



Communications Security
Establishment Canada

Centre de la sécurité
des télécommunications Canada



CSEC SIGINT Operations Instruction

CSOI-4-3

Protecting the Privacy of Canadians in the Use and Retention of Material for SIGINT

**Last Updated:
11 April 2011**

Table of Contents

1. INTRODUCTION	4
1.1 Objective.....	4
1.2 Authority.....	4
1.3 Context	5
1.4 References	6
1.5 Application	6
1.6 Accountability	7
1.7 Amendment Process	7
1.8 Inquiries	7
1.9 Review	8
2. HANDLING OF CPRI USED IN THE PRODUCTION OF EPRS	9
2.1 Introduction	9
2.2 Severing of Data	9
2.3 Need-to-Know	9
2.4 “Clean Desk” Approach	9
2.5 Avoid Making Copies.....	10
2.6 Restrict Access to Draft Report	10
2.7 EPR Sign-off	10
2.8 Retention and Storage of EPRs	10
3. HANDLING OF CPRI NOT USED IN THE PRODUCTION OF EPRS.....	12
3.1 Introduction	12
3.2 Avoid Making Copies.....	12
3.3 “Clean Desk” Approach	12
3.4 Need-to-Know	12
3.5 Severing of Data	12
3.6 Retention of Metadata Analysis	12
3.7 Sharing of SIGINT Information with GC Clients	13
3.8 Storage of Charts and Working Aids.....	13
3.9 IRRELEVANT	13
3.10 IRRELEVANT	14
3.11 Sharing of Nationality Status to Prevent Inadvertent Targeting.....	14
3.12 Information Disclosures	15
3.13 Open Source Intelligence.....	15
4. INTERNAL REVIEWS OF CPRI HOLDINGS	16
4.1 Biannual Reviews of All Holdings	16
4.2 Monthly Reviews of Annotated Traffic NOT Used in EPRs	17

5. SUMMARY OF OPERATIONAL ROLES AND RESPONSIBILITIES	18
5.1 Overview	18
6. DEFINITIONS	20
6.1 Associated Material	20
6.2 Canadian	20
6.3 Canadian Identity Information (CII).....	20
6.4 Canadian privacy-related Information (CPRI)	20
6.5 Canadian SIGINT Production Chain.....	20
6.6 Need-to-Know	21
6.7 Personal information.....	21
6.8 Open Source Intelligence.....	21
6.9 Privacy Incident.....	21
ANNEX 1 -- OPERATIONAL AREA BIENNIAL CONFIRMATION OF REVIEW ACTIVITY FORM.....	22
CSOI-4-3 PROMULGATION.....	23

1. Introduction

1.1 Objective

As per paragraph 273.64(2)(b) of the *National Defence Act* (NDA), CSEC is required to take active measures to protect the privacy of Canadians in the performance of its mandated activities. These instructions provide guidelines to be followed in order to protect Canadian privacy-related information (CPRI) that is encountered in the conduct of day-to-day SIGINT activities. For the purposes of this CSOI, CPRI refers to private communications, communications of a Canadian abroad or information about Canadians or Canadian Identity Information (CII).

These instructions supplement the measures within the *Ministerial Directive on the Privacy of Canadians* and in OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities*.

These instructions focus on the physical and electronic handling measures for CPRI obtained through the conduct of SIGINT activities and used:

- in End Product Reports (EPR), (includes annotated traffic, transcripts, gists, and draft reports); and
- as background information, such as a chart or working aid which is not directly used in the production of intelligence reports.¹

These instructions also provide guidance on the handling of information obtained through information disclosures made to CSEC by Government of Canada (GC) clients.

1.2 Authority

This CSEC SIGINT Operations Instruction is issued under the authority of the CSEC Deputy Chief, SIGINT (DCSIGINT).

¹ Excludes metadata and unannotated traffic in official repositories.

1.3 Context

Given the complexity of the Global Information Infrastructure, CSEC will inevitably encounter CPRI while conducting its SIGINT activities. CSEC is committed to taking reasonable measures and implementing appropriate policies to protect the privacy of Canadians in the handling, retention, use and destruction of this material.

This CSOI shall be used in conjunction with the processes stipulated in CSEC's OPS documents. In the event of any discrepancies between this CSOI and the OPS documents, the OPS documents shall supersede this CSOI.

CPRI can only be retained for these reasons:

- For foreign intelligence value in the production of an EPR;
- For background information to enable analysts to further develop foreign intelligence targets; and
- To prevent inadvertent targeting.

Measures to protect privacy are outlined in several operational policy (OPS) documents:

- OPS-1: *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities*
 - annotating traffic within SIGINT repositories

IRRELEVANT

 - obtaining senior management report release approvals
- OPS-1-1: *Procedures of the Release of Suppressed Information from SIGINT Reports*
 - Limiting and tracking distribution of unsuppressed personal information
- OPS-1-7: *SIGINT Naming Procedures*
 - suppressing Canadian identity information (CII) in SIGINT EPRs
- OPS-1-10: *Operational Procedures for Metadata Analysis* [REDACTED]
 - metadata analysis [REDACTED]
- OPS-1-11: *Retention Schedules for SIGINT Data*
 - conforming to retention and storage guidelines

1.4 References

- *National Defence Act*
 - Ministerial Directive, *Privacy of Canadians*, June 2001
 - Ministerial Authorizations
 - OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities*
 - OPS-1-1, *Procedures for Release of Suppressed Information from SIGINT Reports*
 - OPS-1-7, *SIGINT Naming Procedures*
 - OPS-1-8, *Active Monitoring of Operations to Ensure Legal Compliance and the Protection of the Privacy of Canadians*
 - OPS-1-10, *Operational Procedures for Metadata Analysis* [REDACTED]
 - OPS-1-11, *Retention Schedules for SIGINT Data*
 - OPS-1-13, *Procedures for Canadian* [REDACTED] *Activities*
 - OPS-3-1, *Procedures for* [REDACTED] *Activities*
 - OPS-4-3, *Procedures* [IRRELEVANT]
 - CSOI-4-1, *SIGINT Reporting*
 - CSOI-4-4, *Targeting and Selector Management Using* [REDACTED] *National SIGINT Systems for Intelligence Reporting Purposes*
 - CSOI-5-3, *Canadian SIGINT Production Chain and Access to SIGINT Data*
 - OPS-5-15, *Need-To-Know Guidelines*
 - Standard Operating Procedures (SOP) for SIGINT Information Needs via [REDACTED]@csc-cst.gc.ca
-

1.5 Application

These instructions apply to all individuals and elements within the Canadian SIGINT Production Chain, including GC and Second Party intregrees, authorized to conduct SIGINT activities under the authority of CSEC DCSIGINT. This includes personnel operating under the authority of the Canadian Forces SIGINT Technical Control Authority, Commander, CFIOG.

11 April 2011

1.6 Accountability

The following table outlines responsibilities with respect to these instructions.

Who	Responsibility
Deputy Chief SIGINT	<ul style="list-style-type: none"> • Approving these instructions.
Director General SIGINT Programs	<ul style="list-style-type: none"> • Recommending these instructions for approval.
Director SIGINT Requirements	<ul style="list-style-type: none"> • 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 of Legal Services	<ul style="list-style-type: none"> • Provide advice on these instructions when requested by Director SIGINT Requirements.
SIGINT Directors-General and Directors who are affected by these instructions and the Canadian Forces SIGINT Technical Control Authority	<ul style="list-style-type: none"> • Applying these instructions.
All CSEC managers and Supervisors and CF/DND leaders who are affected by these instructions	<ul style="list-style-type: none"> • Ensuring that their staff has read, understood and complies with these instructions and any amendments to these instructions.
All CSEC/DND staff and CF members who are affected by these instructions	<ul style="list-style-type: none"> • 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 on the SIGINT Programs Oversight and Compliance home page.

1.8 Inquiries

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 [REDACTED]@cse-cst.gc.ca) when necessary.

1.9 Review

The activities outlined in these instructions are subject to internal monitoring for policy compliance, audit, and/or review by various government review bodies, including, but not limited to, the Office of the CSE Commissioner and the Privacy Commissioner.

2. Handling of CPRI Used in the Production of EPRs

2.1 Introduction

When preparing a report that contains CPRI, analysts and reviewers must follow these instructions in order to protect the privacy of Canadians.

For the purposes of this CSOI, EPRs include the following releasable SIGINT products: End Product Reports², SIGINT Summaries and Assessments, and Information Items. Additionally, EPRs include the following non-releasable products: Gists and Technical SIGINT reports (Cryptologic/Communications Information Reports (CIR) [REDACTED])

[REDACTED]

2.2 Severing of Data

Where possible, information about Canadians that does not meet the criteria for retention stated in section 1.3 should be removed from reporting and/or associated material³ unless it cannot easily be severed.

2.3 Need-to- Know

Report drafts and associated material must only be reviewed and edited by individuals with a need-to-know, in accordance with OPS-5-15, *Need-to-Know Guidelines*.

2.4 “Clean Desk” Approach

A “clean desk” approach is to be adopted when dealing with a report in progress and its associated material. When analysts are away from their desks for an extended period (one hour or longer), the report and all associated material must be stored in a temporary holding folder out of sight--either in a drawer or in the overhead storage of the employee’s workstation.

² Instructions for Advance Reports is in CSOI-4-1, Appendix H.

³ Associated material consists of original traffic [REDACTED] gists or transcripts of original traffic, and any collateral information used directly or indirectly in the production of EPRs.

2.5 Avoid Making Copies

As a general rule, copies of traffic items must not be replicated or retained in electronic format outside traffic repositories.

Hard copies of any documents containing CPRI are to be limited to the requirement to attach traffic and other relevant collateral information to EPR.

Hardcopy material containing CPRI that is no longer needed after the release of the report and which was not used in an EPR must be shredded in an approved shredder.

2.6 Restrict Access to Draft Report⁴

Gists and transcripts generated from annotated traffic must be saved in the appropriate transcript repository or in shared folders, access to which must be administered by Level V Supervisors and/or Level IV Managers.

Gists and transcripts derived from this traffic may only be shared via email within immediate teams when it is necessary to do so. CPRI should not be included unless absolutely essential. Emails must be set up in such a way as to render them easily identifiable as containing CPRI. This helps to ensure they are deleted when no longer required, or the retention period expires. Emails may only be sent to those within the report release chain, D2 and SPOC.

2.7 EPR Sign-off

The sign-off sheet, EPR and associated material required for release are to be hand-delivered in a "Privacy Information" holding folder, to the various signing authorities within SIGINT. Blue security pouches must be used to transport reports outside of Secure SIGINT Areas (SSA). Reports which may require DGPC approval may be sent by softcopy to Operational Policy.

2.8 Retention and Storage of EPRs

Approved EPRs and their associated material must be stored in an approved security container in the operational area. The security container must have restricted access. Retention of material is subject to the following criteria:

- Hardcopy EPR and associated material, including completed sign-off sheet, must be retained [REDACTED] as they constitute the official record;
- If the approved security container has been filled to its capacity and the team requires additional space, older EPRs must be sent to

⁴Specific instructions for Advance Reports are in CSOI-4-1, Appendix H.

11 April 2011

Information Holding Services (IHS) for storage. In cases where a team is disbanded, all files subject to retention must be shipped to IHS, as per standard archiving procedures; and

- Boxes containing hardcopy material with CPRI must be visibly labeled “Contains Canadian Privacy-related Information” and “Canadian Eyes Only”.
-

3. Handling of CPRI NOT Used in the Production of EPRs

3.1 Introduction	This section provides instructions on the handling of CPRI obtained through the conduct of SIGINT activities or related to target activity and retained for use in the development of foreign intelligence target knowledge and that will not necessarily be used for an EPR.
3.2 Avoid Making Copies	<p>As a general rule, copies of traffic items or associated material must not be replicated or retained in electronic format outside traffic repositories.</p> <p>Hardcopy material containing CPRI that is no longer required must be shredded in an approved shredder.</p>
3.3 “Clean Desk” Approach	A “clean desk” approach should be adopted when dealing with charts or working aids containing CPRI. Charts and working aids should be out of sight when not in use.
3.4 Need-to-Know	Sharing charts and working aids is permitted on a need-to-know basis within the team without suppressing CPRI. (OPS-5-15)
3.5 Severing of Data	Whenever possible, CPRI that does not meet the criteria for retention stated in section 1.3 should be removed from materials unless it cannot easily be severed.
3.6 Retention of Metadata Analysis	<p>A chart or working aid that contains metadata analysis [REDACTED] may be retained [REDACTED] (OPS-1-10). The chart or working aid must be dated and indicate that it is OPS-1-10 derived.</p> <p>Additionally, charts and working aids containing CPRI that is not related to the foreign intelligence must have the CPRI deleted, blacked out, or suppressed.</p>

**3.7 Sharing of
SIGINT
Information
with GC
Clients**

SIGINT charts or working aids may be shared with GC clients during informal analytic exchanges, as required, to develop foreign intelligence target knowledge. However, the CPRI must be suppressed and neither hard nor soft copies may be provided to clients.

**3.8 Storage of
Charts and
Working Aids**

Electronic copies of charts or working aids containing suppressed CPRI may be stored on the corporate wiki or in shared directories. Electronic copies of charts or working aids containing CPRI must be stored within a restricted-access wiki or shared directory with named access privileges.

IRRELEVANT

IRRELEVANT

IRRELEVANT

11 April 2011

3.10 IRRELEVANT
IRRELEVANT

IRRELEVANT

**3.11 Sharing of
Nationality
Status to
Prevent
Inadvertent
Targeting**

The nationality status of known Canadians who are in some way related to CSEC's foreign intelligence activities (including citizens and permanent residents) should be made available to the Canadian SIGINT Production Chain in order to prevent inadvertent targeting or reporting⁶.

CPRI, including Canadian nationality status, can only be provided outside of the Canadian SIGINT Production Chain through the use of suppressed Canadian Identity Information in EPRs. A request to access suppressed information must be made to Operational Policy (D2) as directed in OPS 1-1, *Procedures for Release of Suppressed Information from SIGINT Reports*.

Once an entity of intelligence interest has been identified as Canadian, the information must be entered into the Target Knowledge Base, and the record must be assigned "Protected Entity Status." This will ensure entities identified as having protected status cannot be targeted.

Second Parties may query CSEC about the nationality of individuals in order to avoid targeting Canadians. Operational Policy (D2) is the only area authorized to respond to these queries on behalf of CSEC. All requests from Second Parties must be forwarded to Operational Policy.

11 April 2011

**3.12
Information
Disclosures**

Client departments often disclose collateral information to CSEC in order to facilitate CSEC's activities. Information disclosures could contain CPRI. CSEC can receive and retain information about Canadians, provided that information is essential to CSEC's mission.

There are several different methods by which clients may disclose information to CSEC. However, all information disclosures must follow these instructions to protect the privacy of Canadians:

- Information about Canadians should only be accessible to those who have a need-to-know; therefore, access controls must in place to restrict access;
- Whenever possible, CPRI should be removed from materials unless it cannot easily be severed;
- Information containing CPRI should be deleted as soon as it is determined the information is of no foreign intelligence value;
- A "clean desk" approach should be adopted when dealing with documents containing CPRI;
- Acknowledgements of client information disclosures or requests for information must be held for [REDACTED] for review and oversight purposes; and
- Level IV Managers are responsible for completing a biannual review (as outlined in section 5.2) of all client disclosures containing CPRI to determine if the information is still of value and meets the criteria for retention as outlined in section 1.3.

**3.13 Open
Source
Intelligence**

Open source intelligence containing CPRI may be retained by operational areas. However, the fact of CSEC's interest in a Canadian, as identified in open source materials, could be sensitive and requires protection. Analysts should apply the need-to-know principle.

4. Internal Reviews of CPRI Holdings

4.1 Biannual Reviews of All Holdings

On a biannual basis, Level IV Managers of operational areas must complete a review of all holdings and complete a “Confirmation of Review” (form located in Annex 1) and send the completed form to SPOC.

Level IV Managers must review the following:

- a) Any shared directories which contain CPRI. Any retained CPRI must continue to meet the established criteria for retention (see section 1.3). Additionally, Level IV Managers must confirm that access to such shared directories is limited to those with a need-to-know. Any documents no longer required must be deleted.
- b) Any traffic annotated for retention over the previous six months that has not been used in the production of EPRs. SPOC will send a list of annotated traffic to the Level IV Manager for review. Retention of this traffic must still meet the relevant criteria (see section 1.3). If the traffic no longer meets the criteria it must be annotated for deletion.
- c) Any traffic annotated INCAS/OUCAS must be reviewed and documentation sent to SPOC showing that legal advice from DLS was obtained prior to annotating for retention (OPS-1, 3.5).
- d) Any working aids that contain CPRI, in order to validate that the documents are still required. If the documents are no longer required they must be deleted or destroyed.
- e) Any disclosure information received from a client containing CPRI in order to validate that the documents are still required. If the documents are no longer required they must be deleted or destroyed.
- f) Access Control Lists for directories to ensure only staff with a need-to-know has access to directory contents.

SPOC will retain operational area confirmations and notifications for use in other review activities, as required.

11 April 2011

**4.2 Monthly
Reviews of
Annotated
Traffic NOT
Used in EPRs**

In addition to the biannual review, on a monthly basis Level IV Managers are responsible for ensuring traffic annotated for retention by their staff and not used in an EPR are still required and meet the criteria for retention (see section 1.3).

Monthly, SPOC will send a report containing all annotated traffic for the month that has not been used in an EPR to Level IV Managers. Level IV Managers must ensure that staff review the list of traffic items and delete those that no longer meet the criteria for retention.

Additionally, for any retained solicitor-client traffic, acquired under Part A of CSEC's mandate, Level IV Managers must provide documentation to SPOC to demonstrate consultation with DLS (OPS-1, 3.5).

Level IV Managers are responsible for retaining the results of these monthly reviews for future audits or reviews.

5. Summary of Operational Roles and Responsibilities

5.1 Overview The following table provides an overview of roles and responsibilities with respect to these instructions.

Who	Responsibilities
SIGINT personnel	<ul style="list-style-type: none"> • Remain well-versed in OPS-1 and complete the OPS-1 on-line quiz annually. • Depending on position held, annotating traffic, as per OPS-1. • Storing CPRI as required. • Maintain awareness of policies-- changes/updates.
Level V Supervisor or CF equivalent	<ul style="list-style-type: none"> • Ensure that analysts receive proper training regarding handling and storage of CPRI; e.g. OPS-1 briefing, and CSOI 4-3, <i>Protecting the Privacy of Canadians in the Use and Retention of Material for SIGINT</i>. • Ensure analysts are aware of policy changes/updates. • Ensure that CPRI retained by the team is properly stored and destroyed. • Ensure that analysts are reviewing, at least twice a year, retained material and revalidating the need for its retention and deleting it if no longer required.
Level IV Manager or CF equivalent	<ul style="list-style-type: none"> • On a monthly basis review annotated traffic not used in EPRs. Keep results of this review available for any audits or reviews and provide documentation on consultation with DLS for Solicitor-Client traffic retained. • Establish hard copy and electronic storage systems to allow for biannual review. • Provide biannual reports to SPOC (see section 4.1).
SIGINT Oversight and Compliance (SPOC)	<ul style="list-style-type: none"> • On a monthly basis review all traffic annotated for retention and validate with operational areas those items which did not result in an EPR.

TOP SECRET//COMINT//CANADIAN EYES ONLY

CSOI-4-3

11 April 2011

	<ul style="list-style-type: none">• Maintain copies of all review documents sent to Production Managers on a monthly basis for immediate access by review bodies.• Track and file emails received from Level IV Managers that confirm DLS consultation for Solicitor-Client traffic retention.
--	---

6. Definitions

6.1 Associated Material	Original traffic [REDACTED] transcripts / gists of original traffic, and any collateral information used in the production of EPRs.
6.2 Canadian	<p>“Canadian” refers to:</p> <ul style="list-style-type: none"> a) a Canadian citizen; b) a person who has acquired the status of permanent resident under the <i>Immigration and Refugee Protection Act</i> and who has not subsequently lost that status under that <i>Act</i>; or c) a corporation incorporated under an Act of Parliament or of the legislature of a province. <p>“Canadian organizations” are also accorded the same protection as Canadian citizens and corporations.</p> <p>A Canadian organization is an unincorporated association, such as a political party, a religious group, or an unincorporated business headquartered in Canada.</p>
6.3 Canadian Identity Information (CII)	<p>CII refers to information that may be used to identify a Canadian person, organization*, or corporation, including, but not limited to, names, phone numbers, email addresses, IP addresses, and passport numbers.</p> <p>* GC Institutions do not fall within this definition.</p>
6.4 Canadian privacy-related Information (CPRI)	Canadian privacy-related information includes private communications, communications of a Canadian abroad or information about Canadians, Canadian corporations or Canadian organizations.
6.5 Canadian SIGINT Production Chain	The Canadian SIGINT Production Chain refers to SIGINT enabling, production, or oversight activities conducted under the authority of DC SIGINT, including those activities delegated to non-CSEC organizations. This does not include the consumption of SIGINT Products, but does include the activities that enable consumption.

6.6 Need-to-Know


Need-to-know is a fundamental aspect of CSEC's information handling system, and a way of further restricting access to classified and protected information. It reflects the principle that not everyone who is cleared to see certain information needs to see all of it.

6.7 Personal information

Personal information is defined in the *Privacy Act* as "information about an identifiable individual that is recorded in any form". See Annex 1 of OPS-1 for the complete definition.

6.8 Open Source Intelligence

Open Source Intelligence is any unclassified, publicly available information that can be found in a variety of different sources including print, television, radio and the internet. OSINT can be used in a variety of different ways



6.9 Privacy Incident

A privacy incident occurs when the privacy of a Canadian is put at risk in a manner that runs counter to, or is not provided for in, an operational policy. In order to remain compliant with operational policies and legal requirements, any person who becomes aware that CPRI has been jeopardized, must report the incident.

ANNEX 1 -- Operational Area Biannual Confirmation of Review Activity Form

Review Date: _____

Operational Area: _____
Full name of operational area

Please check boxes to indicate that a review has been completed for the following:

- ☐ Working aids
- ☐ Annotated traffic – a review of all traffic annotated for retention that has not been used in an EPR to date
- ☐ Solicitor-client annotated traffic (for each provide documentation showing DLS consultation)
- ☐ Access lists for shared directories
- ☐ Contents of shared directories
- ☐ Emails – confirmation from staff that email directories have been reviewed
- ☐ Information disclosures received to confirm they meet the criteria for retention
- ☐ Other: (please list)

Signing this document confirms that, for your operational area, the above have been reviewed to ensure that any Canadian privacy-related information (CPRI) being retained meets the criteria for retention as outlined in CSOI-4-3, section 1.3. Additionally, your signature confirms that access to CPRI is limited to those with a need-to-know. Moreover, your signature also confirms that any items no longer meeting this criteria have been deleted or destroyed.

Signature: _____

Print Name: _____

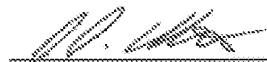
Title: _____

(The email template version (available from SPOC) of this document can be emailed to [REDACTED] or the signed hardcopy version of this document can be sent to SPOC by internal mail.)

CSOI-4-3 Promulgation

Reviewed and Recommended for Approval

I have reviewed and hereby recommend these instructions for approval.



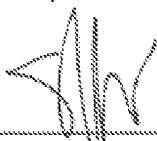
James Abbott
Director General SIGINT Programs

14. AP. 2011

Date

Approved

I hereby approve CSOI-4-3: *Protecting the Privacy of Canadians in the Use and Retention of Material for SIGINT*. These instructions are effective immediately.



Shelly Bruce
Deputy Chief SIGINT

15 April 2011

Date