



CORPORATE AND OPERATIONAL POLICY



PCI-3 **Policy and Communications Instruction** **Releasing Suppressed Information**

Effective Date: 3 July, 2014

Canada

CORPORATE AND OPERATIONAL POLICY

1. Introduction

1.1 Objective These instructions provide guidance on the internal processes that CSE must follow when releasing suppressed information to Government of Canada (GC) or Second Party partners [REDACTED]

These instructions provide guidance on how to interpret and apply OPS 1-1, *Policy on Releasing Suppressed Information*.

1.2 Context In accordance with the *National Defence Act* (NDA) and its agreements with foreign cryptologic agencies, CSE suppresses privacy-sensitive information in its reporting by replacing specific identifying information (such as an email address) with a generic term (such as a “Canadian email address”), thereby making it impossible for the reader to identify the individual. CSE’s Second Party partners also suppress this information in their reports.

Authorized recipients of CSE and Second Party reports may request and receive suppressed information if they have both the legal authority and operational justification to receive it.

1.3 Application These instructions apply to all DGPC staff involved in releasing suppressed information from CSE’s reporting.

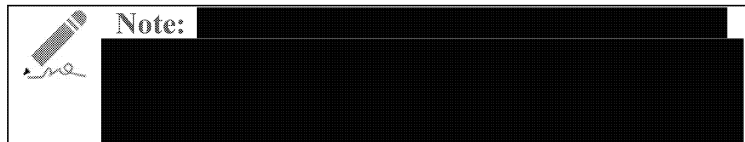
CORPORATE AND OPERATIONAL POLICY

2. General Guidance for Releasing Suppressed Information

2.1 Who Can Request Suppressed Information

Any authorized recipient of CSE reports can request suppressed information, including: GC clients, CSE-employed CROs, Second Party government officials (via their national cryptologic policy centre), [REDACTED] and CSE staff.

Foreign entities may not submit requests for suppressed information directly to CSE. However, GC and Second Party partners may submit a request for suppressed information with the intent of sharing the information with a foreign entity. Any release of suppressed information where the final recipient is a foreign entity requires a Mistreatment Risk Assessment (MRA). See OPS-6, Policy on Mistreatment Risk Management and section 4.3 of these instructions for more information.



2.2 Rationale for the Request

Requesters must provide a justification for their request by explaining their requirement for the information and its relevance to their operational program.

The Privacy and Interests Protection team must assess the rationale for each request in accordance with OPS-1-1 and these instructions.

Continued on next page

CORPORATE AND OPERATIONAL POLICY

General Guidance for Releasing Suppressed Information, Continued

2.3 Assessing the Impact of Release

Before releasing suppressed information, the Privacy and Interests Protection team must assess the validity of the request and whether the request could impact the operational interests of the GC or pose a risk to the privacy of a Canadian or person in Canada. This includes:

Considerations	Examples
Type of information requested	
Relevance of request to Canada's national interests (including any impact on international affairs, defence or security)	
Possible <u>positive</u> impact on a Canadian or person in Canada	
Possible <u>negative</u> impact on a Canadian or person in Canada	

2.4 Advice to the Release Authority

When a GC partner will be the final recipient of the suppressed information, the Privacy and Interests Protection team must assess the requester's justification and provide a recommendation to the release authority.

When information will be released outside Canada (either directly to a Second Party entity or indirectly to a foreign entity), advice to the release authority must include:

- A final recommendation to approve or deny the release;
- The details of the request and rationale submitted by the client;
- An assessment of the rationale submitted by the client and essentiality of the suppressed information to the identified operational objectives;
- An assessment of the impact of the release;
- Any observations or advice provided by domestic stakeholders who have received the suppressed information.

Continued on next page

CORPORATE AND OPERATIONAL POLICY

General Guidance for Releasing Suppressed Information, Continued

**Advice to the
Release
Authority
(continued)**

In making this assessment, the Privacy and Interests Protection team must consult CSE information repositories and GC stakeholders. Analysts may also research open source materials and other available resources as appropriate.

**2.5 Approval
Authorities**

The approval authority for the release of suppressed information ranges from the Privacy and Interests Protection team to the Director General Policy and Communications (DG PC), depending on the type of information being requested (e.g. Canadian identity information (CII) or information about Second Party entities) and the final recipient (i.e. Canadian or Outside Canada). See section 4.3 of OPS-1-1 for more information.

Chapter 8 of these instructions summarizes the approval authorities for releasing suppressed information.

**2.6 Extremely
Time
Sensitive
Requests**

When a request for suppressed information is extremely time-sensitive (e.g. an imminent threat-to-life situation) and DG PC is unable to review the request within a reasonable time, Director, Disclosure, Policy, and Review (DPR) may approve the release of suppressed CII to recipients outside Canada. DG PC must be briefed on any such releases as soon as operationally feasible.

**2.7 Silent
Hours
Releases**

CSE's [REDACTED] should be copied on urgent requests for suppressed information outside of core business hours (silent hours). [REDACTED] will use the call-in list to contact the Privacy and Interests Protection team.

During crisis periods or to support CROs working extended hours [REDACTED] the Manager, Corporate and Operational Policy may authorize [REDACTED] to act as Release Authority for suppressed information.

For more information see the COPCC [REDACTED] SOP B-6, *Support to Operational Policy during Silent Hours*, or contact the Privacy and Interests Protection team.

Continued on next page

CORPORATE AND OPERATIONAL POLICY

General Guidance for Releasing Suppressed Information, Continued

2.8 Exceptional Circumstances

In exceptional circumstances, DG PC may approve, in writing, procedures that deviate from these instructions. DG PC may also delegate alternate authorities for releasing suppressed information.

Any exceptional authorizations must be limited in scope and duration, as appropriate to the circumstances. All entities acting under delegated release authorities must comply with Canadian law, Ministerial direction, and CSE policies and procedures.

CORPORATE AND OPERATIONAL POLICY

3. Repetitive Releases of CII

3.1 Introduction

A repetitive release occurs when a GC or Second Party partner requests information related to a Canadian entity about which it has previously received information. Repetitive releases include supplemental, subsequent and repeat releases.

Each repetitive request must be assessed independently, though the approval process for repetitive releases is modified.

3.2 Supplemental Releases

A supplemental release occurs when:

- A Second Party partner requests suppressed CII that relates to the same Canadian entity as information previously released to that agency; or
- A GC or Second Party partner requests to share CII with a foreign entity that relates to same Canadian entity as information that was previously released to that specific foreign entity.

For supplemental releases, follow the instructions in Chapter 6. Director, Disclosure, Policy and Review (DPR) is the approval authority for supplemental releases.

3.3 Subsequent Release

A subsequent release occurs when:

- A Second Party entity submits a request for specific CII that has already been released to another agency from the same country [REDACTED]
 - A Second Party entity submits a request to share CII that has previously been released to that agency with another agency from the same country [REDACTED]
- or
- A Canadian or Second Party entity submits a request to share specific CII with a foreign entity that was previously released to another agency from the same foreign entity [REDACTED]

For subsequent releases, follow the instructions in Chapter 6. Manager, Corporate and Operational Policy is the approval authority for subsequent releases.

Continued on next page

CORPORATE AND OPERATIONAL POLICY

Repetitive Releases of CII, Continued

3.4 Repeat Releases

A repeat occurs when:

- A Second Party agency submits a request for specific CII that has already been released to the same agency from a different report; or
- A Canadian or Second Party entity requests permission to share CII with a third party that the third party recipient has already received from a different report.

For repeat releases, follow the instructions in Chapter 6. The Supervisor, Privacy and Interests Protection is the approval authority for repeat releases.

CORPORATE AND OPERATIONAL POLICY

4. Releasing CII and Information about Foreigners in Canada to Canadian Recipients

4.1 Introduction

This chapter provides detailed guidance on the process for releasing CII and identity information related to foreigners in Canada to Canadian recipients.

If a GC partner is requesting suppressed information with the intent of sharing it with a foreign entity, follow the process in Chapter 6.

4.2 Release Process

The following table outlines the process for releasing suppressed information to Canadian recipients:

Who	Does What
Requester	<ul style="list-style-type: none"> Submits a request for release of suppressed information
Privacy and Interests Protection team	<ul style="list-style-type: none"> Reviews request to determine if it meets criteria for release Retrieves the suppressed information <ul style="list-style-type: none"> If the information originates from a Second Party report, obtains the information and inputs it into CSE's suppressed information repository Makes a decision on requests for CII and information about foreigners in Canada to Canadian recipients (other than the RCMP)
Supervisor, Privacy and Interests Protection team	<ul style="list-style-type: none"> Makes a decision on the release of information about foreigners in Canada to the RCMP Makes a recommendation on requests for CII from the RCMP
Manager, Corporate and Operational Policy	<ul style="list-style-type: none"> Makes a decision on requests for CII from the RCMP
DG PC	<ul style="list-style-type: none"> Can approve exceptions to this process
Privacy and Interests Protection team	<ul style="list-style-type: none"> If approved, releases the suppressed information to the requester via the appropriate CSE system If denied, advises the requester of the decision Retains records of all releases, including supporting correspondence, in accordance with CSE Information Management standards

CORPORATE AND OPERATIONAL POLICY

5. Advance Releases to Canadian Recipients

5.1 Introduction

To streamline support during a high-level meeting, crisis or other emergency or time-sensitive situation, a Client Relations Officer (CRO) may request the advance release of suppressed information if their clients require the information on an urgent basis.

If the Privacy and Interests Protection team approves an Advance Release, the CRO is delegated responsibility for assessing a client's request in accordance with OPS-1-1 and these instructions.

For more information on advance releases, see section 3.7 of OPS-1-1.

5.2 Who Can Request an Advance Release

Only CSE-employed CROs may request and receive Advance Releases.

Continued on next page

CORPORATE AND OPERATIONAL POLICY

Advance Releases to Canadian Recipients, Continued

5.3 Advance
Release
Process

The following table describes the process for an advance release:

Who	Does What						
CRO	<ul style="list-style-type: none"> Requests the advance release of suppressed information in anticipation of a request from a client <p>Note: The CRO does not submit a formal request for suppressed information at this time</p>						
Privacy and Interests Protection team	<ul style="list-style-type: none"> Makes a decision on the advance release If approved, retains records of the release, including supporting correspondence, in accordance with CSE Information Management standards 						
CRO	<ul style="list-style-type: none"> Acts as release authority for the information Assesses the request: <table border="1"> <tr> <th>If rationale is...</th><th>Then...</th></tr> <tr> <td>Sufficient</td><td>Release information and complete a "Request for release form" as soon as possible</td></tr> <tr> <td>Insufficient</td><td>Do not release information and inform Privacy and Interests Protection team</td></tr> </table> <p>Note: If the client does not request the suppressed information, CRO destroys suppressed information and notifies Privacy and Interests Protection team</p>	If rationale is...	Then...	Sufficient	Release information and complete a "Request for release form" as soon as possible	Insufficient	Do not release information and inform Privacy and Interests Protection team
If rationale is...	Then...						
Sufficient	Release information and complete a "Request for release form" as soon as possible						
Insufficient	Do not release information and inform Privacy and Interests Protection team						

CORPORATE AND OPERATIONAL POLICY

6. Releasing CII or Information about Foreigners in Canada to Recipients Outside Canada

6.1 Introduction

This chapter provides detailed guidance on the process for releasing CII and identity information related to foreigner in Canada where the final recipient is outside Canada. This includes:

- Direct releases to Second Party partners;
- Releases to Second Party partners where the final recipient is a foreign entity; and
- Releases to GC partners where the final recipient is a foreign entity.

6.2 Release Process

The following table describes the process of requesting and releasing suppressed information to a foreign recipient:

Who	Does What
Requester	<ul style="list-style-type: none"> • Submits a request for suppressed information
Privacy and Interests Protection team	<ul style="list-style-type: none"> • Receives the request • Retrieves the suppressed information <ul style="list-style-type: none"> ○ If the suppressed information originates from a Second Party report, obtains the information and inputs it into CSE's suppressed information repository • Drafts an assessment of the request • Makes a recommendation to approve or deny a request
Supervisor, Privacy and Interests Protection team	<ul style="list-style-type: none"> • Makes a decision on repeat releases • Provides recommendation to Manager of Corporate and Operational Policy on all other releases
Manager, Corporate and Operational Policy	<ul style="list-style-type: none"> • Makes a decision on subsequent releases of CII • Provides recommendation to Director, DPR on all remaining requests
Director, DPR	<ul style="list-style-type: none"> • Makes a decision on supplemental releases of CII • Makes a recommendation to DG PC on first-time releases of CII outside Canada • Approves or denies time sensitive requests (i.e. threat-to-life) where DG PC is unavailable

Continued on next page

CORPORATE AND OPERATIONAL POLICY

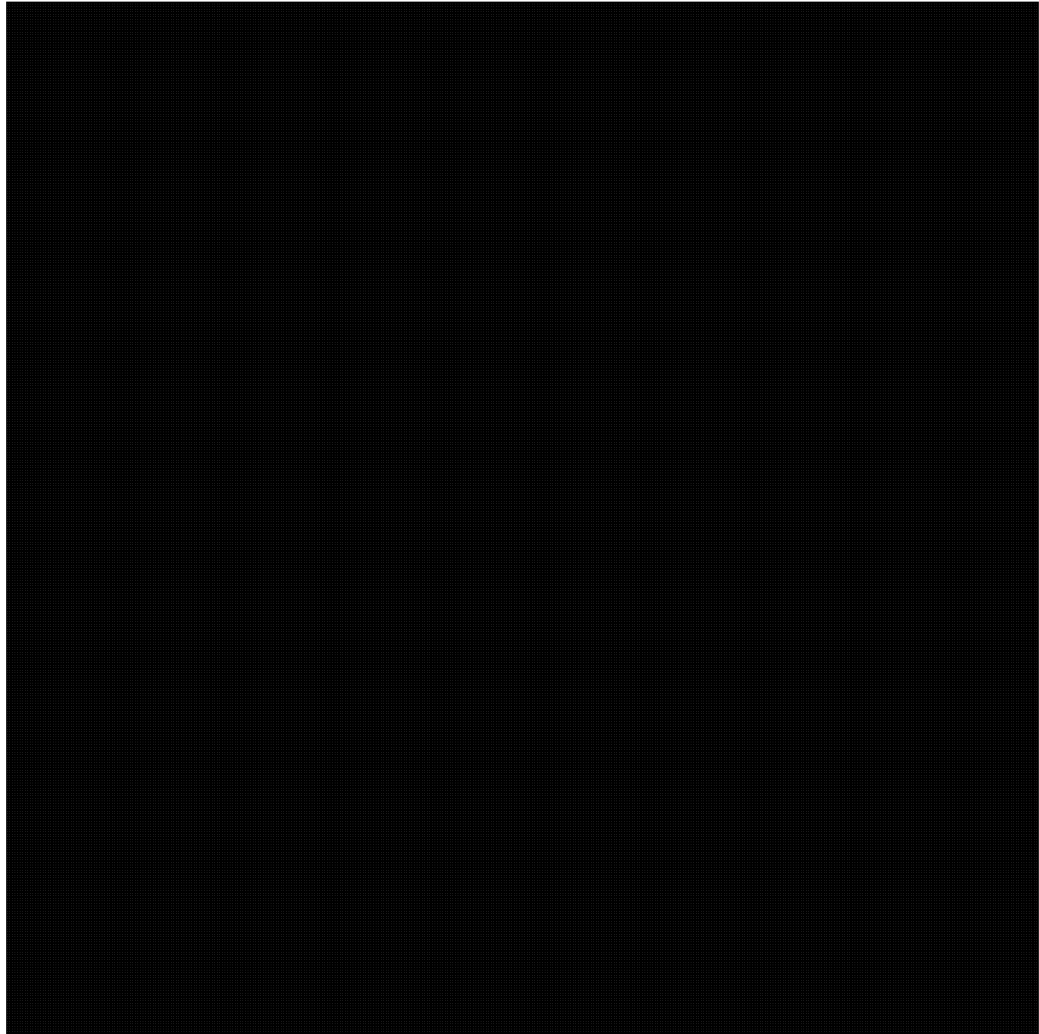
Releasing CII or Information about Foreigners in Canada to Recipients Outside Canada, Continued**Release Process**
(continued)

Who	Does What
DG PC	<ul style="list-style-type: none">• Approves or denies first-time releases of CII outside Canada• Consults with the Chief and the Directorate of Legal Services (DLS), as required• Can approve exceptions to this process
Privacy and Interests Protection team	<ul style="list-style-type: none">• If a request is approved, releases the information via the appropriate CSE system• If a request is denied, advises the requester• Retains records of all releases, including supporting correspondence, in accordance with CSE Information Management standards

CORPORATE AND OPERATIONAL POLICY

7. Releasing Suppressed Information Related to a Second Party Entity

7.1 Introduction



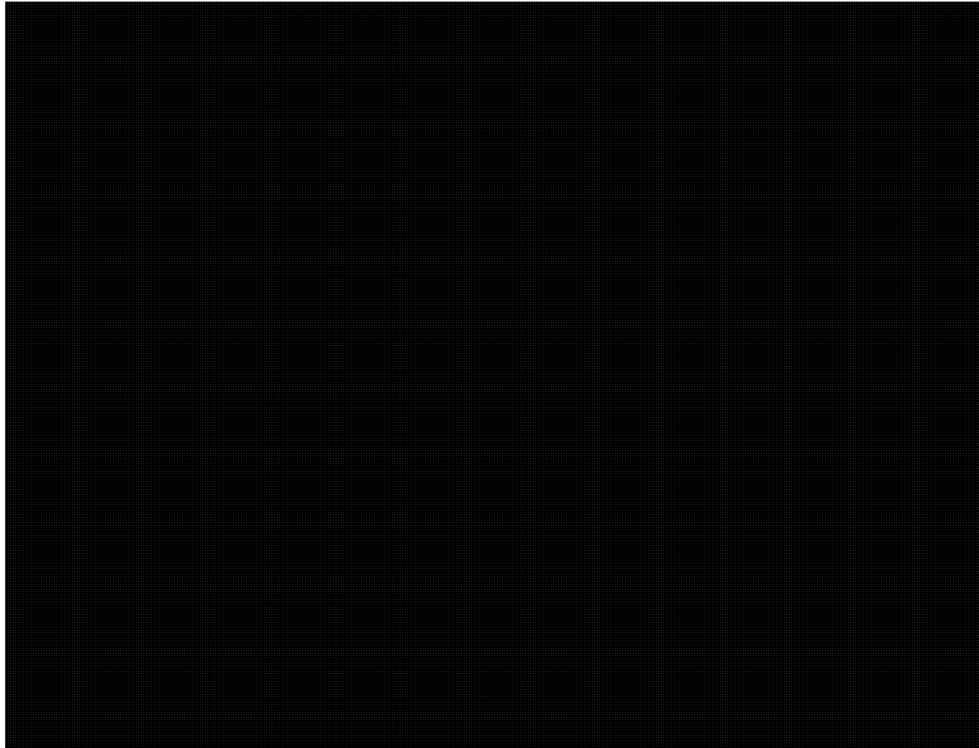
Continued on next page

CORPORATE AND OPERATIONAL POLICY

Releasing Suppressed Information Related to a Second Party Entity, Continued

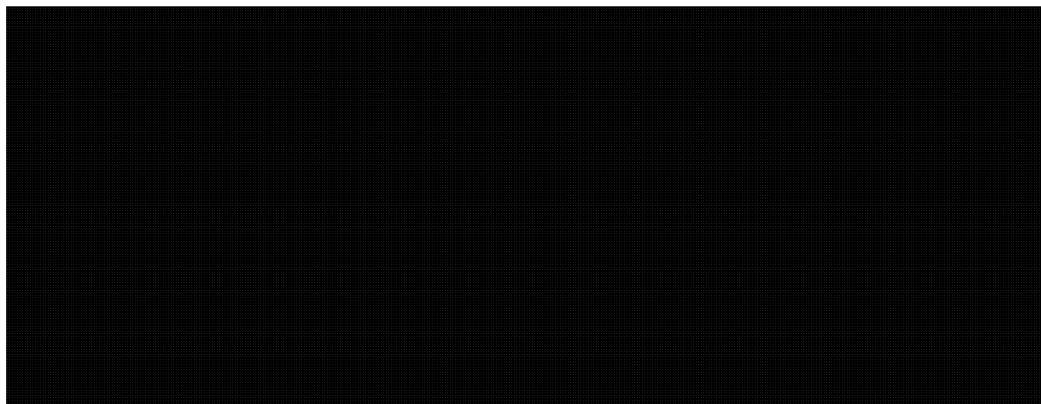
7.2 Canadian Requests for Second Party Information

The following table describes the process for requesting and releasing suppressed information pertaining to a Second Party entity to Canadian recipients:



7.3 Requests from Second Parties

The following table outlines how to respond to Second Party requests for suppressed information:



CORPORATE AND OPERATIONAL POLICY

8. Responsibilities for Releasing Suppressed Information

8.1 Authority for Releasing Suppressed Information

The following table summarizes the roles and responsibilities within DGPC for releasing suppressed information. **Note: Any request for suppressed information can be denied at any stage.**

Who	Responsibility
Privacy and Interests Protection team	<ul style="list-style-type: none"> • Making a decision on: <ul style="list-style-type: none"> ○ Requests for CII and information about a foreigner in Canada to GC recipients other than the RCMP ○ Requests for suppressed information relating to a Second Party entity from CSE reporting to GC recipients
Supervisor, Privacy and Interests Protection team	<ul style="list-style-type: none"> • Making a decision on: <ul style="list-style-type: none"> ○ Repeat releases of CII ○ Releases of information about a foreigner in Canada to Second Parties or the RCMP
Manager, Corporate and Operational Policy	<ul style="list-style-type: none"> • Making a decision on: <ul style="list-style-type: none"> ○ Subsequent releases of CII ○ Releases of CII to the RCMP ○ Releases of information about a foreigner in Canada to a foreign entity • Denying the first-time release of CII to Second Party requesters, as required • Authorizing [REDACTED] staff to release suppressed information during exceptional circumstances
Director, Disclosure, Policy and Review	<ul style="list-style-type: none"> • Making a decision on: <ul style="list-style-type: none"> ○ Requests that are extremely time sensitive where DG PC is unable to review the request within a reasonable time ○ Supplemental releases of CII • Recommending or denying the first-time release of CII outside Canada
DG PC	<ul style="list-style-type: none"> • Making a decision on the first-time release of CII outside Canada • Authorizing the release suppressed information during exceptional circumstances

CORPORATE AND OPERATIONAL POLICY

9. Additional Information

9.1 Accountability

The following table outlines accountabilities within CSE for these instructions:

Who	Responsibility
DG PC	<ul style="list-style-type: none"> • Approves
DLS	<ul style="list-style-type: none"> • Reviews to ensure compliance with the law • Provides legal advice, as required
Director, Disclosure Policy and Review (DPR)	<ul style="list-style-type: none"> • Recommends • Reviews for consistency with CSE's policy framework
Manager, Corporate and Operational Policy	<ul style="list-style-type: none"> • Revises these instructions • Ensures staff compliance
Privacy and Interests Protection team	<ul style="list-style-type: none"> • Complies with these instructions and any amendments • Answers questions regarding implementation

9.2 References

- *National Defence Act*
- *Security of Information Act*
- *Policy on Government Security*
- *CSE Ethics Charter*
- OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities*
- OPS-1-1, *Policy on Releasing Suppressed Information*
- OPS-1-7, *Operational Procedures for naming in SIGINT Reports*
- OPS-6, *Policy on Mistreatment Risk Management*
- *OPS Policy Glossary*
- PCI-1, *Mistreatment Risk Management Process When Sharing Information with Foreign Entities*
- PCI-2, *Sanitizations and Actions-On*
- COPCC [REDACTED] SOP B-6, *Support to Operational Policy During Silent Hours*

Continued on next page

CORPORATE AND OPERATIONAL POLICY

Additional Information, Continued**9.3
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.

**9.4 Audit and
Review**

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

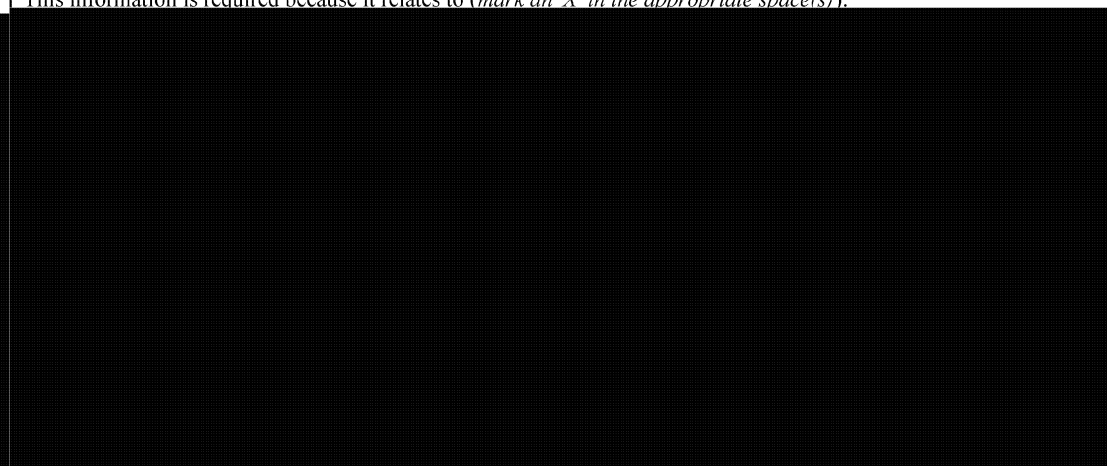
9.5 Enquiries

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

Annex 1: Sample Format for Requests for Suppressed Information via Secure Email

A. Requesting Client's Name	B. Client Title and Organization
C. Report Serial Number	D. Date of Request
E. Information Requested	
F. Rationale for Request (<i>please complete all four questions</i>)	
This information is required because it relates to (<i>mark an 'X' in the appropriate space(s)</i>):	
	
If the request relates to a potential or actual violation of a Canadian law, please cite the law.	
Explain how this information relates directly to an operating program or activity of your department or corporation.	
If the request is for information from a cyber defence report, explain how it relates to the security of a Canadian federal institution's computer system or network, or a network of importance to the Government of Canada.	
G. Please indicate what action, if any, is being contemplated based on this information. (<i>Note that some actions require prior CSE approval.</i>)	
H. Suppressed Information	
Released by:	
Comments:	
This information is provided on the understanding that the requesting department requires the information to perform its lawful duties, and that this information will be handled in accordance with the <i>Access to Information Act</i> and the <i>Privacy Act</i> .	