Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

CSEC IT Security Operational Instructions ITSOI-1-6

Cyber Defence Activities: Compliance Monitoring

Canada

Table of Contents

1. Introduction

1.1 Scope

These instructions address the requirements for conducting Compliance Monitoring of Cyber Defence Activities, in response to OPS-1-8, *Operational Procedures for Policy Compliance to Ensure Legal Compliance and the Protection of the Privacy of Canadians,* and identify compliance monitoring responsibilities for the Cyber Defence Branch, Cyber Defence Team, and ITS Policy, Oversight & Compliance (IPOC).

1.2 Application

These instructions apply to CSEC personnel and any other parties, including secondees, contractors and integrees, involved in conducting or supporting cyber defence activities.

1.3 Objective

As required by law, CSEC must have measures in place to ensure lawfulness and protect the privacy of Canadians when conducting its activities. For Cyber Defence, these measures are set forth in:

- OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities*
- OPS-1-6, *Operational Procedures for Naming and Releasing Identities in Cyber Defence Reports*
- OPS-1-14, *Operational Procedures for Cyber Defence Operations Conducted Under Ministerial Authorization*
- OPS-1-15, *Operational Procedures for Cyber Defence Activities Using System Owner Data*
- *ITS Operational Instructions (ITSOIs)*

Following these instructions will ensure that:

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

1.4 IPOC Compliance Monitoring Program

IPOC has established a compliance monitoring program in accordance with OPS-1-8 to assess the compliance of operational activities with policy instruments, addressing legal requirements and the protection of the privacy of Canadians. This program will document all compliance monitoring activities conducted by IPOC.

2. Compliance Monitoring Roles and Responsibilities

2.1 Roles and Responsibilities The roles and responsibilities for compliance monitoring within IT Security are as follows:

Who	Roles and Responsibilities
Deputy Chief, ITS (DCITS)	• Ensuring that a compliance monitoring program is in place; • Reviewing quarterly compliance monitoring reports.
Director General, Cyber Defence (DGCD)	• Reviewing compliance monitoring plans to ensure they are consistent with operational direction; • Reviewing quarterly compliance monitoring reports.
Director, Program Management and Oversight (PMO)	• Ensuring that a compliance monitoring program is developed and implemented; • Directing the monitoring program as a whole; • Taking a leadership role in addressing any identified deficiencies; • Reviewing quarterly compliance monitoring reports; • Forwarding compliance monitoring reports to DGCD and DCITS.
ITS Policy Oversight and Compliance (IPOC)	• Developing, implementing and updating the policy compliance monitoring program; • Assisting managers in the conduct of policy compliance monitoring; • Maintaining records of policy compliance monitoring activities; • Compiling and forwarding reports; • Coordinating resolution of legal issues; • Providing compliance monitoring reports to Director, PMO with copies provided to D2.
Cyber Defence Team Directors	• Supporting the compliance monitoring program as a whole; • Reviewing reports forwarded to them and taking a leadership role in addressing any identified deficiencies.
Cyber Defence Team Managers	• Conducting policy compliance monitoring in accordance with direction from IPOC; • Reporting any non-compliance to their director, and to IPOC; • Taking appropriate corrective action when non-compliance or weaknesses are identified or communicated to them; • Seeking policy advice, when appropriate.
Cyber Defence Team Operational Personnel	• Cooperating with any elements conducting policy compliance monitoring; • Reporting non-compliance or other weaknesses to the appropriate Manager.

3. Compliance Monitoring Activities

The following table identifies "theme" activities related to lawfulness and protecting the privacy of Canadians that are subject to policy compliance monitoring as per OPS-1-8. These activities and specific categories must be monitored over a 3-year period. The specific categories may be revised over time, as monitoring or operations develop.

3.1 Compliance Monitoring Activity Themes

Theme Activity	Specific Category
Data handling	• Essentiality • Privacy annotations and accountability markings • Access to databases
Reporting	• Sign-off levels
Data retention and disposition	• Retention schedules • Destruction
Collection management	• 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

The annual compliance monitoring plan identifies how IPOC will monitor each of the "theme" activities at least once every three years. Compliance monitoring activities to be conducted by the Cyber Defence Branch, Cyber Defence Team, and IPOC that correspond to the themes identified in OPS-1-8 are outlined in these instructions. These activities may also be modified as cyber defence operations evolve.

For the purpose of these instructions, "The Cyber Defence Team" refers to CSEC personnel, secondees, contractors, or integrees who are authorized to conduct or support cyber defence activities.

3.2 Data Handling

The *Data Handling* theme contains the following sub-items:

- Essentiality: Have essentiality and relevancy tests been met?
- Privacy annotations: Have private communications, in whole or in part, or metadata associated with a private communication that can identify one or both communicants or the communication itself, been marked for the purposes of identifying and tracking the use and retention of cyber defence data collected under Ministerial Authorization?
- Access to databases: Have approvals related to accessing data been obtained? Is data access restricted to only those that require it?

Essentiality

The Cyber Defence Team must ensure relevancy and essentiality tests are incorporated within cyber defence tools, and that relevancy and essentiality rationales are applied at the time the decision is made to retain data and remain compliant with policy.

IPOC will verify that relevancy and essentiality tests are incorporated into the system of record for storing private communications, and that essentiality justifications remain consistent with policy.

Privacy Annotations and Accountability Markings

Recognized private communications must be counted when they are initially used or retained. *Refer to ITSOI-1-2 for guidance on recognizing private communications in data.*

The Cyber Defence Team must notify IPOC when:

- Changes are made to the system of record for tagging, storing and reporting private communications that could impact reported private communications counts.
- Private communications are deleted from the system of record.
- Data that has been used and retained is later determined to contain private communications.
- A service or tool that could impact privacy is being developed.

For compliance monitoring, IPOC will:

- Conduct random sampling of events containing private communications to ensure counts are accurately recorded.
- Verify that privacy annotations and markings are appropriately applied.
- Verify that the system of record tracks modifications to private communications counts.

Access to Databases

CSEC Access

Access to raw cyber defence data is restricted to individuals that have acknowledged the legal and policy requirements for cyber defence operations and have been authorized by DG, Cyber Defence (DGCD).

Cyber Defence Team Supervisors must inform IPOC of new personnel requiring access to raw data, and notify IPOC if a member no longer requires access.

IPOC will oversee access to databases by:

- Administering an annual policy briefing, and providing guidance as required.
- Administering an annual mandatory ITS Policy quiz with a required pass mark to the Cyber Defence Team.
- Administering the ITS Policy Quiz to new employees prior to them being granted data access permissions.
- Maintaining a validated list of staff that have demonstrated an understanding of operational policy and are authorized by DGCD.

Second Party Access

Cyber Defence Team Managers must ensure ITS Cyber Knowledge Bases (CKBs) that contain only used and retained data are compliant with policy regarding Second Party data access, and meet the following conditions:

- Only authorized Second Party users may access used or retained data.
- Users must be aware of any limitations concerning use of the data.

IPOC will conduct compliance monitoring of Second Party access to CKBs to verify that these conditions are met.

3.3 Reporting

The *Reporting* theme contains the following sub-item:

- Sign-off levels: Have all required policy requirements and approvals been obtained for reports?

Cyber Defence Team Managers must ensure all cyber defence reports are compliant with policy and that the appropriate release approvals have been obtained.

For cyber defence report release authorities, see OPS-1, paragraph 4.15. Refer to ITSOI-1-4 for guidance on cyber defence reporting and Recommend and Release Authority Considerations.

IPOC will conduct random sampling of released cyber defence reports to ensure that the required approvals have been obtained and policy requirements have been met. A sample of reports using both automated and manual dissemination processes will be verified.

For any changes to report release mechanisms or processes **the Cyber Defence Team** is responsible for ensuring that policy requirements are met.

3.4 Data Retention and Disposition

The *Data Retention and Disposition* theme contains the following sub-items:

- Retention schedules: Has data or information been retained with the correct protections, for the right purpose and for the correct amount of time?
- Destruction: Has data or information been disposed of after the specified time period? If required, is there a record of the disposition?

Cyber Defence Team Managers must ensure that:

- Automated deletion processes are functioning properly to ensure data collected under Ministerial Authorization that has not been used or retained is deleted within [redacted] Detached metadata must be deleted within [redacted] when no longer relevant.
- Data Provided by a System Owner (DPSO) is tracked in a centralized repository that can be accessed by IPOC. The data must be tagged as non-MA and labelled with an identifier (e.g., event number) to ensure the proper application of retention and disposition schedules.
- Data Provided by a System Owner (DPSO) is deleted within [redacted] of completion of the requested assistance, unless retention is approved by the requestor. If retention is approved by the requestor, consent must be documented and stored in a centralized repository that can be accessed by IPOC.

Cyber Defence Team Members must:

- Ensure raw data that is not accessible by automated deletion processes (e.g., saved on a desktop) is retained or deleted in compliance with specified retention schedules (i.e., [redacted] MA data, and [redacted] for non-MA data).
- Acknowledge and document on a quarterly basis via a Web 2.0 Form submission that they have deleted all locally stored data. *(IPOC will send quarterly verification reminders that will include a link to the Web Form.)*

Cyber Defence Team Managers are responsible for ensuring that their employees have acknowledged and documented deletion of locally stored data.

IPOC will monitor compliance by verifying that:

- Deletion scripts are functioning properly.
- DPSO data is tagged, tracked, and deleted in accordance with retention schedules.
- Cyber Defence Team members have acknowledged deletion of locally stored data in accordance with retention schedules by conducting spot checks of data deletion acknowledgments.

3.5 Collection Management

The *Collection Management* theme contains the following sub-item:

- ITS Data Collection: Is data collected in a manner that is not directed at Canadians or other persons in Canada? Are intercepted private communications properly accounted for and auditable?

Cyber Defence Service and Tool Policy Compliance Verification

The **Cyber Defence Team** must contact IPOC for policy compliance verification when developing a new service or tool framework.

The Cyber Defence Activities Service and Tool Privacy Verification Form (see Annex A) will be used by IPOC to establish whether:

- private communications could be intercepted?
- use of the tool could be directed against Canadians?
- the tool will collect personal information?

The Cyber Defence Activities Service and Tool Privacy Verification Form will also be used to confirm that all intercepted private communications are properly accounted for and the data selection is auditable. The Form must be updated when new tool frameworks or toolsets within an existing service are implemented that involve:

- the possibility of interception private communications
- using Canadian Identity Information (CII) as a search criteria

When a new service or tool framework is developed the relevant **Cyber Defence Team Manager** must complete and sign a Cyber Defence Activities Service and Tool Privacy Verification Form.
Prior to the deployment of any MA or non-MA services or tool frameworks the relevant **Cyber Defence Team Manager** must also complete and sign the Cyber Defence Activities Tool Framework Policy Checklist (see Annex A).
The **Cyber Defence Team** will also provide IPOC with all relevant operational documentation related to cyber defence capability deployments (e.g., Client Consent Briefings, CONOPS, SOPs).

Cyber Defence Operations Signature Selector Verification

When deploying signatures (i.e., automated queries that scan traffic or data in order to detect malicious cyber activity) that contain Canadian selectors:

The **Cyber Defence Team** must:

- Seek approval from the Cyber Defence Team Supervisor for Type 1 signatures (i.e., comprised of a Canadian selector [redacted]
- Seek approval from the Cyber Defence Team Manager for Type 2 signatures (i.e., comprised **only** of a Canadian selector), provide sufficient documentation that the signature returns 100% foreign malicious activity, and notify IPOC.
- Track and review signatures every six months.
- De-task signatures if obsolete, or pulling in legitimate traffic.

Refer to ITSOI-1-1, Section 3 for guidance on signatures and selectors.

For compliance monitoring purposes, the **Cyber Defence Team** must make the signature database accessible to IPOC.

IPOC will verify that the signature database enables the Cyber Defence Team to tag all signatures containing Canadian selectors. Signatures containing Canadian selectors will be reviewed by IPOC for policy compliance.

Cyber Defence Operations Query Auditing for Inadvertent Targeting of Canadians

Cyber Defence Team Managers are responsible for ensuring:

- Analyst queries from the cyber defence data analysis repository at the triage and analysis levels are reviewed to detect any possible anomalous user activity. The results of the review must be documented and submitted to IPOC on a quarterly basis.
- Raw data queries that could be inadvertently directed at Canadians are sampled on a quarterly basis. The results of the review will be documented and submitted to IPOC on a quarterly basis.
- Queries run on tools that may impact privacy are logged, auditable, and backed-up as necessary.
- Any findings of queries inadvertently directed at Canadians are reported to IPOC immediately.

When queries against raw data are sampled, these queries will be logged in the database in order to assist Cyber Defence Team Managers in documenting their compliance monitoring activities for review purposes.

IPOC will verify that the Cyber Defence Team Managers are conducting reviews and that any anomalous activity has been properly addressed.

3.6 Information Management

The *Information Management* theme contains the following sub-item:

- Corporate files related to authorities: Are the required corporate files complete and up to date?

For activities conducted under Ministerial Authorization, the relevant **Cyber Defence Team Managers** must ensure a documented request is received, stored in a corporate repository accessible for review, and IPOC is notified.

Cyber Defence Team Managers must ensure a corporate record for all cyber defence activities is established and maintained. This includes all relevant documentation regarding decisions, and approvals that require policy oversight.
For DPSO activities, the relevant **Cyber Defence Team Managers** must ensure a documented request was received from the system owner, or an appropriate representative of the system owner with the system owner's consent. This request must be stored in a corporate repository accessible for review.

IPOC will conduct compliance monitoring to:

- Verify that a documented request for each activity conducted under Ministerial Authorization is recorded and stored in the client file for the given MA period.
- Verify that non-MA activities are compliant with operational policy and procedures and documented as required.

IPOC will document all compliance monitoring activities and reported compliance and privacy incidents.

3.7 Conditions Imposed by Ministerial Authorizations

The *Conditions Imposed by Ministerial Authorizations* theme contains the following sub-item:

- Required reporting elements: Are the necessary records being kept up to date so that reporting to the Minister will be timely and accurate?

Cyber Defence Team Managers will ensure all private communications used and retained are recorded and counted per federal institution and made available to IPOC upon request.

In order to meet the conditions imposed by Ministerial Authorization IPOC will:

- With assistance from the Cyber Defence Team, prepare reporting for the Minister on the number of private communications used or retained upon expiration of the Ministerial Authorization, or at any time upon request.

- Co-ordinate bi-annual technical audits by non-Cyber Defence Team personnel to verify the integrity of the system of record used to count private communications.

- Review database change logs in order to identify any documented technical modifications to the system of record used to count private communications that could affect the count accuracy.

- Notify Strategic Policy of all new requests for activities conducted under Ministerial Authorization, and verify that the Minister has been notified prior to conducting the cyber defence operation.

3.8 Dissemination

The *Dissemination* theme contains the following sub-items:

- Sharing data: Is data shared according to the rules set out in policy documents?
- Sharing reports: Are reports shared according to the rules set out in policy documents?

Sharing Data

Cyber Defence Team Managers are responsible for:

- Approving use of and access to IT Security CKBs and ensuring data is shared in accordance with policy requirements.

- Ensuring ITS CKBs maintain statistics on the volume of used or retained data shared with Second Parties, including results from signatures which produce output that is automatically used or retained. Documentation of all output shared with Second Parties must be kept and made available to IPOC.

IPOC will conduct random sampling of data share with Second Parties to ensure policy compliance.

Sharing Reports

Cyber Defence Recommend and Release Authorities must:

- Ensure released reports meet the relevant policy requirements outlined in *ITSOI-1-4, Section 2.15.*
- Ensure details concerning the release of cyber defence reports, regardless of the report format type, are recorded in a corporate repository that is accessible to IPOC. Refer to *ITSOI-1-4, Section 2.16* for report release documentation requirements.

IPOC will conduct random sampling of cyber defence reports that are released both through, and outside of automated report dissemination tools to verify policy compliance.

4. Additional Information

4.1 Accountability This table establishes the areas of responsibilities as they relate to these instructions.

Who	Responsibility
Deputy Chief, IT Security	• Approving these instructions
Director, Program Management and Oversight	• Recommending these instructions for approval • Revising these instructions as necessary • Monitoring compliance with these instructions • Communicating guidance to those authorized to conduct cyber defence activities regarding any revisions to these instructions
Manager, Corporate and Operational Policy	• Reviewing these instructions to ensure compliance with CSEC policy

4.2 Amendments Situations may arise where amendments to these instructions are required because of changing or unforeseen circumstances. Such amendments will be communicated to relevant staff, and will be posted on the IPOC website.

4.3 Enquiries For additional information or any questions related to compliance monitoring activities or requirements please contact IPOC.

5. Promulgation

I hereby approve Operational Instructions ITSOI-1-6, *Cyber Defence Activities: Compliance Monitoring*.

These instructions are effective on 2013/10/30.

(Date)

Approved

30/10/13

Toni Moffa

Date

Deputy Chief, IT Security

Reviewed and Recommended for Approval

[redacted]

2013/10/30

Date

A/Director, Program Management and Oversight

6. Annex A

Cyber Defence Activities Service and Tool Privacy Verification Form

Client(s)	**Specific Client name or "All"**
Service or Tool Framework (Note: additional tool frameworks and toolsets require IPOC consultation in advance)	Enter the short name of the Detection Capability
Description	Enter a description and provide examples if needed to help clarify. Attach any amplifying documentation to assist in the review and approval process
[redacted]	
Is data that contains intercepted private communications collected or selected?	Yes, No, or N/A
Please provide documentation explaining where data is collected or selected. If this is unknown, IPOC will work with operations to assist in that determination.	Enter description or documentation reference
Links to supporting documentation	Add CERRID links to supporting documents (e.g. diagrams, CONOPS, etc.) if applicable
Point of Contact (POC)	POC for further information on the service/tool and its deployment.

We have reviewed the information provided and are satisfied that the deployment of this capability does not direct Cyber Defence Operations at Canadians or other persons in Canada. Also, that all intercepted private communications are properly accounted for and the data selection process is auditable.

IPOC Manager Review	Name:	Position:
Signature:		Date:

Relevant Manager(s) in the Cyber Defence Branch **<add additional signatures blocks as required>**

Name:	Position:
Signature:	Date:

NOTES:

- Data must be tagged with the client, date and MA authority.
- Analysts must be able to determine which data is information from an intercepted private communication in order to fulfill MA reporting requirements. IPOC will assist with this determination.

MA Cyber Defence Activities Tool Framework Policy Checklist

Client: Tool Framework:

	Requirement	Comments	Date	Initials
	Client			
☐	Existing MOU in place with client			
☐	Technical discussion with Client, if required *(e.g. system compatibility)*			
☐	Potential risks (business and technical) explained to Client *(May be part of a CONOP, brief, MOU, etc.)*			
☐	Tool framework scope outlined with Client *(May be part of a CONOP, brief, MOU, etc.)*			
☐	Client consent to the deployment			
	CSE			
☐	Prior to technical discussion with Client, consultation with Cyber Defence Branch (CDO) to discuss technical requirements for the tool deployment, if required			
☐	Tool conforms with CSE data retention/deletion policies			
☐	IPOC policy compliance verification – Service & Tool Privacy Verification Form			
☐	Corporate record established/maintained and is auditable			

I certify that the above requirements have been considered. Relevant Manager(s) in the Cyber Defence Branch	
Name:	Position:
Signature:	Date:

Non-MA Cyber Defence Activities Tool Framework Policy Checklist

Client: Tool Framework:

	Requirement	Comments	Date	Initials
	Client			
☐	Client request for assistance (documented)			
☐	Client permission to use data for part (b) of CSE mandate *(For tools returning data to CSE)*			
☐	Client data disposal guidance *(For tools returning data to CSE)*			
☐	Technical discussion with Client *(e.g. system compatibility)*			
☐	Potential risks (business and technical) explained to Client *(May be part of a CONOP, brief, MOU, etc.)*			
☐	Tool scope outlined with Client *(May be part of a CONOP, brief, MOU, etc.)*			
	CSE			
☐	CSE decision to assist documented *(Non-GC only)*			
☐	Evidence tool doesn't intercept PC *(Only if tool returns data to CSE)*			
☐	Consultation with Cyber Defence Branch (CDO) to discuss technical requirements for the tool deployment			
☐	IPOC policy compliance verification – Service & Tool Privacy Verification Form			
☐	Approval from: *(Circle relevant authority)* Operational Manager / DGCD / DC ITS			
☐	Corporate record established/maintained and is auditable			

I certify that the above requirements have been considered, Relevant Manager(s) in the Cyber Defence Branch	
Name:	Position:
Signature:	Date: