s.15(1) - DEF

Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

s.69(1)(c)

SECRET
CERRID #654672
CCM#11-03080

NOV 15 2011

MEMORANDUM FOR THE MINISTER OF NATIONAL DEFENCE

Ministerial Directive to Operationalize the Framework for Addressing Risks in Sharing Information with Foreign Entities

(For Approval)

Summary

- This Memorandum seeks your approval of the attached Ministerial Directive (MD) to operationalize the Framework for Addressing Risks in Sharing Information with Foreign Entities (the Framework), as attached as Annex A.
- This Framework establishes a consistent process of decision making by Deputy Heads and Agency Heads in cases where sharing information with foreign entities may give rise to a substantial risk of mistreatment.
- CSEC is one of five departments and agencies in the security and intelligence community required to implement the Framework through ministerial direction [redacted] The purpose of separate MDs is to address each organization's unique operational needs while remaining consistent with the approved Framework.
- In the case of CSEC, the proposed MD remains consistent with the Framework while proposing to recognize CSEC's unique operational needs as a foreign signals intelligence (SIGINT) agency and its [redacted]
- It is recommended that you approve the attached proposed MD.

Background

- For CSEC, [redacted] the objective of this MD is to focus on operationalizing the Framework. The MD includes all direction from the Framework that is applicable to CSEC and is tailored in the following ways:

- The MD applies to direct and indirect information sharing with foreign entities [redacted]
  - In comparison to other implementing departments and agencies, CSEC has not requested inclusion in the MD of any additional direction on the use of information derived from mistreatment, which is beyond the operational scope of the approved Framework. As CSEC principally deals in information that is derived from SIGINT intercept, it is highly unlikely that the organization would be in receipt of information derived from mistreatment. The majority of SIGINT information CSEC receives is from our Five-Eyes partners [redacted]
  - The Framework directs that agencies assess the reliability and accuracy of information received, and to characterize this information in further dissemination. The MD recognizes that CSEC is a foreign SIGINT agency and not an intelligence assessment agency and therefore directs CSEC to use caveats to address this Framework requirement, as appropriate.
  - Finally, the language in the MD recognizes the unique nature of CSEC's role, [redacted]

- Once CSEC has an MD in place, it will join the Canadian Security Intelligence Service, the Royal Canadian Mounted Police, and the Canadian Border Services Agency who now have Ministerial Directives in place. CSEC will codify in policy interim Human Rights impact assessments and approval protocols that we have been applying to existing sanitization, [redacted] and release policy requirements in the absence of an MD.
- DND/CF is also making substantial progress on developing an MD to implement the Framework in a manner tailored to recognize the unique operational needs of a military organization. This includes the recognition that a number of international law frameworks not expressly referenced in the approved Framework (i.e. International Human Rights Law and the Law of Armed Conflict) have application to CF activities conducted overseas. For DND/CF this MD has the broader objective of providing direction on overall information sharing with foreign entities.

Recommendation

- It is recommended that you approve and sign the attached Ministerial Directive on the Framework for Addressing Risks in Sharing Information with Foreign Entities.

Next Steps

- Should you approve the MD, CSEC will:
    - Implement the Framework through revisions to current operational policy that will reflect the direction in this MD;
    - Keep you informed of any issues related to the implementation of this directive that warrant your consideration; and
    - Provide a copy of the MD to the CSE Commissioner.

John Adams
Chief

Attachment

I concur with the recommendation:

Stephen Rigby
National Security Advisor to the Prime Minister
Privy Council Office

cc: Robert Fonberg, Deputy Minister, National Defence

Framework for Addressing Risks in Sharing Information with Foreign Entities[1]

- Sharing information with foreign entities is necessary in order to respond to national security threats. It is essential that Canadian intelligence and law enforcement authorities are able to maintain strong relationships with foreign entities, and can share information with them on both a routine and an urgent basis.

- Deputy Ministers and Agency Heads have been delegated the responsibility for making decisions with respect to the sharing of information with foreign entities.[2] Departments and agencies must carefully manage relationships with foreign entities, assisted by policies that guide information sharing practices, to ensure that the sharing of information does not give rise to a substantial risk of mistreatment.

Objective

- The following Framework forms part of the suite of directives and policies that govern departments' and agencies' information sharing practices. The objective is to establish a coherent and consistent approach across the Government of Canada in deciding whether or not to send information to, or solicit information from, a foreign entity when doing so may give rise to a substantial risk of mistreatment of an individual.

Canada's Obligations

- 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* (*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.

---

[1] This Framework 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.

[2] For the purpose of this Framework, Deputy Minister also includes the Chief of Defence Staff.

- 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.

- 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.

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.

Information Sharing Principles

- Sharing information with foreign entities is an integral part of the mandates of Canadian intelligence and law enforcement authorities. It is also a formal obligation pursuant to Canada's adoption of various international resolutions and agreements.

- In sharing information, departments and agencies must act in a manner that complies with Canada's laws and legal obligations.

- Departments and agencies must assess and mitigate potential risks of sharing information in ways that are consistent with their unique roles and responsibilities.

- Departments and agencies must also assess the accuracy and reliability of information received, and properly characterize this information in any further dissemination.

- The approval level that departments and agencies require 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.

- Departments and agencies also have a responsibility to keep their respective Ministers generally informed about their information sharing practices.

Decision Making Process

- Departments and agencies are responsible for establishing approval levels that are proportionate to the risks in sharing information with foreign entities. This Framework only 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 responsible Deputy Minister or Agency Head for decision.

- In making his or her decision, the Deputy Minister or Agency Head 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 responsible Deputy Minister or Agency Head may refer the decision whether or not to share information with the foreign entity to his or her Minister, in which case the Minister will be provided with the information described above.

- The Deputy Minister/Agency Head or Minister shall authorize the sharing of information with the foreign entity only in accordance with Canada's legal obligations.

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.

Implementation

- Given the different mandates of departments and agencies, the Framework will be operationalized through individual Ministerial directions.

National Defence
Défense nationale

National Defence Headquarters
Ottawa, Ontario
K1A 0K2

Quartier général de la Défense nationale
Ottawa (Ontario)
K1A 0K2

To: Chief, Communications Security Establishment

Ministerial Directive
Communications Security Establishment
Framework for Addressing Risks in Sharing Information with Foreign Entities[1]

1. Preamble

This Directive is issued under my authority as Minister responsible for the Communications Security Establishment (CSE). This Directive provides direction to CSE on the operationalization of the *Framework for Addressing Risks in Sharing Information with Foreign Entities*,

This directive recognizes the unique roles and responsibilities of CSE in relation to information sharing with foreign entities where such sharing may give rise to a risk of mistreatment. The CSE intelligence mandate is focussed on foreign signals intelligence (SIGINT) collection and reporting to Government of Canada clients in accordance with the Government's intelligence priorities.

Sharing information with foreign entities is necessary to fulfill the CSE mandate. It is essential that CSE be able to maintain strong relationships with foreign entities, and can share information with them on both a routine and an urgent basis. CSE must carefully manage relationships with foreign entities, assisted by policies that guide information sharing practices, to ensure that the sharing of information does not give rise to a substantial risk of mistreatment.

[1] This Ministerial Direction would not change existing legal authorities for sharing information with foreign entities. Although the term foreign entity is not formally defined in the Framework, the term entity is defined in the CSEC legislative framework to mean "a person, group, trust, partnership or fund or an unincorporated association or organization and includes a state or political subdivision or agency of a state." Accordingly, a foreign entity in the context of this directive would include any entity within the meaning of this definition that is not Canadian. The sharing of information with Canadian entities is not subject to this directive.

Canada

[redacted]

As Chief, CSE and the agency head with management and control of the Establishment and all matters relating to it under the CSE legislative framework, you are responsible for making decisions with respect to the sharing of information with foreign entities where there is a substantial risk of mistreatment.

2. Background and Context

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* (CAT). 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.

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.

3. 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 rigidly applied 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.

4. Principles for Sharing Information with Foreign Entities

Sharing information with foreign entities is an integral part of the mandates of Canadian intelligence and law enforcement authorities, including CSE. It is also a formal obligation pursuant to Canada's adoption of various international resolutions and agreements.

In sharing information, CSE must act in a manner that complies with Canada's laws and legal obligations.

CSE must assess and mitigate potential risks of sharing information in ways that are consistent with the unique roles and responsibilities of CSE.

Under the approved Framework "departments and agencies must also assess the accuracy and reliability of information received and properly characterize this information in any further dissemination." When sharing information either directly or indirectly with foreign entities I expect CSE will use caveats that appropriately reflect the nature of its activities and the information it produces as a foreign signals intelligence agency.

The approval levels that CSE 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.

5. Process for Decision Making

Except when there is a substantial risk, CSE is responsible for establishing approval levels and processes 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 and assurances, the matter will be referred to you, the Chief of CSE, for decision.

In making your decision, you 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 fulfill the proposed assurance);
- The views of the Department of Foreign Affairs and International Trade (DFAIT); and.
- The views of other department and agencies, as appropriate, as well as any other relevant facts that may arise in the circumstances.

You may refer the decision whether or not to share information with the foreign entity to me, the Minister of National Defence, in cases where in your opinion I should be the decision-making authority. In these cases, I will be provided with the information described above.

You shall authorize the sharing of information with the foreign entity only in accordance with Canada's legal obligations.

5. Implementation

I expect CSE to establish or amend policies, procedures, and practices as required to implement this Directive. I expect that you will keep me informed, through established reporting mechanisms, of any significant issues related to the implementation of this directive that in your opinion warrant my consideration.

Dated at Ottawa, Ont this 21st day of November, 2011.

The Honourable Peter MacKay, P.C., M.P.
Minister of National Defence

cc. National Security Advisor, Privy Council Office
Deputy Minister of National Defence

s.23

Department of Justice Canada | Ministère de la Justice Canada

Security classification -- Côte de sécurité
Protected B//Solicitor-client Privilege
File number -- Numéro de dossier
7000-33.101
Date
February 3, 2010
Telephone / FAX -- Téléphone / Télécopieur
(613) [redacted] -- (613) 991-7379

MEMORANDUM – NOTE DE SERVICE

TO / DEST: DC SIGINT

FROM / ORIG: [redacted] Counsel, Legal Services
Communications Security Establishment
Via: David Akman, General Counsel, Legal Services

SUBJECT / OBJET: [redacted]

Do not write in this space / Ne pas écrire dans cet espace

[redacted]

JUS 107A (91/10) 7530-21-036-5336

Pages 13 to / à 15

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

[redacted]

Counsel

cc. John Adams, Chief CSE
[redacted] Associate Chief
Toni Moffa, DC ITS
Kathy Thompson, DGPC
Bud Abbott, DGP

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Human Rights Management
Overview

D Group
22 June 2011

Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

Canada

The Framework

- Holds all government agencies and departments responsible for the information they share outside of Canada;
- Is not an operational document;
- [redacted]
- Only applies when there is a Substantial Risk of mistreatment of an individual.

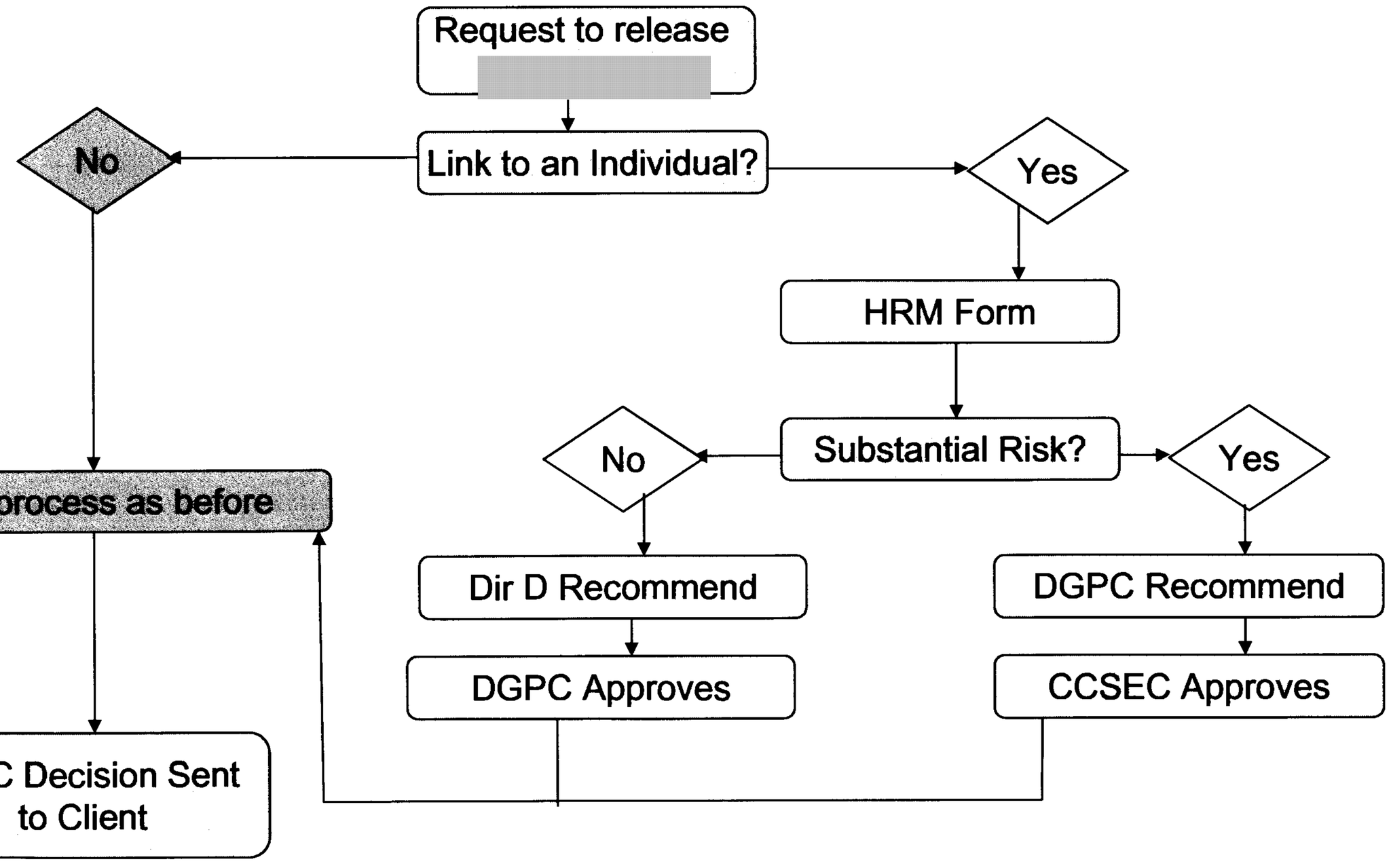
Substantial Risk: "…personal, present, and foreseeable risk of mistreatment.."

Implementation

- Ministerial Directive in draft
  - Will personalize the framework for CSEC
  - [redacted]
  - Other departments also working on MDs
- OPS [redacted] – HRM annex in draft
  - Outline factors to be considered and approval process
  - HRM Summary Template

Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

Approval Process



Page 21

is withheld pursuant to section

est retenue en vertu de l'article

15(1) - DEF

of the Access to Information

de la Loi sur l'accès à l'information

Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

Challenges

- **Timeliness**
  - Several layers in the approval process
  - Many different factors to consider
  - No exceptions for threat to life
- **Workload**
  - Increasing number of requests, significantly more work per request
  -
  -
  -
- **Lack of Guidance**
  - Will be addressed by MD and OPS
  - Decisions based on what we "think" will be in these documents
- **Ongoing litigation and decisions**
  - Interpretation and wording

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

DGPC and Human Rights Management at CSEC

Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

Overview

- Background on the GC Human Rights Framework
- D2 and its role
- Release of SIGINT to [redacted]:
  - Canadian clients
  - 2nd party clients

Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

GC Human Rights Framework

- Framework for Addressing Risks in Sharing Information with Foreign Entities was enacted in 2010
- Establishes a coherent and consistent approach across the Government of Canada when sharing and/or receiving information from foreign entities, which may give rise to a substantial risk of mistreatment
- Ministerial directives being designed to tailor the Framework to the unique mandates of each department/agency.
- CSEC impacted due to Canadian and 2nd party governments dissemination of SIGINT derived intelligence [redacted]

Role of DGPC/D2

- CSEC/D2 (Operational Policy) is the sole authority for approving/denying sanitization [redacted] in Canada.
- Those activities could contribute to the risk of mistreatment of any person, including non-Canadians
- Legal obligation to ensure that our activities (and those of our clients) are not complicit in torture or other cruel, inhuman or degrading treatment or punishment when sharing information.

Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

s.16(2)(c)

Release of SIGINT to [redacted] Canadian Clients

- Although CSEC is approving release of SIGINT-derived intelligence [redacted] the Canadian department/agency requesting the release bears full responsibility for compliance with the Framework

- Therefore, D2 Follows normal procedures to release information inside Canada

- CSEC applies the following caveat to all Canadian client releases of SIGINT information [redacted]

  CSEC approves sharing of this information with (foreign entity). (GC department) is reminded of itsobligations under the Framework for Addressing Risks in Sharing Information with Foreign Entities, which include assessing the risk that sending the information to this particular foreign entity would result in the mistreatment or torture of any individual. If, subsequent to having received this approval from CSEC, (GC department) decides for any reason not to proceed with the proposed information sharing, please advise CSEC/Operational Policy (d2action@cse)."

Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

Release of SIGINT to [redacted] 2nd party clients

- CSEC bears full responsibility on behalf of the Canadian government for applying the Framework when authorizing the release of SIGINT information to [redacted] a 2nd party
- D2 Operational policy processes the requests in consultation with D2 Manager and Director COP
- DGPC is currently the approval authority in most cases
- In certain high risk cases, DLS and CCSEC could be consulted
- In all cases, CSEC/D2 Operational Policy completes a Human Rights Management (HRM) matrix

Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

HRM Matrix

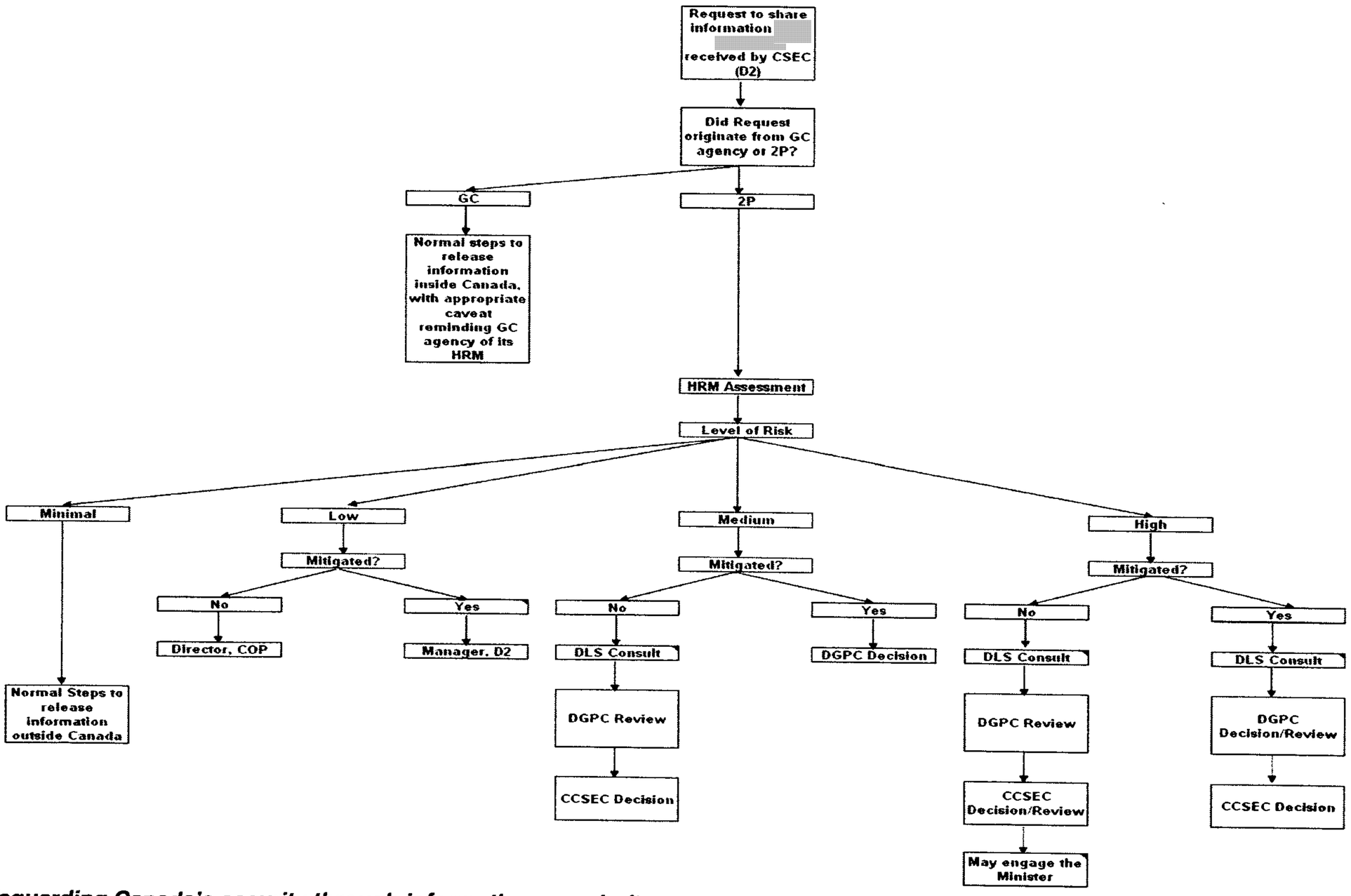
The HRM matrix comprises of:

- General research
  - [redacted]
- Human Rights Record of Foreign Entities
  - Role of foreign agency
  - International human rights agreements
  - DFAIT, CSIS, and US State Department input
  - Previous interactions (i.e. [redacted] NATO etc…)
- Mitigation Measures
- HRM process of the Second party country

s.21(1)(a)

Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

HRM Decision Tree



Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

Canada

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Questions?

Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

Canada

s.15(1) - DEF

Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

TOP SECRET//SI//CEO
CERRID #: 916207
CCM #: 12-00633

1 March 2012

Briefing Note for Director COP and DGPC

D2 Considerations Related to Approval Levels for Human Rights Related Requests

(For Information and Decision)

Background

Canada

and Human Rights:

The human rights-related institutions of the European region - the European Convention on Human Rights, the European Community and the Conference on Security and Cooperation in Europe – constitute one of the most extensive and effective systems designed for the promotion of human rights. Furthermore, Western Europe in general, are pioneers in the field of the international protection of human rights.

The European Convention on Human Rights provides a catalogue of the rights enjoyed by the residents of this area, and gives states, groups, and individuals an unprecedented opportunity to invoke the aid of international agencies should they feel there has been a violation of this right. In addition, in 1987 the European Convention for the Prevention of Torture and Inhuman or Degrading Treatment or Punishment was adopted and ratified by all members of the Council of Europe. The Convention was amended by two protocols that entered into force in 2002. After the European Convention on Human Rights, the Convention for the Prevention of Torture is widely regarded as one of the most important Council of Europe treaties, and ratification of the Convention has been a pre-condition for all states that had joined the Council of Europe in the last few years.

During 2011, Operational Policy (D2) received several requests to share information with member nations. For these requests, D2's analysis and recommendations provided to assist DGPC in the decision-making process were always extensive and reflective of the final decision made.

Policy Considerations

The Framework for Addressing Risks in Sharing Information with Foreign Entities (Framework), ratified by Cabinet on 1 February 2011, and the associated Ministerial Directive (MD) (November 2011) were implemented to establish a coherent and consistent approach across the GC for deciding whether or not to send information to, or solicit information from, a foreign entity (other than Second Party allies) when doing so may give rise to a substantial risk of mistreatment of an individual.

According to the MD, for CSEC, the principle focus of this Directive is information sharing with third parties, It further states that "in sharing information, CSE must act in a manner that complies with Canada's laws and legal obligations", and that "CSE must assess and mitigate potential risks of sharing information in ways that are consistent with the unique roles and responsibilities of CSE".

In a 2010 Memorandum to DGPC

Assessment

Based on information available to CSEC the risk of mistreatment to any person is consistently assessed as low, even if in some the risk of detention were to be assessed as high in certain cases. However, as part of its due diligence, Operational Policy will

continue to conduct HRM assessments and complete the HRM form for all such requests, with the "Recommendation" and "Approval/Denial" actors updated accordingly (D2 [redacted] In addition, D2 Manager can choose to elevate to Director, Corporate and Operational Policy, any requests where the risk of mistreatment is not assessed as low, depending on the level of risk DGPC, or Chief

Recommendation

Based on the assessed low risk of mistreatment, it is recommended that you confirm that the approval level for requests to share information with [redacted] be delegated to the Manager, Operational Policy. This delegation will be valid until [redacted] is approved and promulgated.

Recommended

[redacted]
Director COP

Approved / Denied

Kathy Thompson
DGPC

s.15(1) - DEF

s.16(2)(c)

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

[redacted] and Human Rights

[redacted]

Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

Canada

Overview

- Background on the GC Human Rights Framework
- D2 and its role
- Release of SIGINT to [redacted]
- Canadian clients
- 2nd party clients

Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

GC Human Rights Framework

- *Framework for Addressing Risks in Sharing Information with Foreign Entities* was enacted in 2011
- Established a coherent and consistent approach across the GC when sharing and/or receiving information from foreign entities, which may give rise to a substantial risk of mistreatment
- CSEC's Ministerial Directive signed by the Minister in late 2011
- CSEC impacted because of Canadian and 2nd Party dissemination of SIGINT-derived intelligence [redacted]

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Role of DGPC/D2

- CSEC/D2 (Operational Policy) is the sole authority for approving/denying sanitization and [redacted] in Canada.
- The sharing of sanitized text [redacted] could contribute to the risk of mistreatment of any person, including non-Canadians
- Legal obligation to ensure that CSEC's activities (and those of our clients) are not complicit in torture or other cruel, inhuman or degrading treatment or punishment when sharing information.

Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

Release of SIGINT to [redacted] Canadian Clients

- Although CSEC approves release of SIGINT-derived intelligence [redacted] the Canadian department/agency requesting the release bears full responsibility for compliance with the *Framework*
- Therefore, D2 follows normal procedures to release information inside Canada
- CSEC applies the caveats to all Canadian client releases of SIGINT information [redacted] reminding them of their obligations under the *Framework*

Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

Release of SIGINT to [redacted] 2nd Parties

- CSEC bears full responsibility on behalf of the GC for applying the *Framework* when authorizing the release of SIGINT information to [redacted] a 2nd party, [redacted]
- D2 Operational Policy processes the requests in consultation with D2 Manager and Director,COP
- In certain cases where the risk of torture or mistreatment is assessed as "**Substantial**", DLS and CCSEC are part of the release process
- In all but few cases, CSEC/D2 Operational Policy completes a Human Rights Management (HRM) matrix

Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

Release Authority Chain [redacted]

[redacted]

1. [redacted] appears on a list in Annex 2 ([redacted]: release authority = Manager, D2 [redacted] HRM matrix
2. Risk of mistreatment or torture assessed as "**Speculative**" (i.e., the risk is not "personal, present and foreseeable"): release authority = Director, COP (HRM matrix required)
3. Risk of mistreatment or torture assessed as "**Substantial**" (i.e., "personal, present and foreseeable) but mitigated: release authority = DGPC
4. Risk of mistreatment or torture assessed as "**Substantial**" (i.e., "personal, present and foreseeable) but unmitigated: release authority = CCSEC (who may engage the Minister as required).

All any point, DLS may be or will be engaged

Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

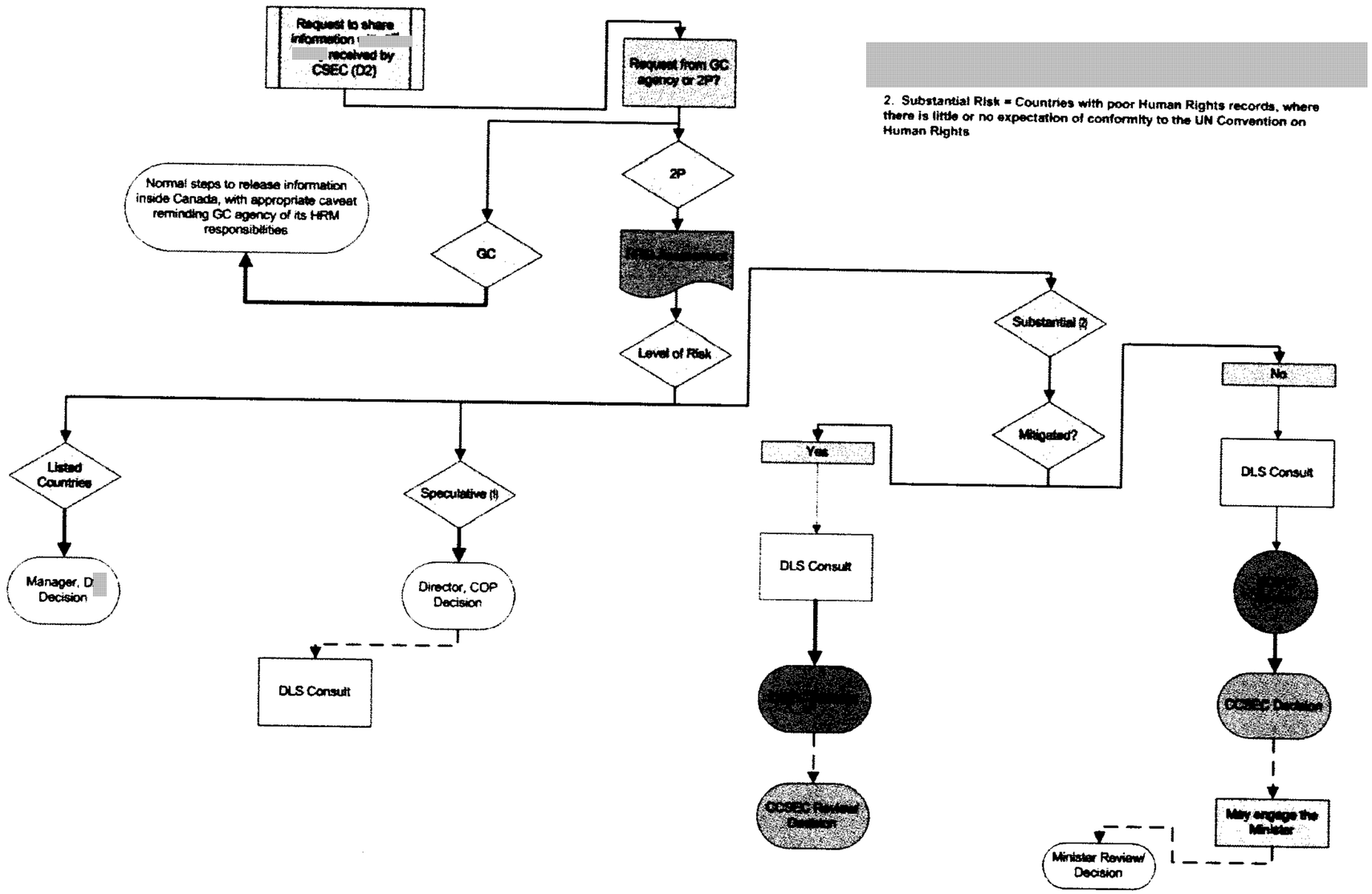
HRM Matrix

The HRM matrix comprises:

- General research, such as:
  - [redacted]
- Human Rights Record of Foreign Entities
  - Role of foreign agency
  - International human rights agreements
  - Reports of torture
  - DFAIT, CSIS, and US State Department input
- MD Criteria:
  - Threat to Canada's national security
  - Importance of sharing the information
  - Status of relationship with foreign entity
  - Rationale for believing there is substantial risk (or not)
  - Proposed mitigation measures

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

HRM Decision Tree



2. Substantial Risk = Countries with poor Human Rights records, where there is little or no expectation of conformity to the UN Convention on Human Rights

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Questions?

Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

Canada

[redacted]

BACKGROUND

General Background

Under the *Ministerial Directive on the Framework for Addressing Risks in Sharing Information with Foreign Entities*, CSEC is required to carefully manage relationships with foreign entities, assisted by policies that guide information sharing practices, to ensure that the sharing of information does not give rise to a substantial risk of mistreatment of any individual. Since the introduction of the Government of Canada *Framework* in 2010, CSEC has been developing methods for best implementing the measures required under this agreement.

[redacted]

Human Rights Assessment Threshold

The requirement to assess the human rights record of a country prior to release of intelligence is conditional on the following criteria being met:

1) The information is destined for a foreign entity, [redacted]

Pages 46 to / à 48

are withheld pursuant to sections

sont retenues en vertu des articles

21(1)(a), 15(1) - DEF, 23

of the Access to Information

de la Loi sur l'accès à l'information

Page 49

is withheld pursuant to sections

est retenue en vertu des articles

15(1) - DEF, 23

of the Access to Information

de la Loi sur l'accès à l'information

Pages 50 to / à 52

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

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Human Rights Management at CSEC

A Briefing for [redacted]
by [redacted]

Overview

- Background on the GC Human Rights Framework
  - Canada's obligations
  - Substantial Risk
  - MD on Assessing Risk
- D2 and its role
  - Types of sharing that require HRM
  - Criteria for assessing risk
- Release of SIGINT to [redacted]
  - Canadian clients
  - 2nd party clients
  - Release authority chain

Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

GC Human Rights Framework

- *Framework for Addressing Risks in Sharing Information with Foreign Entities* enacted in 2010
- Establishes coherent and consistent approach across GC in deciding whether or not to share with and/or receive information from foreign entities when doing so may give rise to a substantial risk of mistreatment
- MD, *Addressing Risks in Information Sharing*, designed to tailor the Framework to CSEC's mandate
- CSEC impacted due to Canadian and 2nd Party governments' dissemination of SIGINT-derived intelligence to [redacted]

Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

Canada's Obligations

- The GC:
  - opposes in the strongest possible terms the mistreatment of any individual by any foreign entity for any purpose
  - has a duty to its citizens and allies to prevent individuals engaging in threat related activities from causing harm, whether in Canada or abroad
  - does not condone the use of torture or other related methods in responding to terrorism and other threats to national security
  - is committed to pursuing a principled and proportionate response to these threats, while promoting and upholding Canadian values

Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

Considerations

- Canada is party to international agreements proscribing torture and other cruel, inhuman or degrading treatments
- Torture is an explicit *Criminal Code* offense, which has extra-territorial application
- Departments and agencies cannot simply stop sharing information in high-risk situations since this would be counter to international obligations to strengthen information sharing for the purposes of combating terrorism

Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

Risk/Strategy

Risk

- An individual is mistreated by a foreign entity as a result of information sent or requested by a department or agency, and initiates litigation against the GC
- GC may be in breach of international obligations, the *Charter* and its own criminal law

Strategy

- Framework attempts to mitigate risk by emphasizing high level of accountability by requiring very senior decision makers – deputy head (Chief) to decide whether or not to share information, and identifies practical considerations to guide his decision
- Serves to reduce risk through its concentration on the need for actions to be taken in accord with Canada's legal obligations

Substantial Risk

- 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
- The test of substantial risk will be satisfied when it is **more likely than not** that there will be mistreatment

Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

MD on Assessing the Risk

- CSEC's longstanding information-sharing alliance with the 5-Eyes will continue
- [redacted]
- CSEC must act in a manner the complies with Canada's laws and legal obligations in sharing information
- The appropriate levels requires must be proportionate to the risk of mistreatment: the higher the risk, the more senior the level of approval to share

Role of D2

- The sole authority in Canada for approving/denying sanitization and [redacted] (OPS-[redacted]) to share information, which could contribute to the risk of mistreatment of any person, including non-Canadians, anywhere
- Required to ensure that D2's activities (and those of our clients) in sharing information [redacted] do not make the GC complicit in torture or other cruel, inhuman or degrading treatment or punishment

Types of Sharing That Require HRM

- Requests from Canadian domestic partners [redacted] CSE intelligence [redacted]
- Requests from 5-Eyes partners [redacted]
- Source approvals to share [redacted]
- Threat-to-life situations
- Requests [redacted]

Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

Criteria to Assess Risk

- Does the report/proposed sanitization involve or potentially involve an identifiable person?
- [redacted]
- What is the importance of sharing the information in light of Canada's national security or other interests?
- What is the nature and imminence of the threat?
- Who is the [redacted] and how is the information relevant in the [redacted]
- What is the human rights record of the foreign agency or country with which the information is to be shared?

Decision-Making Process

- Where it is unclear whether the substantial risk can be mitigated through the use of caveats or assurances, the matter is referred to the CCSEC
- He will consider the following information:
  - the threat to Canada`s national security or other interests, and the nature and imminence of the threat
  - the importance of sharing the information
  - the status of the relationship with the foreign entity, and the assessment of its human rights record
  - the rationale for believing the risk is substantial
  - the proposed measures to mitigate the risk and likelihood of their success rate
  - the views of DFAIT
  - - the views of other departments and agencies

Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

Release of SIGINT [redacted] Canadian Domestic Clients

- Although D2 approves requests to release SIGINT-derived intelligence [redacted] the GC department/agency requesting the release also bears responsibility to comply with the *Framework*
- D2 follows normal procedures to release information inside Canada but attaches this caveat:

  CSEC approves sharing of this information with [*foreign entity*]. [*GC department*] is reminded of its obligations under the *Framework for Addressing Risks in Sharing Information with Foreign Entities*, which include assessing the risk that sending the information to this particular foreign entity would result in the mistreatment or torture of any individual. If, subsequent to having received this approval from CSEC, [*GC department*] decides for any reason not to proceed with the proposed information sharing, please advise CSEC/Corporate and Operational Policy (D2action@cse).

Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

Release of SIGINT to [redacted] 2nd Party clients

- CSEC bears full responsibility on behalf of GC for applying *Framework* when authorizing the release of SIGINT information to [redacted] a 2nd party
- D2 processes the requests in consultation with D2 Manager and Director DPR
- DGPC is often the approval authority although Dir DPR has more authority for cases with lower risk levels
- In certain high risk cases, DLS and CCSEC will be consulted
- In all cases, CSEC/D2 Operational Policy completes a Human Rights Management (HRM) matrix

Release Authority Chain –

1. appears on a list in Annex 2 release authority = Manager, D2 (HRM matrix not as complex)
2. Risk of mistreatment or torture assessed as "**Speculative**" (i.e., the risk is not "personal, present and foreseeable"): release authority = Director, DPR (HRM matrix required)
3. Risk of mistreatment or torture assessed as "**Substantial**" (i.e., "personal, present and foreseeable) but mitigated: release authority = DGPC
4. Risk of mistreatment or torture assessed as "**Substantial**" (i.e., "personal, present and foreseeable) but unmitigated: release authority = CCSEC (who may engage the Minister as required).

All any point, DLS may be or will be engaged

Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

HRM Matrix

The HRM matrix comprises:

- General research, such as:
  - [redacted]
- Human Rights Record of Foreign Entities
  - Role of foreign agency
  - International human rights agreements
  - Reports of torture
  - DFAIT, CSIS, and US State Department input
- MD Criteria:
  - Threat to Canada's national security
  - Importance of sharing the information
  - Status of relationship with foreign entity
  - Rationale for believing there is substantial risk (or not)
  - Proposed mitigation measures

Pages 69 to / à 70

are withheld pursuant to section

sont retenues en vertu de l'article

15(1) - DEF

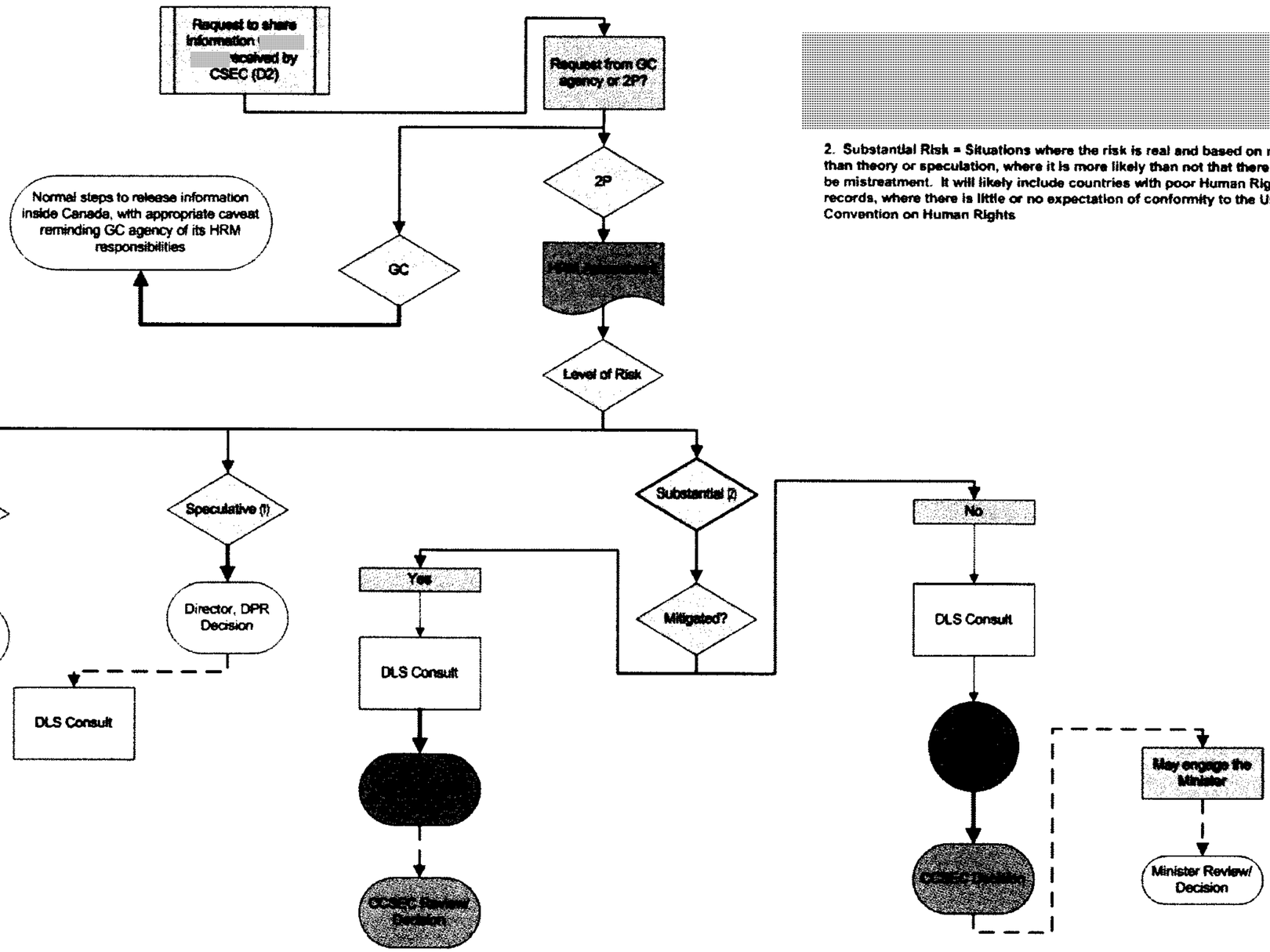
of the Access to Information

de la Loi sur l'accès à l'information

s.15(1) - DEF

Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

HRM Decision Tree



[redacted]

2. Substantial Risk = Situations where the risk is real and based on more than theory or speculation, where it is more likely than not that there will be mistreatment. It will likely include countries with poor Human Rights records, where there is little or no expectation of conformity to the UN Convention on Human Rights

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Questions?

Safeguarding Canada's security through information superiority
Préserver la sécurité du Canada par la supériorité de l'information

Canada

s.21(1)(a)

5.23

TOP SECRET//SI//Canadian Eyes Only
CERRID #1091010

[redacted]

BACKGROUND

General Background

Under the *Ministerial Directive on the Framework for Addressing Risks in Sharing Information with Foreign Entities*, CSEC is required to carefully manage relationships with foreign entities, assisted by policies that guide information sharing practices, to ensure that the sharing of information does not give rise to a substantial risk of mistreatment of any individual. Since the introduction of the Government of Canada *Framework* in 2010, CSEC has been developing methods for best implementing the measures required under this agreement.

[redacted]

Human Rights Assessment Threshold

The requirement to assess the human rights record of a country prior to release of intelligence is conditional on the following criteria being met:

1) The information is destined for a foreign entity, [redacted]

Pages 74 to / à 76

are withheld pursuant to sections

sont retenues en vertu des articles

21(1)(a), 15(1) - DEF, 23

of the Access to Information

de la Loi sur l'accès à l'information

Pages 77 to / à 80

are withheld pursuant to sections

sont retenues en vertu des articles

15(1) - DEF, 23

of the Access to Information

de la Loi sur l'accès à l'information