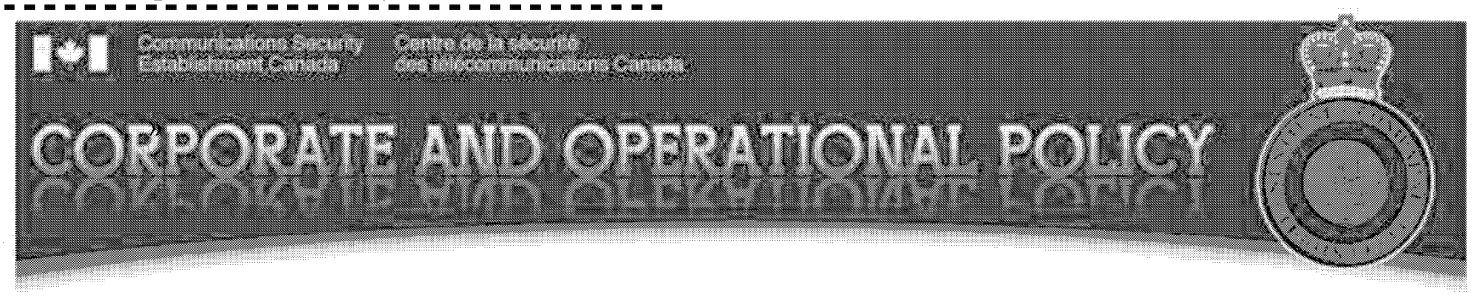




OPS-6: Policy on Mistreatment Risk Management

Effective Date: 5 November 2014

1. Introduction

1.1 Objectives

The objectives of this policy are to:

- Enable CSE to manage the risk of mistreatment of individuals when sharing information with foreign entities;
- Provide guidance on sharing information when risk mitigation is unclear or there is a substantial risk of mistreatment; and
- Ensure CSE applies a coherent and consistent approach when deciding whether or not to share information with foreign entities when doing so may give rise to a risk of mistreatment of an individual.

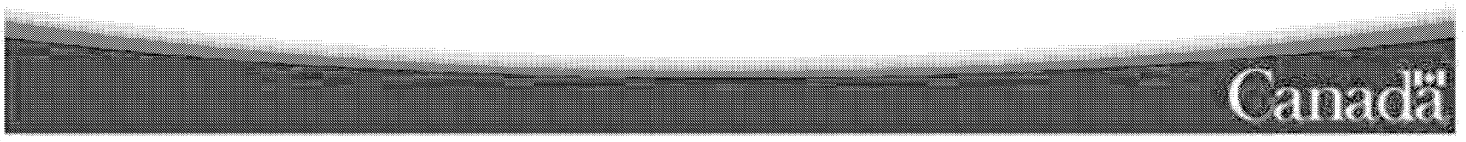
1.2 Context

Sharing information with foreign entities is essential to Canada's ability to respond to national security threats and is a formal obligation pursuant to Canada's adoption of various international resolutions and agreements. There is, however, an inherent risk that sharing information could result in the mistreatment of an individual.

Canada is party to a number of international agreements that prohibit torture and other forms of cruel, inhuman or degrading treatment or punishment (mistreatment), including the *International Covenant on Civil and Political Rights* and the *Convention Against Torture*. Torture is a criminal offence in Canada that has extraterritorial application and the *Criminal Code* prohibits activities that would amount to complicity in torture. More broadly, section 7 of the *Canadian Charter of Rights and Freedoms* (*Charter*) guarantees that everyone has the right to life, liberty and security of the person. Any information sharing linked to foreign torture could be found to violate section 7 of the *Charter*.

Cabinet Confidence *The Framework for Addressing Risks in Sharing Information with Foreign Entities* (The Framework) to manage the risk that sharing information with foreign entities could result in the mistreatment of an individual. Government of Canada (GC) departments and

Continued on next page



Introduction, Continued

Context (continued)

agencies must implement the Framework through Ministerial direction. Accordingly, the Minister of National Defence (the Minister) issued the Ministerial Directive – *Framework for Addressing Risks in Sharing Information with Foreign Entities* (Mistreatment Risk Management MD) to provide direction to CSE on the operationalization of the Framework. The MD requires that CSE develop policies to guide information sharing, including approval authorities that are commensurate with the risk of mistreatment.

1.3 Authority to Share Information

CSE's authority to share information stems from its authority in the *National Defence Act* (NDA) to:

- Acquire, retain and use information from the global information infrastructure for the purpose of providing foreign intelligence (part (a) of the mandate); and
- Provide advice, guidance and services to help ensure the protection of electronic information and information infrastructures of importance to the Government of Canada (GC) (part (b) of the mandate).

All information sharing must be in accordance with:

- The NDA;
- *The Framework* Cabinet Confidence
- *Ministerial Directive – Framework for Addressing Risks in Sharing Information with Foreign Entities* (21 November 2011) (Information Sharing MD);
- IRRELEVANT
- OPS-1: *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities;*
- OPS-1-1: *Procedures for the Release of Suppressed Information from SIGINT Reports;* and
- OPS-1-6: *Operational Procedures for Naming and Releasing Identities in Cyber Defence Reports.*

1.4 Scope

OPS-6 applies to any information that CSE is considering sharing with foreign entities [redacted] that could give rise to a risk of mistreatment. OPS-6 applies to both SIGINT and ITS information.

Continued on next page

Introduction, Continued

Scope (continued)

Types of information that could give rise to a risk of mistreatment include:

- SIGINT reports and sanitized SIGINT;
- Cyber Threat and Cyber Defence reports;
- Suppressed information;
- [redacted]
- Metadata; and
- Information from other government departments.

Information sharing that does not lead to the identification of an individual [redacted] does not require a Mistreatment Risk Assessment (MRA).

Note: [redacted]

1.5 Sharing Information from Other Entities

In accordance with the Framework, CSE is responsible for conducting an MRA when it shares information that originates from another government department [redacted] with a foreign entity.

Either SIGINT, ITS or DGPC is responsible for conducting the MRA, depending on how the information is being shared. See section 3.2 for more information.

1.6 Exemptions to OPS-6

OPS-6 does not apply to:

- **CSE information that GC departments and agencies wish to share with foreign entities.** Each GC department is responsible for managing the risk of information sharing with foreign entities, in accordance with the Framework and any departmental or Ministerial direction, as appropriate.

- **CSE information (including collection, analysis and reports) that Second Party partners intend to use solely in their national channels.** CSE's long-standing information-sharing protocols with Second Parties [redacted] are accounted for in a manner consistent with the Framework.

Continued on next page

Introduction, Continued

Exemptions to OPS-6 (continued)

- **Collection and unanalyzed metadata from [redacted] collection operations conducted by CSE [redacted] where the data is shared [redacted]**

- **Results from activities conducted [redacted] where the Chief is satisfied that the risk of mistreatment for the information sharing is low and has approved the sharing.**

> **Note: CSE must assess the mistreatment risk associated with sharing information and include a clause related to Mistreatment Risk Management (MRM) [redacted] The risk of mistreatment risk must be re-assessed annually, or sooner, if circumstances arise which call the existing assessment into question.**

1.7 Application

OPS-6 applies to CSE staff and other parties (such as secondees, integrees, contractors, students, and CFIOG personnel) when conducting activities under CSE authorities.

1.8 Consequences of Not Complying

Failure to comply with OPS-6 and follow MRM practices when sharing information could have extremely serious consequences, including:

- Risk of mistreatment to individuals;
- Severe damage to Canada's reputation; and
- Legal repercussions, such as civil action (a lawsuit against the GC in which the GC could be found liable) or criminal charges against CSE officials for complicity in torture.

It is imperative that CSE exercise due diligence, and be able to demonstrate that it has done so, when releasing information to foreign entities that may give rise to a risk of mistreatment.

Staff who do not comply with this policy will face management disciplinary sanctions, up to and including termination of employment.

Continued on next page

Introduction, Continued

1.9 Authority

This policy is issued under the authority of Chief, CSE, in accordance with section 273.62(2) of the NDA.

2. Policy

2.1 Principles

In accordance with the Framework and the Mistreatment Risk Management MD, when considering release of information to foreign entities, CSE must:

- Identify and assess the risk of mistreatment; and
- Ensure that approval authorities are commensurate with the risk of mistreatment that may result (see section 4.1 and Annex 1 for more information).

Where CSE has identified a substantial risk of mistreatment, CSE will:

- Examine and apply reasonable measures to mitigate the identified risk;
- Balance the residual risk with the need to share the information;
- Consider the threat to Canada's national security or other interests and the importance of sharing the information and;
- Seek approval for the information sharing from a Director General, Deputy Chief, or the Chief, as appropriate (see section 4.1 and Annex 1 for more information).

Attention: The Chief must approve all information sharing where there is a substantial risk of mistreatment and it is unclear whether the risk can be mitigated through the use of caveats, assurances or other means.

2.2 Information Sharing Requiring an MRA

An MRA is required when CSE shares information:

[redacted]

- Indirectly with a foreign entity through GC or Second Party partners; [redacted]

[redacted]

Continued on next page

Policy, Continued

Information Sharing Requiring an MRA (continued)

How the information is being shared will determine who conducts the MRA and the approval authority for the information sharing (see section 3.2 for more information).

Note: Indirect sharing is the transfer of CSE information to a foreign entity via a GC, Second Party [redacted]

2.3 Assessing Risk

Assessments cannot provide categorical assurances that mistreatment will not occur. However, strict conformity with the MRA process will ensure that CSE has considered relevant factors in its decision-making process and is taking reasonable and appropriate measures to mitigate the risk.

CSE may assess the risk of mistreatment as low, speculative or substantial.

2.4 Mistreatment by a Foreign Entity

If CSE becomes aware that information it has shared with a foreign entity has directly or indirectly led to mistreatment, it will:

- Document the incident, including information related to any non-compliance with caveats;
- Review its activities to determine if the information sharing was done in accordance with CSE policies;
- Propose appropriate action to prevent similar incidents in future (e.g., refraining from further sharing with the entity or addressing gaps in protocols that the incident identified);
- Consider consulting Department of Foreign Affairs, Trade and Development (DFATD) to lodge a protest with the foreign entity, either directly or indirectly through a Second Party partner;
- Inform GC clients that deal with the entity of the incident, as appropriate; and
- Notify the Chief, who may notify the Minister and CSE Commissioner as appropriate, of the incident and CSE's response.

Continued on next page

Policy, Continued

2.5 Reporting Requirements

On a quarterly basis, DG PC is required to report to the Chief on information sharing with [redacted] foreign entities requiring an MRA. These quarterly reports include:

- The number of requests to share information received, broken down by requestor and final recipient;
- How the information has been shared [redacted]
- The number of requests that have been approved (with requestor and final recipient identified);
- The number of requests that have been denied (with requestor and final recipient identified);
- The percentage of requests approved at each level (Manager, Director, Director General and Chief);
- The assessed risk associated with these requests; and
- Any known instances of a recipient's non-compliance with assurances and caveats.

To facilitate this reporting:

- Corporate and Operational Policy will maintain a record of *indirect* information sharing;
- [redacted]
- [redacted]

DG SIGINT Programs and Director PMO will provide this information to Corporate and Operational Policy on a quarterly basis for reporting to DG PC and the Chief.

2.6 Oversight and Accountability

DG PC is the MRA authority within CSE. DG PC maintains oversight of the MRA process and may review a sample from the MRA log on a quarterly basis to ensure information sharing is in accordance with OPS-6.

3. Sharing Information

3.1 Mistreatment Risk Assessment (MRA)

CSE employs a formal and comprehensive methodology to assess the potential risks of mistreatment of individuals as a result of sharing information with foreign entities. MRAs consist of:

- Reviewing CSE's records (including SIGINT reports) [redacted]
- Researching in multiple sources, including reviewing DFATD and Citizenship and Immigration Canada (CIC) assessments (where available);
- Analyzing the information against established criteria in order to evaluate the human rights record of the intended recipients of the information and the risk of detention (i.e. the likelihood that the recipient of the information will be able to detain the person involved);
- Verifying the existence of mistreatment risk considerations in any existing information sharing arrangements;
- Assessing the purpose of the information sharing;
- Assessing the anticipated effectiveness of any risk mitigation (see section 3.6 for more information); and
- Evaluating the foreign entity's compliance with past assurances, as per CSE's records.

Once the MRA is complete, CSE will assess the risk of mistreatment as low, speculative or substantial.

Note: CSE will catalogue all MRA and information sharing decisions based on these assessments. MRA documentation is subject to review by external bodies such as the CSE Commissioner and the Federal Court.

Continued on next page

Sharing Information, Continued

3.2 Who Conducts the MRA?

The following table outlines, according to the recipient and how the information is being shared, the responsibilities for conducting an MRA.

Recipient	How is the information shared?	Who conducts the MRA?
[redacted]		
[redacted] Foreign Entity	Indirectly (through a GC partner)	The GC partner sharing the information
[redacted] Foreign Entity	Indirectly (through a Second Party)	DGPC (with support from DGP / PMO)
[redacted]		

3.3 Low Risk

Information sharing is considered **Low Risk** when an analyst reasonably determines that mistreatment is unlikely. Being a signatory to the *Convention Against Torture* does not automatically render an entity low risk.

3.4 Speculative Risk

Information sharing is considered **Speculative Risk** when an analyst reasonably determines that mistreatment is possible but the assessment is based on theory or speculation. A determination of speculative risk is also appropriate where the recipient has a questionable human rights record or where there are concerns about the recipient's adherence to the *Convention Against Torture*.

A determination of speculative risk is not appropriate if an analyst concludes that mistreatment is likely (i.e. more likely than not) or where mistreatment is possible and, were it to occur, would result in severe harm.

Continued on next page

Sharing Information, Continued

3.5 Substantial Risk

Information sharing is considered **Substantial Risk** when it is reasonably concluded that there is a personal, present, and foreseeable risk of mistreatment. The assessed risk must be real and based on something more than theory or speculation. In most cases, the test for substantial risk will be satisfied when it is more likely than not that there will be mistreatment.

When the final recipient of the information has a poor human rights record and, if detained, the individual is likely to be mistreated, the risk must be assessed substantial.

> **Attention: The "more likely than not" test should not be applied too rigidly because in some cases, particularly where the risk of severe harm is possible, the "substantial risk" standard may be satisfied at a lower level of probability.**

3.6 Mitigating Risk

CSE will use mitigation measures to reduce the risk that an individual could be mistreated as a result of information shared by CSE. These mitigation measures must be limited to factors that are under its control or the control of Second Party partners, as warranted in the circumstances.

This includes:

- Using caveats to impose dissemination controls that prohibit recipients from sharing information or otherwise restricts use of the information;
- Obtaining assurances from the recipient or the Second Party intermediary that no mistreatment will occur;
- Editing the information to reduce the risk of mistreatment (such as suppressing or omitting identifying information of individuals); and
- Mandatory incorporation of human rights provisions in any information-sharing [redacted]

Continued on next page

Sharing Information, Continued

Mitigating Risk (continued)

In addition, CSE will identify any mitigating considerations, i.e., factors that are outside its control but that indicate a mitigated risk in sharing information.

For example, mitigating considerations include:

- Situational factors that would diminish the risk of mistreatment, such as:
  - Efforts by the recipient country to address past cases of mistreatment,
  - [redacted]
  - Modified detention processes that eliminate the risk of mistreatment, and
  - Guaranteed access to detainees;
- CSE's history of sharing with the recipient (this includes reviewing CSE's records to assess the foreign entity's compliance with past assurances and caveats);
- The foreign entity's history of lack of mistreatment or efforts to address past cases of mistreatment; and
- Observations or statements from GC or Second Party partners related to the recipient.

3.7 Unmitigated Risk

If the risk of mistreatment cannot be mitigated (i.e. the proposed mitigation measures are not likely to be effective) or if the risk remains substantial despite mitigation, the information sharing must be assessed as **Substantial Risk**.

3.8 Proportionality

Should the analysis determine that the risk remains substantial, CSE will consider the following, properly characterized in terms of its accuracy and reliability, when deciding whether to share information:

- The threat to Canada's national security or other interests, including 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 CSE's relationship with the foreign entity;
- The views obtained from DFATD;
- The status of other GC entities' relationships with the foreign entity, as appropriate; and
- Any other relevant facts that may arise in the circumstances.

Continued on next page

Sharing Information, Continued

3.9 Annex 2

Annex 2 [redacted]

[redacted]

3.10 Amendments to Annex 2

4. Approvals for Information Sharing

4.1 Approvals

In accordance with the Mistreatment Risk Management MD, approvals for information sharing are commensurate with the risk of mistreatment. When the information is not about a Canadian or person in Canada the approval levels are as follows:

Risk	Approval
[redacted]	
Low	Manager
Speculative	Director
Substantial – Mitigated	Director General or Deputy Chief
Substantial – Unmitigated or insufficiently mitigated	Chief or Minister

Approval authorities may not be delegated downward but may be exercised by anyone officially acting in the position or at a higher level. Nothing precludes a decision-maker from elevating the approval decision should they feel it is warranted.

For more information on approval authorities, see Annex 1.

4.2 Approvals: Information about Canadians

CSE employs a modified approval process for information sharing requests **when the information being shared relates to a Canadian or a person in Canada**.

In light of *Charter* considerations and in accordance with paragraph 273.64(2)(b) of the *National Defence Act*, the Director, Disclosure, Policy and Review (DPR) will, regardless of the MRA findings:

- Review all proposals to share information when the potentially affected person is a Canadian citizen, permanent resident of Canada or any entity in Canada;
- Consult the Directorate of Legal Services (DLS), if required; and
- Brief senior management on the proposal.

If concerns are identified, the decision to share information will require a higher level of approval, as determined by Director DPR. If no concerns are identified, the proposal can be approved in keeping with the levels identified for non-Canadians. These requests must be submitted via the Privacy and Interests Protection team (D2A).

5. Additional Information

5.1 Accountability for OPS-6

The following table outlines accountabilities for revising, reviewing, recommending, and approving this policy.

Who	Responsibility
Chief	• Approves this policy
Directorate of Legal Services	• Reviews for legal compliance • Provides legal advice, as required
Director PMO	• Recommends approval of this policy
DG PC	• Recommends approval of this policy • Ensures operational instructions for MRM are developed and implemented for DGPC
DG SIGINT Programs	• Ensures operational instructions for MRM are developed and implemented for SIGINT
Director, SIGINT Requirements (SPR)	• Recommends approval of this policy
Director, PMO	• Recommends approval of this policy • Ensures operational instructions for MRM are developed and implemented for ITS
Director, DPR	• Reviews this policy for consistency with the policy framework
Corporate and Operational Policy	• Revises this policy, as required • Responds to questions on this policy

5.2 References

- *National Defence Act*
- *Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment*
- *Criminal Code*
- *Canadian Charter of Rights and Freedoms*
- *Ministerial Directive on the Framework for Addressing Risks in Sharing Information with Foreign Entities* (21 November 2011)
- *Framework for Addressing Risks in Sharing Information with Foreign Entities* Cabinet Confidence

Continued on next page

Additional Information, Continued

5.3 Amendment Process

Situations may arise where amendments to this policy are required because of changing or unforeseen events. Significant amendments require the Chief's approval, though this approval may be delegated. Minor amendments may be approved by DG PC. DG PC may amend Annex 2 at any time.

5.4 Review

All CSE activities, including policies and procedures, are subject to management monitoring, audit and review by various government review bodies, including the CSE Commissioner and the Privacy Commissioner.

5.5 Questions

Questions regarding this policy should be addressed to [redacted]@cse-cst.gc.ca.

Annex 1: Approval Authorities and Accountability

A.1.1 Roles and Responsibilities

The following table sets out the roles and responsibilities within CSE for implementing this policy.

Who	Responsibility
Chief	• *Indirect sharing (SIGINT and ITS)*: In consultation with DG PC, approves or denies indirect information sharing where the risk of mistreatment is **substantial and unmitigated** • *Direct sharing (SIGINT)*: In consultation with DC SIGINT, approves or denies direct SIGINT information sharing where the risk of mistreatment is **substantial** • *Direct sharing (ITS)*: In consultation with DC ITS, approves or denies direct ITS information sharing where the risk of mistreatment is **substantial** • *Substantial Risk:* Seeks review by the Minister when there is a substantial unmitigated risk of mistreatment and the Chief determines the Minister should be the decision-making authority • *Mistreatment:* Informs the Minister and the CSE Commissioner, as appropriate, in the event that CSE information may have been linked to mistreatment by a foreign entity
DC SIGINT	• *Direct sharing (SIGINT)*: Advises the Chief on direct SIGINT information sharing where the risk of mistreatment is **substantial and unmitigated**
DC ITS	• *Direct sharing (ITS)*: Advises the Chief on direct ITS information sharing where the risk of mistreatment is **substantial and unmitigated**
DLS	• Provides legal advice, as required • Reviews this policy for compliance with the law

Continued on next page

Annex 1: Approval Authorities and Accountability, Continued

A.1.1 Roles and Responsibilities (continued)

Who	Responsibility
DG PC	• *Indirect sharing (SIGINT and ITS)*: Approves or denies *indirect* information sharing where the risk of mistreatment is **substantial but mitigated** • *Mistreatment:* Directs CSE's response if indirect sharing may have resulted in mistreatment, including notifying the Chief, DC SIGINT or DC ITS, and DLS • *Annex 2:* In consultation with DG SIGINT Programs, approves the Annex 2 [redacted] as well as any amendments • *Operational Instructions*: Ensures MRM operational instructions are developed and implemented for DGPC • *Oversight*: Maintains oversight of the MRA process
DG SIGINT Programs	[redacted]
DG Cyber Defence	

Continued on next page

Annex 1: Approval Authorities and Accountability, Continued

A.1.1 Roles and Responsibilities (continued)

Who	Responsibility
Director PMO	• *Reporting requirements:* Coordinates ITS's input to the quarterly reports to the Chief on information sharing
Director, DPR	• *Indirect sharing (SIGINT and ITS)*: Approves or denies indirect SIGINT and ITS information sharing where the risk of mistreatment is **speculative** • *Information about Canadians*: Reviews all requests that involve information about a Canadian or person in Canada
Manager, Corporate and Operational Policy	• *Indirect sharing (SIGINT and ITS)*: Approves or denies indirect SIGINT and ITS information sharing requests where the risk of mistreatment is **low** • *Indirect sharing (SIGINT and ITS)*: Receives and processes requests from Second Party partners for the indirect release of sanitized SIGINT, suppressed information, or other SIGINT-derived information to non-Second Party entities • *Annex 2*: In consultation with SIGINT, maintains and suggests changes to the Annex 2 [redacted]
Foreign Relations Coordinator	[redacted]
Manager ITS Programs, Oversight and Compliance (IPOC)	

Annex 2: [redacted]

A.2.1 Introduction

Annex 2 [redacted]

[redacted]

Note: DG PC may amend Annex 2 at any time.

Continued on next page

Annex 2: [redacted] Continued

A.2.1
Introduction

[redacted]