligence Review Committee's report on *CSIS' Role in the Matter of Omar Khadr*; as well as the United Kingdom's (U.K.) Intelligence and National Security Committee's reports on *Torture and Intelligence in the Global War on Terror* and *Rendition*. Reports by non-governmental organizations such as Amnesty International, Human Rights Watch, the International Committee of the Red Cross, and Physicians for Human Rights on the treatment of detainees were examined.

**(e) what was the role of the Minister of Public Safety in the formation of the policy referred to in (a);**

The Minister of Public Safety reviewed and approved the policy for CBSA, CSIS, and RCMP.

**(f) what was the role of the Minister of Foreign Affairs in the formation of the policy referred to in (a);**

*The Minister of Foreign Affairs will be responding to this question.*

**(g) which official is ultimately responsible for determining whether "substantial risk" exists, in reference to (a);**

Decisions whether or not to share information are made at a level proportionate to the risk of mistreatment that may result; the greater the risk, the more senior the level of approval that is required. Within each department or agency, the assessment of risk is made at each approval level. As the risks increase, decisions whether or not to share are elevated as well. If it is determined that a substantial risk exists that sending information to, or soliciting information from, a foreign entity would result in the mistreatment of an individual, and it is unclear whether that risk can be mitigated through the use of caveats or assurances, the matter is to be referred to the responsible Deputy Head or equivalent for decision. He or she may in turn decide to refer the decision to his or her Minister.

**(h) who is responsible for deciding to which foreign agencies Canada will provide information, and what are the substantive criteria behind such a decision;**

CBSA

The vast majority of the CBSA's information sharing is conducted under formalized information sharing agreements and treaties with other countries. The human rights record of such countries are considered prior to entering into a formal agreement with that country.

CSEC / DND

*The Minister of National Defence will provide information in relation to CSEC and DND.*

CSIS

CSIS, with the approval of the Minister of Public Safety after consultation with the Minister of Foreign Affairs, may enter into an arrangement or otherwise cooperate with, including the sharing of information, the government of a foreign state or an institution thereof or an international organization of states or an institution

thereof. CSIS enters into these arrangements to fulfill its mandate under the *CSIS Act* to investigate threats to the security of Canada and report and advise on these threats to the Government of Canada and other approved entities.

### RCMP

The mandate of the RCMP is to perform all duties that are assigned to peace officers in relation to the preservation of the peace, as well as the prevention of crime and offences against the laws of Canada. In performing those duties, the RCMP will provide information to a foreign entity on a case by case basis, when appropriate, during the course of a criminal investigation. Sharing of national security related information with foreign agencies is conducted and centrally controlled by National Security Criminal Investigations at National Headquarters. The criteria for deciding whether to exchange information is dependent upon among other things, 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.

### **(i) when deliberating the decision referred to in (h), are the “concluding observations” of United Nations Committee Against Torture reports consulted;**

Departments and agencies routinely consult a variety of documents and sources that may assist them in determining whether or not to share information with foreign entities. Where applicable, this includes the “concluding observations” of United Nations Committee Against Torture reports.

### **(j) what sources are used by the Canadian Security Intelligence Service (CSIS), the RCMP or government officials in considering the human rights records of foreign agencies concerning domestic and international activities, including the treatment and interrogation of detainees;**

To ensure consistency across the Government, and as recommended by Commissioner O'Connor, DFAIT makes its country human rights reports available to the intelligence and law enforcement community. Departments and agencies supplement these reports with a broad range of information, as described below.

### CBSA

The vast majority of the CBSA's information sharing is conducted under formalized information sharing agreements and treaties with other countries. The human rights records of such countries are considered prior to entering into a formal agreement with that country. To help ensure a consistent understanding of the risks of sharing information with foreign entities, DFAIT makes its country human rights reports available to CBSA. All other sources are considered insofar as they are credible and relevant.

### CSEC / DND

*The Minister of National Defence will provide information in relation to CSEC and DND.*

### CSIS

CSIS uses a wide variety of open and classified source materials in considering the human rights records of foreign agencies. These sources include, but are not limited to: CSIS databases; CSIS foreign agency assessments conducted under authority of section 17(1)(b) of the *CSIS Act*; relevant and reliable reporting from CSIS stations abroad and foreign agencies; DFAIT country human rights reports; reporting from organizations such as the United States (U.S.) Department of State, the United Nations, Human Rights Watch, Amnesty International, and others on a case by case basis; and other relevant open source information.

### RCMP

The RCMP routinely consults a number of sources such as: DFAIT (annual human rights reports), U.S. Department of State, Amnesty International, Human Rights Watch, Freedom House, Transparency International

(Corruption Perception Index), DFAIT (country human rights reports), U.K. Foreign and Commonwealth Office (country profiles), Office of the United Nations High Commissioner on Human Rights (Treaty Database), Office of the United Nations High Commissioner for Human Rights (Country visits), the United Nations Committee Against Torture (Concluding observations of the Committee Against Torture), RCMP Liaison Officers, and domestic and foreign partners as appropriate.

**(k) what follow-up procedures are used to verify that information transferred from Canada to foreign agencies does not lead to the commission of acts of torture and other cruel, inhuman or degrading treatment or punishment;**

CBSA

Information sharing treaties and agreements contain provisions for redress should terms and conditions set out not be followed. Where appropriate, diplomatic or other enquiries may be pursued.

CSEC / DND

*The Minister of National Defence will provide information in relation to CSEC and DND.*

CSIS

CSIS employees are obliged to report potential mistreatment to their appropriate supervisors. Relationships with foreign agencies and their human rights records are constantly updated and evaluated based on the most up to date intelligence and open source reporting. The approval level that CSIS requires in order to share information must be proportionate to the risk of mistreatment that may result: the greater the risk, the more senior the level of approval required. When there is a potential risk that sharing information with a foreign entity would result in the mistreatment of an individual, and it is unclear whether that risk can be mitigated through the use of caveats or assurances, the matter is referred to the interdepartmental Information Sharing Evaluation Committee. This committee is responsible for assessing various implications of sharing within the context of Canada's legal obligations and security considerations. In this evaluation, measures to mitigate the risk of mistreatment are considered, including the ability of reputable non-governmental organizations to follow up and monitor detainees.

RCMP

The RCMP shares information with foreign agencies in a manner that complies with Canada's laws and legal obligations. RCMP policy, procedures and the criteria described in h) guide decision making prior to the sharing of information to mitigate the risk that sharing will result in mistreatment. Caveats are included on all national security related information shared within and outside the RCMP in order to limit unintended use of the information and unintended transfer to third parties. Human rights records of foreign agencies are assessed regularly, both before and after sharing, and as indicated in response to j). Reports of allegations or indications of such misbehaviour are carefully assessed by the RCMP in order to determine an appropriate course of action.

**(l) what is the current policy on the use of information obtained by CSIS from foreign agencies when there are suspicions such information was obtained using acts of torture and other cruel, inhuman or degrading treatment or punishment;**

In this respect, CSIS is guided by a Ministerial Direction (MD) approved by the Minister of Public Safety on July 28, 2011. This MD is further prescribed in a CSIS Deputy Director of Operations (DDO) Directive on Information Sharing with Foreign Entities issued on August 24, 2011, which states that when information is likely derived from mistreatment, the information cannot be used for a specific action if there is no serious threat of loss of life, injury, or substantial damage or destruction of property. If there is a serious threat of loss of life, injury, or substantial damage or destruction of property, the report from the interdepartmental Information Sharing Evaluation Committee must be sent to the Director via the appropriate chain of command

and the final decision is to be made by the Director. The Director also may refer the matter to the Minister of Public Safety for decision.

**(m) which departments contributed to the formation of the current policy referred to in (l);**

CSIS consulted PS as well as DoJ and RCMP in formulating the policy.

**(n) how long has the policy referred to in (l) been in place;**

While policies have been in place and increasingly formalized for a number of years, the current MD on "Information Sharing with Foreign Entities" was approved on July 28, 2011, and the current DDO Directive on Information Sharing with Foreign Entities was approved on August 24, 2011.

**(o) which external experts, including academics, NGO representatives, private sector representatives, were consulted in the formation of the policy referred to in (l); and**

The findings and recommendations from Commissioner O'Connor's *Report of the Events Relating to Maher Arar*, Commissioner Iacobucci's *Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati, and Muayyed Nureddin*, Justice Blanchard's security certificate decision in *R v. Mahjoud*, the *Criminal Code*, the *United Nations Convention Against Torture and Other Cruel, Inhuman, or Degrading Treatment or Punishment*, and other relevant documents and organizations were consulted. Reports from Amnesty International, Human Rights Watch, and other relevant documents and organizations were also consulted.

**(p) what was the role of the Minister of Public Safety in the formation of the policy referred to in (l)?**

The Minister of Public Safety approved a Direction to CSIS on July 28, 2011.



# INQUIRY OF MINISTRY DEMANDE DE RENSEIGNEMENT AU GOUVERNEMENT

PREPARE IN ENGLISH AND FRENCH MARKING "ORIGINAL TEXT" OR "TRANSLATION"  
PRÉPARER EN ANGLAIS ET EN FRANÇAIS EN INDIQUANT "TEXTE ORIGINAL" OU "TRADUCTION"

QUESTION NO./N° DE LA QUESTION Q-591	BY / DE M. Cotler (Mont-Royal)	DATE 4 avril 2012
---	-----------------------------------	----------------------

REPLY BY THE MINISTER OF PUBLIC SAFETY  
RÉPONSE DU MINISTRE DE LA SÉCURITÉ PUBLIQUE

Signé par l'honorable Vic Toews

PRINT NAME OF SIGNATORY  
INSCRIRE LE NOM DU SIGNATAIRE

SIGNATURE  
MINISTER OR PARLIAMENTARY SECRETARY  
MINISTRE OU SECRÉTAIRE PARLEMENTAIRE

QUESTION

En ce qui concerne la politique canadienne qui s'applique actuellement à la communication de renseignements à des agences étrangères et à l'utilisation des renseignements fournis par des agences étrangères afin de combattre le terrorisme et d'assurer la sécurité publique : a) quelle politique s'applique actuellement à la communication de renseignements à des agences étrangères dans les cas où cette pratique pose un risque sérieux de torture ou d'autres peines ou traitements cruels, inhumains ou dégradants; – **Voir ci-joint pour le texte complet de la question.**

REPLY / RÉPONSE

ORIGINAL TEXT  
TEXTE ORIGINAL

TRANSLATION  
TRADUCTION

**Q-591<sup>2</sup>** — 4 avril 2012 — M. Cotler (Mont-Royal) — En ce qui concerne la politique canadienne qui s'applique actuellement à la communication de renseignements à des agences étrangères et à l'utilisation des renseignements fournis par des agences étrangères afin de combattre le terrorisme et d'assurer la sécurité publique : a) quelle politique s'applique actuellement à la communication de renseignements à des agences étrangères dans les cas où cette pratique pose un risque sérieux de torture ou d'autres peines ou traitements cruels, inhumains ou dégradants; b) quels ministères ont contribué à l'élaboration de la politique mentionnée au point a); c) depuis combien de temps la politique mentionnée au point a) est elle en place; d) quels experts externes, y compris les représentants du milieu universitaire, d'organisations non gouvernementales (ONG) et du secteur privé, ont été consultés dans l'élaboration de la politique mentionnée au point a); e) quel rôle le ministre de la Sécurité publique a-t-il joué dans l'élaboration de la politique mentionnée au point a); f) quel rôle le ministre des Affaires étrangères a-t-il joué dans l'élaboration de la politique mentionnée au point a); g) qui est responsable en dernier ressort de déterminer l'existence d'un « risque sérieux », tel qu'il est indiqué au point a); h) qui est responsable de décider à quelles agences étrangères le Canada accepte de fournir des renseignements, et quels sont les critères principaux sur lesquels s'appuient les décisions prises à cet égard; i) lors de la prise d'une décision du type indiqué au point h), les « observations finales » des rapports du Comité des Nations Unies contre la torture sont-elles consultées; j) quelles sources le Service canadien du renseignement de sécurité (SCRS), la GRC ou d'autres responsables gouvernementaux utilisent-ils pour connaître le bilan des agences étrangères en matière de respect des droits de la personne, que ce soit dans le cadre de leurs activités intérieures et internationales, y compris en ce qui a trait au traitement et à l'interrogation des détenus; k) quelles procédures de suivi utilise-t-on pour vérifier que les renseignements communiqués par le Canada aux agences étrangères ne donnent pas lieu à des actes de torture ou à d'autres peines ou traitements cruels, inhumains ou dégradants; l) quelle politique s'applique actuellement à l'utilisation des renseignements communiqués au SCRS par des agences étrangères lorsqu'on soupçonne que ces renseignements ont été obtenus au moyen de la torture ou d'autres peines ou traitements cruels, inhumains ou dégradants; m) quels ministères ont contribué à l'élaboration de la politique actuelle mentionnée au point l); n) depuis combien de temps la politique mentionnée au point l) est elle en place; o) quels experts externes, y compris les représentants du milieu universitaire, d'ONG et du secteur privé, ont été consultés dans l'élaboration de la politique mentionnée au point l); p) quel rôle le ministre de la Sécurité publique a-t-il joué dans l'élaboration de la politique mentionnée au point l)?



# INQUIRY OF MINISTRY DEMANDE DE RENSEIGNEMENT AU GOUVERNEMENT

PREPARE IN ENGLISH AND FRENCH MARKING "ORIGINAL TEXT" OR "TRANSLATION"  
PRÉPARER EN ANGLAIS ET EN FRANÇAIS EN INDIQUANT "TEXTE ORIGINAL" OU "TRADUCTION"

QUESTION NO./N° DE LA QUESTION Q-966	BY / DE Mr. Sean Casey (Charlottetown)	DATE October 4, 2012
---	---	-------------------------

REPLY BY THE MINISTER OF PUBLIC SAFETY  
RÉPONSE DU MINISTRE DE LA SÉCURITÉ PUBLIQUE

Signed by the Honourable Vic Toews

PRINT NAME OF SIGNATORY  
INSCRIRE LE NOM DU SIGNATAIRE

SIGNATURE  
MINISTER OR PARLIAMENTARY SECRETARY  
MINISTRE OU SECRÉTAIRE PARLEMENTAIRE

QUESTION

With regard to torture: (a) what is the government's policy on art. 1(1) of the United Nations Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment; (b) is it the policy of the government and its agencies that Canada is opposed to any violation of the article cited in (a); (c) is it the government's policy that s.269.1 of the Criminal Code, including, but not limited to, subsection 4, is consistent with art.1(1) and (2) of the United Nations Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment; and (d) is it the government's policy that information obtained by means of torture and provided to Canada by a third party deemed a non-state, or provided by a state as defined by the United Nations, is contrary to the article cited in (a) and a potential contravention of Section 269.1 of the Criminal Code?

REPLY / RÉPONSE

ORIGINAL TEXT  
TEXTE ORIGINAL

TRANSLATION  
TRADUCTION

Public Safety Canada

d) The Government's policy with respect to information sharing with foreign entities where there is a risk of torture is a matter of public record. The Government opposes in the strongest possible terms the mistreatment of any individual by any foreign entity for any purpose.

In 2011, the Minister of Public Safety issued comprehensive Ministerial Directions (MD) to the Canadian Security Intelligence Service (CSIS), Royal Canadian Mounted Police (RCMP) and Canada Border Services Agency (CBSA) on "Information Sharing with Foreign Entities."

The 2011 MDs deal with Canada's legal obligations with respect to sharing information, and specifically reference the *Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (CAT)* and the *Criminal Code*. The MDs state that Canada neither promotes nor condones the use of torture or other unlawful methods of investigation. They explicitly state that agencies must act in a manner that complies with Canada's laws and legal obligations, including s. 269.1 of the *Criminal Code*, and that they are to avoid any complicity in mistreatment by foreign entities.





# INQUIRY OF MINISTRY DEMANDE DE RENSEIGNEMENT AU GOUVERNEMENT

PREPARE IN ENGLISH AND FRENCH MARKING "ORIGINAL TEXT" OR "TRANSLATION"  
PRÉPARER EN ANGLAIS ET EN FRANÇAIS EN INDIQUANT "TEXTE ORIGINAL" OU "TRADUCTION"

QUESTION NO./N° DE LA QUESTION Q-966	BY / DE M. Sean Casey (Charlottetown)	DATE 4 octobre, 2012
---	--	-------------------------

REPLY BY THE MINISTER OF PUBLIC SAFETY  
RÉPONSE DU MINISTRE DE LA SÉCURITÉ PUBLIQUE

Signé par l'honorable Vic Toews

PRINT NAME OF SIGNATORY  
INSCRIRE LE NOM DU SIGNATAIRE

SIGNATURE  
MINISTER OR PARLIAMENTARY SECRETARY  
MINISTRE OU SECRÉTAIRE PARLEMENTAIRE

QUESTION

En ce qui concerne la torture : a) quelle est la politique du gouvernement à l'égard de l'article 1.1 de la Convention contre la torture et autres peines ou traitements cruels, inhumains ou dégradants des Nations Unies; b) la politique du gouvernement et de ses organismes est-elle de considérer que le Canada doit s'opposer à toute violation de l'article mentionné à a); c) la politique du gouvernement est-elle de considérer que l'article 269.1 du Code criminel, y compris le paragraphe 4, est dans la logique des articles 1.1 et 1.2 de la Convention contre la torture et autres peines ou traitements cruels, inhumains ou dégradants des Nations Unies; d) la politique du gouvernement est-elle de considérer que la communication au Canada, par un tiers qui n'est pas un État ou par un État selon la définition que les Nations Unies en donnent, de renseignements obtenus par la torture est contraire à l'article mentionné à a) et peut constituer une violation de l'article 269.1 du Code criminel?

REPLY / RÉPONSE

ORIGINAL TEXT  
TEXTE ORIGINAL

TRANSLATION  
TRADUCTION

## Sécurité publique Canada

d) La politique du gouvernement relativement à l'échange d'information avec des pays étrangers lorsqu'il y a des risques de torture est une question du domaine public. Le gouvernement s'oppose catégoriquement à ce que de mauvais traitements soient infligés à quiconque par un organisme étranger, quel que soit le but visé.

En 2011, le ministre de la Sécurité publique a transmis des directives ministérielles exhaustives au Service canadien du renseignement de sécurité (SCRS), à la Gendarmerie royale du Canada (GRC) et à l'Agence des services frontaliers du Canada (ASFC) sur l'échange d'information avec des entités étrangères.

Les directives de 2011 sont fondées sur les obligations juridiques du Canada en matière d'échange d'information et font plus précisément référence à la Convention contre la torture et autres peines ou traitements cruels, inhumains ou dégradants et au *Code criminel*. Selon ces directives, le Canada n'approuve pas l'usage de la torture ou d'autres méthodes d'enquête illicites. Elles mentionnent explicitement que les organismes doivent agir dans le respect des lois et des obligations juridiques du

Canada, y compris l'article 269.1 du *Code criminel*, et qu'ils doivent éviter d'être complices de  
mauvais traitements infligés par des organismes étrangers.