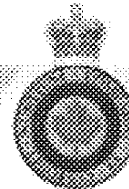




Communications Security  
Establishment Canada

Centre de la sécurité  
des télécommunications Canada

SECRET//SI



## Canadian SIGINT Operations Instruction CSOI-1-2

### The Canadian SIGINT Production Chain and Access to SIGINT Data

Last Updated:  
10 December 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 .....	5
1.6 Accountability.....	5
1.7 Amendment Process.....	6
1.8 Enquiries.....	6
1.9 Review .....	6
<b>2. THE CANADIAN SIGINT PRODUCTION CHAIN .....</b>	<b>7</b>
2.1 The Canadian SIGINT Production Chain .....	7
2.2 SIGINT Production Chain Activities .....	7
2.3 Outside the Canadian SIGINT Production Chain .....	8
2.4 Physical Security Requirements .....	8
<b>3. ACCESS TO RAW SIGINT DATA.....</b>	<b>9</b>
3.1 Raw SIGINT Data .....	9
3.2 Access to Raw SIGINT Data .....	9
3.3 Use of Raw SIGINT Data .....	10
3.4 Access to Raw SIGINT Data Under Part (b) of CSE's Mandate .....	10
3.5 Access to Raw SIGINT Data [REDACTED] .....	11
<b>4. ACCESS TO EVALUATED AND/OR ALTERED SIGINT DATA.....</b>	<b>12</b>
4.1 Evaluated SIGINT Data .....	12
4.2 Altered SIGINT Data .....	12
4.3 Sharing and Disseminating Evaluated and/or Altered SIGINT Data .....	12
4.4 Access to Altered SIGINT Data [REDACTED] .....	12
<b>5. ACCESS TO SIGINT PRODUCTS.....</b>	<b>13</b>
5.1 Non-Releasable SIGINT Products .....	13
5.2 Releasable SIGINT Products .....	13
<b>6. GRANTING ACCESS IN SPECIAL CIRCUMSTANCES .....</b>	<b>14</b>
6.1 Approval Process for Special Circumstances .....	14
<b>7. DEFINITIONS .....</b>	<b>15</b>
Altered SIGINT Data .....	15
Canadian Armed Forces SIGINT Technical Control Authority (CF STCA) .....	15
Canadian SIGINT Production Chain .....	15
Canadian SIGINT Production Chain Activities .....	15

**SECRET//SI**  
**CSOI-1-2**  
**10 December 2013**

Content.....16

Evaluated SIGINT Data.....16

Global Information Infrastructure.....16

Metadata.....16

Need-To-Know.....17

Non-releasable SIGINT products.....17

Raw SIGINT Data.....17

Releasable SIGINT Products.....17

Search Terms.....18

Second Parties.....18

Selectors.....18

SIGINT Clients.....18

SIGINT Data.....19

SIGINT Products.....19

.....19

**CSOI-1-2 PROMULGATION..... 20**

---

# 1. Introduction

---

- 1.1 Objective** The objective of these instructions is to define the Canadian SIGINT Production Chain, in order to determine who can have access to SIGINT data. Access to SIGINT data must be limited due to the potential for exposure to information about Canadians, as well as the potential for compromising SIGINT methods, sources and capabilities. SIGINT data refers to:
- Raw SIGINT data,
  - Evaluated and/or altered SIGINT data, and
  - Non-releasable SIGINT products.

SIGINT data does not refer to releasable SIGINT products.

As stated in the *Policy on Government Security*, CSE is the government's national authority for SIGINT and COMSEC, and is the lead security agency responsible for developing SIGINT-related policy instruments and providing advice and guidance to departments on the protection and distribution of SIGINT.

As such, these instructions introduce or refine the following terms:

- The Canadian SIGINT Production Chain
- Canadian SIGINT Production Chain activities
- Raw SIGINT data
- Evaluated and/or altered SIGINT data
- Non-releasable SIGINT products
- Releasable SIGINT products

- 
- 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** These instructions identify who may have access to SIGINT data and should be used in conjunction with CSSS-100 *Canadian SIGINT Security Standards* when making decisions to grant such access.

These instructions do not address the dissemination, release, disclosure, or sanitization of releasable SIGINT products.

- 1.4 References**
- *Policy on Government Security*, 1 July 2009
  - *Ministerial Directive on the Integrated SIGINT Operational Model (ISOM)*, May 2004
  - OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities*
  - OPS-1-1, *Procedures for Release of Suppressed Information from SIGINT Reports*
  - OPS-1-7, *Operational Procedures for Naming in SIGINT Report*
  - OPS-1-8, *Active Monitoring of Operations to Ensure Legal Compliance and the Protection of the Privacy of Canadians*
  - CSSS-100, *The Canadian SIGINT Security Standards*
  - CSOI-1-1, *The National SIGINT Priorities List Process*
  - CSOI-4-1, *SIGINT Reporting*
  - CSOI-4-2, *Producing Gists for Indications and Warning Purposes*

**1.5 Application** These instructions apply to all individuals and elements within the Canadian SIGINT System authorized to conduct SIGINT activities under the authority of DC SIGINT. This includes Information Technology Security (ITS), Government of Canada (GC), Second Party integrees and personnel operating under the authority of the Canadian Armed Forces (CAF) SIGINT Technical Control Authority (STCA).

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

Who	Responsibility
Deputy Chief SIGINT	Approving these instructions
Director General SIGINT Programs	Recommending these instructions for approval
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)	<ul style="list-style-type: none"> <li>Applying these instructions</li> </ul>
All CSE managers and CAF/DND leaders and supervisors who are affected by these instructions	Ensuring that their staff have read, understood and comply 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** Amendments to these instructions may be required because of changing requirements or unforeseen circumstances. All approved amendments will be announced to staff and posted on the SIGINT Programs Oversight and Compliance (SPOC) web pages.

---

**1.8 Enquiries** Questions related to these instructions should be directed to Operational Managers who in turn will consult with SPOC staff. E-mail inquiries can also be directed to [spoc-staff-dl@cse-cst.gc.ca](mailto:spoc-staff-dl@cse-cst.gc.ca).

---

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

---

## 2. The Canadian SIGINT Production Chain

---

### 2.1 The Canadian SIGINT Production Chain

The Canadian SIGINT Production Chain refers solely to the production and use of SIGINT. This is limited to SIGINT activities conducted under the authority of DC SIGINT, including delegated activities.

To be considered part of the SIGINT Production Chain, individuals must be:

- a CSE employee;
  - a CSE contractor;
  - a GC secondee working at CSE and under the direction of CSE SIGINT management;
  - a CAF member posted to CSE and under the direction of CSE SIGINT management;
  - a CAF or civilian member of Canadian Forces Information Operations Group (CFIOG) or other member of the CAF operating under the CAF STCA;
  - a Second Party [REDACTED] intergee [REDACTED]  
[REDACTED]
  - a deployed CSE employee working under DC SIGINT authority; or
  - a deployed CAF member working under the authority of the CAF STCA.
- 

### 2.2 SIGINT Production Chain Activities

The SIGINT Production Chain refers to those individuals, elements and components that engage in the following:

- *SIGINT-enabling activities:* [REDACTED]
- [REDACTED]

- *SIGINT production activities:* These include activities or tradecraft that use information acquired from the Global Information Infrastructure (GII) to generate foreign intelligence. Examples include: [REDACTED] analysis, reporting and evaluation of intelligence value.

- *SIGINT oversight activities:* These include activities or processes designed to assess and ensure the proper handling of SIGINT data. Examples include: monitoring for compliance with legislation, ministerial direction and policy instruments, creating and amending policy instruments, audit and review.
- *CSE activities associated with protecting networks of importance to the Government of Canada:* [REDACTED]

[REDACTED]

### 2.3 Outside the Canadian SIGINT Production Chain

Individuals who do not conduct Canadian SIGINT Production Chain activities are not treated as a part of the chain and therefore are not eligible for access to SIGINT data. Examples of activities that are not part of the chain include:

- Oversight of activities in SIGINT organizations not directly related to SIGINT business. This includes, but is not limited to: evaluation, management accountability for human resources purposes, financial audit, and personnel security reviews;
- SIGINT product dissemination conducted by persons who are not CSE staff or CAF members, and who are operating outside of the authority of the CAF STCA;
- Liaison with or by GC departments and Second Parties, [REDACTED] activities;
- Operational activities of CSE personnel or CAF members integrated at other organizations and whose activities are governed by the host organizations; and
- Creation of products (e.g. assessments, briefings, etc.) by certain clients.

### 2.4 Physical Security Requirements

In addition, individuals accessing SIGINT data must:

- Be operating in an accredited SIGINT Secure Area (SSA), also known as a Sensitive Compartmented Information Facility (SCIF);
- Be cleared for TOP SECRET (TS); and
- Hold a SIGINT Information Access (SIA) indoctrination.



---

### 3. Access to Raw SIGINT Data

---

#### 3.1 Raw SIGINT Data

Raw SIGINT data is information acquired by Canadian or Allied SIGINT collection activities that has not been evaluated for foreign intelligence or privacy considerations; this may be communications or non-communications content or metadata. Raw SIGINT data includes information acquired through targeted collection operations against foreign intelligence targets as well as research and development activities (e.g. network analysis, signals analysis).

---

#### 3.2 Access to Raw SIGINT Data

Access to raw SIGINT data must be limited due to the potential for exposure to information about Canadians, as well as the potential for compromising SIGINT methods, sources and capabilities.

Individuals conducting Canadian SIGINT Production Chain activities under the authority of DC SIGINT (or delegated authorities) can have access to raw SIGINT data as needed to fulfill their official duties.

Within CSE, direct supervisors of personnel who conduct SIGINT activities under the authority of DC SIGINT are responsible for requesting access to raw SIGINT data as needed to fulfill official duties.

Within the CAF, direct supervisors of personnel who conduct raw SIGINT activities under the authority of the CAF STCA are responsible for requesting access to raw SIGINT data as needed to fulfill official duties. Access requests are assessed and authorized according to the established chain of command.

To ensure that any policy and/or tradecraft-training requirements for access to raw SIGINT data access have been met, supplementary review mechanisms and prerequisites may be put in place for account requests.

Managers must ensure that appropriate procedures for proper handling of the information as well as an intelligence oversight reporting processes are established and documented.

Managers are responsible for ensuring that access is removed, as necessary, when an employee changes positions or leaves the Canadian SIGINT Production Chain.

### 3.3 Use of Raw SIGINT Data

Once access is granted, the protection of SIGINT methods, sources, and capabilities is dependent upon the rigorous application of these instructions, *The Canadian SIGINT Security Standards (CSSS)* and other referenced handling standards.

Individuals accessing raw SIGINT data for the purpose of enabling the production of SIGINT shall:

- Conduct activities only in support of their official duties and to the extent necessary to do their job;
- Apply measures to protect the privacy of Canadians and ensure legal compliance in the conduct of their SIGINT activities, and act in accordance with all relevant SIGINT legislation, ministerial direction and policy instruments;
- Employ only those selectors and/or search terms reasonably likely to produce information in support of clearly identified GC foreign intelligence priorities and in accordance with OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities*; and
- Prevent unauthorized access to raw SIGINT data by applying appropriate security measures.

### 3.4 Access to Raw SIGINT Data Under Part (b) of CSE's Mandate

ITS personnel located in the [REDACTED] and with [REDACTED] can be granted access to raw SIGINT data [REDACTED]

[REDACTED] With their management's recommendation, ITS personnel within those offices will be granted access following formal notification to IPOC and SPOC. ITS personnel in other offices may be granted access to raw SIGINT data dependent on the approval of SPOC and SIGINT Office of Primary Interest (OPI) concurrence. Any request for access to [REDACTED] auditable SIGINT databases must follow [REDACTED] established policy requirements. As part of the SIGINT Production Chain individuals noted above are subject to all provisions outlined in SIGINT policy instruments that govern the handling, storage and dissemination of SIGINT data. Provisions include, but are not limited to, the annual OPS-1 quiz and the biannual "SIGINT and the Law" briefing. It is incumbent on individuals granted access under this section to notify SPOC and IPOC if their circumstances change and they are no longer employed in the appointment under which they received this access.

3.5 Access to  
Raw SIGINT  
Data [REDACTED]  
[REDACTED]

Raw SIGINT data including content and associated metadata, which has been targeted (i.e., selected traffic) by approved [REDACTED] selectors, is provided to the targeting [REDACTED] Non-selected, unaltered raw SIGINT data (i.e., unselected, unminimized metadata) [REDACTED]

**Note:** The provision of *unknown data* to [REDACTED] for technical analysis is dealt with in OPS-1-13, *Operational Procedures Related to Canadian [REDACTED] Collection Activities*.

---

## 4. Access to Evaluated and/or Altered SIGINT Data

---

### 4.1 Evaluated SIGINT Data

Evaluated SIGINT data is raw SIGINT data that has been evaluated for foreign intelligence value.

---

### 4.2 Altered SIGINT Data

Altered SIGINT data is raw SIGINT data that has been altered to protect the privacy of Canadians (e.g., through minimization or suppression), or to protect source information (e.g., sanitization).

---

### 4.3 Sharing and Disseminating Evaluated and/or Altered SIGINT Data

Individuals conducting Canadian SIGINT Production Chain activities under the authority of DC SIGINT (or delegated authorities) who wish to share and/or disseminate SIGINT data to partners and clients outside the SIGINT Production Chain may only do so via a releasable SIGINT product.

---

### 4.4 Access to Altered SIGINT Data

Raw SIGINT data consisting solely of metadata may be made accessible to [REDACTED] as long as identifiers known to belong to Canadians or persons located in Canada are altered in such a way as to render them impossible to identify the persons to whom the identifiers relate.

---

---

## 5. Access to SIGINT Products

---

### 5.1 Non-Releasable SIGINT Products

Non-releasable SIGINT products do not conform to all of the necessary requirements for releasable SIGINT, and include:

- Gists (Indications & Warnings); for more information, please refer to CSOI-4-2, *Producing Gists for Indications and Warning Purposes*;
- Technical SIGINT Reports (Cryptologic/Communications Information Reports (CIR) [REDACTED])
- [REDACTED]

---

### 5.2 Releasable SIGINT Products

Releasable SIGINT products have been:

- Evaluated and deemed to hold foreign intelligence value;
- Associated with clearly identified GC foreign intelligence requirements (GCRs);
- Altered to protect the privacy of Canadians, in accordance with OPS-1-7, *Operational Procedures for Naming in SIGINT Reports*, as necessary;
- Refined to comply with reporting standards and to protect SIGINT methods and sources; and
- Approved for release according to the procedures outlined in OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities* and CSOI-4-1, *SIGINT Reporting*.

Releasable SIGINT products that meet all of these requirements are eligible for release to SIGINT clients and include the following:

- Canadian, [REDACTED] End-Product Reports (EPRs)
  - Advance Reports
  - SIGINT Summaries and Assessments
  - Information Items
  - Tactical Reports (TACREPs)
-

---

## 6. Granting Access in Special Circumstances

---

### 6.1 Approval Process for Special Circumstances

Under exceptional circumstances, individuals outside the Canadian SIGINT Production Chain may be granted access to SIGINT data. This includes:

- Any CAF or DSO personnel who are deployed under DC SIGINT or CAF STCA authority and operating [REDACTED] and are required to [REDACTED] SIGINT [REDACTED] and [REDACTED] personnel.

All such requests must be sent to Manager SPOC, and must include:

- Specifics of whom the exemption is for;
- Specifics of what [REDACTED] data is needed;
- A justification for why the exception is required; and
- An explanation for why access to existing releasable SIGINT products is not sufficient.

Manager SPOC will review and approve requests and consult with Director SPR if required.

All CAF requests will be forwarded to CFIOG Oversight and Compliance for review, and then forwarded to SPOC.

---

---

## 7. Definitions

---

**Altered  
SIGINT Data**

Raw SIGINT data that has been altered to protect the privacy of Canadians (e.g. through minimization or suppression).

---

**Canadian  
Armed Forces  
SIGINT  
Technical  
Control  
Authority (CF  
STCA)**

The Canadian Armed Forces authority responsible for the management of CAF SIGINT and the oversight of CAF SIGINT to ensure compliance with National and CAF SIGINT policies, orders, directives, procedures and standards.

Under the framework of the Integrated SIGINT Operational Model, the CAF STCA operates under the delegated authority of DC SIGINT. The CAF STCA will normally be assigned [REDACTED]

The CAF STCA is responsible for SIGINT technical control over all CAF SIGINT operations, [REDACTED] regardless of the chain of command of the units actually conducting the operations.

---

**Canadian  
SIGINT  
Production  
Chain**

The Canadian SIGINT Production Chain refers to SIGINT enabling, production or oversight activities conducted under the authority of DC SIGINT, including those activities delegated to non-CSE organizations. This does not include the consumption of SIGINT Products, but does include the activities that enable consumption.

---

**Canadian  
SIGINT  
Production  
Chain Activities**

The SIGINT Production Chain refers to those individuals, elements and components that produce and use of SIGINT by engaging in the following activities:

- *SIGINT Enabling activities:* [REDACTED]
- [REDACTED]

[REDACTED]

- *SIGINT Production activities:* These are any activity or tradecraft that uses information acquired from the GII to create foreign intelligence. Examples include, but are not limited to: [REDACTED] analysis, reporting and evaluation of intelligence value.
- *SIGINT Oversight activities:* These are any activity or process designed to assess and ensure the proper handling of SIGINT Data. Examples include, but are not limited to: monitoring for compliance with legislation, Ministerial direction and policy instruments, creating and amending policy instruments, audit and review.
- *Protecting networks of importance to the Government of Canada activities:* [REDACTED]

[REDACTED]

---

<b>Content</b>	Content is defined as the message substance (voice or text, for example) of the communication. [REDACTED] [REDACTED] [REDACTED]
----------------	---

---

<b>Evaluated SIGINT Data</b>	Raw SIGINT data that has been evaluated for foreign intelligence value.
------------------------------	---

---

<b>Global Information Infrastructure</b>	The 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.
--	---

---

<b>Metadata</b>	Metadata is defined as 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, or the whole or any part of its content.
-----------------	---

---



---

**Need-To-Know** Need-to-know is a determination made by an authorized holder of information to assess whether a possible recipient requires access to that information in order to perform an authorized GC function. Need-to-know is a fundamental aspect of CSE's information handling system and is a way of further restricting access to classified and protected information. It reflects the principle that not everyone who is cleared to see certain information necessarily needs to see all of it. See CSSS-100 Canadian SIGINT Security Standards.

---

**Non-releasable SIGINT products** Non-releasable SIGINT products do not conform to all of the necessary requirements for releasable SIGINT, and include:

- Gists (Indications & Warnings); for more information, please refer to CSOI-4-2, *Producing Gists for Indications and Warning Purposes*;
- Technical SIGINT Reports (Cryptologic/Communications Information Reports (CIR) [REDACTED])
- [REDACTED]

---

**Raw SIGINT Data** SIGINT data is any SIGINT information acquired as a result of research and development, or from targeted collection operations against a particular foreign intelligence target, before the information has been evaluated for foreign intelligence value and altered to protect the privacy of Canadians. It may consist of content and/or metadata. Content is defined as the message substance (voice or text) of the communication. [REDACTED]

---

**Releasable SIGINT Products** Releasable SIGINT products are SIGINT products that:

- Have been evaluated and deemed to hold foreign intelligence value;
- Respond to clearly identified Government of Canada foreign intelligence requirements (GCRs);
- If necessary, has been altered to protect the privacy of Canadians, in accordance with OPS-1-7, *Operational Procedures for Naming in SIGINT Reports*;
- Have been refined to comply with reporting standards and to protect

- SIGINT methods and sources; and
- Have been approved for release according to the procedures outlined in OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities* and CSOI-4-1, *SIGINT Reporting*.

---

**Search Terms** Search terms are terms (which may or may not include a wildcard) used for purpose of querying in SIGINT databases in order to identify traffic for further analysis.

---

**Second Parties** Second Parties refer to CSE's SIGINT counterparts and include: the US National Security Agency (NSA), the UK Government Communications Headquarters (GCHQ), Australian Signals Directorate (ASD), and New Zealand's Government Communications Security Bureau (GCSB).

---

**Selectors** Selectors may include a name, [REDACTED], IP or e-mail address, facsimile or telephone number, or other alphanumeric character stream [REDACTED] for the purpose of identifying traffic that relates to national foreign intelligence requirements and isolating it for further processing.

---

**SIGINT Clients** A SIGINT client is a person employed in a GC client organization authorized to receive SIGINT who uses this information for strategic warning, policy formulation, decision-making, and/or day-to-day assessment of foreign entities' capabilities and intentions.

Specific GC organizations could include:

- Department of National Defence (DND) and the Canadian Armed Forces (CAF);
- Department of Foreign Affairs, Trade and Development Canada (DFATD);
- Citizenship and Immigration Canada (CIC);
- Canadian Security Intelligence Service (CSIS); and
- Privy Council Office (PCO).

**Note:** Normally, client organizations are federal-level government departments and agencies, including overseas missions and military commands, but they can also include private contractors of such organizations.

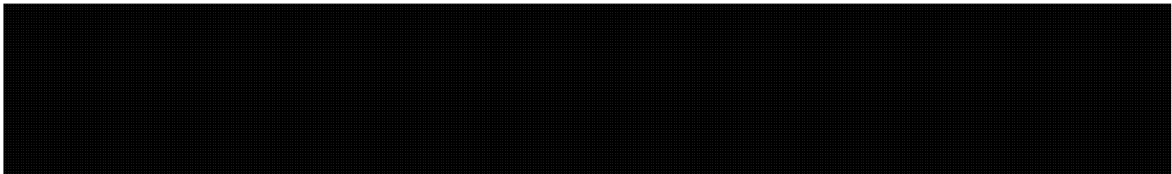
---

<b>SIGINT Data</b>	SIGINT data refers to raw SIGINT data, evaluated and/or altered SIGINT data, and non-releasable SIGINT products. SIGINT data does not refer to releasable SIGINT products.
--------------------	--

---

<b>SIGINT Products</b>	SIGINT products are based on SIGINT data and respond to identified GC foreign intelligence priorities. SIGINT products fall into two categories: releasable (to clients) and non-releasable (limited to the SIGINT Production Chain).
------------------------	---

---



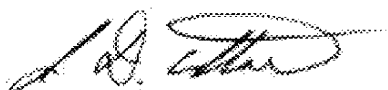
---

## CSOI-1-2 Promulgation

---

### Reviewed and Recommended for Approval

I have reviewed and hereby recommend these instructions for approval.



James Abbott  
Director General Production

26 March 2014

Date

---

### Approved

I hereby approve CSOI-1-2: *The Canadian SIGINT Production Chain and Access to SIGINT Data*. These instructions are effective immediately.

Original signed by DC SIGINT

Shelly Bruce  
Deputy Chief SIGINT

26 March 2014

Date