



# CORPORATE AND OPERATIONAL POLICY



## Policy and Communications (PC)

### Instruction

#### PCI-1

### Mistreatment Risk Management Process When Sharing Information With Foreign Entities

Effective Date: 17 April 2015

## CORPORATE AND OPERATIONAL POLICY

## 1. Introduction

---

**1.1 Operational Scope** These Operational Instructions apply to all DGPC staff, and are to guide the Mistreatment Risk Assessment (MRA) Process that must be performed for all information intended for release to a **foreign entity** that are:

- Based on traffic collected by Communications Security Establishment Canada (CSE); and/or
- Based on any CSE reporting or other information.



---

**1.2 Objective** These Operational Instructions are to provide guidance regarding the interpretation and application of OPS-6, *Mistreatment Risk Management Policy*.

---

**1.3 Application** These Operational Instructions apply to requests from Second Party agencies that require CSE permission to share sanitized text with foreign entities or to act on intelligence.

---

## CORPORATE AND OPERATIONAL POLICY

## 2. Mistreatment Risk Assessment Process

---

### Overview

---

#### 2.1 MRA Requirement

The completion of an MRA is required when information derived from CSE:

- Is to be shared with a foreign entity; and
- Identifies, or relates to, one or more individuals.

The MRA process should be undertaken on a case-by-case basis, as the various components of the proposed sharing may be of different import, depending on circumstances. As such, each portion of the MRA must be evaluated in the context of the instance proposed.

---

#### 2.2

#### 2.3 Release to Foreign Entity via Other Government Department

When the final release to a foreign entity will be done by another Government of Canada (GC) entity other than CSE, that other GC entity is responsible for conducting the MRA. CSE will include the appropriate approved caveats located on CSE's [REDACTED]

---

#### 2.4 Basics of the Form Assessment Criteria

When an MRA is required, the *Mistreatment Risk Assessment and Recommendation Form* (guidelines found in Annex 1) must be prepared to assist in decision making. The *Form* contains four distinct categories of information:

- Request Facts;
- Risk Assessment Criteria;
- Ministerial Directive Factors; and
- Recommendations and Approvals.

The criteria against which the decision must be assessed comprise a variety of factors, including, but not limited to:

- The risk of detention of the individual in question;
  - The human rights record of the entity in question;
- 

*Continued on next page*

## CORPORATE AND OPERATIONAL POLICY

## Overview, Continued

**2.4 Basics of the Form Assessment Criteria**  
(continued)

- The previous history of information exchanges with the entity; and
- The potential for action-on based on the information being exchanged.

See sections 2.5 and 2.6 for more information.

**2.5 Exceptional Circumstances**

There are no exceptional circumstances where CSE may release intelligence without assessing the risk of torture or other cruel, inhumane, or degrading punishment. However, the following exception to the assessment process may be applied:

If the request is...	Then...
Time sensitive	Authorities may be verbally briefed and, if so, the <i>Form</i> is filled out post factum.
Not time sensitive	The request should be reviewed and processed in compliance with the standard procedure as outlined in these Operational Instructions.

## Human Rights Record

**2.6 Researching Human Rights Records**

The following sources must be consulted, if available, to determine the human rights record of any particular country/entity:

- [REDACTED] (Annex 2);
- Department of Foreign Affairs Trade and Development (DFATD) Human Rights Reports;
- United States State Department Human Rights Reports;
- Canada Security Intelligence Services (CSIS) [REDACTED] and [REDACTED]
- SIGINT end product reporting related to mistreatment released in the previous 365 days.

Any other relevant materials from credible and objective sources, including the reports of Second Parties, may be used at the discretion of the analyst.

## CORPORATE AND OPERATIONAL POLICY

## Human Rights Record, Continued

## 2.7 Risk of Detention

The analyst must consider, in assessments, the possibility that the identified individual(s) may be detained.

The risk of detention must be weighed in the context of:

- The human rights record of the entity in question;
- The relationship between the information to be exchanged and the potential for detention;
- Any unique circumstances (i.e. social, cultural, ethnic) which could impact on the potential for detention;
- The uniqueness of the information with regard to the individual in question (e.g., sole source reporting); and
- Any other facts deemed relevant by the analyst or the recommending or approving authority.

## Mistreatment Risk Assessment

## 2.8 Form Criteria

The *MRA Form* outlines information relevant to all factors associated with the information sharing request being considered. It assesses the human rights record of the recipient entity and the quality of information being provided. This allows CSEC to assess the recipient's capabilities to respond to the information and the **likelihood** the person's safety will be endangered in the process. A guideline for completing the *Form* is referenced in Annex 1.

Each instance of proposed information sharing must be evaluated in its unique context; for example, an entity may be a signatory to the *Convention Against Torture (CAT)* (Annex 4), yet have a poor human rights record regarding a specific minority group. In a case such as this, proposed information exchanges that relate to the minority group would be potentially riskier, and may require a higher level of approval or more concrete assurances from the proposed recipient.

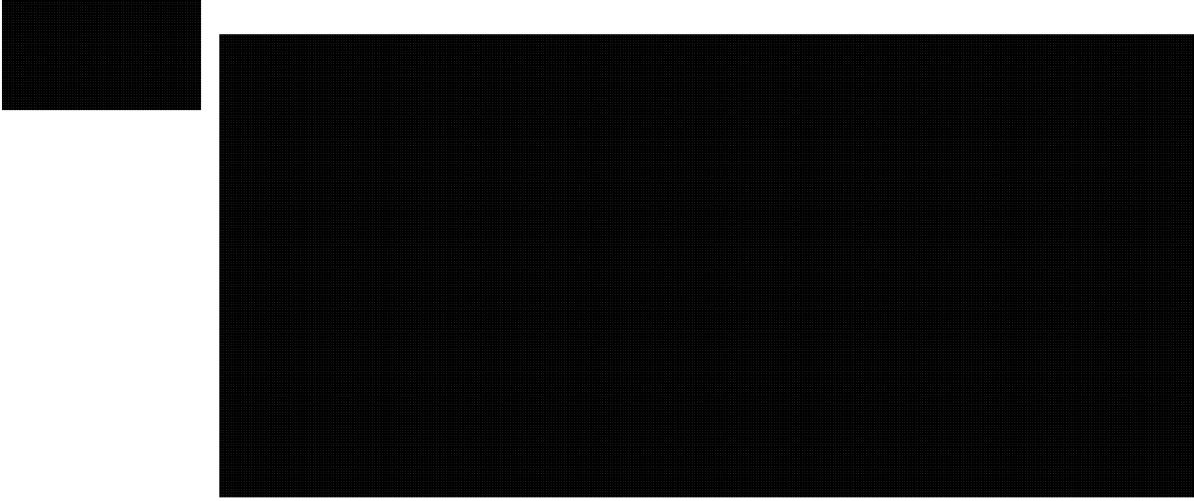


**Attention:** Complete only as many sections of the *Form* as required to derive a reasonable assessment of the mistreatment risk.

## CORPORATE AND OPERATIONAL POLICY

**Mistreatment Risk Assessment Process, Continued**

---

**2.9**As outlined in Annex 2:  
**2.10 Low Risk**


A complete mistreatment risk assessment incorporates factors such as the purpose of the proposed sharing, the value of the intelligence to be shared, and the risk of detention arising from the information sharing. Where the analysis determines that the abovementioned criteria are less likely to enable the mistreatment of an individual, the risk is deemed to be **Low Risk**.

It is important to note that being a signatory to the *CAT* does not automatically render an entity Low Risk. The purpose of the information sharing must be evaluated in each instance and assessed against the materials available to derive a rational risk evaluation.

---

**2.11 Speculative Risk**

When some of the criteria raise suspicion that the wellbeing of the identified individual(s) may be compromised, such as if the final recipient entity has a questionable human rights record, the analyst must consider the risk that the individual will be detained in addition to the risk of mistreatment.

**Speculative Risk** exists in situations where an assessment of the possibility of mistreatment is made. It may also include situations where the final recipient entity can be described as  Such entities intend to conform to international agreements such as the *CAT*, but concerns still exist surrounding the likelihood of mistreatment of any individual(s).

---

## CORPORATE AND OPERATIONAL POLICY

## Mistreatment Risk Assessment Process, Continued

- 2.12 Substantial Risk** When the final recipient has a poor human rights record and, if detained, the individual(s) is/are likely going to be mistreated, the risk is assessed as “Substantial.”

**Substantial Risk** is defined by a risk of mistreatment that is real and based on more than theory or speculation (i.e. it is more likely than not there will be mistreatment). There is no reasonable expectation of the country’s conformity to the *United Nations Convention on Human Rights*.



**Note:** The more-likely-than-not test should not be rigidly applied, as the assessment of “Substantial” may be satisfied at a lower probability when there is a risk of severe harm to the individual(s).

- 2.13 Mitigation** The *Framework for Addressing Risks in Sharing Information with Foreign Entities* requires CSE to address the proposed measures to mitigate any known risk of mistreatment, where the risk is believed to be **substantial**.

Mitigation measures must be limited to factors that are in the control of CSE or Second Parties. These include, but are not limited to:

- Caveats;
- Modifications to the proposed form of words that may decrease the risk of detention;
- Assurances offered by the Second Party and/or foreign entity guaranteeing that no mistreatment will occur; and
- History of information sharing with the foreign entity that demonstrates the recipient country’s adherence to caveats and conditions stipulated in previous instances of information sharing.

- 2.14 Additional Measures** If one or more of these measures are met, the risk of mistreatment may be assessed as “Substantial – Mitigated,” depending on the case-specific circumstances. The analyst may additionally consider precedent, where it exists, to mitigate the risk of mistreatment.

## CORPORATE AND OPERATIONAL POLICY

**Mistreatment Risk Assessment Process, Continued**

**2.15 Unmitigated Risk** If the risk cannot be mitigated to a satisfactory extent, the risk of mistreatment is subsequently classified as “Substantial – Unmitigated.”

**2.16 Approval for MRAs** The following table outlines the approval authority for MRAs.

Risk Assessment	Form is reviewed by...	Decision to release...
Low	Privacy and Interests Protection (D2A) Supervisor	Manager, COP*
Speculative	Manager, COP	Director, DPR*
Substantial – Mitigated	Director, DPR Legal Services (DLS) (optional)	DG PC
Substantial – Unmitigated	DG PC DLS (optional)	Chief, CSE*
Substantial – Unmitigated (Special Case)	DLS Chief	Minister of National Defence

\*Authority may not be downward delegated, but may be exercised by anyone officially acting in the position, or by a someone in a superior position

**2.17 Caveats** If Privacy and Interests Protection personnel share information with a requester from either another GC department or with Second Parties, appropriate **caveats must be applied**. These are available in the D2 Action Primer on the [REDACTED]



## CORPORATE AND OPERATIONAL POLICY

### 3. Additional Information

#### 3.1 Accountability

The following table outlines responsibilities with respect to these instructions

Who	Responsibility
Director General, Policy and Communications (DG PC)	<ul style="list-style-type: none"> <li>• Approves</li> </ul>
Director, Disclosure, Policy and Review (Dir, DPR)	<ul style="list-style-type: none"> <li>• Recommends</li> </ul>
Manager, Corporate and Operational Policy (COP)	<ul style="list-style-type: none"> <li>• Revises these instructions</li> <li>• Ensures staff compliance</li> </ul>
Privacy and Interests Protections Team (D2A) Staff	<ul style="list-style-type: none"> <li>• Complies with these instructions and any amendments to these instructions</li> </ul>
Policy Management	<ul style="list-style-type: none"> <li>• Responds to any questions</li> </ul>

#### 3.2 References

The following materials were consulted in the authorship of this Instruction:

- 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*;
- OPS-6, *Mistreatment Risk Management Policy*.

#### 3.3 Amendments

Situations may arise where amendments to these instructions may be required because of changing or unforeseen circumstances. Any amendments to these instructions will be communicated to relevant staff and posted on the CSE intranet. All amendments are subject to audit and review.

#### 3.4 Review and Audit

The implementation of this policy is subject to internal audit and external review by various government review bodies, including the CSE Commissioner.

#### 3.5 Enquiries

Questions and concerns related to policy can be sent to the Policy Management team at [REDACTED]@cse-cst.gc.ca.

All questions regarding the application of these instructions should be directed to the supervisor of the Privacy and Protection Interests team at [REDACTED]@cse-cst.gc.ca.

CORPORATE AND OPERATIONAL POLICY

Examples of Mistreatment Risk Assessment Scenarios

Assessment Risk	Criteria
Low	
Medium	
High	

## CORPORATE AND OPERATIONAL POLICY

## Annex 1. Mistreatment Risk Assessment and Recommendations Form Guidelines

**A1.1 Template** A template of this Form that may be completed with case-specific details is found on the [REDACTED] [CERRID #1022412].

**NOTE:** [REDACTED]  
[REDACTED] [CERRID #1231619].

**A1.2 Guidelines** This table provides brief instruction on completing the Form. Please note that the level of detail required corresponds to the mistreatment risk.

Section	Instruction
<i>Request Facts</i>	
Background	Present the following text: “As per Ministerial Direction, CSE must consider its imperative to share information against the risk that such provision would give rise to mistreatment of an individual.”
Form of Words	Insert the Client’s proposed wording to be released.  <b>NOTE:</b> This wording may change based on input from equity stakeholders such as Corporate and Operational Policy or reporting teams. Further changes to the proposed text may require additional stakeholder approval.
Second Party Partner (Requester/Client)	Name the Second Party agency/department of CSE internal Client.
[REDACTED]	
Action-On (Purpose for release)	Identify the intentions of the Client if the information is approved for release.
Justification	Identify the purpose and benefit of sharing, as provided by the Client.
Material Consulted	List all material that CSE consulted which lead to the assessment of any mistreatment risk. A list of research materials is found in Section 2.5.
HR Conventions Signed	Indicate whether the final recipient is a signatory to the <i>CAT</i> (Annex 3), and any additional relevant human rights conventions.

*Continued on next page*

## CORPORATE AND OPERATIONAL POLICY

## Mistreatment Risk Assessment and Recommendations Form Guidelines, Continued

Section	Instruction
<i>Request Facts</i>	
HR Enshrined in Law	Indicate whether the final recipient has any domestic laws to address mistreatment.
Enforcement of Laws	Indicate whether the final recipient regularly enforces its laws addressing mistreatment.
<i>Risk Assessment Criteria</i>	
Overall Assessment	<p>Enter one of the following risk classifications based on the mistreatment risk and the effect of mitigating factors:</p> <ul style="list-style-type: none"> <li>• Substantial – Unmitigated</li> <li>• Substantial – Mitigated</li> <li>• Speculative</li> <li>• Low [REDACTED]</li> <li>• [REDACTED]</li> </ul>
Mistreatment Risk (Ministerial Directive Criteria 4. The rationale for believing that there is a substantial risk that sharing the information would lead to the mistreatment of an individual)	<p><b>HR Record of Recipients</b> Summarize all material consulted that identifies human rights concerns related to the final recipient country.</p> <p><b>A Priori Knowledge</b> State any information likely previously known about the identified individual(s) by the final recipient agency. This may include previously released SIGINT known to CSE.</p> <p><b>NOTE:</b> This content is based only on CSE's current knowledge and may not necessarily reflect the reality.</p> <p>[REDACTED]</p> <p>List all specific intelligence included in the proposed form of words that could be used [REDACTED] It may be necessary to evaluate [REDACTED] in order to assess the actionable nature of the intelligence.</p> <ul style="list-style-type: none"> <li>• <i>High Quality:</i> Examples include [REDACTED]</li> <li>• <i>Medium Quality:</i> Examples include [REDACTED]</li> <li>• <i>Low Quality:</i> For example, [REDACTED]</li> </ul>

Continued on next page

## CORPORATE AND OPERATIONAL POLICY

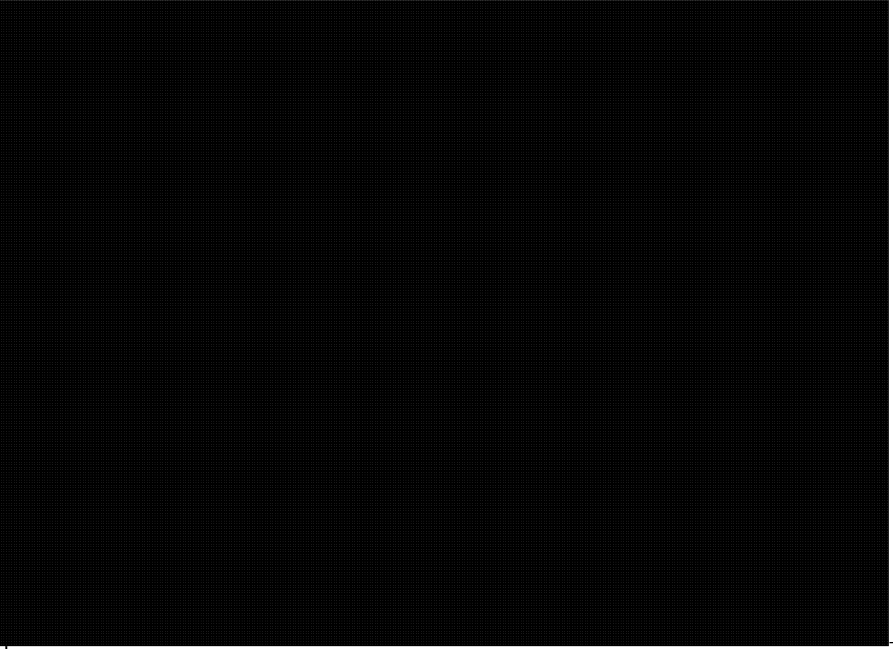
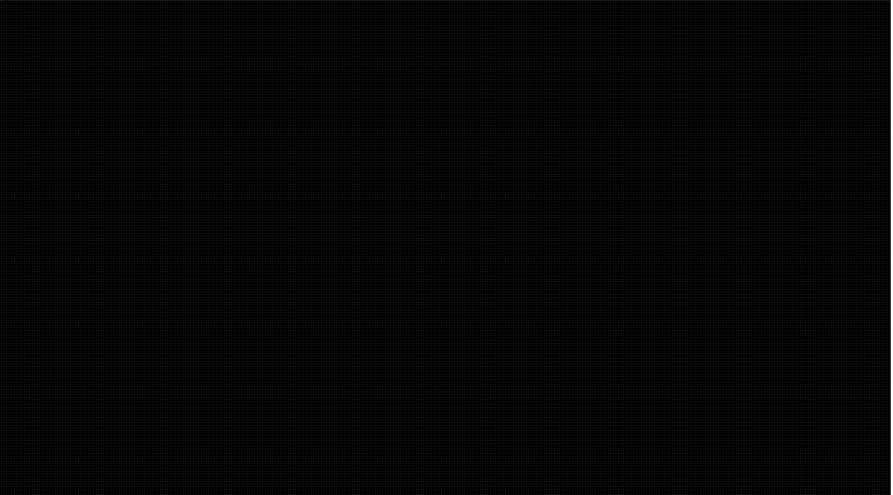
## Mistreatment Risk Assessment and Recommendations Form Guidelines, Continued

Section	Instruction
	<i>Risk Assessment Criteria</i>
Mistreatment Risk (Ministerial Directive Criteria 4. The rationale for believing that there is a substantial risk that sharing the information would lead to the mistreatment of an individual)	<p><b>Quality of Identity Information</b> Assess the quality of the identity information in the form of words which may or may not allow for the true identification of the named individual(s).</p> <ul style="list-style-type: none"> <li>• <i>High Quality:</i> [REDACTED]</li> <li>• <i>Medium Quality:</i> [REDACTED]</li> <li>• <i>Low Quality:</i> [REDACTED]</li> </ul> <p><b>Likelihood of Success</b> [REDACTED] Assess the likelihood that, should the final recipient agency decide to action the intelligence [REDACTED] [REDACTED]</p> <p><b>Likelihood of Recipient Response/Action</b> Assess the likelihood that the final recipient agency would action the intelligence. This may include a consideration of whether the individual is a priority for the security community in that country, or whether there is a Second Party military presence [REDACTED] in the recipient country.</p> <p><b>Detention Risk</b> Evaluate the risk that, should the individual(s) be [REDACTED] apprehended, that the recipient agency would choose to detain them. Consult section 2.6 for further information on classifying this risk.</p> <p><b>Mistreatment Risk</b> Assess the overall risk that the final recipient agency would subject the individual(s) to mistreatment.</p> <ul style="list-style-type: none"> <li>• Substantial – Mitigated</li> <li>• Speculative</li> <li>• Low [REDACTED]</li> <li>• [REDACTED]</li> </ul>

Continued on next page

## CORPORATE AND OPERATIONAL POLICY

# Mistreatment Risk Assessment and Recommendations Form Guidelines, Continued

Section	Instruction
<i>Ministerial Directive Criteria</i>	
1. The threat to Canada's national security or other interests, and the nature and imminence of that threat	Consider the following under this factor: 
2. The importance of sharing the information, having regards to Canada's national security or other interests	Consider the following under this factor: 

Continued on next page

## CORPORATE AND OPERATIONAL POLICY

# Mistreatment Risk Assessment and Recommendations Form Guidelines, Continued

Section	Instruction
<i>Ministerial Directive Criteria</i>	
3. The status of the relationship with the foreign entity with which the information is to be shared	<p>Consider the following under this factor:</p> <ul style="list-style-type: none"> <li>• The GC's relationship with the final recipient entity and/or agency, including DFATD's assessment (if available);</li> <li>• CSE's relationship with the final recipient entity and/or agency;</li> <li>• CSIS's relationship with the final recipient entity and/or agency; and</li> <li>• Second Party relationships with the final recipient entity.</li> </ul>
4. The proposed measures to mitigate the risk, and the likelihood that these measures will be successful	<p>List and explain any proposed measures to mitigate the risk of mistreatment.</p> <p>Some examples of mitigation measures can be referenced in Sections 2.11-2.12.</p>
Caveat	A list of approved caveats for sanitizations involving MRAs can be found on the [REDACTED] Insert all applicable.
Other Mitigating Factors	List any additional approaches that are applicable.
Effect of Mitigating Factors	Explain the justification for accepting the mitigating factors as listed above.
5. The views of DFATD	These should be referenced under Criteria #4 if they are available at the time of the assessment.
6. The views of other departments and agencies, as appropriate, and any other relevant facts that may arise in the circumstances.	These will likely be referenced under Criteria #4. If there are outstanding views that should be included, list them here.

Continued on next page

## CORPORATE AND OPERATIONAL POLICY

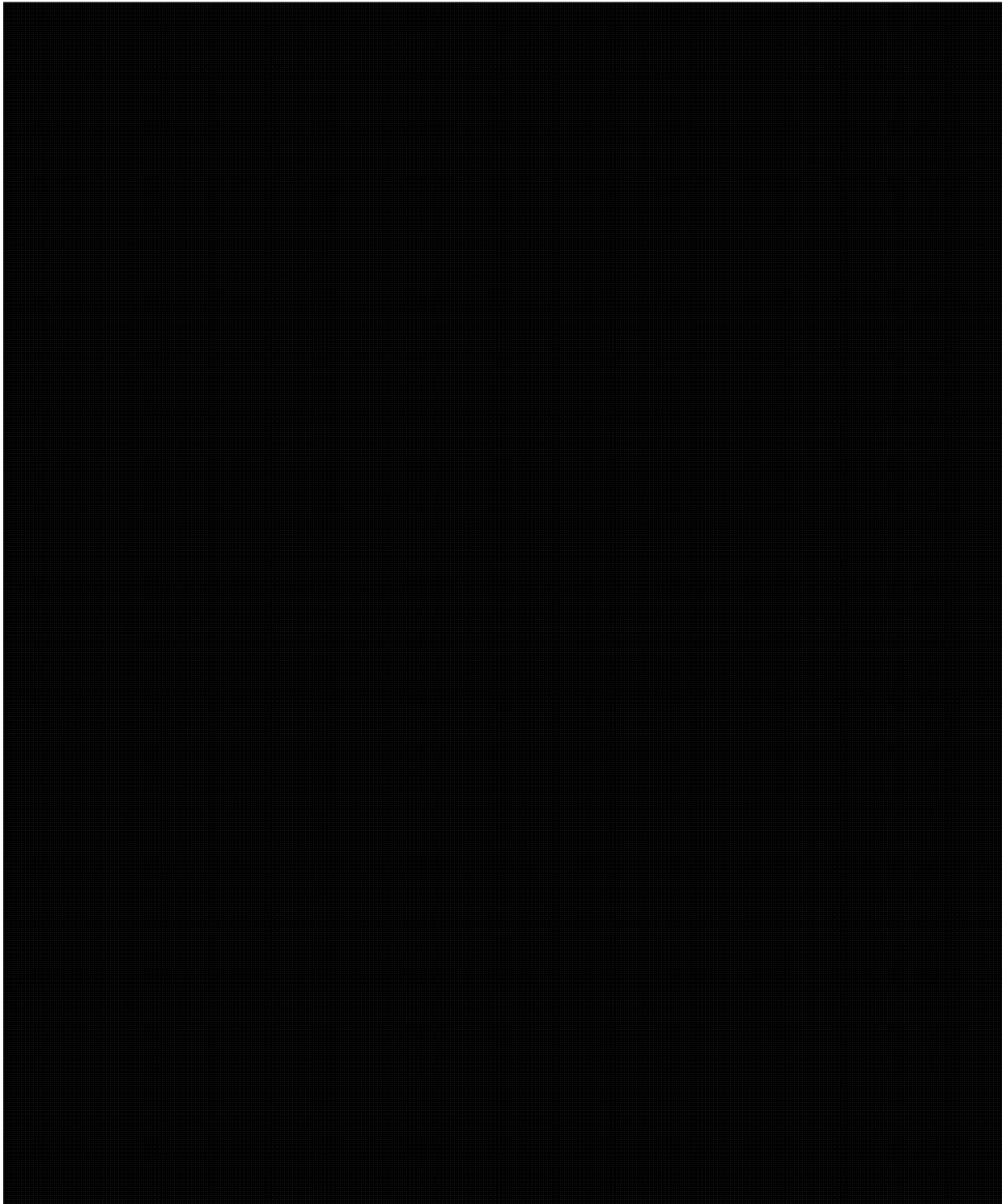
# Mistreatment Risk Assessment and Recommendations Form Guidelines, Continued

Section	Instruction
<i>Required Information for All Risk Levels</i>	
Report Serial Numbers	List the reporting serial number(s) relevant to the sanitization request.
Release Language (CSEC)	If the release is approved, include the MRA caveat that will accompany it.
DGI Consultation	State whether a consultation with DGI occurred, and its outcome.
Source(s)	List the SIGINT or HUMINT sources from which the intelligence was gained.
DLS Consult	State whether DLS was consulted, and the outcome of that consultation.
Recommendations	Ensure there is space for each appropriate authority (dependent on risk level) to recommend or approve/deny the release.



# CORPORATE AND OPERATIONAL POLICY

## Annex 2.



*Continued on next page*

## CORPORATE AND OPERATIONAL POLICY

**Annex 2.**

Continued



**A2.5 Review**

DG PC must review the validity [REDACTED] annually and notify the Manager, Corporate and Operational Policy of any amendments.

## CORPORATE AND OPERATIONAL POLICY

## Annex 3. List of Signatories to the Convention Against Torture

### A3.1 Background

The UN *Convention Against Torture* requires parties to take effective legislative, administrative, judicial, or other measures to prevent acts of torture in any territory under its jurisdiction.

The CAT can be referenced at  
<http://www.ohchr.org/EN/ProfessionalInterest/Pages/CAT.aspx>

### A3.2 Signatories

The following table lists parties to the CAT; current as of 27 December 2012.

Shaded countries are also parties to the *International Covenant on Civil and Political Rights*, which requires parties to recognize that no one shall be subjected to torture or to cruel, inhuman or degrading punishment. The full *Covenant* can be found at

<http://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx>

Afghanistan	Brazil	Denmark	Honduras	Lithuania
Albania	Bulgaria	Djibouti	Hungary	Luxembourg
Algeria	Burkina Faso	Ecuador	Iceland	Madagascar
Andorra	Burundi	Egypt	Indonesia	Malawi
Antigua & Barbuda	Cambodia	El Salvador	Ireland	Maldives
Argentina	Cameroon	Equatorial Guinea	Israel	Mali
Armenia	Canada	Estonia	Italy	Malta
Australia	Cape Verde	Ethiopia	Japan	Mauritania
Austria	Chad	Finland	Jordan	Mauritius
Azerbaijan	Chile	France	Kazakhstan	Mexico
Bahrain	China	Gabon	Kenya	Monaco
Bangladesh	Colombia	Georgia	Kuwait	Mongolia
Belarus	Congo	Germany	Kyrgyzstan	Montenegro
Belgium	Costa Rica	Ghana	Latvia	Morocco
Belize	Cote d'Ivoire	Greece	Lebanon	Mozambique
Benin	Croatia	Guatemala	Lesotho	Namibia
Bolivia	Cuba	Guinea	Liberia	Nepal
Bosnia & Herzegovina	Cyprus	Guyana	Libya	Netherlands
Botswana	Czech Republic	Holy See	Liechtenstein	New Zealand

*Continued on next page*

## CORPORATE AND OPERATIONAL POLICY

### Annex 3. List of Signatories to the Convention Against Torture, Continued

Nicaragua	Portugal	Senegal	Swaziland	Turkmenistan
Niger	Qatar	Seychelles	Sweden	Uganda
Nigeria	Republic of Korea	Sierra Leone	Switzerland	Ukraine
Norway	Republic of Moldova	Slovakia	Tajikistan	United Kingdom
Panama	Romania	Slovenia	TFYR Macedonia	Uruguay
Paraguay	Russia Federation	Somalia	Thailand	Uzbekistan
Peru	Rwanda	South Africa	Timor-Leste	Venezuela
Philippines	San Marino	Sri Lanka	Togo	Yemen
Poland	Saudi Arabia	St. Vincent & Grenadines	Turkey	Zambia

#### A3.3 Additional Information

A spreadsheet containing a complete list of signatories to certain United Nations human rights conventions can be found at



[CERRID #589012].

## CORPORATE AND OPERATIONAL POLICY

## Annex 4. Mistreatment Risk Assessment Process Decision Tree

