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.*