Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Canadian SIGINT Operations Instruction CSOI-5-8

Active Monitoring Procedures for [redacted]

Last Updated:
5 Jan 2009

SIGINT

Canada

Table of Contents

1. Introduction

1.1 Objective

These instructions outline the procedures that apply to the [redacted] in establishing and implementing an active monitoring program for SIGINT systems and processes within their area of responsibility. These instructions also describe how SIGINT Programs Oversight and Compliance conduct compliance validation monitoring of [redacted] active monitoring procedures.

1.2 Authority

This Canadian SIGINT Operations Instruction is issued under the authority of the CSEC Deputy Chief, SIGINT.

1.3 Context

These instructions were created in response to OPS-1-8 *Active Monitoring of Operations to Ensure Legal Compliance and the Protection of the Privacy of Canadians*. Active monitoring is required in order to ensure that SIGINT activities are being pursued using tools and processes that are compliant with CSEC's legal and policy obligations. An active monitoring program also ensures compliance issues are identified, addressed, and tracked.

This instruction focuses on three aspects of [redacted] that require regular auditing:

- Ensuring existing systems, procedures, and practices are legal and compliant;
- Ensuring personnel within the [redacted] have a full understanding of the legal and compliance obligations that apply to their duties;
- Ensuring that legal and compliance issues are tracked and measures are taken to address them.

1.4 References

OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the conduct of CSEC Activities*
OPS 1-8, *Active Monitoring of Operations to Ensure the Legal Compliance and the Protection of the Privacy of Canadians*
OPS-1-13, *Procedures for Canadian* [redacted]

[redacted] *Activities*
OPS 2-1, *Get Policy Wise(GPW-005-07)*
OPS 3-1, *Procedures for* [redacted] *Operations*
OPS 4-1, IRRELEVANT
OPS 4-2,
OPS 4-3,
CSOI-1-1, *The National SIGINT Priorities List(NSPL) Process*

1.5 Application

These instructions apply to all individuals employed within [redacted] and SIGINT Programs Oversight and Compliance (SPOC).

1.6 Accountability

The following table outlines responsibilities with respect to these instructions.

Who	**Responsibility**
Deputy Chief SIGINT	Approving these instructions
Director General SIGINT Programs	Recommending these instructions for approval
Director SIGINT Requirements, SIGINT Programs	• Promulgating and implementing these instructions • Revising these instructions as required • Seeking legal and/or policy advice if required • Responding to questions concerning these instructions
Director [redacted]	Applying these instructions
All SIGINT Directors and managers who are affected by these instructions	Ensuring that their staff has read, understood and complies with these instructions and any amendments to these instructions
All SIGINT staff who are affected by these instructions	Reading, understanding and complying with these instructions and any amendments to these instructions

1.7 Amendment Process

Situations may arise where amendments to these instructions may be required because of changing or unforeseen circumstances. All approved amendments will be announced to staff and will be posted at [redacted]

1.8 Enquiries

Questions related to these instructions should be directed to operational managers, who in turn will consult with SIGINT Programs Oversight and Compliance staff (e-mail) spoc-staff-dl when necessary.

2. [redacted] Validation Check Process: Collection Managers

2.1 Introduction

This section outlines the existing systems, procedures, and practices used by [redacted] collection managers as well as the measures they take to ensure their activities are compliant with CSEC's legal and policy obligations and to ensure the protection of the privacy of Canadians. The collection manager relies on experience, analysis, research and target development skills in producing effective targeting.

2.2 [redacted] Collection Managers

On a daily basis, collection managers are responsible for validating and implementing targeting requests on the basis of:

- appropriate justification
- valid Government of Canada requirements (GCRs)
- adherence to SIGINT priorities, and compliance with policy and legal constraints
- technical feasibility
- ensuring the SIGINT system is not jeopardized

The Collection management team must ensure targeting and collection activities on each selector submitted by CSEC and Second Party analysts are compliant with and abide by Canadian and allied laws, statutes or policies. The [redacted] work is guided by a variety of targeting methods and techniques, as well as special computer applications, formats and protocols applicable to each particular source.

2.3 CSEC Targeting Requests

Collection managers are responsible for validating and implementing targeting requests on behalf of CSEC analysts. In order to complete these targeting requests, collection managers must:

- confirm targeting requests are properly formatted and include applicable handling instructions (i.e. access control lists (ACLs) , zip/categories, expiration dates, a uthorizations as required)
- ensure the targeting requests are directed at a ***foreign*** entity located ***outside*** Canada (as reflected in the digraph/trigraph)
- confirm there is a valid GCR
- confirm targeting requests have a valid and well-defined justification
- confirm targeting requests comply with CSEC mandates and policies
- ensure targeting requests are applied to the appropriate Canadian [redacted] collection assets in accordance with most recent [redacted] rules, restrictions and guidelines
- notify SIGINT sponsoring element of targeting requests results

2.4 Second Party Targeting Requests

Collection managers are responsible for validating and implementing targeting requests on behalf of Second Party analysts. In order to complete these targeting requests, they must:

- confirm targeting requests are properly formatted and include applicable handling instructions [redacted] are applied.
- ensure the targeting requests are directed at a ***foreign*** entity located ***outside*** Canada (as reflected in the digraph/trigraph)
- confirm there is a valid GCR
- confirm targeting requests have a valid and well-defined justification
- confirm targeting requests comply with CSEC mandates and policies
- ensure targeting requests are applied to the appropriate Canadian collection asset in accordance with most recent [redacted] rules, restrictions and guidelines
- notify SIGINT sponsoring element of targeting requests results

2.5 [redacted]

Collection managers receive a daily [redacted] report from [redacted] The report identifies targeted entities that have [redacted] (i.e. that are found to be located within Canada) and therefore, must be de-targeted. On receipt of this report collection managers perform the following actions:

- use current operational policies and guidelines to identify which selector needs to be de-targeted
- query selectors in targeting tool to identify the SIGINT analyst responsible for them
- notify the responsible SIGINT analyst that selector de-targeting has occurred for their target
- ensure [redacted] that have been de-targeted will only be retargeted upon the receipt of data confirming the target has left Canada
- produce a [redacted] summary of [redacted] activity; the [redacted] summary will be documented in CERRID *Corporate Management/Authorities/Policy/Operational Policy* using SLUG: [redacted] **1-8 2.5** [redacted] **Summary yyyy/mm/dd**

2.6 Targeting Dictionary Validation

Collection managers shall conduct a [redacted] comparison of targeted selectors in targeting applications (i.e. [redacted]) with those on active collection in [redacted] dictionaries; any discrepancies will be reported to manager [redacted] The [redacted] checks will be documented in CERRID *Corporate Management/Authorities/Policy/Operational Policy* using SLUG: [redacted] **1-8 2.5 Dictionary yyyy/mm/dd**

3. [redacted] Validation Check Process: [redacted] Managers

3.1 Introduction

The [redacted] management team writes, validates, and, changes if necessary, the following criteria based on established business rules:

- Access control compartments and restrictions (not covered by ECI program)
- Restriction rules to prevent misrouted data
- Data expiry date
- Security classification

[redacted] and data are evaluated in order to perform these functions.

3.2 System Changes

Following system software or hardware changes or upon deployment of new systems, the [redacted] management team shall:

- Revalidate business rules upgrades and maintain a record of these revalidation checks
- Revalidate business rules on a [redacted] basis and maintain a record of the revalidation checks in CERRID *Corporate Management/Authorities/Policy/Operational Policy* using an EXCEL spreadsheet and SLUG: [redacted] **1-8 3.2 Business Rule Revalidation yyyy/mm/dd**

3.3 Data Minimization Required

Regarding data that requires minimization, the [redacted] management team shall:

- Ensure minimization rules are applied to applicable data prior to release of data to appropriate repository
- Revalidate minimized data following system upgrades and upon deployment of new systems

3.4 Request for new dataflow

Upon request for establishment of a new dataflow, the [redacted] management team shall:

- Ensure justification is submitted prior to establishing any new dataflow; new dataflows will only be established as a result of authorized targeting or tasking

- Ensure destination repositories for new dataflows within CSEC are authorized and have a traffic annotation capability if the data is accessible to [redacted] analysts
- Maintain a record of approved dataflow requests in CERRID *Corporate Management/Authorities/Policy/Operational Policy* using SLUG: [redacted] **1-8 3.4 Dataflow Requests yyyy/mm/dd**

4. [redacted] Validation Check Process: Mission Coordinators

4.1 Introduction

The mission coordination team is responsible for all tasking to and from CSEC for CSEC [redacted] collection assets. Tasking is only established upon the completion and signed approval of an Activity Authorization Request (AAR).

4.2 Tasking Request

Upon the receipt of a new tasking request the mission coordination team shall:

- Complete Activity Authorization Request(AAR) and obtain approval
  - ♦ Activity Authorization Requests must include at a minimum:
    - ○ an intelligence requirement
    - ○ associated GCR
    - ○ NSPL Tier Level
    - ○ Sponsoring Element
    - ○ Tracking number
- Maintain an automated record of all tasking requests and make accessible to SPOC upon request

4.3 Tasking Revalidation

Following an initial tasking request the mission coordination team shall:

- Revalidate at [redacted]
- Maintain an automated record of all revalidation requests and make available to SPOC upon request

4.4 [redacted] Tasking Check

On a periodic basis, the mission coordination team shall:

- Confirm collection activity at CSEC and CFIOG collection assets is in accordance with an existing AAR on a [redacted] basis
- Remove any unauthorized tasking immediately until such time as a valid AAR is written and approved
- Report unauthorized tasking to manager [redacted] and SPOC staff and

document in CERRID *Corporate Management/Authorities/Policy/Operational Policy* using SLUG: [redacted]

5. [redacted] Validation Check Process: [redacted] Manager

5.1 Introduction

The [redacted] manager is responsible for tasking, targeting, and [redacted] teams and as such is responsible to ensure all staff adhere to the provisions of this CSOI.

5.2 Application of this CSOI

The [redacted] manager shall ensure staff understand and adhere to the active monitoring procedures outlined in these instructions.

5.3 Vulnerability Noted

In the event that an operational vulnerability is noted during the normal course of operations, the [redacted] manager shall:

- Report any vulnerability or weakness in operational activities to SPOC using the vulnerability report form (see ANNEX C for details)
- Include a plan to address the weakness identified in the report
- Document the vulnerability in CERRID *Corporate Management/Authorities/Policy/Operational Policy* using SLUG: [redacted]

5.4 Occurrence of Non-Compliance Incident

Upon the discovery of an incident of non-compliance, the manager [redacted] shall:

- Immediately report incidents in accordance with operational policy
- Document the occurrence in CERRID *Corporate Management/Authorities/Policy/Operational Policy* using the Incident report form (ANNEX D) and SLUG: [redacted]

5.5 [redacted] Compliance Checks

The manager [redacted] is responsible for ensuring all monthly [redacted] compliance checks completed by collection mangers, [redacted] managers, and mission coordinators are available in CERRID as described in this document and accessible to SPOC staff.

5.6 [redacted] staff Legal and Compliance Policy Sign-off

The [redacted] manager is responsible for maintaining a copy of staff policy sign off sheets(ANNEX B) in CERRID *Corporate Management/Authorities/Policy/Operational Policy* using SLUG: [redacted] and make available to SPOC upon request.

6. Personnel

6.1 Introduction

This section outlines the measures to be taken by [redacted] staff to ensure they have a thorough understanding of CSEC legal obligations with respect to protecting the privacy of Canadians.

6.2 Policies

All [redacted] staff will be knowledgeable with respect to policies and guidelines pertaining to legal compliance and protecting the privacy of Canadians. (See **Annex A** for a list of applicable guidelines and policies.)

[redacted] staff will, on an annual basis, read and acknowledge having read all documents listed in Annex A.

[redacted] manager is responsible for assisting staff in their understanding of all applicable policies and guidelines.

7. SPOC Compliance Validation Monitoring Process

7.1 Introduction

This section outlines procedures for SPOC staff in assessing the [redacted] validation process for compliance with CSEC policy instruments aimed at ensuring compliance and protection of the privacy of Canadians.

7.2 Frequency of compliance validation monitoring activities

The frequency of SPOC compliance validation checks and processes are outlined in the following table.

Step	Action
1	[redacted] - Review a sample of active monitoring checks done by [redacted] -[redacted] **1-8 2.5 [redacted] Summary yyyy/mm/dd** -[redacted] **1-8 2.6 Dictionary yyyy/mm/dd** -[redacted] **1-8 3.4 Dataflow Requests yyyy/mm/dd** - Review a sample of active monitoring logs created by [redacted] -[redacted] **1-8 3.2 Business Rule Revalidation yyyy/mm/dd** - Review all tasking [redacted] by [redacted]
2	[redacted] - Review [redacted] Staff Legal and Compliance document sign-off forms - Review active monitoring procedures to ensure they are up-to-date - Review [redacted] targeting dictionary validation check - Document any anomalies in policy or procedures and take appropriate follow-up action
3	As required: - Document any vulnerability from a compliance perspective and ensure appropriate remedial action is taken - Report incidents of non-compliance to the appropriate

	authority for follow-up action
4	Periodically: - Conduct oversight compliance spot checks on targeting, tasking, and dataflow activities and procedures

ANNEX A

[redacted] personnel must be knowledgeable on all laws, policies and guidelines pertaining to legal compliance and the protection of the privacy of Canadians. It is critical that [redacted] staff have a thorough understanding of the information contained within the following documents:

Law:

- *The National Defence Act*
- *Section 16 of the CSIS Act*
- *Section 8 of the Canadian Charter of Rights and Freedoms*
- *Section 184 of the Criminal Code*
- [redacted]
- *Privacy Act*

Policies:

- *OPS-1, Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities*
- *OPS 1-8, Active Monitoring of Operations to Ensure Legal Compliance and the Protection of the Privacy of Canadians*
- *OPS 1-13, Procedures for Canadian* [redacted] *Activities*
- *OPS 3-1, Procedures for* [redacted] *Operations*
- IRRELEVANT
-
-

GPW Documents:

- [redacted]
-

CSEC SIGINT Operations Instructions:

- *CSOI-1-1: The National SIGINT Priorities List (NSPL) Process*
- *CSOI-3-3: Instructions for Initiating and Processing Request for* [redacted] *collected via* [redacted]
- *CSOI-3-7* [redacted] *Authorities*

ANNEX B

Dataflow Analyst: ______________________________ ______________________________	Date
Laws:	
[redacted]	
The National Defence Act	
Section 16 of the CSIS Act	
Section 8 of the Canadian Charter of Rights and Freedoms	
Section 184 of the Criminal Code	
[redacted]	
Privacy Act	
Policies:	
[redacted]	
OPS-1 Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities	
OPS 1-8 Active Monitoring of Operations to Ensure Legal Compliance and the Protection of the Privacy of Canadians	
OPS 1-11 Retention Schedules for SIGINT Data	
OPS 1-13 Procedures of Canadian [redacted]	
OPS 3-1 Procedures for [redacted] Operations	
OPS 4-1 IRRELEVANT	
OPS 4-2	
OPS 4-3	
OPS 5-7 ECI Handling Standards	
OPS 5-14 The SIGINT Classification System	
CSEC SIGINT Operations Instructions:	
[redacted]	
CSOI-1-1 The National SIGINT Priorities List (NSPL) Process	

IRRELEVANT

CSOI-3-3 Instructions for Initiating and Processing Request for [redacted] collected via [redacted]

CSOI-3-5 [redacted] Operations In Support of Canadian Forces

CSOI-3-7 [redacted] Authorities

CSOI-5-8 [redacted] Procedures for SIGINT Activity Area [redacted]

Collection Manager: ______________________________ ______________________________	**Date**
Laws:	
[redacted]	
The National Defence Act	
Section 16 of the CSIS Act	
Section 8 of the Canadian Charter of Rights and Freedoms	
Section 184 of the Criminal Code	
[redacted]	
Privacy Act	
Policies:	
[redacted]	
OPS-1 Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities	
OPS 1-8 Active Monitoring of Operations to Ensure Legal Compliance and the Protection of the Privacy of Canadians	
OPS 1-13 Procedures of Canadian [redacted] Activities	
OPS 3-1 Procedures for [redacted] Operations	
OPS 4-1 IRRELEVANT	
OPS 4-2	
OPS 4-3	
GPW Documents:	
[redacted]	
[redacted]	
[redacted] Targeting Justification	
CSEC SIGINT Operations Instructions:	
[redacted]	

CSOI-1-1 The National SIGINT Priorities List (NSPL) Process	
CSOI-3-3 Instructions for Initiating and Processing Request for [redacted] collected via [redacted] CSOI-3-7 [redacted] Authorities CSOI-4-4 Targeting and Selector Management	

Mission Coordination Analyst:

____

____

Date

Laws:

[redacted]

The National Defence Act

Section 16 of the CSIS Act

Section 8 of the Canadian Charter of Rights and Freedoms

Section 184 of the Criminal Code

[redacted]

Privacy Act

Policies:

[redacted]

OPS-1 Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities

OPS-1-8 Active Monitoring of Operations to Ensure Legal Compliance and the Protection of the Privacy of Canadians

OPS-1-13 Procedures of Canadian [redacted] Activities

OPS-3-1 Procedures for [redacted] Operations

CSEC SIGINT Operations Instructions:

[redacted]

CSOI-1-1 The National SIGINT Priorities List (NSPL) Process

CSOI-3-7 [redacted]

CSOI- 5-8 [redacted] Procedures for SIGINT Activity Area [redacted]
[redacted]

ANNEX C

Vulnerability Report

Date:

Nature of vulnerability (*provide detailed explanation of vulnerability being reported*)

Corrective Action Taken:

Analyst:

Manager:

SPOC POC:

ANNEX D

Incident Report

Date:

Nature of Incident: (*provide detailed explanation of incident being reported*)

Impact on Privacy:

Corrective Action Taken:

Analyst:

Manager:

SPOC POC:

CSOI-5-8 Promulgation

Reviewed and Recommended for Approval

I have reviewed and hereby recommend this instruction for approval.

James Abbott
A/Director General SIGINT Programs

Date

Approved

I hereby approve CSOI-5-8: Active Monitoring Procedures for [redacted] This instruction is effective immediately.

Peter Cork
A/CSEC Deputy Chief SIGINT

Date