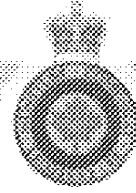




Communications Security  
Establishment Canada

Centre de la sécurité  
des télécommunications Canada



# Canadian SIGINT Operations Instruction CSOI-4-4

## Targeting Identifiers For Foreign Intelligence Under Part (a) of CSE's Mandate

Last Updated  
December 16, 2013

*SIGINT*

Canada

## Table of Contents

---

<b>1. INTRODUCTION.....</b>	<b>4</b>
1.1 Objective.....	4
1.2 Authority.....	4
1.3 Context .....	4
1.4 References .....	5
1.5 Application .....	6
1.6 Accountability .....	6
1.7 Amendment Process .....	6
1.8 Enquiries.....	7
1.9 Review .....	7
<b>2. TARGETING IDENTIFIERS .....</b>	<b>8</b>
2.1 Introduction .....	8
2.2 Identifiers.....	8
2.3 [REDACTED].....	8
2.4 [REDACTED] and Selection Contexts at CSE.....	9
2.5 Strong Selection.....	9
2.6 Identifier Management and Validation.....	10
2.7 Roles and Responsibilities.....	10
<b>3. DOCUMENTING TARGETING REQUESTS .....</b>	<b>12</b>
3.1 Introduction .....	12
3.2 TKB Records .....	12
3.3 Identifiers, [REDACTED] and Strong Selection.....	12
3.4 Permutations .....	12
3.5 Source of Selection Criteria.....	13
3.6 Foreign Assessment – Nationality and Location .....	13
3.7 Intelligence Priority .....	15
3.8 Justification.....	15
3.9 Demonstrating Legal Compliance .....	16
3.10 Targeting Request.....	16
3.11 Automated Approval System.....	17
<b>4. LEVERAGING COLLECTION PROGRAMS.....</b>	<b>19</b>
4.1 Introduction .....	19
4.2 Canadian [REDACTED] .....	19
4.3 [REDACTED] .....	19
4.4 [REDACTED] .....	20
4.5 Leveraging [REDACTED] Assets - Background.....	20
4.6 Leveraging [REDACTED] Assets - Documentation.....	20
4.7 Leveraging [REDACTED] Assets - Prohibition .....	21
4.8 [REDACTED] .....	21
<b>5. SPECIAL PROVISIONS .....</b>	<b>22</b>

5.1 Introduction .....	22
5.2 Targeting in a Crisis Situation .....	22
5.3 Non Specific Location or Nationality – Special Digraphs .....	22
5.4 Dual/ Multiple Nationalities .....	23
5.5 Boolean Expressions.....	23
5.6 [REDACTED] .....	23
5.7 “Context-Neutral” Identifiers .....	24
5.8 [REDACTED] in Canada .....	25
5.9 [REDACTED] .....	25
5.10 Individual and Communal Identifiers – [REDACTED] .....	26
5.11 [REDACTED] .....	27
5.12 [REDACTED] .....	27
5.13 [REDACTED] .....	27
 6. INADVERTENT TARGETING INCIDENTS .....	 28
6.1 Inadvertent Targeting of a Canadian or Person in Canada .....	28
6.2 Inadvertent Targeting of Allied Persons or Persons in Allied Territory .....	28
 7. IDENTIFIER MANAGEMENT .....	 29
7.1 Introduction .....	29
7.2 Annual Validation.....	29
7.3 Updating Targeting Requests .....	30
7.4 De-Targeting Requests .....	30
7.5 Roles and Responsibilities for Identifier Management.....	30
7.6 TKB Record Keeping .....	31
7.7 Target [REDACTED] .....	31
7.8 Targeting [REDACTED] .....	32
 8. DEFINITIONS .....	 34
8.1 Canadian .....	34
8.2 Collection .....	34
8.3 [REDACTED] .....	34
8.4 ELINT .....	34
8.5 Entity .....	34
8.6 Foreign.....	34
8.7 Foreign Intelligence.....	35
8.8 Global Information Infrastructure (GII) .....	35
8.9 Identifier .....	35
8.10 “In Canada” .....	35
8.11 Interception.....	35
8.12 Metadata .....	35
8.13 [REDACTED] SIGINT Collection .....	35
8.14 Private Communication .....	35
8.15 [REDACTED] .....	36
8.16 [REDACTED] .....	36
8.17 Second Party .....	36
8.18 [REDACTED] .....	36
8.19 Strong Selection.....	36
8.20 Target (verb).....	37

8.21 [REDACTED] ..... 37

8.22 Traffic..... 37

ANNEX 1: SUMMARY OF [REDACTED] TARGETING RULES UNDER PART (A) OF CSE’S MANDATE..... 38

    A1.1 Introduction ..... 38

    A1.2 Table ..... 38

ANNEX 2: GUIDANCE ON [REDACTED] ..... 40

    A2.1 Overview ..... 40

    A2.2 Details ..... 40

ANNEX 3: ROLES AND RESPONSIBILITIES FOR [REDACTED] TARGETING ..... 41

    A3.1 Roles and Responsibilities ..... 41

ANNEX 4: NOTIFYING CANADIAN PARTNERS..... 43

    A4.1 Introduction ..... 43

    A4.2 Proposed Form of Words..... 43

CSOI-4-4 PROMULGATION..... 44

---

---

## 1. Introduction

---

**1.1 Objective** These instructions provide direction to employees in the Canadian SIGINT Production Chain<sup>1</sup> regarding targeting activities using identifiers to leverage national SIGINT collection assets, for the purpose of acquiring information from the Global Information Infrastructure (GII) to produce foreign intelligence, in response to Government of Canada (GC) priorities, in accordance with CSE's foreign intelligence authorities specified under Part (a) of the Mandate.

This document supersedes CSOI- 4-4, *Targeting and Selector Management Using [REDACTED] National SIGINT Systems For Intelligence Reporting Purposes*, dated 5 March 2009.

---

**1.2 Authority** This Canadian SIGINT Operations Instruction (CSOI) is issued under the authority of the CSE Deputy Chief, SIGINT (DC SIGINT).

---

**1.3 Context** In a SIGINT context, to "target" means to single out for collection or interception purposes.

Under Ministerial Authorizations (MAs) for collection activities, CSE must satisfy the following four conditions to demonstrate it is appropriately managing the risk of intercepting private communications:

- The interception will be directed at foreign<sup>2</sup> entities located outside Canada;
- The information to be obtained could not be reasonably obtained by other means;
- The expected foreign intelligence (FI) value of the information that would be derived from the interception justifies it; and,
- Satisfactory measures are in place to protect the privacy of Canadians and

---

<sup>1</sup> The Canadian SIGINT Production Chain is defined in CSOI-5-3, *The Canadian SIGINT Production Chain and Access to SIGINT Data*.

<sup>2</sup> According to existing conventions, the 5-Eyes recognize each other's state sovereignty and show respect for each other's laws by pledging not to target one another's communications. Therefore, CSE treats SIGINT allies (i.e. the United States, United Kingdom, Australia and New Zealand) as non-foreign. [REDACTED]

[REDACTED]

to ensure that private communications will only be used or retained if they are essential to international affairs, defence or security.

These instructions outline the information that must be recorded and the steps that must be followed to ensure that CSE targeting activities using identifiers to leverage national SIGINT collection assets for intelligence reporting under Part (a) authorities are compliant with the four MA conditions and fully auditable.

Specifically, operational areas must document available facts and analytical assumptions indicating that a targeted entity is foreign and located outside of Canada. Furthermore, all targeting activities must be associated with a foreign intelligence priority of the GC, aligned with the National SIGINT Priorities List (NSPL). Collection of operationally meaningful and compliant material is achieved through strong selection, coupled with the use of [REDACTED] to eliminate unwanted traffic.

Finally, CSE must maintain an electronic repository of all selection criteria which it has reasonable grounds to believe are associated with foreign entities located outside Canada in relation to a foreign intelligence priority. Accordingly, these instructions also provide guidelines on identifier management.

---

#### 1.4 References

- OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities*
  - OPS-1-1, *Procedures for the Release of Suppressed Information from SIGINT Reports,*
  - OPS-1-8, *Active Monitoring of Operations to Ensure Legal Compliance and the Protection of the Privacy of Canadians*
  - OPS-1-13, *Procedures for Canadian [REDACTED] Activities*
  - OPS-3-1, *Procedures for [REDACTED] Activities*
  - CSOI-1-1, *The National SIGINT Priority List (NSPL) Process*
  - CSOI-3-3, *Requesting [REDACTED] Collected via [REDACTED] Operations*
  - CSOI-3-7, *[REDACTED] Authorities*
  - CSOI-5-3, *The SIGINT Production Chain and Access to SIGINT Data*
  - CSSS-103, *The SIGINT Classification System*
  - *The Canadian Security Intelligence Service Act*
  - IM-1, *CSE Information Management Policy*
-

**1.5 Application** These instructions apply to all individuals and elements within the Canadian SIGINT Production Chain, including Government of Canada (GC) and Second Party integrees, authorized to conduct SIGINT activities under the authority of CSE Deputy Chief, SIGINT. This includes personnel operating under the authority of the Canadian Armed Forces SIGINT Technical Control Authority.

**1.6 Accountability** The following table outlines responsibilities with respect to these instructions.

Who	Responsibility
DC SIGINT	Approving these instructions
Director General SIGINT Programs	Recommending these instructions for approval
Director SIGINT Requirements, SIGINT Programs	<ul style="list-style-type: none"><li>* Promulgating and implementing these instructions</li><li>* Revising these instructions as required</li><li>* Seeking legal and/or policy advice if required</li><li>* Responding to questions concerning these instructions</li></ul>
All CSE Directors-General and Directors who are affected by these instructions and the Canadian Armed Forces SIGINT Technical Control Authority (CAF STCA)	Applying these instructions
All CSE managers and CAF/DND leaders and supervisors who are affected by these instructions	Ensuring that their staff has read, understands and complies with these instructions and any amendments to these instructions
All CSE, DND staff and employees and CAF members who are affected by these instructions	Reading, understanding and complying with these instructions and any amendments to these instructions

**1.7 Amendment Process** Situations may arise where amendments to these instructions may be required because of changing or unforeseen circumstances. All approved amendments will be announced to staff and will be posted on the SIGINT Programs website.

**1.8 Enquiries** Questions related to these instructions should be directed to operational managers, who in turn will consult with SIGINT Programs Oversight and Compliance (SPOC) staff (e-mail spoc-staff-dl) when necessary.

---

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

---



---

## 2. Targeting Identifiers

---

### 2.1 Introduction

There are specific statutory and policy requirements on selection criteria used to leverage national SIGINT systems to acquire information from the GII for intelligence reporting under Part (a) authorities.

In order to comply with MA conditions for intercepting communications, the selection criteria must be:

- directed at foreign<sup>3</sup> entities located outside Canada;
- associated with GC intelligence priorities;
- related to an external component of a communication; and,
- subjected to annual review to ensure consistency with GC intelligence priorities.

These instructions outline how the use of “identifiers” meets the above statutory and policy requirements for compliant selection criteria.

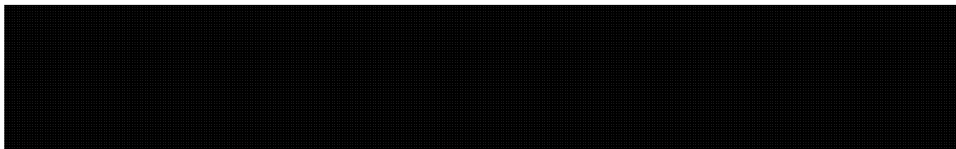
---

### 2.2 Identifiers

Identifiers are alphanumeric strings that may be used to reliably identify a person, organization, corporation or machine/network, in a pre-defined context on the GII, like an e-mail address, a telephone number, an IP address.

---

### 2.3



Examples of [REDACTED] include:

- [REDACTED]
- [REDACTED]
- [REDACTED]

---

<sup>3</sup> According to existing conventions, the 5-Eyes recognize each other's state sovereignty and show respect for each other's laws by pledging not to target one another's communications. Therefore, CSE generally treats SIGINT allies (i.e. the United States, the United Kingdom, Australia and New Zealand) as non-foreign.



\* [REDACTED]

A list of [REDACTED] approved for targeting is available on the CSE SIGINT [REDACTED] or via [REDACTED]. Analysts may propose new [REDACTED] by sending a ticket through the IT Service Desk.

---

**2.4 [REDACTED] and Selection Contexts at CSE**

At CSE, the concept of [REDACTED] is implemented in conjunction with the requirement to select information on the basis of [REDACTED] of communications. [REDACTED]

For example, an identifier that is assigned the [REDACTED] when it is submitted for targeting through Canadian collection systems, will only select traffic which contains the [REDACTED] identifier in the [REDACTED] and [REDACTED] but not in the [REDACTED]. Consult the CSE SIGINT [REDACTED] for further details on [REDACTED] implementation.

---

**2.5 Strong Selection**

SIGINT aims to optimize the selection of information of FI interest while minimizing the risk to the privacy of Canadians and persons in Canada. This principle has become known as “strong selection”.

Targeting [REDACTED]  
[REDACTED] strong selection strategy because it [REDACTED]  
[REDACTED]


The following are examples of strong selection strategies that may be [REDACTED]

- \* [REDACTED]
- \* [REDACTED]
- \* [REDACTED]

The documentation requirements associated with strong selection are outlined in section 3 of these instructions.

---

<sup>5</sup> [REDACTED]  
[REDACTED]

 **Note:** Other types of selection criteria, [REDACTED] on the GII may also achieve strong selection, and are addressed in separate CSOIs.

## 2.6 Identifier Management and Validation

All targeting activities must be managed and re-validated on an annual basis, at a minimum, to ensure continued compliance. The validation process is described in section 7 of these instructions.

All deployed selection criteria must be stored and readily accessible for review in [REDACTED] directory, and handled in accordance with the Agreement for the Transfer of Archival Records between CSE and Library and Archives Canada (LAC)<sup>6</sup>.

## 2.7 Roles and Responsibilities

The following table outlines the roles and responsibilities associated with targeting identifiers for intelligence reporting:

Who does it	Roles and Responsibilities
[REDACTED] Team Leaders (TLs), [REDACTED] Supervisors	<ul style="list-style-type: none"> <li>* Ensure analysts: <ul style="list-style-type: none"> <li>o have attended all mandatory policy briefings, including the Privacy Annotation &amp; Sign Off Procedures briefing and the SIGINT Legal Framework briefing;</li> <li>o have successfully completed the annual OPS-1 quiz; and</li> <li>o are familiar and comply with all related operational policies, procedures, and instructions.</li> </ul> </li> <li>* Provide direction and guidance, as required.</li> <li>* Ensure analysts validate targeted identifiers on a regular basis, at least annually, in accordance with OPS-1-8.</li> <li>* Inform SPOC when Canadians, allied persons or persons in Canada or in allied territory have been inadvertently targeted and report which</li> </ul>

<sup>6</sup> Under the agreement, all records documenting CSE involvement in the identification and execution of individual taskings and targeting, including SIGINT development and overall coordination and specific taskings with [REDACTED] are considered “archival records” and must be selected and transferred to the care and control of the LAC when they are no longer required by SIGINT.

	corrective measures were applied (refer to OPS-1 for details, and consult SPOC's online form).
<b>DGI and CFIOG Analysts</b>	<ul style="list-style-type: none"> <li>• Conduct research and document that all conditions for targeting have been met.</li> <li>• Propose targeting justifications for the pre-approved list, as required.</li> <li>• Submit targeting requests to [REDACTED]</li> <li>• On an annual basis, or more frequently as required, validate targeted criteria, and de-target those which are no longer valid, or which are pulling traffic of no foreign intelligence value, or for which there is no longer an associated intelligence priority.</li> <li>• Ensure that all targeting and selection criteria management activities are compliant with these instructions.</li> </ul>
[REDACTED]	<ul style="list-style-type: none"> <li>• Develop, implement and maintain targeting actions in the [REDACTED] system.</li> <li>• Approve and maintain the list of pre-approved targeting justifications.</li> <li>• Validate and action referred targeting requests.</li> <li>• De-target selection criteria in certain circumstances (see section 7).</li> <li>• Inform analysts of targeting request status (when referred for manual review) and identifier status (targeted or de-targeted).</li> </ul>
<b>SPOC</b>	<ul style="list-style-type: none"> <li>• Provide guidance, as required.</li> <li>• Respond to incidents of inadvertent targeting of Canadians or persons in Canada and ensure mitigation is complete (see section 6).</li> </ul>
<b>Operational Policy</b>	<ul style="list-style-type: none"> <li>• Provide guidance, as required.</li> <li>• Act as a liaison with partners when foreign assessments require consultations (see 3.6).</li> <li>• Track cases of inadvertent targeting and corrective measures taken (as per section 6).</li> <li>• Approve targeting requests in a crisis situation, in accordance with paragraph 5.2 of these instructions.</li> </ul>

---

## 3. Documenting Targeting Requests

---

### 3.1 Introduction

In order to deploy identifiers to collect information from the GII, the following elements of information must be researched and documented in the Target Knowledge Base (TKB):

- Identifier(s) and applicable [REDACTED]
- Source of selection criteria;
- Foreign assessment of associated entities;
- Intelligence priority;
- Targeting justification or expected results.

The elements of information are explained below, followed by detailed instructions on how to prepare a targeting request.

---

### 3.2 TKB Records

All identifiers must be associated with an entity record (person, organization, group, [REDACTED]) of foreign intelligence interest in the TKB. Care should be taken to clearly establish the link between an identifier and its user(s) or subscriber(s), which enables teamwork and review.

---

### 3.3 Identifiers, [REDACTED] and Strong Selection

Assigning a [REDACTED] within which an identifier is believed to be valid and

[REDACTED]

[REDACTED]  
[REDACTED] “strong selection” strategy.

[REDACTED] have a set of attributes, which include [REDACTED]  
[REDACTED] These attributes affect the strength or precision of the selection strategy. Consult the CSE SIGINT [REDACTED] for up-to-date information on enabled [REDACTED] at CSE.

---

### 3.4 Permutations

Permutations are format variations of an identifier within a given [REDACTED]

For example, an identifier such as [REDACTED] could appear

as [REDACTED]  
[REDACTED]

An identifier could also be permuted depending on the [REDACTED]  
[REDACTED] the telecommunications network.

Permutations are usually applied and deployed automatically by the SIGINT system once a targeting request has been approved. Consult [REDACTED] for more information.

---

### 3.5 Source of Selection Criteria

The source of the identifier or selection criteria must be documented and assigned the appropriate classification.

Examples of sources include, but are not limited to:

- \* Open Source (Press articles, etc.),
- \* HUMINT (CSIS information),
- \* COMINT (traffic content or metadata),
- \* SIGINT End Product Reports (EPRs).

When a source reference number exists (eg. a SIGINT report serial or a traffic identity number), it should be recorded in the TKB, for tracking purposes.

In certain circumstances, there may be multiple sources, which may all be documented.

In the event that a source is particularly sensitive, a codename or other form of protection may be applied, as appropriate.

Consult CSSS-103, *The SIGINT Classification System*, for guidance on assigning appropriate classification markings for source information.

---

### 3.6 Foreign Assessment – Nationality and Location

It is the analyst's responsibility to determine whether there is sufficient information to make an informed assessment<sup>7</sup> about the foreign status of an entity.

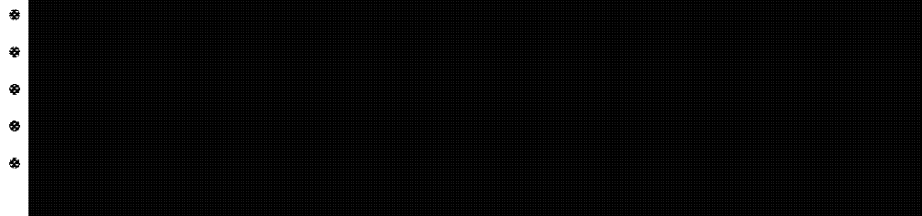
For targeting to be compliant, the foreign status of the entity associated with the identifier must be assessed by considering factors which could reveal the likely nationality and location of the entity.

---

<sup>7</sup> The standard applied to an informed assessment is one of "reasonableness", that is the assessment must be based on analysis that would reasonably lead a reviewer to the same conclusion.

Various elements of information may assist in making this assessment, including:

- \* contextual information from COMINT collection, intelligence reporting, open source publications, etc.;



When making a foreign assessment, consideration must be given to the fact that identifiers may be [REDACTED] and these may or may not reflect the foreign status of the user (see section 5 on context-neutral identifiers).

Analysts may encounter information which raises the possibility that an entity of interest may be Canadian or in Canada (e.g. the person studied or worked in Canada, or has close relatives in Canada). In such cases, analysts may make enquiries of the Department of Foreign Affairs, Trade and Development Canada (DFATD) or the Canadian Border Services Agency (CBSA) through Corporate and Operational Policy (D2), to obtain passport and/or citizenship information in order to clarify the status of the entity.

	<b>Note:</b> A foreign assessment is made against a person or group of persons, [REDACTED] [REDACTED] DFATD and CBSA usually require a date and place of birth in order to provide accurate information about the status of a person of interest.
--	---

Once analysts have sufficient information to make a foreign assessment, they must document it by assigning each entity:

- \* one or more appropriate location digraphs<sup>8</sup>, e.g. [REDACTED]
- \* an appropriate [REDACTED] trigraph indicating nationality (one or more country digraphs<sup>9</sup>, as appropriate) and function (single letter code representing an entity's function, such as [REDACTED])

[REDACTED]

<sup>8</sup> Where more than one location digraph is applicable, only the first one will be sent to collection sites.

<sup>9</sup> Where more than one foreign nationality digraph is applicable, all will be forwarded to collection sites. Only one function letter will be [REDACTED]

Consult [REDACTED] for the approved list of targeting digraphs and trigraphs; refer to section 5 for guidance on special digraphs.

---

**3.7 Intelligence Priority** Entities must be linked to relevant intelligence priorities, in line with the priorities set out in the NSPL.

---

**3.8 Justification** A justification documents why an identifier is being targeted, by answering as many of the following questions as possible:

- Who is the entity of intelligence interest?
- Why is it proposed for targeting?
- What is the entity suspected or known to be doing?
- What is the expected result of the targeting activity?

Examples of adequate justifications are:

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

Below are examples of inadequate justifications:

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

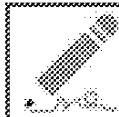
In some cases, the justification will contain information that is not shareable with Second Party partners. Such information must not be [REDACTED] [REDACTED] must bear the Canadian Eyes Only (CEO) marking.

With the automated processing of targeting requests, a list of pre-approved justifications has been drafted by DGI teams and validated by [REDACTED]. This list is maintained by [REDACTED] and updated as required. In order to facilitate the handling of the justification field in targeting systems, each justification entry is abbreviated [REDACTED].

When preparing a targeting request, analysts will select one of the pre-approved justifications. If none is adequate, they will propose a new



justification to their TL, who will forward to [REDACTED] for validation. [REDACTED] will add the new justification to the pre-approved list, as required.



**Note:** It is recommended that, where appropriate, a justification be drafted in such a way as to allow for targeting more than one individual, to avoid the unnecessary proliferation of similar justifications.

**3.9  
Demonstrating  
Legal  
Compliance**

A valid foreign location digraph, foreign nationality and function trigraph [REDACTED] intelligence priority, and justification demonstrate that analysts have reasonable grounds to believe that targeting activities are aimed at a foreign entity located outside Canada, in response to a GC foreign intelligence priority.



**ATTENTION:** Analysts are responsible for ensuring that targeting and selection criteria management are compliant with requirements described in these instructions.

**3.10 Targeting  
Request**

Once all the elements have been adequately documented in the TKB, analysts may proceed with submitting a targeting request, as follows:

Step	Who does it	Action
1	DGI and CFIOG Analyst	<p>Submits fully documented targeting request for validation, including the following elements of information:</p> <ul style="list-style-type: none"><li>* a target identification number (TID) generated by the TKB,</li><li>* an identifier [REDACTED]</li><li>* an entity name,</li><li>* an entity nationality [REDACTED]</li><li>* an entity location (digraph),</li><li>* an associated intelligence priority,</li><li>* a pre-approved targeting justification,</li><li>* a targeting priority, with justification,</li><li>* a security classification,</li><li>* [REDACTED]</li><li>* [REDACTED]</li></ul> <p>As appropriate, other elements may be included,</p>

		such as a CEO comment or justification.  In order to complete a targeting request, analysts must confirm the targeting activity is being conducted under Part (a) of the CSE Mandate, as per the NDA.
2		Most requests are handled by an automated targeting tool, which : <ul style="list-style-type: none"><li>* approves, or</li><li>* rejects, or</li><li>* pools, or</li><li>* refers requests for manual inspection, as appropriate.</li></ul> processes requests (exceptions) that are referred for manual inspection.

### 3.11 Automated Approval System

The automated approval system causes each targeting request to be:

- \* approved, or
- \* rejected, or
- \* pooled, or
- \* referred for manual inspection.

Targeting requests that pass all the rules in the targeting tool are automatically approved and forwarded to collection systems.

Targeting requests which fail one or more rules are rejected. Requesters receive a notification of the rejection with the reason. As appropriate, they may modify and resubmit the request.


A pooled request is one which passes all the rules but is put on hold as a result of the system being unable to process it. Pooled requests are expected to be automatically processed at a later date.

All referred targeting requests are manually validated by █████ in accordance with CSOI-3-7, █████ *Authorities*. Specifically, █████ validates that:

- \* the selection string is in the proper format,
- \* the targeting is directed at a foreign entity located outside Canada,
- \* the targeting is related to an active intelligence priority on the NSPL, and
- \* the targeting justification is adequate.

[REDACTED] approved requests are forwarded to the collection systems. Requests which do not pass manual validation do not proceed to collection systems. Requesters receive a notification of the rejection with the reason. As appropriate, they may modify and resubmit the request.

Requests which are not handled by the automated tool (i.e. [REDACTED]) are received by [REDACTED] in the form of an e-mailed template, which [REDACTED] validates manually and forwards to the collection system, as it does for referred requests.

	<p><b>Note:</b> There may be exceptional circumstances under which analysts will [REDACTED]. Regardless of the means by which targeting requests are submitted, all targeting requests must be tracked by [REDACTED].</p>
---	---

---

## 4. Leveraging Collection Programs

---

### 4.1 Introduction

Approved targeting requests (either processed by the automated tool or manually by [REDACTED]) are deployed to appropriate collection programs, in accordance with the specifics of the requests, including precedence, prioritization, capacity, national sensitivities, etc.

Targeting of identifiers is done under the principle of [REDACTED], that is, [REDACTED]

[REDACTED]

for policy or operational reasons.

---

### 4.2 Canadian [REDACTED]

Most targeting requests to leverage Canadian collection programs are handled via the automated tool. Please note that certain targeting requests directed at specific programs (eg. [REDACTED]) may require forwarding to [REDACTED] using **both** automated and manual processes.

---

### 4.3 [REDACTED] [REDACTED]

Most targeting requests for collection [REDACTED] are handled by the automated targeting tool.

Targeting requests involving complex selection criteria (i.e. other than

[REDACTED]

Complex selection for [REDACTED] or target discovery will be addressed in separate instructions.

---

---

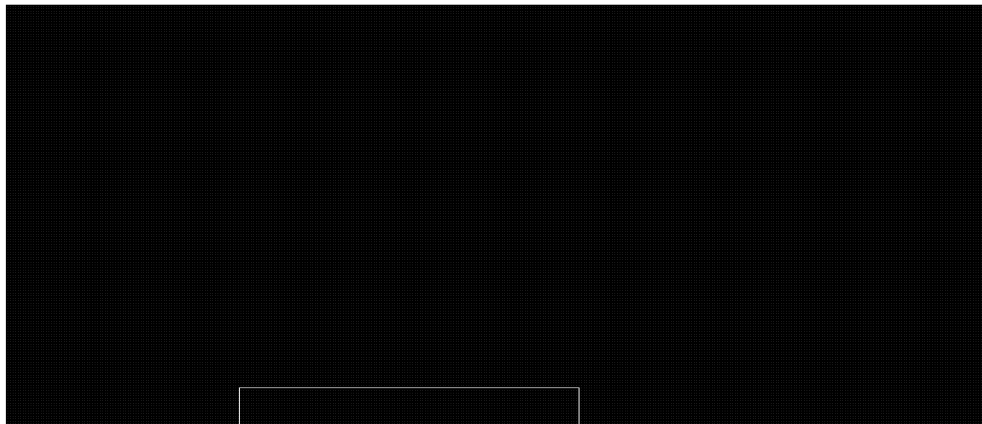
4.4 [REDACTED] Please consult [REDACTED] targeting collection managers for guidelines on leveraging [REDACTED] assets.



**ATTENTION:** Certain fields in the targeting request, such as intelligence priority and justification, may not be shared with [REDACTED]

---

**4.5 Leveraging  
[REDACTED] Assets -  
Background**



[REDACTED]  
according to the process documented in relevant [REDACTED] guidelines, and in accordance with OPS-3-1, *Procedures for [REDACTED]* [REDACTED] Activities.

Under the legal and policy framework for [REDACTED] all [REDACTED] activities conducted under Part (a) authorities must meet the conditions outlined in section 1.3 and section 2.1 of these instructions.

---

**4.6 Leveraging  
[REDACTED] Assets -  
Documentation**

In order to request targeting via [REDACTED] methods, selection criteria will be submitted with the standard documentation outlined in 3.10, by a [REDACTED] analyst, through the automated targeting tool or other established mechanism to leverage an existing [REDACTED] operation or to request a new [REDACTED] or [REDACTED] operation.

In addition to the information specified in section 3.10, the following elements may be included with the request to assist in developing the [REDACTED] strategy:

- [REDACTED]
- [REDACTED]
- [REDACTED]

- whether the request is to be forwarded to CSE [REDACTED] program only, or whether it could be sent to applicable [REDACTED]

If no existing [REDACTED] operation meets a given request, a new project must be proposed in accordance with published guidelines.

For specific guidance on targeting through [REDACTED] activities, please contact [REDACTED] targeting collection managers. For policy information on the [REDACTED] Program, refer to OPS-3-1, *Procedures for [REDACTED] Activities*. For details on the [REDACTED] approval process, refer to Annex 2 of these instructions.

#### 4.7 Leveraging [REDACTED] Assets - Prohibition

CSE is prohibited from using identifiers associated with persons in Canada (including [REDACTED]) to run queries in databased information, such as an [REDACTED] made accessible through [REDACTED] operations.

Advice issued by CSE's Department of Legal Services in July 2013, and informed by a Federal Court decision of 2011, indicates that [REDACTED] Solicitor-Client Privilege

#### 4.8 [REDACTED]

Requests for [REDACTED] must be done in accordance with CSOI-3-3, *Requesting [REDACTED] Collected via [REDACTED] Operations*.

IRRELEVANT

---

## 5. Special Provisions

---

### 5.1 Introduction

This section provides specific guidance on various targeting scenarios which require manual validation by [REDACTED] and/or special approvals. In any situation where additional guidance is required, please contact SPOC or [REDACTED] for further assistance.

---

### 5.2 Targeting in a Crisis Situation

In circumstances where the life and safety of Canadian individuals are threatened (e.g. during a kidnapping), and [REDACTED] provided they have obtained the **prior approval** of Corporate and Operational Policy (D2).

Such approvals may be granted on a case-by-case basis. Resultant traffic must be closely monitored and identifiers must be de-targeted as soon as the situation is resolved or, when the identifiers no longer pull traffic related to GC intelligence priorities.

---

### 5.3 Non Specific Location or Nationality – Special Digraphs

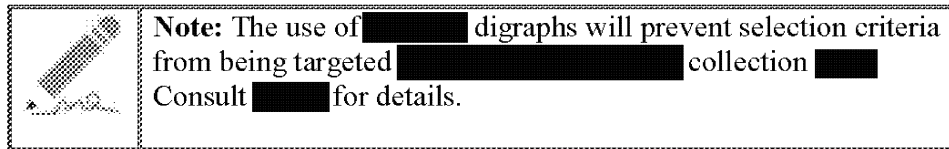
The following are special targeting nationality or location digraphs, which may only be used under circumstances described below:

- \* The [REDACTED] digraph may be used for nationality or geographic location in the context of SIGINT development efforts only. Any selection criteria submitted with the [REDACTED] digraph must be reviewed and updated with a precise country digraph as soon as the nationality and/or location of the entity of interest has been determined, within [REDACTED] of the initial targeting request. If a determination may not be made within [REDACTED] the selection criteria will be identified for de-targeting, unless analysts provide [REDACTED] with an adequate justification to continue targeting for a [REDACTED]
- \* The [REDACTED] digraph may be used for geographic location for [REDACTED]-related or [REDACTED] targeting only<sup>11</sup>.
- \* [REDACTED] digraphs, such as [REDACTED] may be used on an exceptional basis (e.g. for [REDACTED]) and do not

---

<sup>11</sup> [REDACTED] targeting is addressed in a separate CSOI.

negate the requirement to conduct appropriate target research and update the digraph to reflect the most up-to-date location (see section 7.8 for more details on [REDACTED]). [REDACTED] digraphs must not include 5-Eyes countries or territories.



#### 5.4 Dual/ Multiple Nationalities

In accordance with a 2012 DLS opinion, [REDACTED] Solicitor-Client Privilege  
[REDACTED] Solicitor-Client Privilege

In circumstances where a target has multiple foreign nationalities, these may be recorded in the TKB, and may be forwarded to collection [REDACTED] when included on targeting requests. Multiple foreign locations may be recorded in the TKB, however only [REDACTED] in the list will be passed in targeting requests.

#### 5.5 Boolean Expressions

In certain circumstances, the use of an [REDACTED] combination may not be sufficient to exclude unwanted material. In such cases, it is possible to combine selection criteria with boolean operators (AND, OR, NOT) to restrict collection to meaningful information.

For example, when targeting an [REDACTED] that is associated [REDACTED]  
[REDACTED]  
[REDACTED] combination to exclude unwanted material.

Current capabilities for targeting complex or boolean expressions are limited; please contact [REDACTED] for assistance.

#### 5.6 [REDACTED]

Although [REDACTED] they may be [REDACTED]. As such, analysts must demonstrate knowledge of [REDACTED] prior to targeting to ensure compliance and proportionality of collection.

Additional information must be documented regarding the expected function and volume of traffic associated with [REDACTED] in order to:



- demonstrate that CSE is directing its activities at foreign entities located outside of Canada,
- provide an additional layer of assurance that private communications will not be collected intentionally, and
- ensure that targeting requests will be accepted at collection [REDACTED] where volume restrictions are in effect.

Analysts will provide the following information for all [REDACTED] targeting requests, in addition to the elements outlined in paragraph 3.10 above:

1. [REDACTED]

2. [REDACTED]

When the expected volume of traffic for the [REDACTED] proposed for targeting is unknown, a comment to that effect must be included in the targeting request.

[REDACTED] are only [REDACTED] and as such, may **not** be targeted on their own.

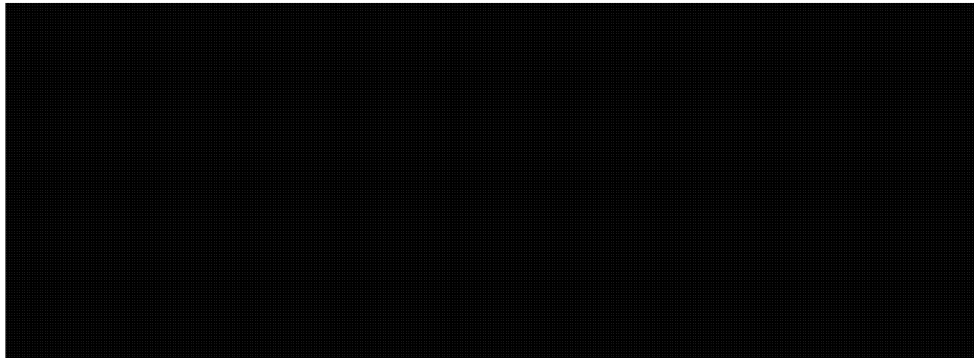


**ATTENTION:** Whenever possible, other selection criteria (such as [REDACTED]) will be added to [REDACTED] to optimize collection and limit traffic volumes. [REDACTED] must be combined with other criteria or with information about its usage in order to be considered for targeting.

#### 5.7 “Context-Neutral” Identifiers

Some identifiers on the GII do not have a [REDACTED]

For example, [REDACTED]

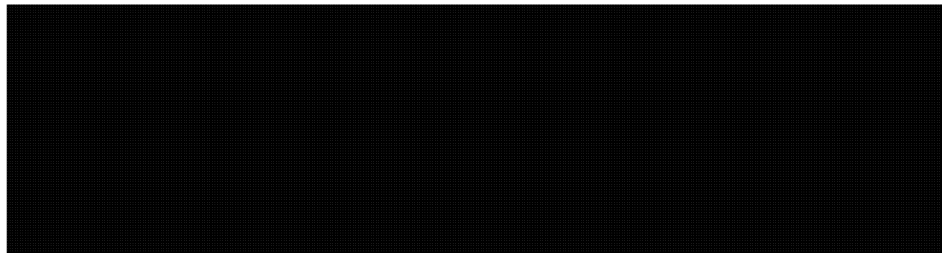


In such cases, the identifier may be targeted when it may be demonstrated that the entity associated with it is:

- \* foreign (not Canadian, not 5-Eyes), and
- \* located outside Canada and 5-Eyes territory.

Analysts must adequately document the foreign assessment (see paragraph 3.6), based either on metadata or target knowledge acquired via other SIGINT sources or collateral information. This information will be stored in the TKB.

5.8



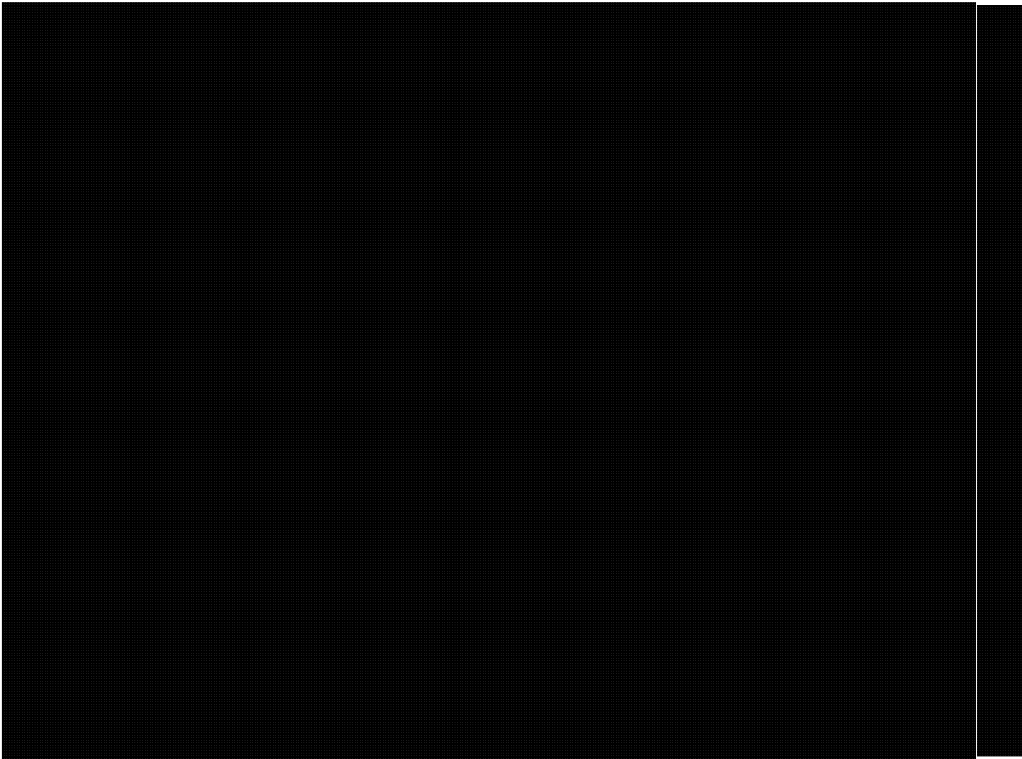
Analysts must have adequate information to demonstrate that the associated entity is foreign. This information will be included in the targeting request forwarded to [REDACTED] and stored in the TKB.




**Attention:** [REDACTED] targeting activities are prohibited against [REDACTED] located in Canada. Please consult OPS-3-1, *Procedures for [REDACTED] Activities* for details.

5.9







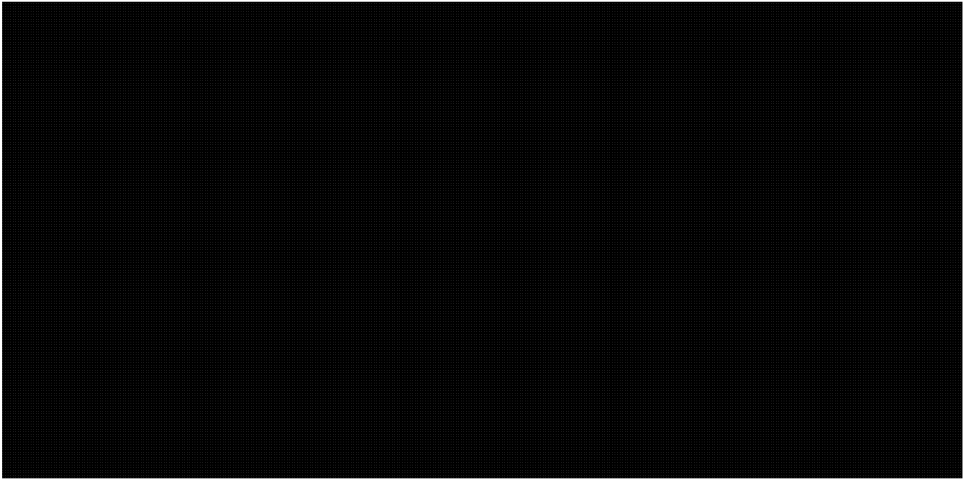
**Attention:** [REDACTED]

[REDACTED]

[REDACTED] See OPS-3-1, *Procedures for* [REDACTED]

[REDACTED] *Activities*, for details.

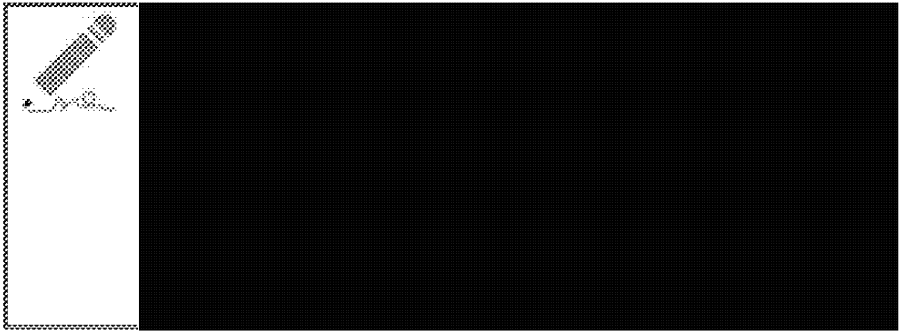
5.10 Individual  
and Communal  
Identifiers –



13 [REDACTED]

[REDACTED]

[Redacted]



5.11 [Redacted]  
[Redacted]

[Redacted]

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

5.12 [Redacted]  
[Redacted]

[Redacted]

[Redacted] Refer to Annex 1 of these instructions for details.

5.13 [Redacted]  
[Redacted]

[Redacted]

[Redacted] Contact [Redacted] for assistance.

---

## 6. Inadvertent Targeting Incidents

---

### 6.1 Inadvertent Targeting of a Canadian or Person in Canada

Should the communications of a Canadian or person in Canada be inadvertently targeted, analysts must fill out an online form located on the SPOC webpage on CSE's classified Intranet, in accordance with the process stated in OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities*. These incidents are reported to the Office of the CSE Commissioner.

Associated entity records in the TKB will be marked as "Protected" to prevent any recurrence of inadvertent targeting.

---

### 6.2 Inadvertent Targeting of Allied Persons or Persons in Allied Territory

In accordance with 5-Eyes agreements, targeting must not be directed at entities of allied nationality located anywhere, or against any entity located in allied territory.



**Attention:** Analysts must report any inadvertent targeting incident for any allied person or any person in allied territory using the online form on the SPOC website.



---

## 7. Identifier Management

---

### 7.1 Introduction

Given that subscribers [REDACTED] numbers, IP addresses, etc., can and do change over time, it follows that targeted identifiers must be reviewed on a regular basis to ensure compliance.

Without periodic review, the following situations could arise:

- CSE could misidentify entities in reporting and analysis. For example, [REDACTED]
- CSE could conduct targeting activities that are no longer associated with an intelligence priority;
- CSE could inadvertently target a Canadian through what was previously identified to be a foreign identifier.

---

### 7.2 Annual Validation

To determine whether identifiers may remain targeted from a policy compliance perspective, analysts must validate the following four elements of the targeting request, at a minimum annually:

- The identifiers are associated with a foreign entity (documented through an [REDACTED] from the approved list<sup>14</sup>);
- The identifiers are associated with an entity located outside Canada and allied territories (documented through a targeting location digraph from the approved list);
- The identifiers are associated with an intelligence priority of the GC and aligned with the NSPL;
- The justification outlining the reason for targeting is adequate and remains valid.

The automated targeting tool [REDACTED] messages to remind analysts of their responsibilities to validate targeting activities for all identifiers that are handled through it, well ahead of the expiry date.

Analysts may want to consider de-targeting compliant identifiers that yield traffic which they do not have time to debrief due to competing priorities, in order to free up system resources.

---

<sup>14</sup> The list of approved targeting nationality [REDACTED]s and location digraphs is available through [REDACTED]

**7.3 Updating  
Targeting  
Requests**

On a regular basis, as often as is necessary, analysts are responsible for updating active targeting requests with any element of information that may have changed (e.g. a different location digraph). For specifics, please see paragraphs 7.7 through 7.9 below.

**7.4 De-  
Targeting  
Requests**

When any of the elements in paragraph 7.2 above no longer hold for a given identifier, analysts must send a de-targeting request to [REDACTED] with the following information:

- \* the [REDACTED] combination;
- \* [REDACTED]
- \* Reason for de-targeting (e.g., entity was observed to be located in the U.S.).

The targeting history, including the reason for de-targeting, along with the date range during which the identifier was targeted, must be recorded in the [REDACTED]. Where possible, [REDACTED] associated with [REDACTED] targeting systems should be updated to reflect the reason for de-targeting, for awareness and continuity.

**7.5 Roles and  
Responsibilities  
for Identifier  
Management**

The table below outlines the roles and responsibilities for managing and de-targeting identifiers.

Who Does It	Action	
[REDACTED] [REDACTED] Analyst	On a regular basis, [REDACTED] reviews traffic collected for all identifiers to ensure they remain valid and required, i.e. continue to meet all conditions for targeting outlined in paragraphs 7.2.	
	<b>If...</b>	<b>Then...</b>
	the identifiers are associated with a foreign entity (nationality and location are non 5-Eyes), and the associated traffic is linked to a GC intelligence priority,	maintain targeting.
	the identifiers are no longer associated with a foreign entity,	de-target.
	the traffic generated is not of foreign intelligence value,	de-target.
	there is no longer a GC requirement for the information in the traffic,	de-target.

[REDACTED]	Actions de-targeting requests, according to CSOI-3-7, [REDACTED] <i>Authorities.</i>
[REDACTED] PM and TL; CFIOG supervisor	Ensures that analysts are validating targeted identifiers individually, at a minimum, annually. Sets operational priorities and gives direction on identifier management when faced with resource limitations.

#### 7.6 TKB Record Keeping

Corporate record keeping requirements apply to all information resources of “business value”, including those created or acquired in the context of approved targeting activities, because they:

- enable informed decision making and the delivery of programs, services, and ongoing operations; and
- support CSE reporting, performance and accountability requirements.

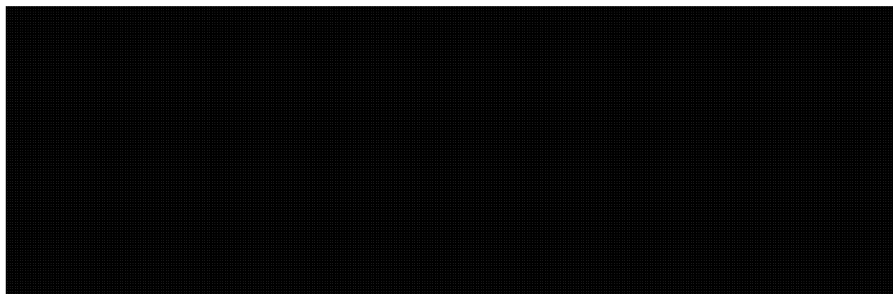
Analysts, Team Leaders and/or Supervisors must ensure that records associated with approved targeting activities in the TKB are accurate and current. The TKB entries, including the entity name, system-generated target identity number, foreign nationality, foreign location, associated intelligence priority, and targeting justification, constitute official records and must be retained for operational continuity and for review and audit purposes.

Any traffic associated with a TKB record must be handled in accordance with OPS-1-11, *Retention Schedules for SIGINT Data*.

Team Leaders or Supervisors are responsible for overseeing the management of targeting information, including ensuring that targeted entities in TKB are reassigned when there is a change in personnel or responsibilities.

For more details on information management requirements and standards, please contact the Information Holdings Services (IHS) within CIO.

#### 7.7 Target

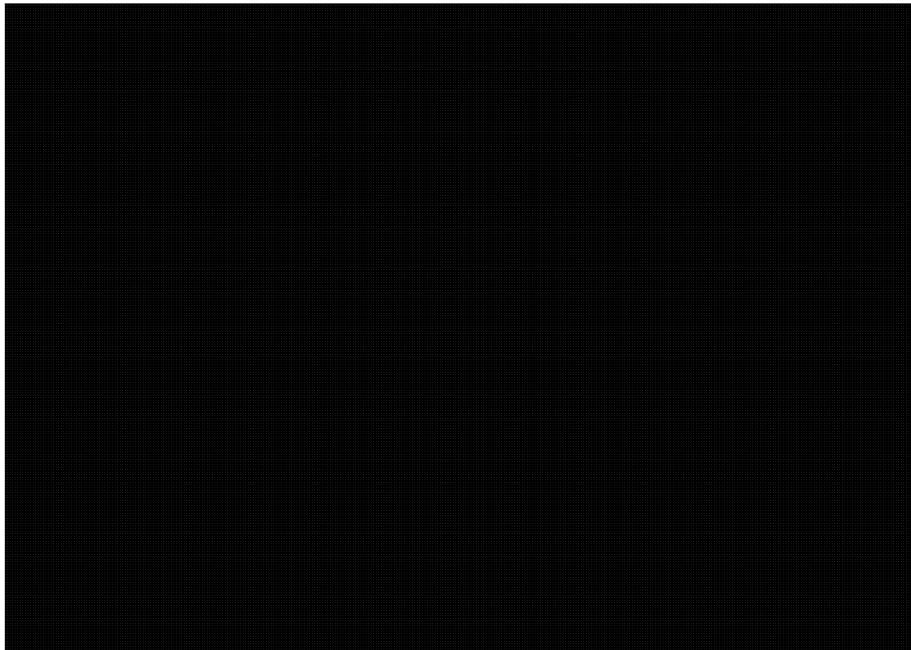




[REDACTED]  
analysts will update the corresponding targeting request with the current location digraph and re-submit for validation.

---

## 7.8 Targeting



**Attention:** Analysts are responsible for de-targeting any other identifiers (including individual e-mail addresses)



In order to [REDACTED] targeting, analysts must make an informed assessment that the [REDACTED]. This assessment may be based on target knowledge (e.g. [REDACTED]) or on metadata analysis, including the periodic review of information stored in SIGINT repositories.

While querying on identifiers [REDACTED] is generally not permitted without special authorization, for the **sole purpose** of avoiding targeting incidents, analysts may query on such identifiers to [REDACTED]. Prior to launching queries in audited repositories, analysts must contact auditors to indicate the purpose of the query and request permission to proceed. Results of these metadata queries will not be used in reporting unless the target is in foreign territory.

[REDACTED]  
[REDACTED] identifier(s) must immediately be de-targeted,  
and an incident report must be completed in accordance with section 6 of  
these instructions.

---

## 8. Definitions

---

### 8.1 Canadian

“Canadian” refers to:

- a) A Canadian citizen, or
- b) A person who has acquired the status of permanent resident under the *Immigration and Refugee Protection Act* (IRPA), and who has not subsequently lost that status under that *Act*, or
- c) A corporation incorporated under an Act of Parliament or of the legislature of a province.

For the purposes of these procedures, “Canadian organizations” are also accorded the same protection as Canadian citizens and corporations. A Canadian organization is an unincorporated association, such as a political party, a religious group, or an unincorporated business headquartered in Canada.

---

### 8.2 Collection

For the purposes of these instructions, collection refers to the acquisition of information from the GII, through [REDACTED] techniques.

---

### 8.3 [REDACTED]

[REDACTED]

[REDACTED] (OPS-3-1)

---

### 8.4 ELINT

Electronic Intelligence (also known as ELINT) is technical and intelligence information derived from the acquisition of foreign non-communications electromagnetic emissions from non-nuclear sources, e.g. radar, navigation aids, jamming systems and some remote control systems.

---

### 8.5 Entity

A person, group, trust, partnership, fund, unincorporated association, or organization, including a state or political subdivision.

---

### 8.6 Foreign

In the context of the NDA and the *Canadian Security Intelligence Service Act* (CSIS Act), “foreign” refers to non-Canadian. However, for targeting purposes, by convention, CSE treats SIGINT allies (i.e. the U.S., UK, Australia and New Zealand) as non-foreign. Therefore, for the purposes of

these instructions, “foreign” generally refers to non 5-Eyes.

---

**8.7 Foreign Intelligence**

Foreign intelligence 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.

---

**8.8 Global Information Infrastructure (GII)**

Global Information Infrastructure (GII) includes electromagnetic emissions, communications systems, information technology systems and networks, and any data or technical information carried on, contained in, or relating to those emissions systems and networks.

---

**8.9 Identifier**

For the purposes of these instructions, an identifier is an alphanumeric string that may be used to identify a person, organization, corporation, or machine/network, for example, an e-mail address, a telephone number, an IP address. This was formerly known as a “selector”.

---

**8.10 “In Canada”**

“In Canada” refers to Canada’s territory, internal waters, territorial sea (i.e. up to the 12 nautical mile limit), and the associated airspace.

---

**8.11 Interception**

Interception takes place when traffic that has been acquired through [REDACTED] collection is subsequently forwarded to the traffic repository from the [REDACTED] (OPS-1-13)

---

**8.12 Metadata**

Information associated with a telecommunication to identify, describe, manage or route that telecommunication or any part of it as well as the means by which it was transmitted, but excludes any information or part of information which could reveal the purport of a telecommunication, the whole or any part of its content.

---

**8.13 [REDACTED] SIGINT Collection**

[REDACTED] SIGINT collection is the process of intercepting foreign communications as they [REDACTED] the GII. Traditionally, [REDACTED] collection has been done against [REDACTED]

---

**8.14 Private Communication**

“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”.

---

8.15 [REDACTED] is a [REDACTED] assigned by the intelligence community [REDACTED]

[REDACTED]

The following are examples of [REDACTED] used to define the scope of identifiers:

- \* [REDACTED]
  - \* [REDACTED]
  - \* [REDACTED]
- 

8.16 [REDACTED]

[REDACTED]

---

**8.17 Second Party**

In the SIGINT community, Second Party refers to CSE’s international counterparts and include: the U.S. National Security Agency (NSA), the UK Government Communications Headquarters (GCHQ), Australia’s Signals Directorate (ASD), and New Zealand’s Government Communications Security Bureau (GCSB).

---

8.18 [REDACTED]  
Data

[REDACTED]

---

**8.19 Strong Selection**

In the context of targeting activities, for a selection strategy to be considered strong, or effective, it must optimize the identification of communications of FI interest, and minimize the identification of communications of no FI interest.

One means of achieving strong selection is to [REDACTED]

[REDACTED]



The following are fictitious examples of strong selection strategies that may be forwarded to SIGINT collection systems:

- \* [REDACTED]
- \* [REDACTED]
- \* [REDACTED]

Strong selection may also be achieved through [REDACTED]



[REDACTED] a foreign entity of intelligence interest. These are addressed in separate instructions.

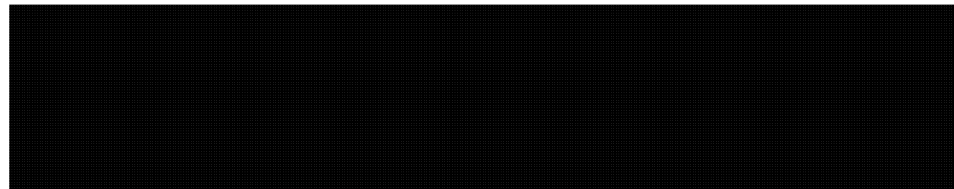
---

**8.20 Target  
(verb)**

To single out for collection or interception purposes. One “targets” an identifier to a collection system dictionary or directory (filtering and selection tool) to collect only wanted data.

---

**8.21 [REDACTED]  
[REDACTED]**



---

**8.22 Traffic**

Traffic is defined as the content or payload of a telecommunication or data plus the associated metadata acquired from the GII; this includes [REDACTED]



Annex 1: Summary of [REDACTED] Targeting Rules Under Part (a) of CSE’s Mandate

A1.1  
Introduction

The following table summarizes existing rules for [REDACTED] targeting activities conducted under Part (a) of the CSE Mandate (paragraph 273.64(1)(a) of the *National Defence Act* (NDA)), for intelligence reporting purposes.

A1.2 Table

If the targeted entity is...	may the following [REDACTED] collection sources be leveraged?	
	[REDACTED]	[REDACTED]
[REDACTED]	No <sup>1</sup>	No <sup>1</sup>
	No <sup>2</sup>	No
	No	No
	No <sup>2</sup>	No
	No <sup>2</sup>	No <sup>3</sup>
	Yes	Yes
	No <sup>2 &amp; 4</sup>	No <sup>4</sup>
	No <sup>2 &amp; 4</sup>	No <sup>4</sup>
	Yes	Yes
	No	No
	No <sup>4</sup>	No <sup>4</sup>
	Yes <sup>5</sup>	Yes <sup>5</sup>

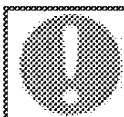
<sup>1</sup> The latest guidance from DLS is that [REDACTED] Solicitor-Client Privilege  
[REDACTED] Solicitor-Client Privilege

<sup>2</sup> For guidance on exceptional circumstances, contact Corporate and Operational Policy, D2.

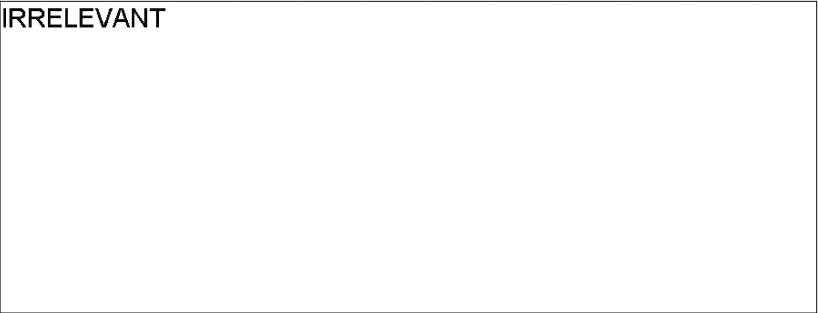
<sup>3</sup> Such targeting requires the approval [REDACTED]

<sup>4</sup> Collection of Electronic Intelligence (ELINT) and [REDACTED] are

approved, because the emitters of such signals have no expectation of privacy, and the acquisition activity is not directed at a particular entity, it is done in bulk.



IRRELEVANT

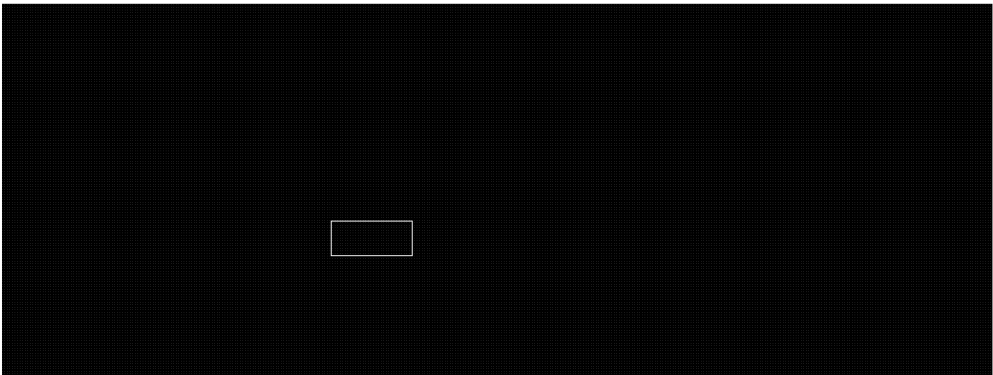




Annex 2: Guidance on [redacted]

(Originally Issued 3 September, 2010)

A2.1  
Overview



A2.2 Details



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

## Annex 3: Roles and Responsibilities For [REDACTED] Targeting

**A3.1 Roles and Responsibilities** Roles and responsibilities for [REDACTED] targeting under part (a) are outlined in the following table.

Step	Who Does It	Action						
1	Intelligence Analyst	<p>Documents the following information in the TKB and enters it in the appropriate [REDACTED] targeting service or mechanism:</p> <ul style="list-style-type: none"><li>* a foreign assessment (nationality and location digraphs) of entity of intelligence interest;</li><li>* one or more active GCR(s);</li><li>* a valid justification (expected FI value);</li><li>* a target identifier (TID) generated by the TKB;</li><li>* selectors (e.g., [REDACTED] such as email address and [REDACTED]); and,</li><li>* source of selectors (SIGINT traffic id, HUMINT information, etc.).</li></ul> <p>Includes other elements of information, if available, or appropriate:</p> <ul style="list-style-type: none"><li>* [REDACTED]</li><li>* [REDACTED]</li><li>* [REDACTED]</li><li>* [REDACTED]</li></ul> <p>Forwards request to [REDACTED] via email or targeting tool, as appropriate.</p>						
2	[REDACTED]	<p>Validates the targeting request and ensures that it is associated with:</p> <ul style="list-style-type: none"><li>* foreign entities located outside Canada;</li><li>* GC intelligence priorities;</li><li>* a valid justification; and,</li><li>* a target identifier (TID) generated by the TKB.</li></ul> <table><tr><th>If...</th><th>Then ...</th></tr><tr><td>Satisfied that request is compliant,</td><td>forwards to [REDACTED] at CSE, and [REDACTED] when appropriate.</td></tr><tr><td>Not satisfied,</td><td>returns request to sender with reason for denial. Sender may update request with supplemental information and resend to [REDACTED] when appropriate.</td></tr></table>	If...	Then ...	Satisfied that request is compliant,	forwards to [REDACTED] at CSE, and [REDACTED] when appropriate.	Not satisfied,	returns request to sender with reason for denial. Sender may update request with supplemental information and resend to [REDACTED] when appropriate.
If...	Then ...							
Satisfied that request is compliant,	forwards to [REDACTED] at CSE, and [REDACTED] when appropriate.							
Not satisfied,	returns request to sender with reason for denial. Sender may update request with supplemental information and resend to [REDACTED] when appropriate.							

3	[REDACTED] ([REDACTED]) Team	Reviews targeting request and establishes whether an existing [REDACTED] operation can meet the request.	
		<b>If...</b>	<b>Then ...</b>
		request can be met by existing operation,	Selectors are deployed and dataflow is established in accordance with applicable procedures.
4	Intelligence Analyst	request cannot be met by existing operation,	[REDACTED] assesses the requirement and drafts an operational plan, in accordance with applicable procedures.
		Reviews resulting traffic and updates or validates targeting request, as required. Requests must be validated at least once per year. If any of the compliance requirements become invalid (e.g. GCR has expired, traffic is not of intelligence value, etc.), the analyst must request that the associated [REDACTED] activities cease immediately.	

## Annex 4: Notifying Canadian Partners

---

### A4.1 Introduction

In the course of conducting FI activities, CSE may become aware that an entity of intelligence interest, which was initially assessed to be foreign and located abroad, is a Canadian citizen, or a citizen of an allied country, or is located in Canada or in allied territory. In these circumstances, CSE must cease all activities directed at the entity. This means that no information about the entity may be reported to partners after the point of discovery.

CSE operational managers may advise domestic partner agencies in receipt of SIGINT reporting in which the subject of a report was discovered post facto to be Canadian or of allied nationality, or was discovered to be located in Canada or in allied territory, that CSE has ceased all activities against associated subject. This is to ensure adequate handling of the SIGINT information.

---

### A4.2 Proposed Form of Words

Below is a proposed form of words to notify partners of an interruption in activities related to an inadvertent targeting or naming incident.

“As you may have noticed in CSE’s reporting database, reports [REDACTED] were cancelled because they did not comply with standard reporting practices. Further analysis has revealed that a subject of these reports is Canadian [or of allied nationality, or is in Canada, or allied territory], and as such, CSE is unable to pursue activities against this subject under its foreign intelligence mandate authorities [or under its international agreements in the case of allied subjects/territory]. We request that you please destroy/delete all copies of referenced reporting.

If you require clarification, please contact our Corporate and Operational Policy team in D2 [or call op manager?].

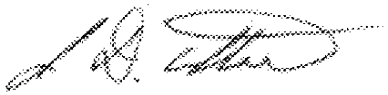
Should you wish to pursue a request for assistance, please contact CSE or your CSE liaison office, which will provide the requisite request template for signature from an executive or equivalent and forward to CSE.”

## CSOI-4-4 Promulgation

---

### Reviewed and Recommended for Approval

I have reviewed and hereby recommend these instructions for approval.



James Abbott  
Director General SIGINT Programs

19 December 2013

Date

---

### Approved

I hereby approve CSOI-4-4: *Targeting Identifiers For Foreign Intelligence* Under Part (a) of CSE's Mandate. These instructions are effective immediately.

Original signed by DC SIGINT

20 December 2013

Shelly Bruce  
Deputy Chief SIGINT

Date