Date Updated: 23-Dec-14

S121 SIGINT Reporting Basics

Delivered by: [redacted]

Table of Contents

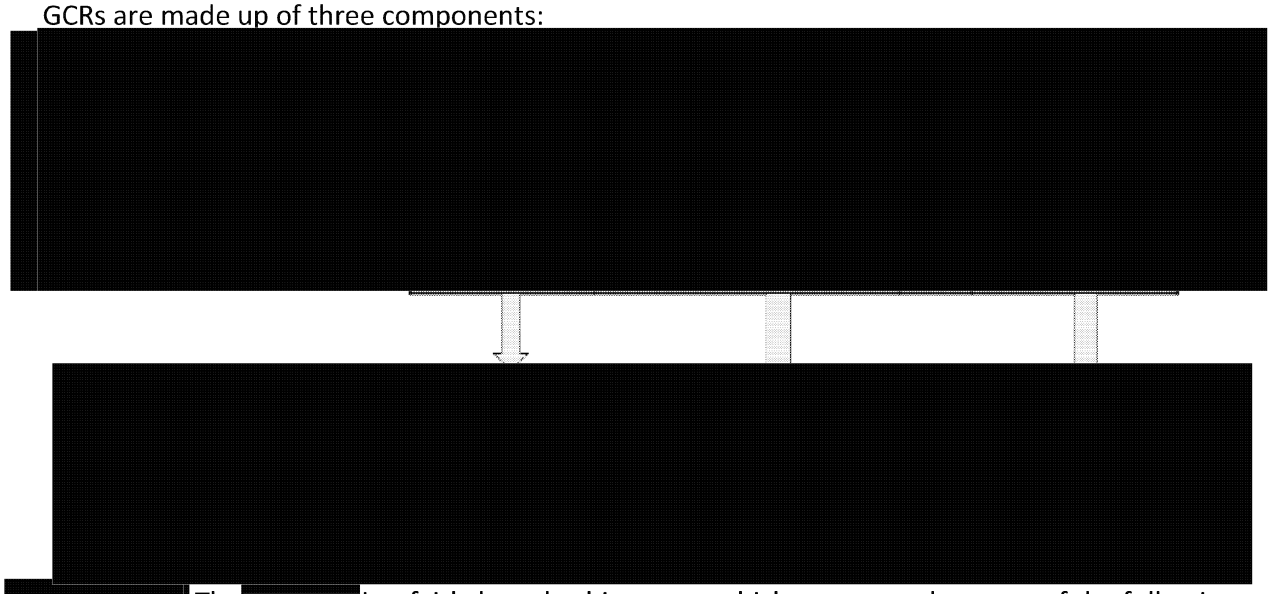
Module 1: Requirements

Government of Canada Requirements (GCRs)

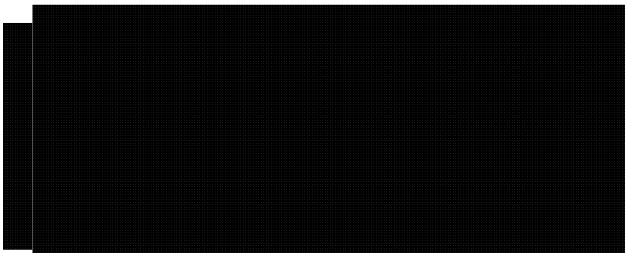
Government of Canada Requirements (GCRs) reflect the Government of Canada's ongoing intelligence requirements. GCRs are generated by the SIGINT Programs Operational Requirements group (SPOR), based on feedback from clients stating their areas of interest. A general statement of a requirement is used as the basis for a GCR. For example, there is a GCR for [redacted]

Components of a GCR

GCRs are made up of three components:



[redacted] The [redacted] is a fairly broad subject area which corresponds to one of the following requirements:



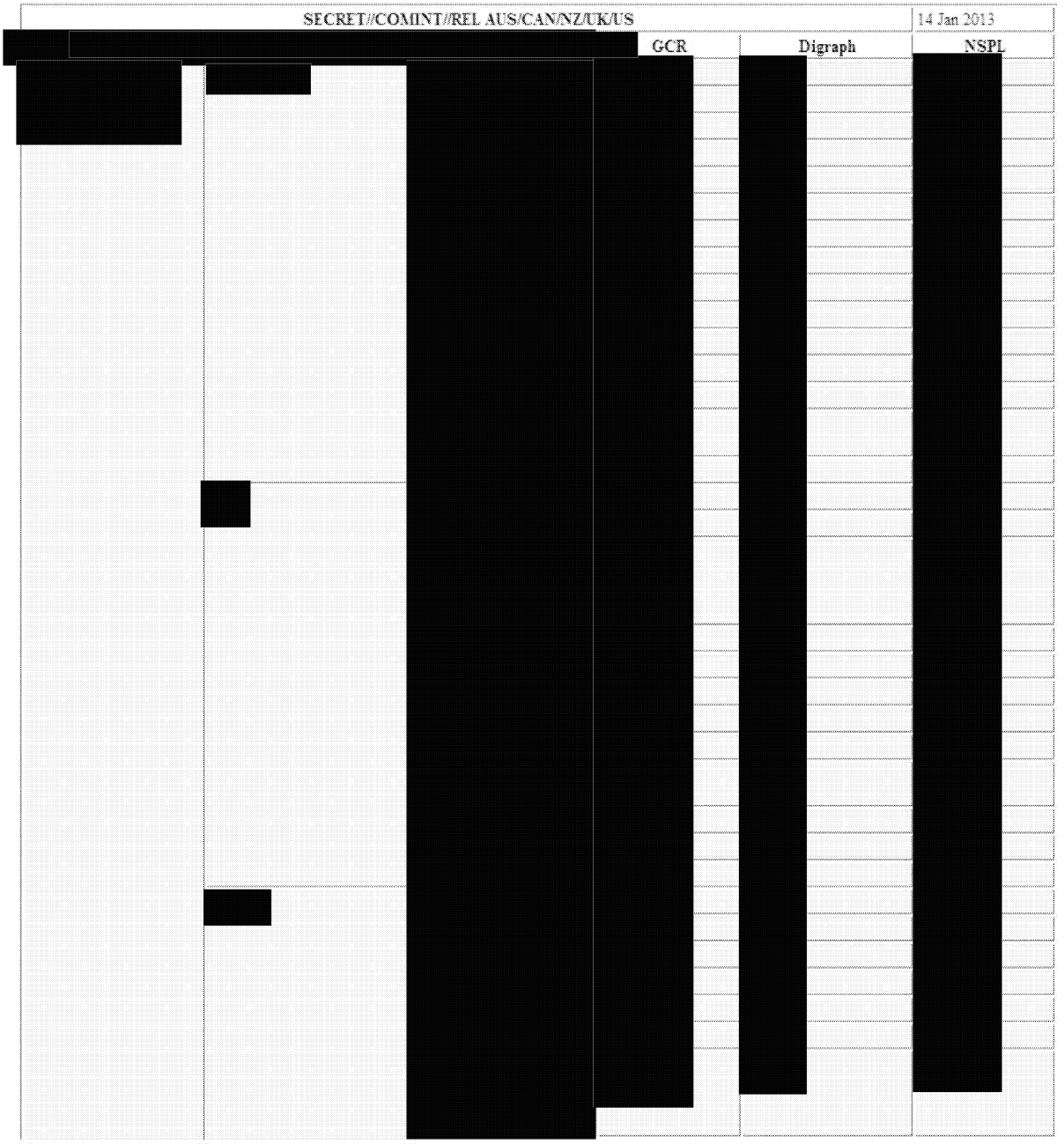
In the example above, [redacted] relates to [redacted] on the list of [redacted] requirements.

[redacted] The [redacted] further defines the category. In the example above, [redacted] relates to [redacted]

[redacted] The [redacted] is a [redacted] that indicates a [redacted] In the example above, [redacted] relates to [redacted]

Type “go gcr” into your [redacted] browser or use the following link:

[redacted]



National SIGINT Priorities List (NSPL)

The National SIGINT Priorities List (NSPL) is a tiered list which officially defines issues of national interest from a SIGINT perspective and the level of interest and effort afforded to each one. The priorities are ranked 0 to 4, [redacted] The list is divided into:

- **Standing Issues**
- **Watching Briefs**

Standing Issues

Standing Issues reflect items of long-term interest or concern to the Government of Canada (GC). [redacted]

[redacted] are not listed as priorities – rather, [redacted] are highlighted. As a result, no [redacted] but issues related to [redacted] can place it in several tiers (e.g., [redacted] would appear in tier 1, whereas [redacted] would appear in tier 3).

Watching Briefs

Watching Briefs represent items of short- to medium-term interest to GC [redacted]

[redacted] on the Watching Briefs are also ranked in alignment with the tiers and will rise and fall in priority as the situation dictates. They are normally [redacted]

Type “go NSPL” into your [redacted] browser or use the following links:

[redacted]

CSE (e) Version 2014.2.1 20 June 2014 TOP SECRET//SI//CEO//CSE EYES ONLY

WATCHING BRIEFS and NATIONAL SIGINT PRIORITIES LIST

CSE				CAF		
Watching Briefs	Standing Issue	Focus Area	Tier	Standing Issue	Focus Area	Watching Briefs
[redacted]			0			
[redacted]	[redacted]	[redacted]	1	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	2	[redacted]	[redacted]	[redacted]

Client Requests/RFIs

A Client Request is an individual client's specific information need that falls under a more general GCR. In [redacted] this item can contain an "RFI (Request for Information)". Clients can use this field to provide specific details about the request, such as [redacted]

Information submitted to CSE that is specified in the "Request for Information (RFI)" field must reflect the fact that CSE does not target Canadian, US, UK, New Zealand, or Australian persons and entities. The following is an example of a Client Request:

[redacted]

Feedback

Feedback is a client's reaction to or comment about a SIGINT End-Product Report (EPR) and may serve as an informal evaluation of the information as well as a method for identifying new or adjusting existing client requirements.

The feedback component in [redacted] contains three rating categories:

Rating	Details
Exceptional	[redacted]
Satisfied Need	
Improvements Needed	

Actionable Intelligence

Actionable intelligence is identified in the feedback portion of [redacted] when action is taken as a direct result of SIGINT reporting. This feedback is normally entered by Client Relations Officers (CROs) on behalf of clients, by clients themselves, or by anyone who receives feedback from clients, e.g., Team Leaders.

There are three possible definitions of action broken down into Canadian (including GC and CF) and Allied actions:

Action	Details
[redacted]	
[redacted]	
[redacted]	

The following are examples of feedback:

Exceptional

[redacted]

Actors

Name	Organization	Position	Type
[redacted]	Royal Canadian Mounted Police	SIHU	Creator

Satisfied Need

[redacted]

Actors

Name	Organization	Position	Type
[redacted]	Canadian Security Intelligence Service	SME	Creator

Improvements Needed

[redacted]

Actors

Name	Organization	Position	Type
[redacted]	Intelligence Assessment Secretariat	Analyst	Creator

GCRs EXERCISE

CSE Authorities

National Defence Act

According to the *National Defence Act s. 273.64*, the CSE mandate has three parts:

Part A:
To acquire and use information from the global information infrastructure for the purpose of providing Foreign Intelligence (FI)[1], in accordance with Government of Canada intelligence priorities

Part B:
To provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada

Part C:
To provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties

Questions to ask yourself as an analyst:	
1. Is my activity directed at a foreign person or entity? 2. Is the foreign person or entity located outside of Canada?	➢ If you answer **YES** to all questions, you can operate under **Part A**. Proceed in accordance with Operational Policy.
3. Does the expected information or intelligence relate to the capabilities, intentions or activities of the foreign person or entity? 4. Does the expected information or intelligence relate to an intelligence priority of the Government of Canada?	➢ If you answer **NO** to any question, this activity cannot be conducted under Part A. IRRELEVANT IRRELEVANT

Note: Analysts in the Intelligence Branch operate mostly under Part A or C.

[1] FI is information or intelligence about the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group as they relate to international affairs, defence or security (*National Defence Act*, section 273.61).

CSIS Act

IRRELEVANT

SIGINT Privacy Annotations and Accountability Markings

OPS-1

The OPS-1 policy document requires analysts to apply SIGINT privacy annotations to traffic containing privacy information for retention or deletion (traffic pertaining to **Part A of the mandate only**;IRRELEV
IRRELEVANT

SIGINT privacy annotations are markings applied to SIGINT traffic containing ***recognized***:

- private communications[2]
- communications of a Canadian located outside of Canada
- information about Canadians that does not contain FI
- solicitor-client communications

It is the responsibility of analysts whose functions are directly related to the production of SIGINT reports to annotate appropriately SIGINT traffic that is ***recognized*** as falling into one the categories described above. SIGINT privacy annotations must be applied to **all** traffic containing privacy information **except** when the traffic comes from one of the following sources:

- [redacted]: annotate only "information about Canadians with no FI" (IACN); mark AM (Accountability Marking) for one-end Canadian e-mails containing FI
  [redacted] receive the full range of privacy annotations.)
- [redacted]: annotate only IACN)
- IRRELEVANT no annotations allowed

SIGINT privacy annotations are to be applied **only to traffic in** [redacted] from CSE [redacted] collection sources. See OPS-3-1 *Procedures for* [redacted] *Activities* for details related to [redacted] traffic and SIGINT privacy annotations.

The following tables show the privacy annotations you are required to make in [redacted] when you recognize communications containing privacy information. Table 1 shows the annotations to be used for traffic containing privacy information other than solicitor-client communications. Table 2 provides the annotations to be used for traffic containing solicitor-client communications.

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

Table 1. Privacy annotations for non-solicitor-client communications

Location	If one communicant is physically located in Canada[1]		If one communicant is a Canadian[2] physically located outside Canada		Both communicants are foreigners located outside Canada, but the communication contains information about a Canadian [2,3]		Recognized one-end Canadian e-mails [redacted]
Source	[redacted]						
Essentiality	Contains FI essential to international affairs, defence or security of Canada	Not essential// annotate for deletion	Contains FI essential to international affairs, defence or security of Canada	Not essential// annotate for deletion	Contains FI essential to international affairs, defence or security of Canada	Not essential// annotate for deletion	Contains FI essential to international affairs, defence or security of Canada
Annotation	INCA	INCAN	OUCA	OUCAN	(None required)	IACN	AM

Table 2. Privacy annotations for solicitor-client communications*

Location	If one communicant is physically located in Canada[1]		If one communicant is a Canadian[2] physically located outside Canada	
Source	[redacted]			
Essentiality	Contains FI essential to international affairs, defence or security of Canada	Not essential// annotate for deletion	Contains FI essential to international affairs, defence or security of Canada	Not essential// annotate for deletion
Annotation	INCAS	INCASN	OUCAS	OUCASN

* See the **special handling procedures** in the notes on Solicitor-Client Communications in OPS-1.

[1] This is a private communication, with geography being the determining factor (i.e., one of the communicants must be located in Canada. See paragraph 8.18 for the definition. Should an analyst recognize traffic where both the originator and the recipient are Canadians, or are both in Canada, or where one communicant is in Canada and the other is a Canadian located outside Canada, the traffic must be annotated for deletion. All associated selectors must be reviewed and SPOC and [redacted] must be notified; see paragraph 2.8.

[2] See paragraph 8.2 for the definition of a Canadian.

[3] There is no requirement to maintain statistics on these communications; however, for privacy reasons, those communications that do not contain FI essential to international affairs, defence or the security of Canada are to be annotated for deletion

[4] Although this marking is not required under any MA, for accountability purposes, [redacted] one-end Canadian e-mail [redacted] must be marked

[5] See paragraphs 3.5 and 3.8 for definition and handling instructions related to solicitor-client communications

Storing privacy information

The *Procedures for the Storage of Privacy Information*[3] document provides instructions on how to handle and store privacy information that is retained. All privacy information (reports, intercept and documentation) must be filed using special **Temporary Document Holders** (specially marked file folders marked Mandate A or Mandate C that you can obtain from your Team Leader).

The following information must be recorded on the outside cover of the Temporary Document Holder:

- Security classification
- Serial number
- Date of report

The following documentation is required and must be included in each folder:

- copy of the raw traffic (for [redacted] intercept)
- in the case of [redacted] traffic, the gist/translation
- copies of any translations produced
- draft/edit copies of the report, including metadata
- Product Release Form sign-off approval sheet IRRELEVANT IRRELEVANT

End-Product Reports (EPRs) containing privacy information pending editorial review or release authority must be protected in the Temporary Document Holder when you leave your workstation for extended periods of time (e.g., lunch or meetings). During regular business hours, place the privacy information in the Temporary Document Holder and store it "out of sight" in either your locked workstation drawer or locked flipper cabinet. At the end of each business day all "in-progress work" must be placed within the Temporary Document Holder, which must be secured within the team's security cabinet.

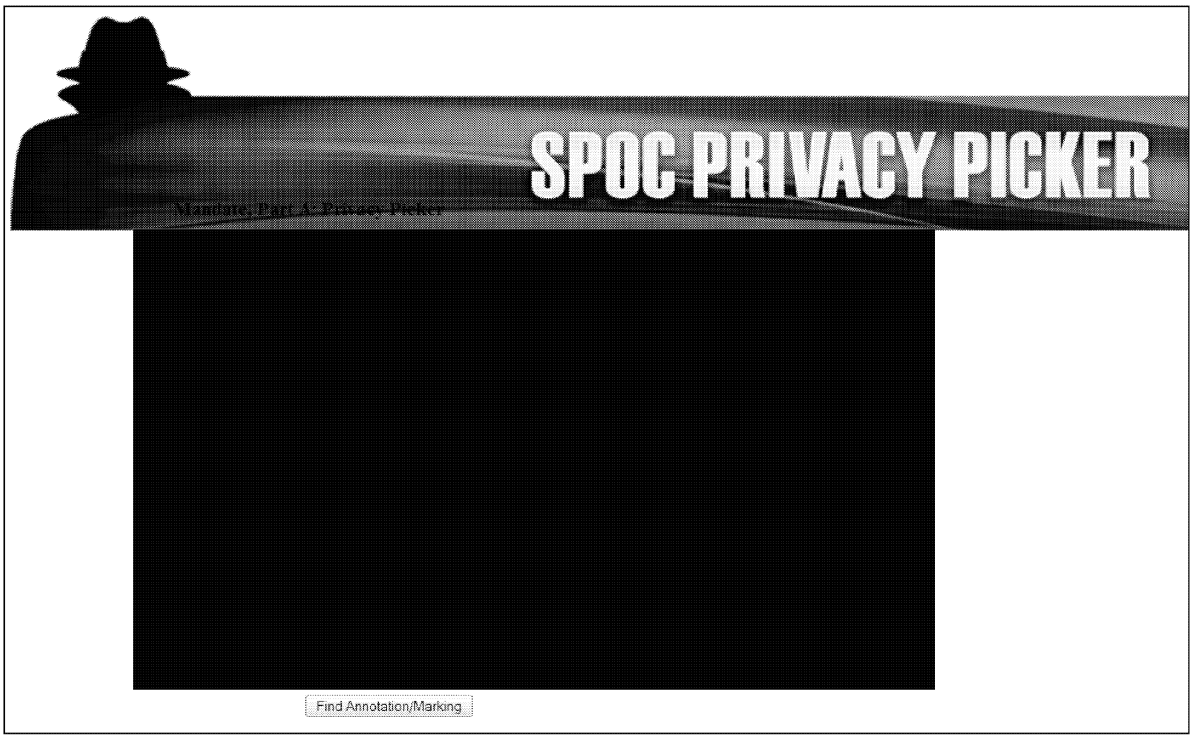
Any traffic retained for background purposes only and has not been reported (no serial number or report date) must also be stored in the team's security cabinet in the appropriate Temporary Document Holder (for Mandate A or Mandate C).

All documentation containing privacy information that is **not** to be retained must be destroyed using a shredder approved by Corporate Security for the secure destruction of TOP SECRET information. Do **not** discard documents containing privacy information in burn bags.

All e-mail copies of Advance Reports (see Appendix H of CSOI-4-1 *SIGINT Reporting*) containing privacy information must be destroyed the first working day of each month for any EPRs that were produced (**not to exceed 34 days**).

[redacted]

SPOC Privacy Picker



[redacted]

Module 2: Collection

Mandate

Part A of CSE's legislated mandate, under paragraph 273.64 (1) (a) of the *National Defence Act,* provides the authority to acquire and use information for the purpose of providing foreign intelligence in accordance with Government of Canada (GC) intelligence priorities, provided that **CSE's activities shall not be directed at Canadians or any person in Canada** and shall be subject to measures to protect the privacy of Canadians in the use and retention of intercepted information.

All selectors and methods used in collection and acquisition activities under Part A of the Mandate shall be **directed at foreign entities located outside Canada** and shall be consistent with GC intelligence priorities.

In the event that the selector (e.g., phone number or e-mail address) of a Canadian or a person in Canada is inadvertently targeted, the following actions must be taken as soon as possible:

Step	Action
1	The selector must be de-targeted.
2	Any existing traffic resulting from that selector must be destroyed (i.e., marked for deletion).
3	Any End-Product Reports based on the traffic must be cancelled.
4	CSE's SIGINT Programs Oversight and Compliance (SPOC) and Operational Policy [redacted] must be notified and apprised of the actions taken.

Types of Collection

[redacted] ***Collection*** involves [redacted] is largely handled by [redacted] group.

[redacted] ***Collection*** involves [redacted] is largely handled by [redacted]

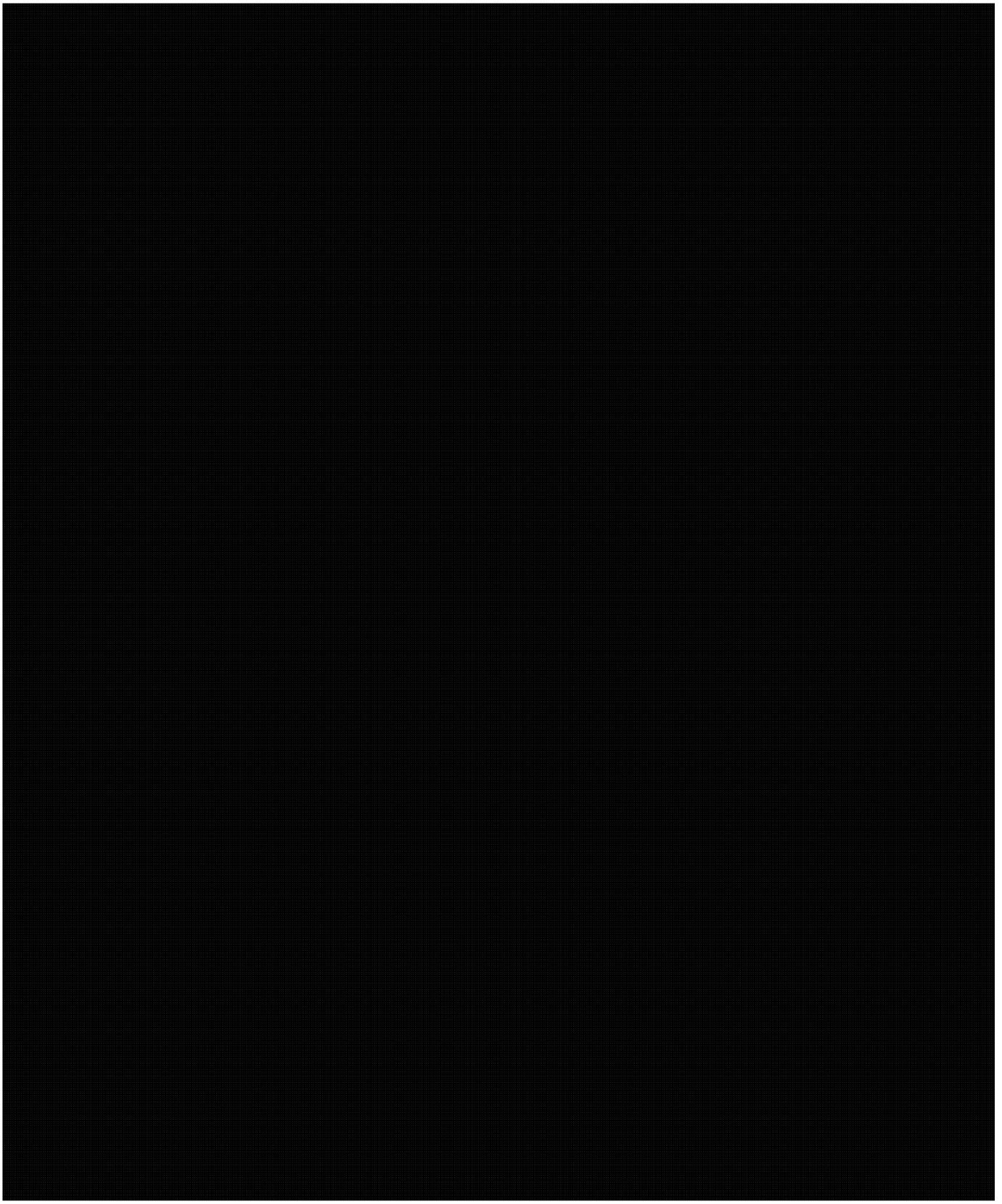
Collection Programs

[redacted] **Collection Programs** – The main [redacted] collection programs are as follows:

[redacted]

[redacted] (CSE's [redacted] is located at CFS Leitrim).

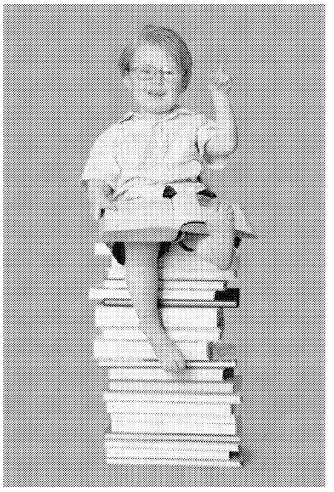
[redacted]



[redacted] **Collection Program** – [redacted] performs [redacted]

IRRELEVANT

Legal and Policy Privacy Concerns



Canadian Guidelines

- OPS-1 (Ensuring Privacy of Canadians)
- OPS 3-1 [redacted]

IRRELEVANT

- One-end Canadian communications

[redacted] *helps to ensure the legality of tasking/targeting. SPOC helps to ensure compliance with policy.*

2nd Party Guidelines

- US – United States SIGINT Intelligence Directive (USSID-18)
- UK – Human Rights Act (HRA)
- Australia – Intelligence Services Act (ISA)

TERMINOLOGY EXERCISE

Module 3: Research and Analysis

IRRELEVANT

Report Research

Analysts must keep up-to-date with several events on a daily basis. Analysts will scan a variety of sources to augment their reporting, including:

- End-Product Reports (EPRs) via [redacted]
- Open source resources, and
- Traffic databases.

End-Product Reports

Analysts should scan EPRs in [redacted] to:

- [redacted]

Open source resources

IRRELEVANT

Traffic databases

Analysts scan **traffic** for foreign intelligence (FI) information that will be written into a SIGINT report. FI is information or intelligence about the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group as they relate to international affairs, defence or security (*National Defence Act*, section 273.61). Foreign intelligence is NEW information, which can be used by the client for background information, decision-making or further analysis.

Most traffic is stored in the [redacted] and accessed using the [redacted] through the [redacted] component in [redacted] which allows analysts to [redacted] the content of a [redacted] traffic item. [redacted] can be made and stored in [redacted] is accessed through [redacted] Analysts scan the [redacted] daily for [redacted] fax traffic for any potentially reportable information. Presently, all fax traffic goes through [redacted] that uses [redacted] technology.

Determining reportability

The first step in writing a report is finding reportable traffic, i.e., FI. Within the Canadian context, its purposes are to protect Canada's interests, to facilitate the policy process, and to provide advantage in the pursuit of overall government policy objectives. In general, foreign intelligence deals with events outside Canada, [redacted]

Consider the following questions to determine if the traffic is reportable:
Is there a requirement (GCR) for the report?
Is the information intelligence or open source?
Is it foreign intercept?
Is there enough intelligence to warrant a report?
Are the ideas in the traffic clear enough to make a cohesive report?
Is there a need for [redacted]?

IRRELEVANT

IRRELEVANT

Guidelines for analysis

IRRELEVANT

Biases & Assumptions

IRRELEVANT

IRRELEVANT

Research

IRRELEVANT

Research tools

Some of the frequently used analyst **research tools** include:

[redacted] is CSE's end-product database management system, where all end-products that CSE produces or receives from Second Parties are stored. Analysts are given access to reports based on [redacted] the need-to-know principle. [redacted] is a tool to:

- query items of interest that have previously appeared in SIGINT reporting,
- check facts such as spellings, place names, and titles,
- review one's own reporting,
- keep abreast of partners' reporting, and
- identify any gaps in collection or reporting by using partners' reporting as a reference.

[redacted] is CSE's target knowledge database for storing and managing target information. [redacted] is a tool to:

- manage target information,
- target and detarget selectors, and
- conduct traffic analysis.

CTSN (Canadian Top Secret Network) is CSE's secure online link with its Government of Canada (GC) partners in the security and intelligence community. CTSN is a tool to:

- access the extranet site of each department,
- view valuable open source and classified information, and
- search for [redacted] in each of the six member departments and other related GC departments (RCMP, the Department of Justice, the Solicitor General's office, and CRA).

[redacted] is a [redacted] is integrated with [redacted] and will gradually be integrated with [redacted] applications. [redacted] is a tool to:

[redacted]

[redacted] is an online wiki resource with references that [redacted] by all members of CSE. [redacted] provides analysts with the ability to manage their knowledge. Analysts have access to data from [redacted] using [redacted] tool to [redacted] and share their work with others. [redacted] is a tool to:

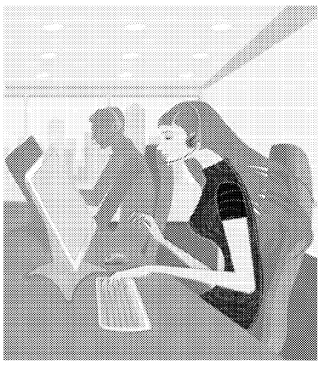
[redacted] fax, [redacted]

- link to the CSE Intranet, [redacted] and [redacted]

ADDITIONAL RESEARCH TOOLS

- CSE Intranet
  - CSE Library Services
  - SIGINT Reporting Working Aids
  - [redacted]
  - [redacted]
- [redacted]
- In-house reference material
- Open source intelligence [redacted]
- [redacted] for open-source target-related research
- Periodicals
- Internet (via a [redacted] network system such as [redacted] or [redacted] for target-related research)
- Area specialists within your division or in other divisions

RESEARCH EXERCISE



Module 4: SIGINT Reports

Types of SIGINT reports

Signals Intelligence (SIGINT) involves the interception and analysis of (foreign) communications and non-communications signals. The term SIGINT comprises:

End-Product Reports (EPRs)

These are also called **COMINT** (Communications Intelligence) reports are issued in response to a GCR. COMINT is derived from foreign communications by other than the intended recipients passed by electromagnetic means. The intelligence is focused on several different sources, primarily foreign [redacted] EPRs conform to established reporting standards (CSOI-4-1).

[redacted] SIGINT Reports

These are usually issued solely to [redacted] of SIGINT. Some examples of [redacted] SIGINT Reports are Cryptologic/Communications Information Reports (**CIR**) and [redacted]

CIR reports contain cryptologic, communications [redacted] They are distributed solely between Second Party agencies [redacted] that assist in SIGINT and Information Technology Security (ITS) activities. They are always at least TS//SI and "CIR" appear in the report serial number; (e.g.: [redacted] Two reports may be issued If your traffic meets both CIR reporting requirements and regular reporting criteria. CIRs use special Delivery Distribution Indicators (DDIs). For details, search on *DDI* in the [redacted] or see Module 9.

Reports containing any of the following information should be issued as a CIR (**Note**: [redacted]

Topic	Requirements
[redacted]	[redacted]
[redacted]	Details concerning [redacted] in the following areas: [redacted]

	• [redacted]
[redacted]	Details on the following subjects: • [redacted]
[redacted]	The following details for [redacted] • [redacted]

The information described above should be reported according to the priorities as follows:

Priority 1 [redacted]

Priority 2

Priority 3

Priority 4

ELINT Reports

These are based on [redacted] intelligence derived from the intercept of foreign non-communications signals. ELINT reports also conform to CSOI-4-1 standards, but have unique characteristics of classification and metadata.

Foreign Instrumentation Signals Intelligence (FISINT)

These contain technical and intelligence information derived from the interception of foreign instrumentation signals (FIS) such as those associated with telemetry, beaconry, electronic interrogators, arming, fusing and firing systems and computer command signals.

Gists

These are indications and warning (**I&W**) reports being produced for immediate and specific distribution (generally to military persons).

Special purpose reports

These are items of operational correspondence that bridge a gap between e-mail correspondence and formal SIGINT end product. Style, presentation, labeling (serialization) and classification may vary. Examples include: SIGINT Summaries, SIGINT Assessments, and Information Items.

Canadian sensitivities

SIGINT reports are divided into two main types, based on distribution:

Canadian Eyes Only (CEO) reports contain intelligence that is of a sensitive nature either to Canada or to a Second Party country; therefore, such reports are limited to a Canadian readership and must not be released to Second Parties.

SIGINT Community (COM) reports are reports that CSE shares with one or more Second Party SIGINT agencies.

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 Team Leader or Production Manager.

If the information could ...	Then issue it...	Examples
[redacted]	RESTRICTED	[redacted]
	RESTRICTED	
	CEO	
	CEO	
	CEO	

[redacted]		
	CEO	[redacted]
	CEO	
	CEO	
	CEO	

Report classification

IRRELEVANT

Caveats

IRRELEVANT

Serial numbers

IRRELEVANT

Serial Number Tables

Classification	Details	Serial #
CONFIDENTIAL//SI	not used at CSE	[redacted]
SECRET	ELINT reporting	
SECRET//SI (SPOKE)		
TOP SECRET	ELINT reporting	
TOP SECRET//SI (UMBRA)		
TOP SECRET//SI (UMBRA)	**Gist report**	

Control/Dissemination	Details	Serial #
GAMMA	- always TOP SECRET//SI	[redacted]
Canadian Eyes Only (CEO)	- sensitive to Canadian interests - not to be shared with other nations	
R-Series (Restricted)	- always CEO - always TOP SECRET//SI (or GAMMA) - named distribution list	
IRRELEVANT		

Complete information on SIGINT classifications and serial numbers can be found in CSSS-103 SIGINT Classification Standards.

SERIAL NUMBER EXERCISE

Organizational Strategies

IRRELEVANT

IRRELEVANT

Inverted pyramid

IRRELEVANT

EXAMPLE – Inverted Pyramid

IRRELEVANT

Lead Plus Equal Facts

IRRELEVANT

EXAMPLE – Lead Plus Equal Facts

IRRELEVANT

Chronological Account

IRRELEVANT

EXAMPLE – Chronological Account

IRRELEVANT

Module 5: SIGINT Report Layout

IRRELEVANT

Attribution

IRRELEVANT

Note: Refer to Chapter 4.2 of *CSOI-4-1 SIGINT Reporting* for more information about **Attribution**.

AVOID

[redacted]

Focusing on the domestic end – When drafting reports involving Canadian or Second Party persons or entities, focus on the activities, capabilities and intentions of the foreign target. For example, in a report based on an e-mail from a [redacted] the attribution could take the following form:

[redacted]

The Lead

IRRELEVANT

IRRELEVANT

Block Headings

IRRELEVANT

Key Points

Key points emphasize the bottom line.

IRRELEVANT

Structure

IRRELEVANT

Analysis

IRRELEVANT

Structure

IRRELEVANT

KEY POINTS & ANALYSIS EXERCISE

Titles

IRRELEVANT

IRRELEVANT

Title slugs

IRRELEVANT

Checking the title

IRRELEVANT

TITLES EXERCISE

Module 6: SIGINT Style

Twelve easy steps for revising

IRRELEVANT

Abbreviations and acronyms

IRRELEVANT

Style guidelines

IRRELEVANT

Analytic comments

IRRELEVANT

FORMAT – IRRELEVANT

IRRELEVANT

Collateral

IRRELEVANT

SOURCES - IRRELEVANT

IRRELEVANT

FORMAT – IRRELEVANT

IRRELEVANT

METADATA – IRRELEVANT

IRRELEVANT

Footnotes

IRRELEVANT

FORMAT – IRRELEVANT

IRRELEVANT

Point of contact (POC)

IRRELEVANT

FORMAT – IRRELEVANT

IRRELEVANT

SIGINT STYLE EXERCISE

Module 7: Naming Policy

Overview

To comply with national legislation, CSE and its four SIGINT collaborators have policies governing the inclusion of names and other identifying information in SIGINT reports. Although the specific restrictions vary from agency to agency, the rule of thumb is that private individuals (citizens and permanent residents), firms and organizations cannot be named or otherwise identified in SIGINT product; only a generic reference (e.g. "a Canadian citizen", "a US bank", "a UK organization") can be used.

Note: Refer to **OPS-1-7 *SIGINT Naming Procedures*** and Chapter 4.4.1*, Rules on reporting identities* in *CSOI-4-1 SIGINT Reporting*, for more information about CSE's naming policy.

Basic policy

Any information that might tend to identify a Canadian or Second Party person (citizen or permanent resident), corporation or organization must be suppressed from end-product reports. Such identifiers include:

- names
- nicknames
- [redacted]
- e-mail addresses
- [redacted]
- telephone numbers
- IP addresses
- [redacted]
- passport numbers
- [redacted]

If reference to the Canadian or Second Party identity is necessary for the sake of the intelligence story, the identifying information must be replaced with a generic term, such as the following:

- a Canadian person
- a US organization
- an Australian company

Further examples are provided in the Naming Procedures Guide.

Validity wording

Where there is doubt whether an individual, organization or corporation mentioned in traffic is foreign or non-foreign ("non-foreign" means Australian, Canadian, New Zealand, UK or US), it is best to err on the side of caution and use the generic term with the appropriate validity word, such as:

- a possible UK resident
- a probable US firm

When foreign intelligence traffic refers to an unspecified Canadian or Second Party person, organization or corporation, the report text should use wording such as "an unnamed US official" or "an unspecified Canadian company", rather than merely "a US official" or "a Canadian company". This will ensure that readers do not submit requests for identity information that CSE/CFIOG does not have.

Validity wordings range over a continuum from “impossible” to “certain” and may be modified by other terms such as “highly” or “somewhat”. Here is an ordered list of suggested validity wordings:

Canadian naming exemptions

A Canadian entity may be named in the following circumstances:

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- IRRELEVANT
- [redacted]

* approval required; see **OPS-1-7, Section 3 “Exceptions”**.

[redacted]

Contextual identification

The *National Defence Act* and Ministerial Directive require that CSE has measures in place to protect the privacy of Canadian entities in SIGINT reports. Since there are times when a Canadian entity can be identified by means of a situation referred to in a report (a 'context'), that contextual identification must be approved by senior management. Refer to **OPS-1-7 *SIGINT Naming Procedures.***

The information in this working aid is intended to supplement and clarify the direction found in **OPS-1-7 *SIGINT Naming Procedures***. SIGINT staff should contact [redacted] with any questions about naming or using contextual identification in reporting.

You don't need a name to identify a Canadian in a SIGINT report. If your report provides enough contextual information that a reasonably well-read person (someone who routinely reads a major newspaper, watches TV news or visits news websites) can guess or research the identity of the person, company or organization whose name you are referring to, it's called a 'contextual identification.'

A contextual identification cannot use a generic suppression phrase (e.g. "named Canadian person") – these are used for suppressed specific identities only. If the entity is identified in the traffic used for the report, follow normal procedures for the use of the generic suppression phrase. If the entity is only identified contextually in a report, you should not use the generic phrase "named".

How is a suppressed identity different from a contextual identification?

A Canadian (or Second Party) identity is suppressed by using a generic phrase like "named Canadian (CA-1)" when it is necessary to include the specific identity in a SIGINT report.
A suppressed identity becomes a contextual identification when an informed reader can deduce the identity of the individual based on information given.

Examples:

- [redacted] related reporting
- [redacted]

How do I know whether there is a contextual identification?

Often, contextual identification is not as clear-cut as in the examples above. You must ask yourself whether an alert reader, by looking at all the information in the report, could narrow the range of entities associated with the contextual information to just one.

Consider whether the alias [redacted] is a contextual identification. At first glance this is okay, since there are thousands of Canadians who could be regarded as [redacted] Later in the report, references to [redacted]

Still okay, as there are probably a [redacted] Still later in the report, we learn tha[redacted]

[redacted] The alias identity is now *not okay*, since it is *unlikely* that there were [redacted] If it is likely that there had been only [redacted] it would be possible for a reader of the report to use that information to recognize or find the identity of [redacted]

It is important to consider the converse as well. Would the reader require "specialized knowledge" (from foreign magazines and newspapers, technical publications or other non-SIGINT information) 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) by sending an e-mail to [redacted]

How can I decide whether or not to use a contextual identification in my draft report?

If you have an essential reference that contextually identifies a Canadian entity in your draft report, you have three options to consider:

Option 1: Make the alias and/or the accompanying information less specific so that there could be several possible entities that fit the information, and therefore contextual identification is no longer a possibility, or

Option 2: If the contextual identification is essential to the foreign intelligence story go through the contextual identification approval process described in this document, or

Option 3: If you have no doubt as to the identity of the Canadian entity referred to, use a normal suppression phrase (e.g., "a named Canadian company") and follow the regular procedures for using a suppressed identity.

If the same contextual identification occurs regularly (e.g., [redacted] or is expected to occur repeatedly over a certain period of time, ask your manager to apply for a blanket exemption (contact [redacted] for more information).

Contextual naming exemption request

Use the following items as a checklist when making a request to use a contextual identification in a report (all of this information must be submitted to [redacted]

1. Make sure that the contextual identification is the best option to use for the FI story.
2. Advise [redacted] that you are working on such a report (D2 needs to advise [redacted]
3. As soon as D2 is notified that a contextual identification request is likely:
   a. D2-staff determine the schedule of the [redacted] so that consideration of the request can be scheduled into the [redacted] work day at the earliest opportunity.
   b. D2 staff examines the request sent to [redacted] to ensure that the information is complete.

c. D2 sends a recommendation containing all the information obtained from the requester or reporting team to DGPC, copying the D2 Manager and the Director of Corporate and Operational Policy.
d. [redacted] examines the recommendation as schedule permits.
e. [redacted] notifies D2 staff of approval or denial.
f. D2-staff immediately pass the approval or denial to the requester.

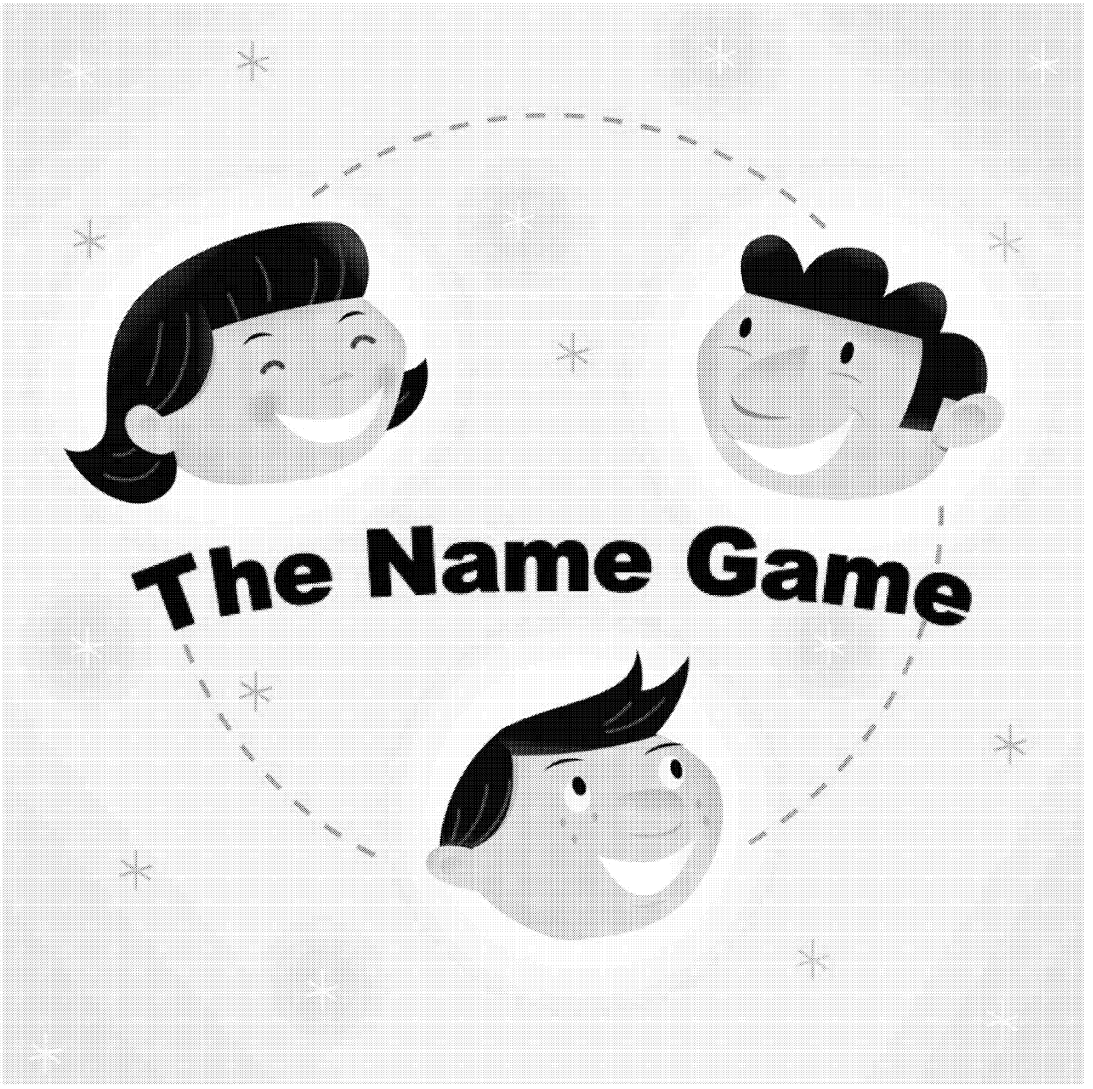
4. Include **ALL** of the following information in the request to [redacted]
   a. The full name of the entity that is contextually identified
   b. A brief explanation of why an informed reader would know who the entity is (e.g., entity is frequently named in recent media).
   c. A copy of the entire draft report, with the contextual identity highlighted. If the report is long, isolate separately the paragraph(s) that has the contextual identification phrase.
   d. The proposed distribution of the report.
   e. Details on whether or not the report has been signed off by [redacted]
   f. The requested deadline for the approval. Include reasoning if request is urgent.

5. If the contextual identification is ultimately approved and the report is released:
   a. Send the report serial number to [redacted]
   b. Enter the actual name of the entity and the contextual description used in the report into the [redacted] compartment.

What if the entity belongs to a Second Party?

IRRELEVANT

NAMING EXERCISE



Module 8: Write-to-Release

Overview

Write-to-Release (WTR) is an initiative to prepare COMINT reports at the lowest classification possible. WTR involves sanitizing, usually to the SECRET level, all key information that can be released outside COMINT channels. The primary aim is to conceal the fact that the information is derived from COMINT, thus protecting COMINT sources, methods and techniques and to permit wider dissemination. The result of this process is a report which contains COMINT and non-COMINT paragraphs.

Analysts should review the **OPS-5-3 Write-to-Release (WTR)** procedures document to familiarize themselves with the policies and procedures.

Prerequisites for WTR

IRRELEVANT

[redacted]

IRRELEVANT

Disguising the COMINT

IRRELEVANT

WTR Exemption List

IRRELEVANT

WTR EXERCISES

Module 9: Metadata

TAG line

IRRELEVANT

[redacted]

The [redacted] is a trigraph identifying the source of the intelligence. The first two letters represent the country [redacted] for example:

[redacted]

Some countries [redacted] are represented by digraphs that are different from ones that may seem natural. For example:

[redacted]

The third letter in the [redacted] trigraph identifies the functional association [redacted] providing the intelligence information.

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

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

[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

IRRELEVANT

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

Because some of the definitions given in the TAG manual are ambiguous or counter-intuitive, selecting the correct third letter can be tricky in some cases. Following are a few pointers:

The third letter…	is used for…
[redacted]	

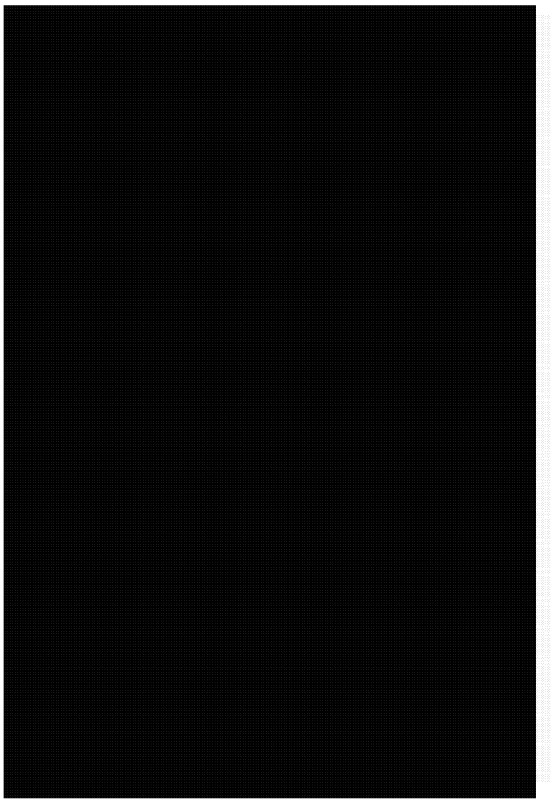
The intelligence source must not be confused with the communications source [redacted] Although the intelligence source and communications source are frequently the same, the intelligence source must be the one identified when there is a difference.

One way of checking for the proper [redacted] is to compare it with the attribution: the two should match. For example:

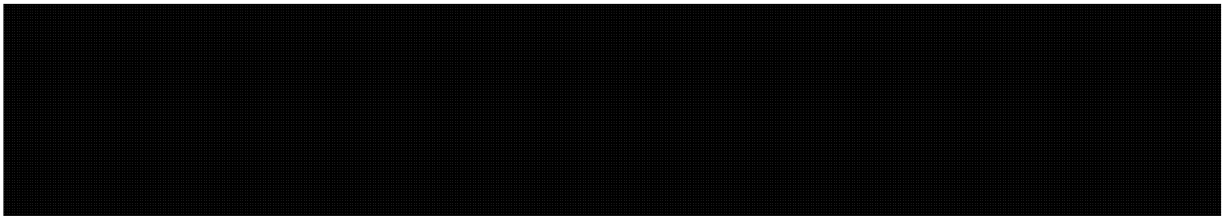
[redacted]

Subject/Topic component

The subject/topic component, consisting of one or more tetragraphs, is the second element of a TAG entry. The first letter of a subject/topic tetragraph indicates the general subject:



The last three letters identify the specific topic. Example:

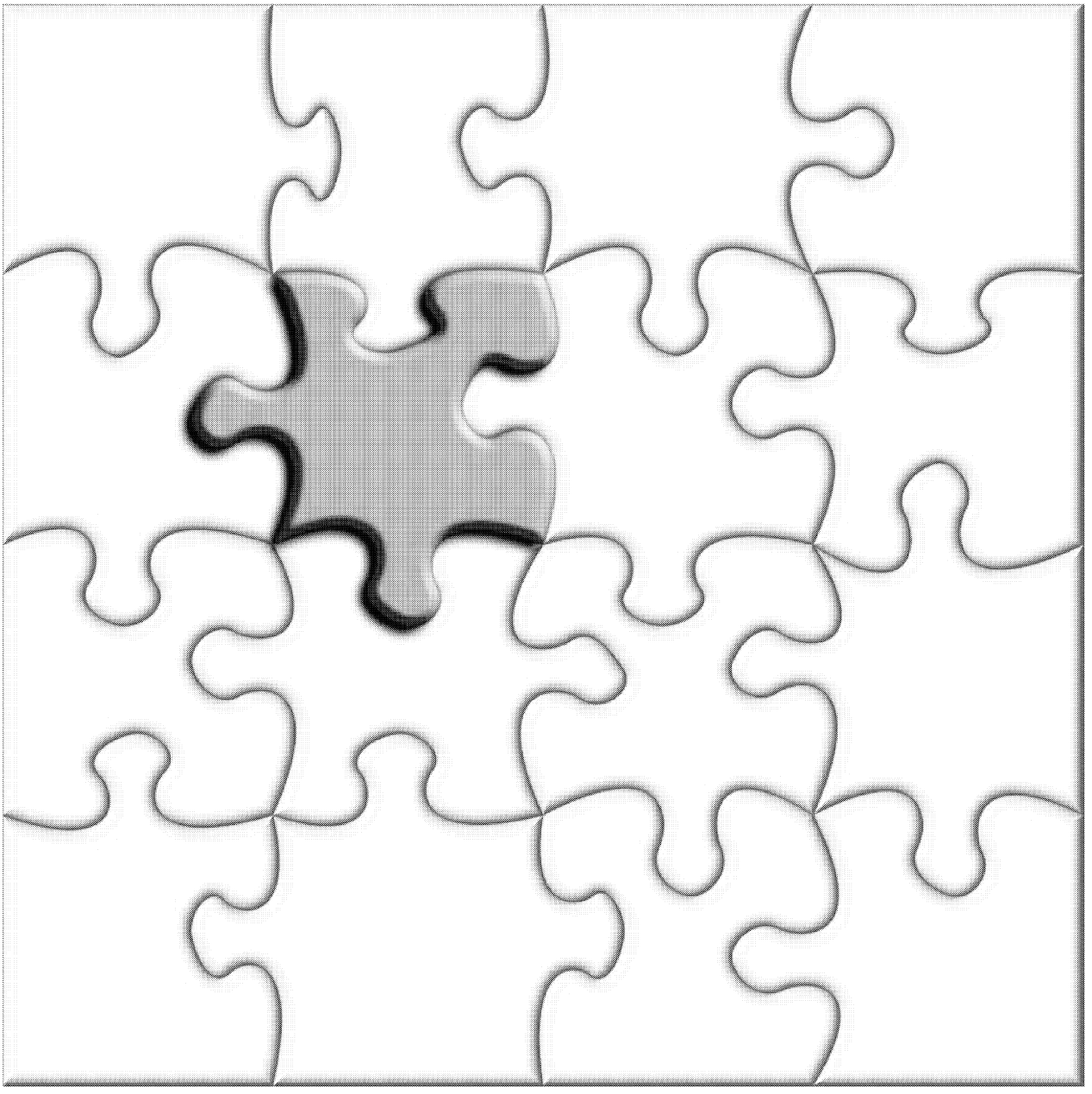


Principal component

This component consists of one or more digraphs representing the [redacted] involved in the report.

All approved digraphs and their permitted uses in reporting are listed in the *TAGs Working Aid* which can be found under "Metadata" on the SIGINT Reporting Working Aids page of the DGI web.

TAGs EXERCISE



Delivery Distribution Indicators (DDIs)

A delivery distribution indicator (DDI) is a [redacted] used to route messages electronically to specific databases and elements within national SIGINT centres, primarily NSA. Every end-product report shared with the US must bear the proper DDIs to ensure that it reaches the appropriate offices in NSA. No more than 13 DDIs can be used on any report.

There are two sets of DDIs: one used exclusively for end-product reports, and one used exclusively for Cryptologic Information Reports (CIRs). **Under no circumstances should CIR DDIs be used on end-product reports.**

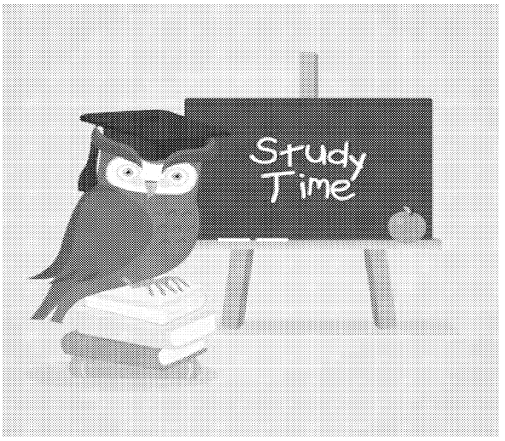
Using the correct DDIs for end-product reports

IRRELEVANT

Using the correct DDIs for CIR reports

IRRELEVANT

DDI EXERCISE



Correcting, cancelling, and reissuing a report

IRRELEVANT

Annexes

Annex 1: SIGINT That Matters: What's the Angle?

IRRELEVANT

IRRELEVANT

IRRELEVANT

IRRELEVANT

IRRELEVANT

IRRELEVANT

Annex 2: Titles That Don't Say Anything of Sub

IRRELEVANT

IRRELEVANT

Annex 3: Words to say instead of “said”

IRRELEVANT

Annex 4: SIGINT Style Sheet

SIGINT Style Sheet

IRRELEVANT

IRRELEVANT

IRRELEVANT

Annex 5: Naming Procedures Reference Guide

Persons in Canada	
Entity in traffic	***Suggested wording in report***
Named Canadian **citizen**	"a Canadian citizen"
Honorary Canadian citizen	Use name in report
Named **permanent resident** of Canada	"a Canadian resident"
Named **deceased Canadian** citizen or permanent resident (dead **less** than 20 years)	"a deceased Canadian"
Named **deceased Canadian** citizen or permanent resident (dead **more** than 20 years)	Use name in report
Named **foreigner in Canada** (even if he/she has a special visa, such as a work or student permit)	“a named person in Canada”
Honorary Consul in Canada	"a Canadian citizen"
[redacted]	Use name in report
	“a named person in Canada”
	“a named person in Canada”
Named **Second Party national** in Canada	Use generic term (e.g., "a British citizen")
Named **Canadian in Canada** acting on behalf of a foreign government, corporation or organization	"a Canadian citizen"
Named **Canadian member of an identified terrorist group** in Canada	"a Canadian member of [name of terrorist group]"
Named **Canadian whose life is in immediate danger**	Use name in report, or suppress it and send it to recipients by other means[i]
[redacted]	Use name in report, or suppress it and send it to recipients by other means[i]
Named Canadian who has committed or plans to	Use name in report, or suppress it and send

commit a life-threatening act	it to recipients by other means[i]
Canadians Outside Canada	
[redacted]	Use name in report with no reference to Canadian status [redacted]authorization required)
Named Canadian member of a terrorist group	"a Canadian member of [name of terrorist group]"
Named Canadian working for an international organization	Use title in report if necessary for clarity, with no reference to Canadian status
Current and Former Government of Canada Officials	
Speaker of the House of Commons	"a Canadian Member of Parliament"
A current Cabinet minister acting in an official capacity	Use title in report
A named opposition party	“an opposition party”
Name of “the Official Opposition”	“an opposition party”
Name of the governing party	“the governing party”
A senior federal public servant (director general or higher) acting in an official capacity	Use title in report
A federal public servant at or below the director level	“a [department name] official”
[redacted]	
General in the Canadian Forces	“a Canadian general stationed in [location]”
Federal Government Bodies	
Federal departments and agencies	Use name in report

Federal Crown corporations	Use name in report
Provincial, Territorial or Municipal Entities	
The Premier of Ontario	COM report: "a senior provincial official"; CEO report: "a senior official of Ontario" or "the premier of a Canadian province"
An Alberta Cabinet minister	COM report: "a senior provincial official"; CEO report: "a senior official of Alberta"
The British Columbia Ministry of Education	"a Canadian provincial ministry"
Nova Scotia	As geographic reference: Use name in report; as administrative entity: "a Canadian province"
Winnipeg	As geographic reference: Use name in report; as administrative entity: "a Canadian city"
Non-governmental Entities	
A former prime minister or Cabinet minister	"a Canadian citizen"
President of [redacted] Inc.	"a senior officer of a Canadian company"
[redacted] Inc. (incorporated in Canada)	“a Canadian company”
[redacted] Inc.’s parent company, incorporated in [redacted]	Use in report
Canadian president of [redacted] Ltd., a subsidiary of [redacted]	"a senior officer of a Canadian subsidiary of a [redacted] firm"
[redacted] Ltd. of [redacted]	Use in report
[redacted] (not incorporated in Canada)	Use in report
[redacted] (used as a brand name)	Use in report (e.g., [redacted])
[redacted]	
[redacted] located in Toronto	Use in report

[redacted]	
The Globe and Mail	As a source of unclassified collateral, use in report As a media outlet, "a Canadian newspaper"
[redacted]	
Conferences, festivals or exhibitions	Use name in report, provided the specific activities or the organizers are not discussed
[redacted]	
Addresses and Locations	
[redacted]	"an identified Ottawa address"
	Use in report (name used as a geographic location)
	Use in report (used as a geographic location)
	"an Ottawa hotel" (describes the hotel's business activities)
	Use in report (flight used as a location)
	"a Canadian airline" (describes the airline's business activities)

[redacted] Identifiers

[redacted]

Miscellaneous

[redacted]

[redacted]