Policy and Communications Instruction
Sanitizations and Actions-On
PCI-2

Effective Date: 16 June 2014

1. Introduction

1.1 Objective

These Instructions describe the internal processes CSE follows for sanitization/action-on requests relating to SIGINT information.

For guidance on requests related to information derived from IT Security activities, please contact the supervisor of the Privacy and Interests Protection team.

1.2 Context

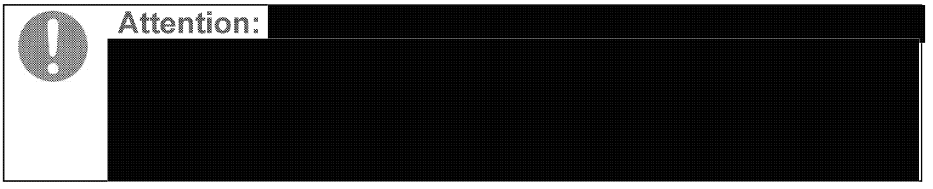
In accordance with the *Policy on Government Security*, CSE is responsible for protecting and distributing SIGINT within Canada. This includes protecting Special Intelligence (SI) sources and processing technologies.

CSSS-100, *Canadian SIGINT Security Standards,* states that CSE must approve all sanitization of SI. Deputy Chief SIGINT (DC SIGINT) is the final CSE authority for approving sanitizations and actions-on. This authority has been delegated to the Director General, Policy and Communications (DG PC).

1.3 Application

These instructions apply to requests from CSE, Government of Canada (GC) partners, and Second Party clients who require CSE's permission to share sanitized text or take action upon SI reports.

This document supersedes OPS-5-9, *End-Product Sanitization/Action-On Procedures*, dated May 2002.



Continued on next page

Introduction, Continued

1.4 Accountability

This table outlines the accountabilities for revising, reviewing, recommending and approving this document.

Who	What
DG PC	Approves
DLS	Reviews
Director, Disclosure Policy and Review (DPR)	• Recommends • Reviews for consistency with the policy framework
Manager, Corporate and Operational Policy	• Revises • Ensures Staff Compliance
Privacy and Interests Protection team	Complies with these instructions and any amendments

1.5 References

- *National Defence Act*
- *Security of Information Act*
- *Policy on Government Security*
- OPS-1-1, *Procedures for the release of Suppressed Information from SIGINT Reports*
- OPS-1-7, *Operational Procedures for naming in SIGINT Reports*
- OPS-4-1, *Operational Procedures for Assistance to Law Enforcement and Security Agencies Under Part (C) of the CSEC Mandate*
- OPS-6, *Operational Policy on Mistreatment Risk Management*
- CSSS-100, *Canadian SIGINT Security Standards*
- QRPC policies, guidelines and agreements
- *CSE Ethics Charter*
- *Operational Policy Glossary*

1.6 Enquiries

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.

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

2. Overview

2.1 Action-On Requests

Action-on requests are sent to the Privacy and Interests Protection team when a client proposes to take any action as a result of information derived from SIGINT.

An action-on request must be approved by CSE if the SI source could be jeopardized. This often, but not always, involves a sanitization.

2.2 Sanitization Requests

Sanitization requests are sent to the Privacy and Interests Protection team when a client proposes to make SI information available to personnel that are not indoctrinated for SI, or when a client wishes to downgrade the classification level of the information while maintaining the SI protection.

2.3 Permission to Quote Requests

Permission to quote requests are sent to the Privacy and Interest Protection team when a client proposes to include SI material in an assessment or paper that retains SI control markings, original wording and original classification

2.4 Client Accreditation

All clients seeking information must have the appropriate accreditation to receive the information. Requests must be submitted online to the Privacy and Interests Protection team by individuals accredited to view SIGINT material and with a need-to-know.

3. Processing Requests

3.1 Validating the Requirement

When reviewing client requests, the Privacy and Interests Protection team must determine whether a sanitization or action-on is required.

A request for sanitization or action-on will not be approved if:

- There is no [redacted] that would allow the information to be shared (except in exceptional circumstances); or
- Intelligence relates to communications information.

In addition, a request for a sanitization/action-on is not required when:

- The [redacted] (this negates the need for a request); or
- The information is being disseminated within SI channels at the original classification of the report (this is a "Permission to Quote").

> **Note:** Sanitizations without a [redacted] may be approved on a case-by-case basis. For further information please consult the Supervisor of the Privacy and Interests Protection team.

3.2 Required Information

The Privacy and Interests Protection Team requires the following information for a sanitization or action-on request:

[redacted]

Continued on next page

Processing Requests, Continued

3.3 Sanitized Text

When reviewing a sanitization request, the Privacy and Interests Protection team must assess whether the proposed text for dissemination:

- Contains only essential information;
- Has a level of detail consistent with the [redacted]
- [redacted] and
- Is consistent in format to other documents from the requesting department.

3.4 Additional Considerations

The release of information through a sanitization or action-on may result in a variety of outcomes. To reduce the likelihood that the outcomes are detrimental to the GC, CSE, or an individual or group, the Privacy and Interests Protection team must consider the following:

- Is there an imminent threat to life?
- Is the SI from a collection [redacted]
- Is the request related to law enforcement?
- Does the information include a Canadian, Second Party identity or suppressed foreign identity?
- If the request is an action-on only, will the action take place within GC channels or outside Canada?

3.5 Release Outside of Canada

Sanitization requests that involve a named Canadian or a foreigner in Canada, and are intended for a recipient outside Canada may be subject to the procedures outlined in OPS-1-1, *Procedures for the Release of Suppressed Information from SIGINT Reports.*

Similarly, if information is requested by a foreign entity for release outside of Five Eyes channels and the proposed text allows for the identification of an individual, the request is subject to the Mistreatment Risk Assessment as outlined in PCI-01, Mistreatment Risk Assessment Process When Sharing Information with Foreign Entities. GC departments are responsible for assessing the risk of mistreatment, in accordance with their own Ministerial Directives.

Continued on next page

Processing Requests, Continued

3.6 Consultation

When reviewing sanitization or action-on requests based on CSE reporting or collection, the Privacy and Interests Protection team may consult:

- The relevant CSE reporting and/or collection areas; and
- The Directorate of Legal Services (DLS) and CSE's Disclosure Support Unit, for risks related to disclosure in legal or judicial proceedings

When a request is based on Second Party reporting or collection, the Privacy and Interests Protection team must follow Quinquepartite Reporting Policy Conference (QRPC) Guidelines and agreements (see paragraph 4.3).

4. Approval Process

4.1 Approval Authority

The authority to approve sanitizations and actions-on rests within DGPC at varying management levels. Depending on the circumstances of the request, the Privacy and Interests Protection Team may consult or request approvals from CSE senior management or Second Parties. For further information on roles and responsibilities see section 6.1.

4.2 Second Party Approval

In situations where Second Party equities are implicated in the sanitization or action-on process, QRPC Guidelines and relevant Second Party documentation should be consulted for additional guidance. In urgent threat-to-life situations, the appropriate DGPC representative may approve a sanitization without seeking prior approval from Second Parties, however, Second Parties must be notified as soon as possible after the fact. For information on appropriate approval authorities please see section 6.1.

Note: If a sanitization or action-on is based on Second Party reporting or collection, Second Party approval may be required before approaching CSE senior management. (See paragraph 4.3, Second Party Approval Required – Sanitizations/Actions-on, for details.)

For information on when Second Party approval is not required please consult the [redacted]

4.3 Second Party Requests

Second Party clients requiring a sanitization of CSE end-product reports or information based on Canadian collection must first seek approval from their own SIGINT agencies. These agencies will seek CSE approval when the sanitization or action-on will be:

- Used in legal or judicial proceedings;
- Used by law enforcement where the intention is to detain or arrest;
- Based on CSE GAMMA end-products;
- Passed to recipients outside national and official channels; or
- Released at the CONFIDENTIAL, RESTRICTED, PROTECTED or UNCLASSIFIED level.

Continued on next page

Approval Process, Continued

4.4 Urgent After-Hour Approval

The Privacy and Interests Protection team work on a rotational schedule and are on-call 24/7. In the case of an urgent request during silent hours, COPCC staff will refer to the schedule posted on the [redacted] and contact the individual on call.

The team member on call must follow regular protocol and approval processes when dealing with these urgent requests.

4.5 Emergency Approval

Clients may approve sanitizations or actions-on **only** if there is an imminent threat to life and no time to contact CSE for approval (i.e. action or information is needed within minutes).

The Privacy and Interests Protection team must be notified as soon as possible after the fact. In notifying CSE, clients must provide the required information listed in paragraph 3.2 as well as an explanation of the circumstances that required the emergency approval. The Privacy and Interests Protection team must notify any relevant stakeholders as soon as they are informed of such a situation.

5. Dissemination

5.1 Handling

When approving a request, the Privacy and Interests Protection team must include the appropriate caveats. A list of caveats for both Government of Canada and Second Party clients can be found on the [redacted]

The approved sanitized text or action-on information may only be disseminated as approved by CSE and as stipulated in the caveats.

> **Note:** Unless the request is for an UNCLASSIFIED release, the information remains classified or designated and must be treated in accordance with the *Security of Information Act*, the *Policy on Government Security* and departmental security standards.

5.2 Use of Suppressed Information

Identity information related to Canadians, persons in Canada, and Second Party entities may not be used in sanitizations/actions-on unless the identity has been released in accordance with OPS-1-1.

5.3 File Retention

The Privacy and Interests Protection team must maintain a record of client requests as part of the decision process. For further information on the procedures related to the file retention process please contact the Supervisor of the Privacy and Interest Protection Team.

5.4 Classification Markings

When responding to a client request the Privacy and Interest Protection team must ensure that the email response carries an appropriate classification marking.

Email responses include references to report numbers and therefore must be classified at the same level as the report in the original request.

6. Roles and Responsibilities

6.1 Roles and Responsibilities

This table describes the key roles and responsibilities for sanitization or action-on requests. For further information on assessing risk of mistreatment or the release of suppressed identity information refer to OPS-6 and OPS-1 respectively.

Who	Responsibilities
Directorate of Legal Services	• Providing legal advice, as required
[redacted]	• May be consulted on requests based on Restricted reporting
[redacted]	• May be consulted on requests associated with Canadian sources
DG PC	• Making decision on requests for use in legal or judicial proceedings (may consult with DC SIGINT)
Manager, Corporate and Operational Policy	• Making decision on requests involving: ○ Law enforcement [redacted] ○ Releases at the CONFIDENTIAL, RESTRICTED or UNCLASSIFIED levels
Manager of Appropriate Reporting Team	• May be consulted on sensitive releases based on CSE reporting
Supervisor, Privacy and Interests Protection Team	• Providing recommendations on requests that require senior management approval • Making decisions on CSIS and RCMP action-on requests to disclose CII [redacted]
Disclosure Support Unit	• May be consulted regarding requests that may entail risk of disclosure in legal or judicial proceedings
Privacy and Interests Protection Team	• Processing requests • Obtaining required approvals • Managing and coordinating the approval and consultation process • Answering questions as required • Providing final replies to requests • Maintaining records of requests