Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Canadian SIGINT Operations Instructions

CSOI-4-1

SIGINT Reporting

Last Updated:

25 June 2014

SIGINT

Canada

Table of Contents

1. Introduction

1.1 Objective

These instructions provide direction to CSEC and CFIOG staff regarding the content, presentation and technical aspects (externals) of SIGINT reports. Their purpose is to ensure compliance with legal and policy requirements (reporting standards) and to promote quality and consistency in CSEC and CFIOG reporting (guidelines).

1.2 Authority

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

1.3 Supersession

This document supersedes OPS-5-2, SIGINT Reporting Procedures.

1.4 References

- OPS-1, Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities
- OPS-1-7, Operational Procedures for Naming in SIGINT Reports
- OPS-1-11, Retention Schedules for SIGINT Data
- OPS-5-3, Write-to-Release Procedures

1.5 Standards versus guidelines

As suggested in section 1.1, this document contains two types of reporting instructions: guidelines and standards.

Guidelines represent best practice in SIGINT report-writing style. Use them intelligently, balancing them against your own knowledge of the subjects you report on and of the various users of your reports. Deviate from them if there is compelling reason to do so.

Standards are instructions that must be followed. Here are a few examples:

- Reports must have the correct protective markings (classification, control system markings and dissemination control markings).
- Politically sensitive reports must be sent to the appropriate addressees.

- Reports must safeguard information that could be used to identify Canadian or Second Party individuals, corporations or organizations, in accordance with OPS-1-7.
- The information in reports must be accurate.

1.6 Application

This CSOI applies to all CSEC and CFIOG staff engaged in authoring, editing, reviewing or releasing SIGINT reports.

SIGINT reports include, but are not limited to, the following types of reports:

- COMINT reports
- Cryptologic Information Reports (CIRs)
- ELINT reports
- FISINT reports
- IRRELEVANT
- I&W GIST reports
- SIGINT Assessment reports
- SIGINT Summary reports
- SIGINT Support Element (SSE) reports
- Synopsis reports

1.7 Accountability

This 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
Associate Director Mission Management (AMM), SIGINT Programs Group	• Promulgating and implementing these instructions • Seeking legal and/or policy advice if required
Director General Intelligence and Intelligence Branch Directors	Applying these instructions
Production Support, Intelligence Branch	• Maintaining these instructions • Answering questions concerning these instructions
All CSEC and CFIOG managers who are affected by these instructions	Ensuring that their staff complies with these instructions and any amendments to these instructions
All CSEC and CFIOG staff who are involved in authoring, editing, reviewing or releasing SIGINT reports	Complying with these instructions and any amendments to these instructions

1.8 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 CSOI website.

1.9 Enquiries

All questions regarding this CSOI should be directed to CSEC/[redacted]

2. Authoring a Report: A Step-by-step Guide

2.1 Before you write		
Step	**Action**	**Resources**
1	If you are planning to prepare one of the following special types of reports, please consult the associated reference document before you begin. • CEO, RESTRICTED or involving a Second Party national sensitivity • A Synopsis report • An I&W Gist report • SIGINT Summary, SIGINT Assessment • Cryptologic Information Report (CIR) • A report containing [redacted] information • A report containing [redacted] information • A report containing ELINT data • A report containing [redacted] data • A native format report IRRELEVANT	Reporting Nationally Sensitive Information (including CEO and Restricted) Synopsis Reports Producing Gists for I&W Purposes SIGINT Summaries and Assessments CIRs Using [redacted] Information [redacted] Reporting ELINT Reporting [redacted] Reporting "Native Format" Reporting
2	Determine the classification and distribution that your report will have. You will need this information to select the correct report template. If you're using the Default Product Template, go to Step 5.	Special Reporting Conventions
3	On the [redacted] toolbar, click the Bookmark icon. In the Standard Templates folder, find the appropriate template and click it.	
4	Create a new report from the template by clicking Create Draft From on the left side of the [redacted] toolbar.	
5	Determine whether a tear-line can be included in the report.	Write-To-Release Reporting
6	Click Preview, then click Product Release Form. Click Open. Complete the form on the screen and print a copy.	Product Release Form

2.2 Writing your report		
Step	**Action**	**Resources**
1	On the [redacted] toolbar, click Edit, then click Editor.	
2	In the [redacted] pane, compose the report according to the procedures in this CSOI.	Report layout Write-To-Release Reporting
3	On the [redacted] toolbar, click the Save icon.	

2.3 Entering the report metadata		
Step	**Action**	**Resources**
1	**TAGs** For each TAG line required, select the appropriate TAGs, then click Add TAG Line.	About the TAGs page TAGs Working Aid
2	**Traffic** [redacted]	About the Traffic page Identifying the traffic Contribution percentage Traffic language OPS-1/S.16 category
3	**Distribution** NB: This step applies only to reports shared with Second Parties. On the [redacted] toolbar, click Distribution, then select all appropriate DDIs. [redacted] If you are **not** using a template, please see the detailed instructions for selecting CAGs and PLAs.	About the Distribution page About DDIs DDI Working Aid for regular reports DDI Working Aid for CIRs About CAGs
4	**Actors** Assign each person the correct role (type). Make sure the Actors list matches the signatories on the Product Release Form.	About the Actors page
5	**General Metadata** *Additional Warnings*: Select any that apply. *Type*: Select the report type (CIR, [redacted] *Reason for Write to Release Exemption*: If your report does not have a tear-line, select the appropriate reason. *RFI ID*: If your report addresses an RFI, enter the number. *SIR*: If your report addresses an SIR, enter the number.	About the General Metadata page

6	**Attachments** This step applies only to reports to which attachments must be added. To add an attachment to a report, click Attachments, then click Attach a file or Attach from clipboard. Complete the fields in the popup window and click Attach.	About the Attachments page

2.4 The edit/release process		
Step	**Action**	**Resources**
1	[redacted]	
2	[redacted]	
3	[redacted] IRRELEVA	SIGINT Report Release Authorities
4	[redacted]	

	[redacted]	Product Release Form
5	[redacted] IRRELEVANT	Product Release Form Retention Schedules for SIGINT Data (OPS-1-11)

3. Fundamentals of SIGINT Reporting

3.0.1 Overview

This part describes the key principles that apply to SIGINT reports, and the ingredients of a good SIGINT report.

3.0.2 Contents

This part contains the following sections:

- General principles of SIGINT reporting
- Characteristics of a good SIGINT report

3.1 General principles

3.1.1 Emphasis on SIGINT

Your job as a SIGINT analyst is to report the **SIGINT facts**. However, be sure to include all appropriate cross-references, clearly-labelled analytic comments, and collateral that explains, clarifies or refutes the SIGINT.

3.1.2 Focus on foreign intelligence

One of CSEC's mandates is to provide the Government of Canada with foreign intelligence (for the official definition of foreign intelligence, see section 8.9 of OPS-1). This means that in drafting your reports, you must focus on the activities of foreign intelligence targets. For example, if a report covers discussions between a foreign person and a Canadian, emphasize the foreign person's description or assessment of the discussion, and not the identity, statements or views of the Canadian. For more information and more detailed examples, see the section on report focus.

3.1.3 Use of generic identifiers

Replace the names and other identifying information of Canadian and Second Party persons, corporations and organizations with generic terms, except under specific circumstances. For more information, see the chapter on identities in reports.

3.1.4 Need to know

CSEC and CFIOG disseminate SIGINT reports only to authorized persons and organizations that are appropriately cleared and indoctrinated for access and have a need to know.

Having a need to know means having a requirement for the information in order to be able to perform one's duties or functions. For more information, see the Need-to-Know Guidelines (OPS-5-15).

3.1.5 Classification

Be sure to classify SIGINT information at a level consistent with

- the potential damage to Canada's national interest if the information were compromised
- the requirement for the protection of sources and collection methods

For further guidance, see SIGINT Classification Standards (CSSS-103).

3.2 Characteristics of a good SIGINT report

3.2.1 Relevant

Make sure the information in the report meets one or more customer requirements.

3.2.2 Timely

Issue the report while the information it contains is still useful to the client.

3.2.3 Accurate

Make sure the information in the report is correct and complete.

3.2.4 Objective

Make sure the interpretations and conclusions in the report are free of distortion or manipulation due to self-interest or bias.

3.2.5 Clear and concise

IRRELEVANT

3.2.6 Written for the reader

IRRELEVANT

4. Report Content and Presentation

4.0.1 Overview

This part provides guidelines on the layout of a SIGINT report and on how to include attribution, collateral and identities in a report. It also describes the various style conventions specific to SIGINT reporting (acronyms, capitalization, spelling, etc.) and how to add attachments to a report.

4.0.2 Contents

This part contains the following chapters:

4.1 Report Layout

4.1.0.1 Overview

This chapter describes the main structural components and subcomponents of SIGINT reports and provides guidelines for organizing the contents of each component and subcomponent.

4.1.0.2 Structural components

IRRELEVANT

4.1.0.3 Journalistic principles

IRRELEVANT

4.1.0.4 Contents

This chapter contains the following sections:

- The report title
- Title slugs
- The report body: Structure and formatting
- The report body: Content
- Analytic comments
- Footnotes

4.1.1 The report title

4.1.1.1 What it's for

IRRELEVANT

4.1.1.2 Title components

IRRELEVANT

4.1.1.3 Title classification

IRRELEVANT

4.1.1.4 The subject

IRRELEVANT

4.1.1.5 Capitalization in the subject

IRRELEVANT

4.1.1.6 Length

IRRELEVANT

4.1.1.7 Verb tense

IRRELEVANT

4.1.1.8 Punctuation

IRRELEVANT

4.1.1.9 Dates in titles

IRRELEVANT

4.1.1.10 Collateral in titles

IRRELEVANT

4.1.1.11 Tear-line titles

In general, titles of tear-line portions are subject to the same rules as overall report titles, with the following exceptions:

- classify tear-line titles at the SECRET level (usually S//REL TO CAN, AUS, GBR, NZL, USA or S//CEO)
- omit attribution

4.1.2 Title slugs

4.1.2.1 Purpose of slugs

IRRELEVANT

4.1.2.2 Slug types

IRRELEVANT

4.1.2.3 Special slugs

IRRELEVANT

4.1.2.4 Generic slugs

IRRELEVANT

IRRELEVANT

4.1.3 The report body: Structure and formatting

4.1.3.1 Components

IRRELEVANT

4.1.3.2 Block headings

IRRELEVANT

4.1.3.3 Heading content

IRRELEVANT

4.1.3.4 Classifying block headings

IRRELEVANT

IRRELEVANT

4.1.3.5 Classifying paragraphs

IRRELEVANT

4.1.3.6 Tables

IRRELEVANT

IRRELEVANT

4.1.3.7 Lists

IRRELEVANT

4.1.3.8 Images

IRRELEVANT

IRRELEVANT

4.1.4 The report body: Content

4.1.4.1 Components

IRRELEVANT

4.1.4.2 Key points

IRRELEVANT

4.1.4.3 Analysis

IRRELEVANT

4.1.4.4 Details

IRRELEVANT

4.1.4.5 The lead

IRRELEVANT

4.1.4.6 Lead contents

IRRELEVANT

4.1.4.7 Lead style

IRRELEVANT

4.1.4.8 When the lead is a summary

IRRELEVANT

IRRELEVANT

4.1.4.9 When the lead is not a "Summary"

IRRELEVANT

IRRELEVANT

4.1.4.10 Collateral or comments in the lead

IRRELEVANT

4.1.4.11 Dates/times in the lead

IRRELEVANT

4.1.4.12 Parenthetical data in the lead

IRRELEVANT

IRRELEVANT

4.1.4.13 The rest of the report

IRRELEVANT

4.1.4.14 What to include

IRRELEVANT

4.1.4.15 Sequence

IRRELEVANT

4.1.4.16 Focus on foreign intelligence

When a report covers discussions between a foreign person and a Canadian or Second Party [redacted], ensure that the emphasis of your report is on the **foreign person's assessment** of the discussion, not on the identity, statements, or views of the Canadian or Second Party [redacted]

In example 1 below, the reporter properly emphasizes [redacted], not the statements themselves.

Example 2 shows how a report **incorrectly** focuses on the views and statements of a Canadian [redacted]

Example 1: Correct Approach

In this example, [redacted] are the focus.

[redacted]

Example 2: Incorrect Approach

In this example on the same subject, the reporter **incorrectly** focuses on [redacted] actions and statements.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

4.1.5 Analytic comments

4.1.5.1 Purpose

IRRELEVANT

4.1.5.2 Comment placement

IRRELEVANT

4.1.5.3 Flagging of comments

IRRELEVANT

4.1.5.4 Collateral is not comment

IRRELEVANT

4.1.5.5 Metadata analysis is not comment

When a report's conclusions are based on an analysis of metadata (e.g., contact chaining), do not use the "Comment" flag.

4.1.5.6 Comments that do not require flagging

Do not flag comments in tear-lines.

You may include shorter comments (single words or phrases) in a report either directly or in parentheses, as appropriate, without flagging them. The following are examples of materials that do not need to be flagged:

- aliases or alternative spellings;
- "not further identified" or "no further information";
- identifications of people, locations, etc. based on metadata or non-SIGINT information.

4.1.5.7 Comment paragraphs

IRRELEVANT

4.1.6 Footnotes

4.1.6.1 Purpose

IRRELEVANT

4.1.6.2 Footnote structure

IRRELEVANT

4.1.6.3 Footnote placement

IRRELEVANT

4.1.6.4 How to add a footnote

IRRELEVANT

4.1.6.5 Classification

IRRELEVANT

4.1.6.6 Cross-references

IRRELEVANT

IRRELEVANT

4.1.6.7 Lists of references

IRRELEVANT

4.1.6.8 Reference format

IRRELEVANT

4.2 Attribution

4.2.0.1 Introduction

IRRELEVANT

4.2.0.2 Definitions

IRRELEVANT

4.2.0.3 Contents

This chapter contains the following sections:

- Attribution in the body of the report
- Attribution in the title

4.2.1 Attribution in the body of the report

4.2.1.1 Identifying the intelligence source

IRRELEVANT

4.2.1.2 Placement of attribution

IRRELEVANT

4.2.1.3 [redacted]

[redacted]

4.2.1.4 [redacted]

[redacted]

4.2.1.5 Focus on the foreign target

When drafting reports involving Canadian or Second Party (US, UK, Australian or New Zealand) persons or entities, especially when one of the communicants is a Canadian or Second Party person or entity, focus on the activities, capabilities and intentions of the foreign intelligence target. See OPS-1 for the rules concerning the reporting of communications of persons located in Canada, Canadians outside Canada, and information about Canadians.

For example, in a report based on an e-mail [redacted] the attribution could take the following form:

[redacted]

4.2.1.6 [redacted]

[redacted]

4.2.1.7 Avoid double attribution

IRRELEVANT

4.2.1.8 Avoid empty attribution

IRRELEVANT

4.2.1.9 Secondary sources

IRRELEVANT

IRRELEVANT

4.2.1.10 Attribution after the lead

IRRELEVANT

4.2.1.11 Avoid conversational style

IRRELEVANT

4.2.2 Attribution in the title

4.2.2.1 Requirement for attribution

IRRELEVANT

4.2.2.2 Attribution not required

IRRELEVANT

4.2.2.3 Attribution required

IRRELEVANT

IRRELEVANT

4.3 Collateral

4.3.0.1 Introduction

This chapter provides guidelines for the effective use of collateral information in SIGINT reporting.

4.3.0.2 Definition

Collateral is non-SIGINT information that is included in SIGINT reports because it contributes in some way to the SIGINT story.

Non-SIGINT information is information that is not derived from SIGINT intercept (traffic), analyzed or processed SIGINT, or SIGINT reports.

Note: Press information passed from one target to another or discussed by communicants is SIGINT intercept, not collateral.

4.3.0.3 Types of information

Collateral may be derived from unclassified sources such as media reports, Web sites and reference publications, or from classified sources such as non-SIGINT reports produced by members of the Canadian or allied intelligence community.

4.3.0.4 Contents

This chapter contains the following sections:

4.3.1 The role of collateral

4.3.1.1 Contribution of collateral

IRRELEVANT

4.3.1.2 Collateral provides context

IRRELEVANT

4.3.1.3 Emphasis on the SIGINT

IRRELEVANT

4.3.1.4 Last piece of the puzzle

IRRELEVANT

4.3.1.5 Collateral is not comment

IRRELEVANT

4.3.2 Restrictions on collateral

4.3.2.1 Background

Certain restrictions apply to the use of all collateral information, **whether classified or not**. These restrictions relate to issues such as permission to use the collateral, the use of a Canadian or Second Party identity, and the role of collateral.

4.3.2.2 Canadian identities

Treat identities derived from collateral the same way as those derived from SIGINT.

When a Canadian identity appears in collateral that is being used in a report, replace it with a generic term such as "Canadian company" or "Canadian person" unless the identity qualifies for inclusion under the Operational Procedures for Naming in SIGINT Reports (OPS-1-7) and is essential to the understanding of the report.

4.3.2.3 Second Party identities

When a Second Party identity appears in collateral that is being used in a report, follow the national rules of the country concerned; see the Operational Procedures for Naming in SIGINT Reports (OPS-1-7), Annexes 3 to 6.

4.3.2.4 Copyright

IRRELEVANT

4.3.2.5 Consent

When issuing a report containing collateral, comply with all the original restrictions imposed on the collateral you are citing unless the originating agency has granted you permission to do otherwise.

4.3.2.6 ORCON

IRRELEVANT

4.3.2.7 Commentary not to be used

IRRELEVANT

4.3.2.8 Availability

IRRELEVANT

4.3.2.9 Quotations

IRRELEVANT

4.3.2.10 Using collateral in tear-line reports

IRRELEVANT

4.3.3 Placement and flagging of collateral

4.3.3.1 Placement

IRRELEVANT

4.3.3.2 Flagging of collateral

IRRELEVANT

4.3.3.3 Automated flagging

IRRELEVANT

4.3.3.4 Classification

IRRELEVANT

IRRELEVANT

IRRELEVANT

4.3.3.5 Collateral that does not require flagging

IRRELEVANT

4.3.4 Unclassified collateral

4.3.4.1 Definition

Unclassified collateral includes radio and television broadcasts, wire service reports, newspapers, periodicals, reference works, public reports of government departments and agencies, and other information that has not been classified by a Canadian or Second Party government department or agency.

4.3.4.2 Identify the source

IRRELEVANT

4.3.4.3 Canadian and Second Party media

IRRELEVANT

4.3.4.4 Foreign media

IRRELEVANT

4.3.4.5 Books and pamphlets

IRRELEVANT

IRRELEVANT

4.3.4.6 Reference works

IRRELEVANT

4.3.5 Classified collateral

4.3.5.1 Definition

IRRELEVANT

4.3.5.2 Types

IRRELEVANT

4.3.5.3 Disclosing sources of collateral

IRRELEVANT

4.3.5.4 Description of collateral type

IRRELEVANT

4.3.5.5 Dating the collateral

IRRELEVANT

4.3.5.6 ORCON material

IRRELEVANT

4.3.6 Record-keeping requirements

4.3.6.1 What to keep

IRRELEVANT

4.3.6.2 Purpose

IRRELEVANT

4.3.6.3 Entering information about collateral in [redacted]

IRRELEVANT

4.4 Identities

4.4.0.1 Introduction

This chapter provides general guidance on the inclusion of identifying information about Canadian and Second Party nationals, organizations and corporations in SIGINT reports.

4.4.0.2 Contents

This chapter contains the following sections:

- Rules on reporting identities
- Marking and handling suppressed information
- Contextual identification

4.4.1 Rules on reporting identities

4.4.1.1 Naming policies

In keeping with the legal authorities governing its activities, it is CSEC policy to protect the privacy of Canadians by suppressing the identities of Canadian persons, corporations and organizations in SIGINT reports, except in specific circumstances. CSEC's naming policy and procedures are described in detail in the Operational Procedures for Naming in SIGINT Reports (OPS-1-7).

For Second Party identities, it is CSEC policy to honour the naming rules of Second Party partners. For summaries of Second Party naming policies, see Annexes 3 to 6 of OPS-1-7. More detailed guidance is provided in the following policy documents:

- Australia: [redacted]
- New Zealand: [redacted]
- United Kingdom: [redacted]
- United States: [redacted]

4.4.1.2 Identifying Canadian federal public servants

You may identify senior federal public servants, acting in their official capacity, by **title**, but only if such identification is necessary to understand the foreign intelligence or assess its importance. In practice, it usually is necessary, if for no other reason than to ensure that the report is shown to the official in question.

"Senior federal public servants" means directors general and above. For federal public servants at the director level and below, you may use only a generic reference, such as "a [redacted] official". **Note:** According to section 4.4 of OPS-1-7, a generic reference is required only for "federal public servants below the level of Director", but this is incorrect; a generic reference must also be used for directors.

4.4.2 Marking and handling suppressed information

4.4.2.1 Need for retention

When you have to suppress the identity of a Canadian or Second Party person, organization or corporation in a report, you are required to enter the name in [redacted] so that Operational Policy (D2) can retrieve it later if necessary (see "Release of identities" below). In the case of a Canadian or Second Party terrorist, you should include all available information (e.g., phone number, e-mail address) to assist CSIS and other law enforcement agencies.

4.4.2.2 Marking idents in [redacted]

IRRELEVANT

Note 1	When a suppressed ident appears more than once in a report, only the first occurrence should be "marked"; the alias should be used for all other occurrences.
Note 2	You may use abbreviations to simplify subsequent reference to the aliases of suppressed idents (e.g., CA1 for named Canadian citizen 1, CA2 for named Canadian citizen 2, etc.). However, it is best not to use abbreviations to refer to unidentified Canadians (this tends to confuse the reader); if it is absolutely essential to use such abbreviations, be sure to clearly distinguish them from abbreviations for suppressed idents (e.g., UC1 for unnamed Canadian 1, UC2 for unnamed Canadian 2, etc.).

4.4.2.3 Release of identities

Access to ident information in the [redacted] database is strictly controlled. All requests – whether by GC departments, Second Parties or even CSEC staff – for the release of names or other identifying information suppressed from end product must follow the process described in the Procedures for the Release of Suppressed Information from SIGINT Reports (OPS-1-1).

4.4.3 Contextual identification

4.4.3.1 Definition

Contextual identification occurs when an end-product report provides enough detail about a suppressed Canadian or Second Party entity so that a reasonably well-read person can easily guess the identity behind the alias.

Contextual identification is equivalent to naming and is therefore not permitted.

Note: In isolated cases, combining the information in two or more reports may result in contextual identification. It is not necessary to take active measures to prevent this possibility, but cross-report contextual identification is not be used as a means of circumventing the naming rules.

4.4.3.2 Types of contextual identification

There are three ways in which contextual identification can occur:

1. The alias is too specific. For example, if Untel Manufacturing Co. of Canada is the only company in Canada that makes widgets, using the alias "a Canadian widget manufacturer" in a report constitutes contextual identification.
2. The information accompanying the alias reveals its identity. For example, the sentence [redacted] was involved.
3. The alias and the accompanying information combined give away the identity.

The key point here is that in determining whether your report identifies a Canadian or Second Party entity by context, you must consider all the relevant information in the report.

4.4.3.3 Determining whether there is contextual identification

Often, contextual identification is not as clear-cut as in the examples above. This can make it difficult to determine whether there is contextual identification. However, there are a couple of questions you can ask yourself to help you make the determination:

1. Looking at all the information in the report, not just the individual bits of information, could an alert reader narrow the range of entities associated with the information to just a few?

   Suppose a report contains the following information:
   - [redacted]
   -
   -

2. Would a reasonably well-read Canadian (someone who routinely reads a major newspaper, watches TV news or visits news websites) be able to figure out whom or what I'm referring to in this report?

   For example, a reference to [redacted] reporting would provide no protection for the person's identity.

It is important to consider the converse as well. Would a reader have to have "specialized knowledge" (knowledge that could only be obtained from foreign magazines and newspapers, technical publications or other non-SIGINT information that seldom receives mass media attention) to determine the identity of the person, company or organization behind the alias? If so, it is probably not a case of contextual identification.

If you're not sure, check with Operational Policy (D2).

4.4.3.4 What to do if there is contextual identification

If the answer to question 1 or 2 above is yes, the information in your report will result in contextual identification of a Canadian or Second Party entity. You then have two options:

1. make the alias and/or the accompanying information less specific, so that contextual identification is no longer a realistic possibility; or
2. if the contextual identification is essential to the intelligence story, request the necessary approvals. See section 5.4 of the Operational Procedures for Naming in SIGINT Reports (OPS-1-7).

4.4.3.5 Posting of approvals and authorizations

The links below provide access to the lists of blanket approvals for contextual identifications and threat-to-life naming and [redacted] The lists are also posted on the Intelligence Branch website under Publications.

- List of Blanket Identification Approvals
- [redacted]

4.5 SIGINT Style Guide

4.5.0.1 Introduction

This chapter provides guidelines on the elements of style that relate specifically to SIGINT reporting. The goal is to promote quality, consistency and clarity in CSEC and CFIOG reports.

4.5.0.2 Style

IRRELEVANT

4.5.0.3 Key elements of SIGINT style

IRRELEVANT

4.5.0.4 Clarity

IRRELEVANT

4.5.0.5 Brevity

IRRELEVANT

4.5.0.6 [redacted]

[redacted]

4.5.0.7 Contents

This chapter contains the following sections:

4.5.1 Abbreviations and acronyms

4.5.1.1 Definitions

IRRELEVANT

4.5.1.2 Purpose

IRRELEVANT

4.5.1.3 How to use

IRRELEVANT

4.5.1.4 Approved abbreviations and acronyms

IRRELEVANT

4.5.1.5 Correct forms

IRRELEVANT

4.5.1.6 NFI

IRRELEVANT

4.5.1.7 Countries

IRRELEVANT

4.5.1.8 Organizations

IRRELEVANT

4.5.1.9 Plurals

IRRELEVANT

4.5.1.10 Foreign abbreviations and acronyms

IRRELEVANT

4.5.2 Capitalization

4.5.2.1 General rule

IRRELEVANT

4.5.2.2 Initial caps

IRRELEVANT

4.5.2.3 Full caps

IRRELEVANT

4.5.3 Code words, cover names and cover numbers

4.5.3.1 Code words

IRRELEVANT

4.5.3.2 Cover names

IRRELEVANT

4.5.3.3 Cover numbers

IRRELEVANT

4.5.4 Dates

4.5.4.1 Format

IRRELEVANT

IRRELEVANT

4.5.4.2 Stating the year

IRRELEVANT

4.5.4.3 Hyphenation in date ranges

IRRELEVANT

4.5.4.4 Hyphenation in date modifiers

IRRELEVANT

4.5.5 Geographic coordinates

4.5.5.1 When to use

Include coordinates for place names or locational data only when they are likely to be of value to the reader. For example, the expected readers of a particular product line may require only general location information.

Avoid using coordinates in report titles, summary paragraphs, or lead sentences of longer reports (four or more paragraphs). Include them in the body of the report.

If you include coordinates in a tear-line, make sure you have sufficient [redacted] for the level of detail provided.

4.5.5.2 Types of coordinates

IRRELEVANT

4.5.5.3 Unnecessary coordinates

IRRELEVANT

4.5.5.4 Placement of coordinates

IRRELEVANT

IRRELEVANT

4.5.5.5 Degrees-minutes-seconds (DMS) notation

IRRELEVANT

4.5.5.6 Decimal-degrees notation

IRRELEVANT

4.5.5.7 Military Grid Reference System (MGRS) notation

IRRELEVANT

4.5.5.8 Universal Transverse Mercator (UTM) notation

IRRELEVANT

4.5.6 Linguistic Information

4.5.6.1 Language used

IRRELEVANT

4.5.6.2 Peculiarities

IRRELEVANT

4.5.6.3 Foreign words

IRRELEVANT

4.5.6.4 Obscenities

IRRELEVANT

4.5.7 Measurements

4.5.7.1 Reporting measurements given in SI units

IRRELEVANT

4.5.7.2 Reporting measurements given in non-SI units

IRRELEVANT

4.5.8 Military equipment and unit designators

4.5.8.1 Contents

This section covers the following topics:

- Military aircraft
- Aircraft designators in reports
- Weapon systems
- Weapon system designators in reports
- missiles
- Unit designators
- Unit designators in reports

4.5.8.2 Military aircraft

IRRELEVANT

4.5.8.3 Aircraft designators in reports

IRRELEVANT

4.5.8.4 Weapon systems

IRRELEVANT

4.5.8.5 Weapon system designators in reports

IRRELEVANT

4.5.8.6 Missiles

IRRELEVANT

4.5.8.7 Unit designators

IRRELEVANT

4.5.8.8 Unit designators in reports

IRRELEVANT

4.5.9 Money

4.5.9.1 How to report

IRRELEVANT

4.5.9.2 Currency names

IRRELEVANT

4.5.9.3 Format

IRRELEVANT

4.5.9.4 Conversion rate

IRRELEVANT

4.5.10 Numerical Expressions

4.5.10.1 Spelled out

IRRELEVANT

4.5.10.2 Numerals

IRRELEVANT

4.5.10.3 Punctuation and spacing

IRRELEVANT

4.5.10.4 Hyphenation in modifiers

IRRELEVANT

4.5.10.5 Hyphenation in ranges

IRRELEVANT

4.5.10.6 Fractions

IRRELEVANT

4.5.10.7 Ordinals

IRRELEVANT

4.5.11 Quotations

4.5.11.1 General rule

IRRELEVANT

4.5.11.2 Approved uses

IRRELEVANT

4.5.11.3 Maps, charts and diagrams

Fax and e-mail intercept may contain maps, charts and/or diagrams. Consider whether the information lends itself to narrative reporting or would be easier for the customer to grasp in "native format" (i.e., insert the traffic in the report as an image, or attach an image to the report). Keep in mind that if you opt for native format, you must

- embed the appropriate classification marking in the image
- suppress any Canadian or Second Party identities in the image
- remove any [redacted] or irrelevant information from the image
- provide English translations for any foreign-language markings on the image

For more details on native format reporting, see Appendix M.

4.5.11.4 Punctuation

IRRELEVANT

4.5.11.5 Interpolations

IRRELEVANT

4.5.12 Ships

4.5.12.1 [redacted]

IRRELEVANT

IRRELEVANT

4.5.12.2 [redacted]

IRRELEVANT

4.5.12.3 [redacted]

IRRELEVANT

4.5.12.4 Spelling

IRRELEVANT

4.5.12.5 Capitalization

IRRELEVANT

4.5.12.6 Italics

IRRELEVANT

4.5.13 Spelling

4.5.13.1 General rule

IRRELEVANT

4.5.13.2 Personal names

IRRELEVANT

4.5.13.3 Country names

IRRELEVANT

4.5.13.4 Place names

IRRELEVANT

IRRELEVANT

4.5.13.5 Nationalities

IRRELEVANT

4.5.13.6 Organization names

IRRELEVANT

4.5.13.7 Ship names

IRRELEVANT

4.5.14 Time

4.5.14.1 Format

IRRELEVANT

4.5.14.2 Format rules

IRRELEVANT

4.5.14.3 Multiple time entries

IRRELEVANT

4.5.14.4 General phrases

IRRELEVANT

4.5.14.5 Local time

IRRELEVANT

IRRELEVANT

4.5.15 Validity wording

4.5.15.1 Purpose

IRRELEVANT

4.5.15.2 SIGINTese

IRRELEVANT

IRRELEVANT

4.5.15.3 Fact

IRRELEVANT

4.5.15.4 Probability

IRRELEVANT

4.5.15.5 Possibility

IRRELEVANT

4.6 Attachments

4.6.1 Introduction

IRRELEVANT

4.6.2 Definition

IRRELEVANT

4.6.3 Attachments and report serial numbers

IRRELEVANT

4.6.4 Adding attachments to reports

IRRELEVANT

5. Report Externals

5.0.1 Introduction

IRRELEVANT

5.0.2 Contents

This part contains the following chapters:

5.1 General Metadata Page

5.1.1 Introduction

This chapter provides guidelines for filling in the General Metadata page in [redacted]

5.1.2 Important fields

IRRELEVANT

5.1.3 Additional warnings

IRRELEVANT

5.1.4 Type

IRRELEVANT

5.1.5 Precedence

IRRELEVANT

5.1.6 Reason for write-to-release exemption

IRRELEVANT

5.1.7 RFI IDs

IRRELEVANT

5.1.8 SIR

If your report addresses a standing intelligence requirement (SIR), enter the SIR number in the SIR box. If more than one SIR is addressed, put a comma between the SIR numbers. The letter component of SIRs must be in lower case: [redacted]

5.2 Distribution Page

5.2.0.1 Introduction

This chapter provides guidelines on filling in the Distribution page in [redacted] The selections you make on this page determine which agencies in the Canadian and Second Party intelligence communities receive copies of your report via [redacted]

Note: This chapter applies only to reports shared with one or more Second Parties. For CEO and Restricted reports, the Distribution page should be left blank.

5.2.0.2 Use templates

IRRELEVANT

5.2.0.3 Procedure if not using a template

IRRELEVANT

5.2.0.4 Contents

This chapter contains the following sections:

- Collective address groups (CAGs)
- Plain-language addresses (PLAs)
- Delivery distribution indicators (DDIs)

5.2.1 Collective address groups (CAGs)

5.2.1.1 Definition

IRRELEVANT

5.2.1.2 CAGs in templates

IRRELEVANT

5.2.1.3 Write-in addressees

IRRELEVANT

5.2.1.4 Selecting a CAG

IRRELEVANT

5.2.1.5 Excluding recipients from a CAG

IRRELEVANT

5.2.1.6 Finding out the list of recipients

IRRELEVANT

5.2.2 Plain-language addresses (PLAs)

5.2.2.1 Definition

IRRELEVANT

5.2.2.2 Selecting PLAs individually

1. IRRELEVANT
2.
3.
4.

5.2.2.3 Selecting [redacted] addressees

IRRELEVANT

5.2.2.4 Adding sub-addressees to a PLA

IRRELEVANT

5.2.3 Delivery distribution indicators (DDIs)

5.2.3.1 Definition

A delivery distribution indicator (DDI) is a [redacted] used to route messages electronically to specific databases and elements within national SIGINT centres, primarily NSA.

5.2.3.2 Limit

No more than 14 DDIs can be used on any report.

5.2.3.3 Two sets of DDIs

There are two sets of DDIs: one used for regular reports (i.e., reports released outside the SIGINT community), and one used exclusively for CIRs.

In Slingshot, both sets have been lumped into one table. To make sure you are selecting the proper DDIs, follow the instructions below.

5.2.3.4 Selecting regular DDIs

It is important to select DDIs for all of the [redacted] involved in your report, and for all applicable subjects. Here's how.

[redacted]

7. If your report is

IRRELEVANT

8.

5.2.3.5 Selecting CIR DDIs

IRRELEVANT

5.3 Traffic Page

5.3.1 Introduction

This chapter provides guidelines for filling in the Traffic page in [redacted]

5.3.2 Purpose

Use this page to record information about the source material on which your report is based.

Note: [redacted] entry is mandatory. If you attempt to release a report without entering source information, you will receive an error message.

5.3.3 Procedure

For each piece of traffic used in your report, do the following:

1. Identify the traffic
2. Select the contribution percentage (if necessary)
3. Select the language of the traffic
4. IRRELEVANT

5.3.4 Identify the traffic

IRRELEVANT

5.3.5 Contribution

IRRELEVANT

5.3.6 Select the language

IRRELEVANT

IRRELEVANT

5.4 TAGs Page

5.4.0.1 Introduction

This chapter provides guidelines for filling in the TAGs page in [redacted]

5.4.0.2 Definition and purpose of TAGs

TAG stands for Topic and Area Guide. TAGs are alphabetic codes used to identify a report's intelligence source, subject area and major participants. The TAGs that apply to a report are grouped together in one or more TAG lines.

The main uses are to

- simplify database retrieval strategies
- match reports to Government of Canada Requirements (GCRs), and
- facilitate automated distribution of reports.

For a full description of the TAG system, see [redacted]

5.4.0.3 Format

A TAG line contains three components in the following order:

- the [redacted]
- the subject/topic component
- the principal component

5.4.0.4 Contents

This chapter contains the following sections:

- [redacted]
- Subject/topic component
- Principal component
- Creating TAG lines in [redacted]
- Effective use of the TAG system

5.4.1 [redacted]

5.4.1.1 General information

The [redacted] is usually the first element in a TAG entry. It consists of three letters. The first two letters identify the source [redacted] and the third letter identifies the [redacted] the intelligence information.

Omit the [redacted] in the TAG entry only when the report is

- based on ELINT or FISINT and the source of the signal cannot be determined, or
- a Summary Report or Assessment Report based on reports with different [redacted]

5.4.1.2 Digraphs

CSEC and its SIGINT partners have established a system of digraphs to represent the countries, areas and organizations of the world for the purposes of collection and traffic analysis, cryptanalysis, and reporting. In reports, digraphs are used in both the [redacted] and the principal component.

All approved digraphs and their permitted uses in reporting are listed in the Digraphs working aid. To propose new digraphs or changes in existing ones, contact [redacted]

5.4.1.3 Distinction between intelligence source and communications source

It is important to distinguish between the **intelligence source** and the **communications source**.

- The intelligence source is the individual or entity that provides the information being reported.
- The communications source is the communications [redacted]

5.4.1.4 [redacted] should reflect intelligence source

Except in two cases (see below), the [redacted] must represent the **intelligence** source. In other words, the [redacted] should match the person or organization to which the information is attributed in the body of the report.

- **Exception 1**: In reports based on IRRELEVANT traffic, the [redacted] will depend on the target and will be determined by the PM concerned.

- **Exception 2**: Where the entity providing the intelligence is a Canadian or [redacted] entity, the [redacted] must reflect an alternative source, usually the entity receiving the information.

5.4.1.5 Intelligence source function letter

IRRELEVANT

5.4.1.6 Some third letters used incorrectly

IRRELEVANT

5.4.1.7 Third-letter IRRE

IRRELEVANT

5.4.1.8 Third-letter IRRE

IRRELEVANT

5.4.1.9 Third-letter IRRE

IRRELEVANT

5.4.1.10 [redacted] for [redacted]

IRRELEVANT

5.4.1.11 [redacted] for [redacted] digraph

IRRELEVANT

5.4.1.12 Uses of [redacted]

IRRELEVANT

5.4.2 Subject/Topic Component

5.4.2.1 General information

IRRELEVANT

5.4.2.2 Overlapping definitions: [redacted] and [redacted]

IRRELEVANT

5.4.2.3 Overlapping definitions: [redacted] and [redacted]

IRRELEVANT

5.4.2.4 Distinction between [redacted] and [redacted]

IRRELEVANT

5.4.2.5 Subject TAGs required for [redacted] reports

IRRELEVANT

5.4.3 Principal Component

5.4.3.1 General information

IRRELEVANT

5.4.3.2 Digraphs for [redacted]

IRRELEVANT

5.4.4 Creating TAG lines in [redacted]

IRRELEVANT

5.4.5 Effective Use of the TAG System

5.4.5.1 Include all the right TAGs

IRRELEVANT

5.4.5.2 Inclusion of source digraph in principal component

Frequently, the source (the country specified in the [redacted] is involved closely in the matters discussed in the report and therefore should also figure in the principal component. However, when the source country is not directly involved in the intelligence story, its digraph should **not** be included in the principal component. See the examples below.

IRRELEVANT

5.4.5.3 Multiple TAG lines

IRRELEVANT

5.4.5.4 Two or more sources

IRRELEVANT

IRRELEVANT

5.5 Actors Page

5.5.1 Introduction

IRRELEVANT

5.5.2 Purpose

IRRELEVANT

5.5.3 Types of Actors

IRRELEVANT

5.5.4 How to select Actors

IRRELEVANT

5.5.5 Selecting the right Actors

IRRELEVANT

5.5.6 Special Actor required for RESTRICTED [redacted] reports

IRRELEVANT

6. Corrections and Cancellations

6.0.1 Introduction

IRRELEVANT

6.0.2 Contents

This part contains the following sections:

6.1 Determining whether to correct or cancel

6.1.1 Introduction

IRRELEVANT

6.1.2 When to correct a report

IRRELEVANT

6.1.3 When to cancel a report

Cancel a report when:

- its entire contents are found to be incorrect because of new SIGINT information or a re-evaluation of the original data
- it is underclassified (i.e., the classification of one or more of the original report's paragraphs was lower than required, or one or more dissemination controls were omitted)
- it is overclassified (i.e., the classification of one or more of the original report's paragraphs was higher than required, or one or more unnecessary dissemination controls were included), preventing potential users from seeing information they might need
- it was issued CEO but should have been shared with one or more Second Parties
- it was sent to one or more ineligible addressees (for reports with an incomplete distribution, see section 6.2.4)
- it inadvertently discloses a Canadian or Second Party identity

If more than one of the above applies, select the one closest to the top of the list.

6.1.4 When not to correct or cancel

IRRELEVANT

6.2 Corrections

6.2.1 Correcting the report text

IRRELEVANT

6.2.2 Correcting the tear-line portion

IRRELEVANT

6.2.3 Correcting a TAG line

IRRELEVANT

6.2.4 Incomplete distribution

IRRELEVANT

6.3 Cancellations

6.3.1 Erroneous contents

IRRELEVANT

6.3.2 Report underclassified

IRRELEVANT

6.3.3 Report overclassified

IRRELEVANT

IRRELEVANT

6.3.4 CEO report should have been COM

IRRELEVANT

IRRELEVANT

6.3.5 Incorrect distribution

IRRELEVANT

IRRELEVANT

6.3.6 Disclosure of identity

If you inadvertently disclose a Canadian or Second Party identity, do the following:

1. Notify your supervisor.
2. Cancel and reissue the report, following the instructions below.
3. Complete SPOC's Inadvertent Targeting and Naming Incidents web form.

A. Reissue the report	IRRELEVANT
	9. Preview the report in [redacted] and make sure that all references to the identity have been minimized or eliminated. Have the report checked by your editor or releaser.

	Important: 1. Determine whether, because of the change in identity status, an OPS-1 or other **special sign-off** is now required. If so, you must obtain the appropriate signatures before release. 2. IRRELEVANT
B. Cancel the original report	IRRELEVANT Please cancel and destroy all copies of this report, which does not comply with standard reporting practices. The report has been reissued IRRELEVANT 4. 5. 6.

Appendix A: Report Classification

A.0.1 Introduction

IRRELEVANT

A.0.2 Definition of classification

IRRELEVANT

A.0.3 Classification requirement

IRRELEVANT

A.0.4 Contents

This appendix contains the following sections:

- General aspects of classification
- Paragraphs
- Block headings
- Other components

A.1 General aspects of classification

A.1.1 Classification of SIGINT reports

IRRELEVANT

A.1.2 Classification of report components

IRRELEVANT

A.1.3 Classification of COMINT reports

IRRELEVANT

A.2 Paragraphs

A.2.1 Determining the classification

IRRELEVANT

A.2.2 Selecting the classification

IRRELEVANT

A.2.3 Multiple paragraphs under one block heading

IRRELEVANT

A.3 Block headings

A.3.1 Classifying the block heading

IRRELEVANT

A.3.2 Selecting the classification

IRRELEVANT

A.4 Other components

A.4.1 Attachments

IRRELEVANT

A.4.2 CIRs

IRRELEVANT

A.4.3 Collateral

IRRELEVANT

A.4.4 Footnotes

IRRELEVANT

IRRELEVANT

A.4.5 Images

IRRELEVANT

A.4.6 POC information

IRRELEVANT

A.4.7 Tables

IRRELEVANT

A.4.8 Tear-lines

IRRELEVANT

A.4.9 Title

IRRELEVANT

Appendix B: Reporting Nationally Sensitive Information

B.0.1 Introduction

This appendix provides guidelines to help the reader determine what information is "nationally sensitive" and how such information should be reported. In particular, it provides a set of criteria to assist in deciding what information should be reported in the RESTRICTED series as opposed to just Canadian Eyes Only (CEO).

B.0.2 Contents

This appendix covers the following topics:

- "Feedback" reports
- Canadian sensitivities (including how to distinguish between CEO information and RESTRICTED information)
- Second Party sensitivities
- Sensi-checking
- Severing (issuing more than one report)
- Preparing CEO and RESTRICTED reports in [redacted]

B.1 "Feedback" reports

IRRELEVANT

B.2 Canadian sensitivities

The instructions below are only guidelines, not hard and fast rules. Under special circumstances, information that does not meet the criteria below may have to be reported in the CEO series; this decision should be made in consultation with the Task Leader or Production Manager.

The main categories of Canadian sensitivities, and how the information should be reported (RESTRICTED or CEO), are listed in the table below.

If the information could ...	Then it should be issued ...	Examples
[redacted]	RESTRICTED	[redacted]
[redacted]	RESTRICTED	[redacted]
[redacted]	CEO	[redacted]

[redacted]	CEO	[redacted]
[redacted]	CEO	[redacted]
[redacted]	CEO	[redacted]
[redacted]	CEO	[redacted]
[redacted]	CEO	[redacted]
[redacted]	CEO	

B.3 Second Party sensitivities

IRRELEVANT

B.4 Sensi-checking

IRRELEVANT

B.5 Severing (issuing more than one report)

In all cases where the distribution of a report has to be limited in some way because of Canadian or Second Party sensitivities, you should consider whether it is feasible to "sever" the report, i.e., to issue two versions of the report:

- one containing only the non-sensitive information, which would be issued to a wider distribution.
- the other containing only the sensitive information (with a reference to the other version), which would be issued to a narrower distribution.

When a report is severed, a note should be sent to the CROs indicating that both versions are based on the same traffic.

Examples of severing

Here are two examples of cases in which the report could be severed:

1. [redacted]

2. [redacted]

B.6 Preparing CEO and RESTRICTED reports in [redacted]

B.6.1 CEO reports

IRRELEVANT

B.6.2 RESTRICTED reports

IRRELEVANT

Appendix C: Write-To-Release Reporting

C.0.1 What is "write to release"?

The "write to release" (WTR) concept was introduced some years ago as part of an initiative to disseminate actionable intelligence more quickly to readers who can use it. To that end, SIGINT report authors are required to include a "sanitized" version of the COMINT information in their reports whenever possible. Sanitization is the process of disguising COMINT to protect sensitive sources and methods so that the information can be released outside COMINT channels.

C.0.2 What is a tear-line report?

In [redacted] (Web) format, a tear-line report looks much the same as any other report. The main difference lies in the formatting applied to the report for transmission over [redacted] In a tear-line report, a copy of the non-COMINT portion is placed below the COMINT portion and enclosed between two broken lines (- - - - -) so that it can be separated manually or electronically for forwarding to non-COMINT readers.

C.0.3 What's the relationship between WTR and tear-lines?

Initially, the tear-line was just one of several ways of achieving the goals of WTR. Over the years, however, it has become the predominant method, and tear-line reporting is now virtually synonymous with WTR.

C.0.4 Multiple tear-lines

If necessary to meet the requirements of different client groups, you can add more than one tear-line to a report.

C.0.5 More information

For more information about WTR, see:

- CSEC's Write-to-Release Procedures (OPS-5-3)
- NSA's Sanitization: A Guide for SIGINT Reporters

C.0.6 Contents

This appendix covers the following topics:

- Determining a report's eligibility for WTR
- Writing the tear-line portion of a report
- Including collateral or comments in a tear-line
- Releasing a tear-line report

C.1 Determining a report's eligibility for WTR

C.1.1 Decision matrix

IRRELEVANT

(d) Will it be necessary to include one or more suppressed idents in the tear-line portion? Ref: WTR Procedures, section 3.4	Yes	No tear-line
	No	Go to Writing the report

C.1.2 List of [redacted]

IRRELEVANT

C.1.3 Timeliness and [redacted]

IRRELEVANT

C.1.4 [redacted]

IRRELEVANT

C.2 Writing the tear-line portion of a report

C.2.1 General guidelines

IRRELEVANT

C.2.2 Attribution in a tear-line

IRRELEVANT

IRRELEVANT

C.3 Including collateral or comments in a tear-line

C.3.1 Collateral

IRRELEVANT

C.3.2 Comments

IRRELEVANT

IRRELEVANT

C.4 Releasing a tear-line report

C.4.1 Preparing to release

IRRELEVANT

C.4.2 Release procedures

IRRELEVANT

Appendix D: SIGINT Summaries and Assessments

D.0.1 Introduction

This appendix provides guidelines for producing SIGINT Summaries and SIGINT Assessments.

D.0.2 What is a SIGINT Summary?

IRRELEVANT

D.0.3 What is a SIGINT Assessment?

IRRELEVANT

D.0.4 Contents

This appendix contains the following sections:

- How to prepare a SIGINT Summary
- How to prepare a SIGINT Assessment

D.1 Preparing a SIGINT Summary in [redacted]

D.1.1 Getting started

IRRELEVANT

D.1.2 Formatting

IRRELEVANT

D.1.3 Classification

IRRELEVANT

D.1.4 TAGs

IRRELEVANT

D.1.5 Traffic

IRRELEVANT

D.2 Preparing a SIGINT Assessment in [redacted]

D.2.1 Getting started

IRRELEVANT

D.2.2 Formatting

IRRELEVANT

D.2.3 Classification

IRRELEVANT

D.2.4 TAGs

IRRELEVANT

IRRELEVANT

D.2.5 Traffic

On the Traffic page, include all previously reported SIGINT under one metadata entry, as follows:

IRRELEVANT

1.
2.
3.
4.
5.
6.
7.

Appendix E:
Cryptologic Information Reports (CIRs)

E.0.1 Introduction

IRRELEVANT

E.0.2 What is a CIR?

IRRELEVANT

E.0.2 Contents

This appendix covers the following topics:

- CIR reporting requirements
- CIR reporting priorities
- Preparing a CIR in [redacted]

E.1 CIR reporting requirements

IRRELEVANT

IRRELEVANT

E.2 CIR reporting priorities

IRRELEVANT

E.3 Preparing a CIR in [redacted]

IRRELEVANT

Appendix F: Information Items

F.1 Purpose

IRRELEVANT

F.2 Template

IRRELEVANT

F.3 Report layout and content

IRRELEVANT

F.4 Title

IRRELEVANT

Appendix G: [redacted] Reporting

G.0.1 Purpose

This appendix provides guidelines for the preparation of all reports containing [redacted] data.

G.0.2 Contents

This appendix contains the following sections:

- Introduction
- Reports containing classified [redacted] data
- Reports containing UNCLASSIFIED [redacted] data

G.1 Introduction

G.1.1 Definition

[redacted]

G.1.2 Sources of [redacted] data

[redacted] data collected using SIGINT systems is [redacted] the covername [redacted] The data is classified SECRET//COMINT but may be reported at the SECRET level (see section G.2).

Some [redacted] data is available from open sources. It may be used only as UNCLASSIFIED collateral (see section G.3).

G.1.3 Classified [redacted] data

On 31 August 2004, [redacted] data via the [redacted] network.

CSEC receives two types of [redacted] data feeds, both of which include [redacted] from all [redacted]

- [redacted]
-

G.1.4 Application

[redacted] reports are subject to all guidelines in this CSOI that do not conflict with those described below. For guidance on reports containing [redacted] information from [redacted] see Appendix I.

G.1.5 Reporting of [redacted] data under CSEC's mandates

Under mandate A, CSEC is permitted to provide [redacted] information associated with foreign entities outside Canadian territory (Canadian territory consists of Canada's land mass, the Arctic archipelago and the waters around Canada's land mass out to a distance of 12 nautical miles). Providing [redacted] data about a Canadian anywhere or any person or entity in Canadian territory is not permitted. The same rules apply to persons and entities of Second Party partners and persons and entities located in Second Party countries and their dependencies.

IRRELEVANT

G.1.6 Support

For technical help, contact [redacted]@cse-cst.gc.ca).

For report review or guidance, contact [redacted]

For policy assistance, contact [redacted] or SPOC.

G.2 Reports Containing Classified [redacted] Data

G.2.1 Classification of reports

Release reports that contain [redacted] data only or a combination of [redacted] and ELINT as ELINT reports (reports in the [redacted] or [redacted] series). To do this in [redacted] you must select [redacted]

G.2.2 Information that can be reported at the SECRET level

The following elements may be reported at the SECRET level:

- [redacted]

G.2.3 [redacted] not to be reported

[redacted] may also contain [redacted] -related [redacted] This information is **not** to be reported.

G.2.4 Report content

If your report contains coordinates, follow the instructions in the main entry on geographic coordinates.

If your report contains references to ships, follow the instructions in the main entry on ships.

If your report contains [redacted] information, follow the instructions in Appendix I.

G.2.5 Entering [redacted] in [redacted]

IRRELEVANT

G.2.6 Report edit/release: Printing the Metadata sheet

IRRELEVANT

G.3 Reports Containing UNCLASSIFIED [redacted] Data

G.3.1 Open-source [redacted] data

Some [redacted] data can be found in open sources. Such data is usually available only for [redacted] This data is often found on the Internet.

G.3.2 Using UNCLASSIFIED [redacted] data

Open-source [redacted] data is UNCLASSIFIED collateral and may be reported only in conjunction with SIGINT data. If you use UNCLASSIFIED [redacted] data in a report, you should enter the source of the data on the Traffic page in [redacted] using the [redacted]

G.3.3 Report content

If your report contains coordinates, follow the instructions in the main entry on geographic coordinates.

If your report contains references to ships, follow the instructions in the main entry on ships.

If your report contains [redacted] information, follow the instructions in Appendix I.

Appendix H: Advance Reports

H.1 Definition

An Advance Report is an informal, partially vetted SIGINT report containing incompletely analyzed information. It is intended as a vehicle for timely reporting of highly perishable intelligence.

H.2 When to prepare an Advance Report

Prepare an Advance Report only when the standard report-writing, editing and release process would jeopardize prompt delivery of the information.

H.3 Writing the Advance Report

When preparing your Advance Report, follow the instructions below.

- Prepare the Advance Report as an e-mail.
- Limit your Advance Report to what your customers need to know right away. You can include background information and less important details in the serialized report to follow.
- Do not include any [redacted]
- Write as clearly and concisely as possible.
- Classify the Advance Report correctly.
- Suppress idents. The naming rules are the same for Advance Reports as they are for formal reports.
- Obtain all required signatures on a Product Release Form. Advance Reports are subject to the OPS-1 and IRRELEVANT sign-off procedures (see below).
- Generate a tracking number for your Advance Report as follows: [redacted]
- Enter the number at the top of the e-mail and on the Product Release Form. This will make it easier to track your report and match it with the associated serialized report.

H.4 Quality control

Before sending out your Advance Report, you must have it checked by a release authority (usually a TL or a PM).

H.5 Sign-offs

IRRELEVANT

Before sending out an Advance Report based on traffic that falls into an OPS-1 category, you must obtain the appropriate signatures (see the OPS-1 sign-off table). If the Advance Report has to be sent out during silent hours, the on-call PM or director will make the necessary arrangements for sign-off by senior managers. In threat-to-life situations during silent hours, a manager may authorize the report's release; DGI's or DC SIGINT's signature must be obtained later (see section 6.4 of OPS-1-7).

H.6 Distribution

Once the Advance Report is approved for release, e-mail it only to the CROs serving the clients for whom it is intended, with copies to the TL, the PM, the Director and DGI.

In the e-mail, place the following information above the Advance Report:

- a list of the intended recipients,
- the following handling instructions:

  This is an unedited Advance Report intended solely for the specified recipients; no further dissemination is permitted. A serialized report will follow. When that report is issued, all electronic and print copies of this Advance Report must be destroyed.

H.7 Serialized report

Prepare a serialized report as soon as possible after sending out the Advance Report.

Note: If CSIS or OPS-1 sign-offs were required for the Advance Report, they must be obtained, again, for the serialized report.

After issuing the serialized report, send the CROs who received the Advance Report an e-mail containing the following:

- the serial number,
- the Advance Report tracking number (e.g., [redacted]
- a request to confirm that all electronic and print copies of the Advance Report have been destroyed.

Appendix I: [redacted] Reporting

I.0.1 Purpose

This appendix provides guidelines on the use of [redacted] data in SIGINT reports.

I.0.2 Contents

This appendix contains the following sections:

- Introduction
- Report content
- Report externals

I.1 Introduction

I.1.1 Definition

A [redacted] report is any report that contains information obtained by means of SIGINT [redacted] techniques [redacted] ELINT, [redacted] FISINT). This does not include [redacted] derived from [redacted] etc.

I.1.2 Application

[redacted] reports (i.e., all reports containing [redacted] data) are subject to all guidelines in this CSOI that do not conflict with those described below. Reports containing [redacted] data are also subject to CSOI-5-9, *Using* [redacted] *Information.*

I.1.3 [redacted] reporting under CSEC's mandates

Under mandate A, CSEC is permitted to provide [redacted] information associated with foreign entities outside Canadian territory (Canadian territory consists of Canada's land mass, the Arctic archipelago and the waters around Canada's land mass out to a distance of 12 nautical miles). Providing [redacted] information about a Canadian anywhere or any person or entity in Canadian territory is not permitted. The same rules apply to persons and entities of Second Party partners and persons and entities located in Second Party countries and their dependencies.

IRRELEVANT

I.1.4 Support

For technical help, contact [redacted]@cse-cst.gc.ca).

For report review or guidance, contact [redacted]

For policy assistance, contact [redacted] or SPOC.

I.2 Report content

I.2.1 [redacted] information

Use only as much [redacted] as your clients need (i.e., apply the need-to-know principle). A description of the [redacted] may suffice (e.g., [redacted] is planning …"). If [redacted] are required, the [redacted]

If a client needs to know the [redacted] in the report, you may include it, but avoid explaining how the [redacted] was obtained, as this can reveal sources and methodology. Depending on the distribution, an explanation may be included in some RESTRICTED reports.

Examples of comments describing the [redacted] information in a report:

> Comment: The [redacted] not associated with a [redacted] is variable and may be confirmed by the originator if required.
>
> Comment: The [redacted] in this report, unless otherwise specified or associated with a [redacted] are generally [redacted]

Make sure that [redacted] do not convey [redacted] than is possible for the type of [redacted]

I.2.2 [redacted]

[redacted]

I.2.3 [redacted]

[redacted]

I.2.4 [redacted] and tear-lines

Include as much [redacted] information in the tear-line portion of a report as there is [redacted] for. In most cases, there is not enough [redacted] for [redacted] but you can include a description of the [redacted] In some instances, you may have to omit the [redacted] information entirely.

I.2.5 [redacted]

IRRELEVANT

I.2.6 Maps and imagery

All maps or imagery used in **any** SIGINT report (i.e., [redacted] reports and non-traditional reports) **must** be on an official CSEC map template, unless the map or imagery was provided by a partner agency [redacted] and is on that agency's own official template. The official CSEC map templates are accessible only from [redacted] or an official CSEC web map service that incorporates the CSEC map templates. Maps produced in other mapping applications [redacted] are **not** to be included in **any** SIGINT report.

Avoid including hits that result from collection anomalies [redacted] on the map or imagery.

Avoid including anything that shows capabilities and methodology (e.g., [redacted] in maps or imagery distributed to non-SIGINT producers, unless absolutely necessary. [redacted]

I.2.7 [redacted] using [redacted]

In general, avoid including images of [redacted] in SIGINT reports, unless they are RESTRICTED or limited to SIGINT producers, as such images reveal capabilities and methodology and may be confusing to non-expert readers.

I.2.8 [redacted] using [redacted] or [redacted]

In general, avoid including images of [redacted] in SIGINT reports, unless they are RESTRICTED or limited to SIGINT producers, as such images reveal capabilities and methodology.

[redacted]

I.3 Report externals

I.3.1 TAGs for [redacted] reports

Select [redacted] as one of the subject TAGs, except when:

- [redacted]

For reports containing ELINT [redacted] select **both** [redacted] and [redacted]

I.3.2 Traffic for [redacted] reports

Every [redacted] report must have at least one [redacted] traffic item:

- For ELINT [redacted] etc.), use the "ELINT" traffic type (see section I.3.3 below).
- For all other types of [redacted] traffic type (see section I.3.4 below).

When the report contains [redacted] information based on more than one selector or [redacted] criterion, or derived from more than one database:

- [redacted]

If there are too many selectors or [redacted] to enter in [redacted] (it only takes [redacted] traffic items), contact [redacted] for instructions.

If target sensitivities prevent you from putting the selector (or any other information) in the traffic item, contact [redacted] for instructions.

I.3.3 ELINT traffic type

IRRELEVANT

I.3.4 [redacted] traffic type

IRRELEVANT

IRRELEVANT

I.3.5 Special Actor [redacted] reports

IRRELEVANT

I.3.6 Report edit/release: Printing the Metadata sheet

IRRELEVANT

Appendix J: Key points and CSE Analysis

J.1 Rationale

IRRELEVANT

J.2 Key points

IRRELEVANT

J.3 CSE Analysis

IRRELEVANT

J.4 Key points - Content

IRRELEVANT

IRRELEVANT

J.5 Key points - Format

IRRELEVANT

IRRELEVANT

J.6 CSE Analysis - Content

IRRELEVANT

IRRELEVANT

J.7 CSE Analysis – Format

IRRELEVANT

Appendix K: ELINT Reporting

K.0.1 Purpose

This appendix provides guidelines for the preparation of all ELINT reports.

K.0.2 Contents

This appendix contains the following sections:

K.1 Introduction

K.1.1 Definitions

ELINT is technical and [redacted] intelligence information derived from the intercept of foreign non-communications electromagnetic emissions from non-nuclear, non-radioactive sources.

[redacted]

K.1.2 Application

ELINT reports are subject to all guidelines in this CSOI that do not conflict with those described below. All reports containing ELINT are subject to the guidelines in this CSOI unless otherwise noted.

K.1.3 ELINT reporting under CSEC's mandates

Under mandate A, CSEC is permitted to provide ELINT information associated with foreign entities outside Canadian territory (Canadian territory consists of Canada's land mass, the Arctic archipelago and the waters around Canada's land mass out to a distance of 12 nautical miles). Providing ELINT about a Canadian anywhere or any person or entity in Canadian territory is not permitted. The same rules apply to persons and entities of Second Party partners and persons and entities located in Second Party countries and their dependencies.

IRRELEVANT

K.1.4 Support

For technical help, contact [redacted]@cse-cst.gc.ca).

For report review or guidance, contact [redacted]

For policy assistance, contact [redacted] or SPOC.

K.2 ELINT-only reports

K.2.1 Classification

ELINT reports can be classified from S//REL TO CAN, AUS, GBR, NZL, USA up to TS//SI/TK//REL TO CAN, AUS, GBR, NZL, USA. Non-COMINT and/or non-TK ELINT reports are issued in the [redacted] or [redacted] series, depending on the sensitivity of the data used.

Note that [redacted] ELINT reports are not write-to-release (WTR) reports and are not subject to WTR rules concerning dates, comments, collateral and so on. All ELINT reports must follow the regular SIGINT style guidelines set out in this CSOI.

K.2.2 [redacted] reporting

For information about the reporting of [redacted] data, see Appendix G.

K.2.3 No references to COMINT reports

Avoid including references to COMINT reports in [redacted] and [redacted] ELINT reports. If it is necessary to include such references, you must add COMINT control markings.

K.2.4 Report content

If your report contains coordinates, follow the instructions in the main entry on geographic coordinates.

If your report contains references to ships, follow the instructions in the main entry on ships.

If your report contains [redacted] information, follow the instructions in Appendix I.

If your report contains abbreviations commonly used in ELINT reporting, they may not need to be expanded. See the list of approved abbreviations and acronyms.

K.2.5 General Metadata page

IRRELEVANT

K.2.6 TAGs

For reports containing [redacted], select [redacted] as one of the subject TAGs.

For reports containing [redacted] select [redacted] as one of the subject TAGs.

For all ELINT reports [redacted] that contain [redacted] data, include both [redacted] and [redacted] in the TAG line.

K.2.7 DDIs

There are special DDIs for reports containing ELINT. To determine which ones are appropriate for your report, see the ELINT DDIs working aid.

> **Note:** The special ELINT DDIs are not included in the DDI Guide in [redacted]
> You must select them from the All DDIs list in the Group box.

K.2.8 Entering [redacted] in [redacted]

IRRELEVANT

K.2.9 Report edit/release: Printing the Metadata sheet

IRRELEVANT

K.3 COMINT reports containing ELINT

K.3.1 Classification

Reports containing both ELINT and COMINT **must** bear COMINT control markings.

K.3.2 Report content

If your report contains coordinates, follow the instructions in the main entry on geographic coordinates.

If your report contains references to ships, follow the instructions in the main entry on ships.

If your report contains [redacted] information, follow the instructions in Appendix I.

K.3.3 TAGs

For reports containing [redacted], select [redacted] as one of the subject TAGs.

For reports containing [redacted], select [redacted] as one of the subject TAGs.

For all ELINT reports [redacted] that contain [redacted] data, include both [redacted] and [redacted] in the TAG line.

K.3.4 DDIs

There are special DDIs for reports containing ELINT. To determine which ones are appropriate for your report, see the ELINT DDIs working aid.

Note:	The special ELINT DDIs are not included in the DDI Guide in [redacted] You must select them from the All DDIs list in the Group box.

K.3.5 Entering [redacted] in [redacted]

IRRELEVANT

K.3.6 Report edit/release: Printing the Metadata sheet

IRRELEVANT

Appendix L: SIGINT Report Release Authorities

L.1 Purpose

This appendix provides guidance on the approvals required to release SIGINT reports.

L.2 Requirement for sign-off

All SIGINT reports must be signed off by appropriate release authorities.

For most reports, a team leader or production manager may approve release.

However, if a report meets one or more of the criteria below, approval by one or more other release authorities is required.

- IRRELEVANT
- The report contains Mandate A data with a Canadian privacy angle (see section L.4).
- The report has other sensitive content (see section L.5).

L.3 IRRELEVANT

IRRELEVANT

L.4 Reports containing Mandate A data with a Canadian privacy angle

Reports of this type fall into one of four categories. The categories and the associated release authorities are described in the table below.

If the report is based on ...	It must be ...	Category
a CSEC-collected communication to or from a person or entity in Canada	recommended for release by a Director in [redacted] and signed off by [redacted]	OPS-1A
a Second Party-acquired communication to or from a person or entity in Canada, or to or from a Canadian outside Canada	recommended for release by a PM or PLM in [redacted] and signed off by [redacted]	OPS-1B

a communication or metadata containing information about a Canadian **and** the report includes information about a Canadian (even if the information is "minimized") **Note**: [redacted]	recommended for release by a PM or PLM in [redacted] and signed off by [redacted]	OPS-1C
a CSEC-collected communication to or from a Canadian outside Canada	recommended for release by a Director in [redacted] and signed off by DC SIGINT	OPS-1E

Note 1: In threat-to-life situations during silent hours, a manager may approve the release of a report; [redacted]s or DC SIGINT's signature must be obtained later (see section 6.4 of OPS-1-7).
Note 2: [redacted] is not a communication, so a report based on [redacted] collection does not require OPS-1A, OPS-1B or OPS-1E sign-off. However, if a report based on [redacted] collection contains information about a Canadian, it requires OPS-1C sign-off.
Note 3: Be sure to mark the traffic with the appropriate category on the Traffic page in [redacted] For further information, see section 5.3.7.

L.5 Reports with other sensitive content

If the report …	It must be reviewed, prior to release, by …
includes [redacted] metadata or content	a Level IV manager in [redacted] (during silent hours, contact COPCC)
contains [redacted]	the Deputy Commanding Officer, [redacted] or designate
is based on [redacted] from [redacted] **and** makes it obvious that the communication is [redacted]	a Level IV manager in [redacted]
is based on [redacted] from [redacted] but does **not** make it obvious that the communication is [redacted]	Director [redacted] or a Level IV manager designated by Director [redacted] [redacted]
[redacted]	
is to be released in whole or in part to [redacted] or [redacted]	the PM or a TL in [redacted] or [redacted], or Director [redacted]
is to be released in whole or in part [redacted]	a PM or PLM in [redacted]

IRRELEVANT

contains a contextual identification	see OPS-1-7, chapter 5
contains a threat-to-life identification	see OPS-1-7, chapter 6
is RESTRICTED and does not have a predefined distribution	[redacted] to determine the distribution

Appendix M: "Native Format" Reporting

M.1 Purpose

This appendix provides instructions for preparing SIGINT reports containing "native format" materials.

M.2 Definition of "native format" reporting

In some cases, intercepted information would be more useful in its original form or would be difficult to convey in the standard SIGINT reporting format. Examples include maps, charts, diagrams, [redacted] Including such materials with minimal changes in a SIGINT report is referred to as native format reporting.

M.3 Criteria for native format reporting

Native format reporting is an option in the following situations:

- the information would be more useful to clients in its original form (e.g., maps, diagrams);
- the information cannot be easily conveyed in narrative form;
- the information is lengthy or highly complex and can be presented in its original form;
- transposing the material into the standard SIGINT reporting format would be time-consuming and would add little value.

M.4 Second Party intercept and native format reporting

Before using traffic from Second Party collection in a native format report, you must obtain approval from the Second Party concerned. Contact Operational Policy (D2).

M.5 How to prepare a native format report

The steps for preparing a native format report are described in the table below.

Step	Action
1	Make sure the intercept meets a valid intelligence requirement.
2	Make sure that the intercept meets at least one of the criteria for native format reporting.
3	Consult with Operational Policy if the traffic is from a Second Party source.
4	Remove all metadata from the intercept.
5	Remove any references to the communication mode (e.g., fax) in the main body of the intercept.
6	Minimize all Canadian and Second Party identities in accordance with OPS-1-7.
7	Add the appropriate overall classification (e.g., TOP SECRET//COMINT): • For images, embed the classification in the file wherever possible. • For text documents, insert the classification in the header, if possible. Do not add portion markings to the text.
8	Where necessary: • remove irrelevant information or features; • make whatever changes are needed to make text readable; • provide English or French equivalents for foreign terms.
9	Wherever possible, make the native format material an attachment to the report (instead of pasting it into the report).
10	Proceed with the rest of the standard report preparation process.

CSOI-4-1 Promulgation

I hereby approve CSOI-4-1, instructions for SIGINT Reporting. These instructions are effective immediately.

Michael Devaney
CSE Deputy Chief SIGINT

30 Oct 06
Date

Reviewed and Recommended for Approval

Peter Cork
Director General SIGINT Programs

11 OCT 06
Date

Shelly Bruce
Director General Intelligence

11 Oct 06
Date