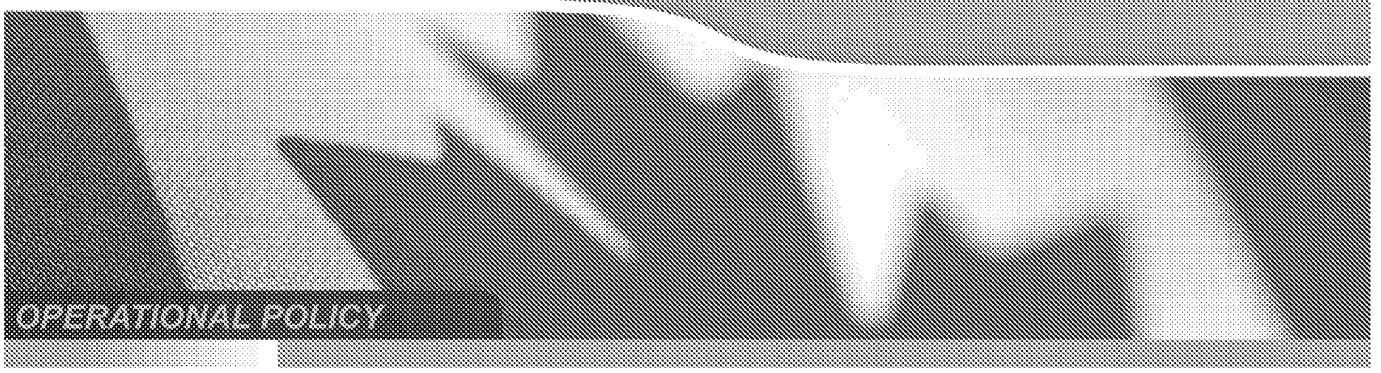
Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

OPS-1-8

Operational Procedures for Policy Compliance Monitoring to Ensure Legal Compliance and the Protection of the Privacy of Canadians



Canada

Table of Contents

1. Introduction 2
1.1 Scope 2
1.2 Objective 2
1.3 Policy 3
1.4 Context 3
1.5 Application 3
1.6 Authority 4
2. How Compliance Monitoring Works 5
What Must be Monitored 5
2.1 Themes 5
How Compliance Monitoring Happens 6
2.2 General 6
2.3 IPOC and SPOC Reporting Responsibilities 6
2.4 Reporting to Deputy Chiefs 6
Follow-up Actions for Policy Non-Compliance 7
2.5 Reporting to Deputy Chiefs General Follow-on Actions for Non-Compliance 7
2.6 Follow-on Actions for Needed Improvements 7
3. Roles and Responsibilities for Policy Compliance Monitoring Activities 8
3.1 Responsibilities 8
4. Accountability for OPS-1-8 10
4.1 Accountability 10
4.2 References 10
4.3 Amendments 10
4.4 Enquiries 10
5. Definitions 11
5.1 Accountability Markings (AM) 11
5.2 Business Information 11
5.3 Canadian 11
5.4 Compliance Monitoring 12
5.5 Data 12
5.6 Information about Canadians 12
5.7 Integree 12
5.8 Ministerial Authorization 13
5.9 Privacy Annotations 13
5.10 Private Communication 13
5.11 Retention 14
5.12 Secondee 14
5.13 Selectors 14
5.14 Targeting 14

5.15 Tasking 14

Annex 1 15

1. Introduction

1.1 Scope

These procedures describe CSEC's policy compliance monitoring program, which demonstrates the legal compliance of CSEC's mission operations that might impact lawfulness/privacy. These procedures describe at a high level what must be monitored, and assign responsibility for the program's management and oversight.

These procedures describe only the activities required to monitor compliance with the legal and privacy related provisions of OPS-1 Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities and other relevant policy instruments, individual procedures, or operating instructions. Compliance monitoring for other purposes is not covered in these procedures.

These procedures supersede OPS-1-8, Active Monitoring of Operations to Ensure Legal Compliance and the Protection of the Privacy of Canadians, dated 11 March 2009.

1.2 Objective

CSEC's mandate as the National Cryptologic Agency consists of three parts:

a) acquire and use information from the global information infrastructure (GII) for the purpose of providing foreign intelligence, in accordance with Government of Canada (GC) intelligence priorities;

b) provide advice, guidance and services, to help ensure the protection of electronic information and of information infrastructures of importance to the GC; and

IRRELEVANT

These are commonly referred to as part (a), part (b), IRRELEVAN of the Mandate, respectively. It is important to demonstrate that CSEC has an effective management-control framework, in addition to policies and

Continued on next page

1.2 Objective (continued)

requirements. The purpose of these procedures is to ensure that when conducting operational activities under part (a), part (b) or IRRELE of its Mandate, CSEC can demonstrate compliance with policy instruments, addressing

- legal requirements, and
- protection of the privacy of Canadians

Following these procedures will ensure that:

- CSEC management and staff follow authorized policies and procedures related to the privacy of Canadians and the lawfulness of their activities,
- there is written verification that regular monitoring is conducted, and
- gaps or errors in existing policies, procedures or processes are identified, which supports a compliance monitoring program that is responsive to changing requirements.

1.3 Policy

IT Security Policy Oversight and Compliance (IPOC) and SIGINT Programs Oversight and Compliance (SPOC), in cooperation with SIGINT and IT Security operational elements, must establish a compliance monitoring program in their respective activity areas to assess the compliance of operational activities with policy instruments addressing legal requirements and the protection of the privacy of Canadians. This program shall document all compliance monitoring activities.

1.4 Context

CSEC must comply with the law in all of its activities. In addition, all operations must be conducted in accordance with the policies and practices set out in CSEC policy instruments and in accordance with any ministerial direction provided to CSEC. These procedures provide guidance to CSEC managers to help them assess and demonstrate compliance with the law and the applicable policy instruments in the activities for which they are responsible.

1.5 Application

These procedures apply to CSEC management and staff, including secondees, contractors and integrees, involved in conducting or supporting policy compliance monitoring. They also apply to CFIOG in the conduct of its operations under part (a) IRRELEVA of the CSEC Mandate.

1.6 Authority

These procedures form part of the policy framework in place to ensure legal compliance, including the protection of the privacy of Canadians, which stem from and include:

- the laws of Canada, including the National Defence Act, part V.1, and the Privacy Act, and the Criminal Code
- the Ministerial Directive on the Privacy of Canadians
- the *Ministerial Directive on CSE's Accountability Framework*, and
- OPS-1, Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities.

2. How Compliance Monitoring Works

What Must be Monitored

2.1 Themes

The following table identifies "theme" activities related to lawfulness and protecting the privacy of Canadians that are subject to policy compliance monitoring. The relevant Canadian SIGINT Operations Instructions (CSOIs) and IT Security Operating Instructions (OIs) describe in more detail what must be assessed.

The table lists the activities and specific categories that must be monitored over a 3-year period. The specific categories may be revised over time, as monitoring or operations develop.

Activity	Specific Category
Data handling	• Essentiality • Privacy annotations and accountability markings • Access to databases
Reporting	• Sign-off levels • Contextual identification
Data retention and disposition	• Retention schedules • Destruction
Collection management	• SIGINT Tasking • SIGINT Targeting • IT Security data collection
Information management	• Corporate files related to authorities
Conditions imposed by Ministerial Authorizations	• Inputs to Reports to Minister
Dissemination	• Sharing data • Sharing reports

How Compliance Monitoring Happens

2.2 General

SPOC and IPOC will develop compliance monitoring plans describing how they will monitor each of the activities listed in this document at least once every three years. Other activities may be added to these plans as policy development progresses or as monitoring is implemented. Complete information about the specific activities that must be monitored will be promulgated by SPOC in CSOIs and by IPOC in OIs, which will be updated as required. Compliance monitoring records must be retained for a minimum of five years for audit or review purposes.

2.3 IPOC and SPOC Reporting Responsibilities

IPOC will report biannually to the Director, Program Management and Oversight (PMO) on compliance monitoring activities and issues within IT Security. SPOC will report biannually to the Director, SIGINT Requirements on compliance monitoring activities and issues with SIGINT. Information copies of all biannual report should also be provided to D2.

2.4 Reporting to Deputy Chiefs

In IT Security,

- Director PMO will report annually to DC ITS, in collaboration with DG Cyber Defence (DGCD).

In SIGINT,

- Director, SIGINT Requirements will report biannually to DG SIGINT Programs (DGP), and
- DGP will report annually to DC SIGINT.

In addition to the annual reports, any serious non-compliance issue will be reported to the appropriate Deputy Chief in accordance with paragraph 2.5.

Follow-up Actions for Policy Non-Compliance

2.4 Reporting to Deputy Chiefs General Follow-on Actions for Non-Compliance

If compliance monitoring activities identify non-compliance with policy instruments that support legal compliance and/or protection of the privacy of Canadians, then the following actions must be taken:

- The manager responsible for the area where the non-compliance was observed must:
  - advise IPOC or SPOC as appropriate
  - ensure corrective action is taken
  - work with SPOC or IPOC to track actions taken and monitor future activity to ensure ongoing compliance
  - advise his or her director[1], and

- IPOC or SPOC will prepare a report on the non-compliance that includes
  - a description of the event or issue
  - an analysis of the impact on lawfulness and/or privacy of Canadians
  - any corrective action taken and/or follow-up required, and

- IPOC or SPOC will forward the report to the appropriate managers and directors. In the case of privacy-related non-compliance incidents, the report will also be forwarded to Operational Policy. In the case of lawfulness-related non-compliance incidents, the report will also be forwarded to DGPC with an info copy to DLS.

	**Note:** The same steps must be taken if any non-compliance with policy instruments that support legal compliance and/or protection of the privacy of Canadians is observed outside the framework of compliance monitoring.

2.6 Follow-on Actions for Needed Improvements

If a manager identifies deficiencies or areas for improvement related to ensuring legal compliance and/or protecting the privacy of Canadians in operational activities, monitoring measures, or operational policy instruments, then the manager must advise IPOC or SPOC as appropriate. IPOC or SPOC will make recommendations regarding any needed follow-on actions, notify all the parties concerned, and prepare a record of the action taken.

[1] The director may direct that non-compliance incidents of a minor nature need not be reported to him or her individually.

3. Roles and Responsibilities for Policy Compliance Monitoring Activities

3.1 Responsibilities

This table describes the key responsibilities inside CSEC with respect to the process of monitoring for policy compliance.

Who	Responsibility
Deputy Chiefs	• Ensuring that an effective compliance monitoring program is in place • Reviewing compliance monitoring reports submitted to them
• DGP • DGCD and Director PMO	• Ensuring that a compliance monitoring program is developed and implemented • Reviewing compliance monitoring reports submitted to them • Forwarding compliance monitoring reports to the Deputy Chiefs
Directorate of Legal Services	• Providing legal advice, when requested
• Director SIGINT Requirements • Director PMO	• Directing the monitoring program as a whole • Reviewing reports forwarded to them • Taking a leadership role in addressing any identified deficiencies • Forwarding compliance monitoring reports to DGs
• SPOC • IPOC	• Developing and implementing a policy compliance monitoring program • Assisting managers in the conduct of policy compliance monitoring • Maintaining records of policy compliance monitoring activities conducted by managers • Compiling and forwarding reports • Coordinating resolution of legal issues

3.1 Responsibilities (continued)

Who	Responsibility
Operational Directors	• Supporting the monitoring program as a whole • Reviewing reports forwarded to them and taking a leadership role in addressing any identified deficiencies
• IT Security and SIGINT managers • CFIOG HQ	• Conducting policy compliance monitoring as directed in these procedures and in accordance with direction from IPOC or SPOC • Reporting any non-compliance to their director as well as to IPOC or SPOC • Taking appropriate corrective action when non-compliance or weaknesses are identified or communicated to them • Seeking legal and policy advice, when appropriate, via approved channels
SIGINT and IT Security operational area personnel and any other parties acting under CSEC authorities, as well as Operational Policy staff	• Cooperating with any elements conducting policy compliance monitoring • Reporting non-compliance or other weaknesses to the appropriate Manager
Director, Audit and Evaluation, and Ethics (DAEE)	• Conducting periodic reviews and audits of the effectiveness of these procedures and of operational compliance with associated policy instruments • Communicating relevant results to the Director, Corporate and Operational Policy (COP), Director, SIGINT Requirements and Director, PMO.
Corporate & Operational Policy	• Addressing policy gaps when identified • Conducting compliance monitoring of its own activities • Reporting any non-compliance to DGPC

4. Accountability for OPS-1-8

4.1 Accountability

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

Who	Responsibility
DC SIGINT	Approve
DC IT Security	Approve
DGPC	Approve
General Counsel, DLS	Review to ensure compliance with the law
Director, Corporate and Operational Policy	Review for consistency with the policy framework
Operational Policy	• Revise • Respond to related questions

4.2 References

- National Defence Act, Part V.1
- Privacy Act
- *Ministerial Directive on CSE's Accountability Framework*, June 2001
- Ministerial Directive on the Privacy of Canadians, June 2001
- Ministerial Authorizations related to various programs
- OPS-1, Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities
- Criminal Code, PartVI

4.3 Amendments

Situations may arise where amendments to these procedures are required because of changing or unforeseen circumstances. These amendments will be communicated to relevant staff and will be posted on the Operational Policy website.

4.4 Enquiries

Questions related to these procedures should be directed to operational managers, who in turn will contact IPOC, SPOC and/or Operational Policy staff.

5. Definitions

5.1 Accountability Markings (AM)	Markings applied by analysts to recognized one-end Canadian emails [redacted] acquired through the [redacted] program, and retained by CSEC because they are essential to international affairs, defence or security.
5.2 Business Information	Business information is information of, from, or about a Canadian company (incorporated under the laws of Canada or a province) the disclosure of which could reasonably be expected to: • result in material financial loss or gain to, or could reasonably be expected to prejudice the competitive position of, the Canadian company, or • interfere with contractual or other negotiations of the Canadian company. (Treasury Board "Security Organization and Administration Standard" and the Access to Information Act, 20(1)(c) and (d)) In some situations this may apply to GC entities (e.g., crown corporations, special operating agencies, etc.).
5.3 Canadian	"Canadian" refers to a) a Canadian citizen, or b) a person who has acquired the status of permanent resident under the Immigration and Refugee Protection Act (IRPA), and who has not subsequently lost that status under that Act, or c) a corporation incorporated under an Act of Parliament or of the legislature of a province. (NDA, section 273.61). For the purposes of this procedure, "Canadian organizations" are accorded the same protection as Canadian citizens and corporations. A Canadian organization is an unincorporated association, such as a political party, a religious group, or an unincorporated business headquartered in Canada.

5.4 Compliance Monitoring	IPOC (for IT Security) and SPOC (for SIGINT) will periodically and independently assess operational activities for compliance with policy instruments in place to ensure legal compliance and to protect the privacy of Canadians.
5.5 Data	For purposes related to compliance monitoring of activities conducted under part (a) of the CSEC Mandate, data is defined as traffic and bulk unselected metadata, and unknown data acquired from the Global Information Infrastructure (GII). For purposes related to compliance monitoring of activities conducted under part (b) of the CSEC mandate, data is defined as information obtained from computer systems or networks of importance to the GC.
5.6 Information about Canadians	This has two meanings: IRRELEVANT IRRELEVANT the term information about Canadians refers to: ○ any personal information about a Canadian, or ○ business information about a Canadian corporation.
5.7 Integree	A person seconded to CSEC from one of CSEC's cryptologic partner organizations.

5.8 Ministerial Authorization

An authorization provided in writing by the Minister of National Defence (the Minister) to CSEC to ensure that CSEC is not in contravention of the law if, in the process of conducting operational activities under part (a) or part (b) of its Mandate, it should intercept private communications. MAs may be granted in relation to an activity or class of activities specified in the authorization pursuant to

- subsection 273.65(1) of the NDA for the sole purpose of obtaining foreign intelligence, or
- subsection 273.65(3) of the NDA for the sole purpose of protecting the computer systems or networks of the GC from mischief, unauthorized use or interference.

When such an authorization is in force, Part VI of the Criminal Code does not apply in relation to an interception of a private communication, or in relation to a communication so intercepted.

5.9 Privacy Annotations

SIGINT privacy annotations are markings applied to SIGINT traffic in traffic repositories for the purpose of identifying private communications, communications of Canadians located outside Canada, solicitor-client communications, and information about Canadians to be retained or deleted. It is the responsibility of analysts whose functions are directly related to the production of SIGINT reports to annotate appropriately SIGINT traffic that is recognized as falling into one the categories described above.

IT Security privacy annotations are markings applied by the CND Team for the purpose of identifying and tracking the use and retention of CND data collected under an MA, when that data is:

- a private communication, in whole or in part, or
- metadata associated with a private communication that can identify one or both communicants or the communication itself.

5.10 Private Communication

"Any oral communication, or any telecommunication, that is made by an originator who is in Canada or is intended by the originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it, and includes any radio-based telephone communication that is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it." (Criminal Code, section 183)

5.11 Retention	The holding of records in either electronic or hard copy form within an organization.
5.12 Secondee	An individual who is temporarily moved from another GC entity or private organization to CSEC, and who at the end of the assignment returns to the originating organization.
5.13 Selectors	A name, [redacted] IP or e-mail address, facsimile or telephone number, or other alphanumeric character stream [redacted] for the purpose of identifying traffic that relates to national foreign intelligence requirements and isolating it for further processing.
5.14 Targeting	To single out for collection or interception purposes.
5.15 Tasking	• A directive to acquire, record and monitor a [redacted] • A directive to analyze or report intelligence information; the activity deriving therefrom. • In Information Technology, a directive to produce, modify, enhance or support hardware, software or documentation. • A request by analysts for sustained collection [redacted] Submitted via a tasking request (AAR).

Annex 1

Definition of Personal Information in the Privacy Act, s. 3

"Personal information" means information about an identifiable individual that is recorded in any form including, without restricting the generality of the foregoing,

(a) information relating to the race, national or ethnic origin, colour, religion, age or marital status of the individual,

(b) information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,

(c) any identifying number, symbol or other particular assigned to the individual,

(d) the address, fingerprints or blood type of the individual,

(e) the personal opinions or views of the individual except where they are about another individual or about a proposal for a grant, an award or a prize to be made to another individual by a government institution or a part of a government institution specified in the regulations,

(f) correspondence sent to a government institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to such correspondence that would reveal the contents of the original correspondence,

(g) the views or opinions of another individual about the individual,

(h) the views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the individual by an institution or a part of an institution referred to in paragraph (e), but excluding the name of the other individual where it appears with the views or opinions of the other individual, and

(i) the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual,

but, for the purposes of sections 7, 8 and 26 and section 19 of the Access to Information Act, does not include

(j) information about an individual who is or was an officer or employee of a government institution that relates to the position or functions of the individual including,

(i) the fact that the individual is or was an officer or employee of the government institution,
(ii) the title, business address and telephone number of the individual,
(iii) the classification, salary range and responsibilities of the position held by the individual,
(iv) the name of the individual on a document prepared by the individual in the course of employment, and
(v) the personal opinions or views of the individual given in the course of employment,

(k) information about an individual who is or was performing services under contract for a government institution that relates to the services performed, including the terms of the contract, the name of the individual and the opinions or views of the individual given in the course of the performance of those services,

(l) information relating to any discretionary benefit of a financial nature, including the granting of a licence or permit, conferred on an individual, including the name of the individual and the exact nature of the benefit, and

(m) information about an individual who has been dead for more than twenty years.