



Communications Security
Establishment Canada

Centre de la sécurité
des télécommunications Canada



OPS-1-13

Operational Procedures Related to
Canadian [REDACTED] Collection Activities

OPERATIONAL POLICY

Canada

Table of Contents

1. Introduction.....	1
Policy Scope and Application.....	1
Legal Authorities	4
2. DESCRIPTION OF [REDACTED] COLLECTION PROGRAMS	6
[REDACTED]	6
[REDACTED]	9
[REDACTED]	9
[REDACTED]	11
3. APPROVAL PROCESS FOR [REDACTED] COLLECTION ACTIVITIES	12
4. DATA COLLECTION - ALL PROGRAMS	14
Collection – Traffic.....	14
Collection – Metadata	15
5. DATA USE AND RETENTION – ALL PROGRAMS	16
Use – Traffic	16
Use – Metadata	18
Use – Unknown Data	19
Retention	20
6. DATA SHARING - ALL PROGRAMS.....	21
7. ACCOUNTABILITY FOR OPS-1-13	24
8. Definitions.....	26
Annex 1 – Personal Information	35

1. Introduction

Policy Scope and Application

1.1 Scope

These procedures govern CSEC's [REDACTED] collection activities carried out under paragraph 273.64(1)(a) of the *National Defence Act* (NDA) (part (a) of the Mandate), which comprise:

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



FYI: These procedures address [REDACTED] collection activities conducted under part (a) of the Mandate only. For activities conducted under 273.64(1)(c) of the NDA (part (c) of the Mandate), see OPS-4-1, *Operational Procedures for Assistance to Law Enforcement and Security Agencies under Part (c) of the CSEC Mandate*. For information on CSEC's [REDACTED] activities, see OPS-3-1.



Note: The terms “collection” and “interception” have been redefined. For further information, see Chapter 8.

1.2 Objective

The purpose of these procedures is to:

- document the approval processes for conducting these programs¹
- prescribe an accountability trail for these activities

Continued on next page

¹ In these procedures, the term “program” is to be read as encompassing or equating to the terms “activity” and/or “class of activities”, where applicable.

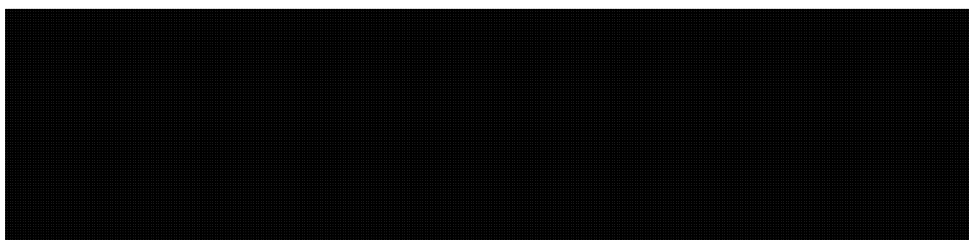
1.2 Objective
(continued)

- provide direction to those involved in these programs regarding the collection, use and retention of associated data acquired pursuant to Ministerial Directives (MDs)² and Ministerial Authorizations (MAs), and
- outline measures in place to protect the privacy of Canadians as required by:
 - paragraph 273.64(2)(b) of the NDA
 - the *Ministerial Directive on the Privacy of Canadians*
 - OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities*

1.3 Policy

All CSEC SIGINT [REDACTED] collection described herein, aimed at acquiring foreign intelligence (FI), must:

- comply with the relevant laws of Canada, including the *Charter of Rights and Freedoms*, the *Privacy Act*, the *Criminal Code*, and the NDA
- comply with all relevant MDs, including the
 - *Ministerial Directive on the Privacy of Canadians*
 - *Ministerial Directive on the Collection and Use of Metadata*
 - *Ministerial Directive on CSE's Accountability Framework*, and
 - *Ministerial Directive on the Integrated SIGINT Operational Model*
- comply with the MA in force related to the specific activity or class of activities
- comply with relevant policies and procedures
- be directed against foreign entities located outside Canada and linked to Government of Canada (GC) intelligence priorities
- be subject to measures to protect the privacy of Canadians in the use and retention of intercepted information, and
- be carried out only with the knowledge and approval of CSEC management.



Continued on next page

² Throughout these procedures, each reference to a MD is a reference to the most recent edition of that MD.

1.3 Policy
(continued)

[REDACTED]

**1.4 Involvement
of other GC
Departments or
Agencies**

CSEC may work with the Canadian Forces Information Operations Group (CFIOG), or other GC departments or agencies, while undertaking any [REDACTED] collection activity described in these procedures.

1.5 Application

These procedures apply to CSEC and CFIOG staff, secondees, contractors, integrees and any other parties who are involved in, or make use of data from, any of the following programs conducted under the authorities noted in this chapter:

[REDACTED]

**1.6 Previous
Procedures**

These procedures supersede OPS-1-13, *Procedures for Canadian* [REDACTED] [REDACTED] dated 1 December 2010.

Legal Authorities

- 1.7 Authorities** CSEC conducts its [REDACTED] collection activities under the authority of:
- paragraph 273.64(1)(a) of the NDA, which directs CSEC “to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence priorities”
 - the *Ministerial Directive on the Collection and Use of Metadata*, and
 - a valid MA.³
-
- 1.8 Privacy Protection Measures** All activities conducted pursuant to part (a) of the Mandate must:
- not be directed at Canadians anywhere or any person in Canada, and
 - be subject to measures to protect the privacy of Canadians in the use and retention of intercepted information.
-
- 1.9 MA Conditions and Requirements** In issuing an MA, the Minister of National Defence (“the Minister”) requires that the following conditions be met:
- the interception will be directed at foreign entities located outside Canada
 - the information to be obtained could not reasonably be obtained by other means
 - the expected foreign intelligence 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 to ensure that private communications will only be used or retained if they are essential to international affairs, defence or security.
- The Minister also requires special handling of solicitor-client communications (see the related paragraph in OPS-1).
-

³ Because the collection programs governed by these procedures may result in the interception of private communications, each program may be conducted only with a valid MA issued pursuant to subsection 273.65(1) of the NDA. An MA authorizes CSEC [REDACTED] or the CFIOG, as applicable, to intercept private communications acquired through the class of activities described in the MA for that program. Private communications may be intercepted for the sole purpose of obtaining foreign intelligence in accordance with GC intelligence priorities.

**1.10 Informing
the Minister**

**Information Relating to Private Communications and Solicitor-Client
Communications**

The MAs in force for the SIGINT programs described in these procedures require that CSEC record and report to the Minister information relating to private communications and solicitor-client communications. (See paragraph 5.1 for more information.)

Serious Issues (MA-related)

The Chief, CSEC must also report to the Minister when any serious issue arises in the implementation of the MAs, including but not limited to a sustained substantial decrease in the value of these sources of foreign intelligence, or any sustained major increase in recognized private communications or solicitor-client communications. All such serious issues are to be reported as soon as possible to SIGINT Programs Oversight and Compliance (SPOC) and Corporate and Operational Policy (D2). Where there is no such issue, an explicit statement to this effect must be inserted in the report to the Minister referred to in para 5.1.

Serious Issues (Not MA-related)

Whenever there is a serious issue which may not be related to an MA, it is to be reported as soon as possible to SIGINT Programs Oversight and Compliance (SPOC) and to Corporate and Operational Policy (D2). In this context, a "serious issue" is any issue, event or development pertaining to Canadian [REDACTED] collection activities which could represent or lead to non-compliance with para's 1.3, 1.8 or 1.9 of these procedures, or otherwise have potential implications for lawfulness, privacy or Ministerial reporting.

2. DESCRIPTION OF [REDACTED] COLLECTION PROGRAMS

2.1 General This chapter describes each of the four [REDACTED] collection programs.

[REDACTED]

**2.2 [REDACTED]
Program
Description**

[REDACTED]

2.3 [REDACTED]

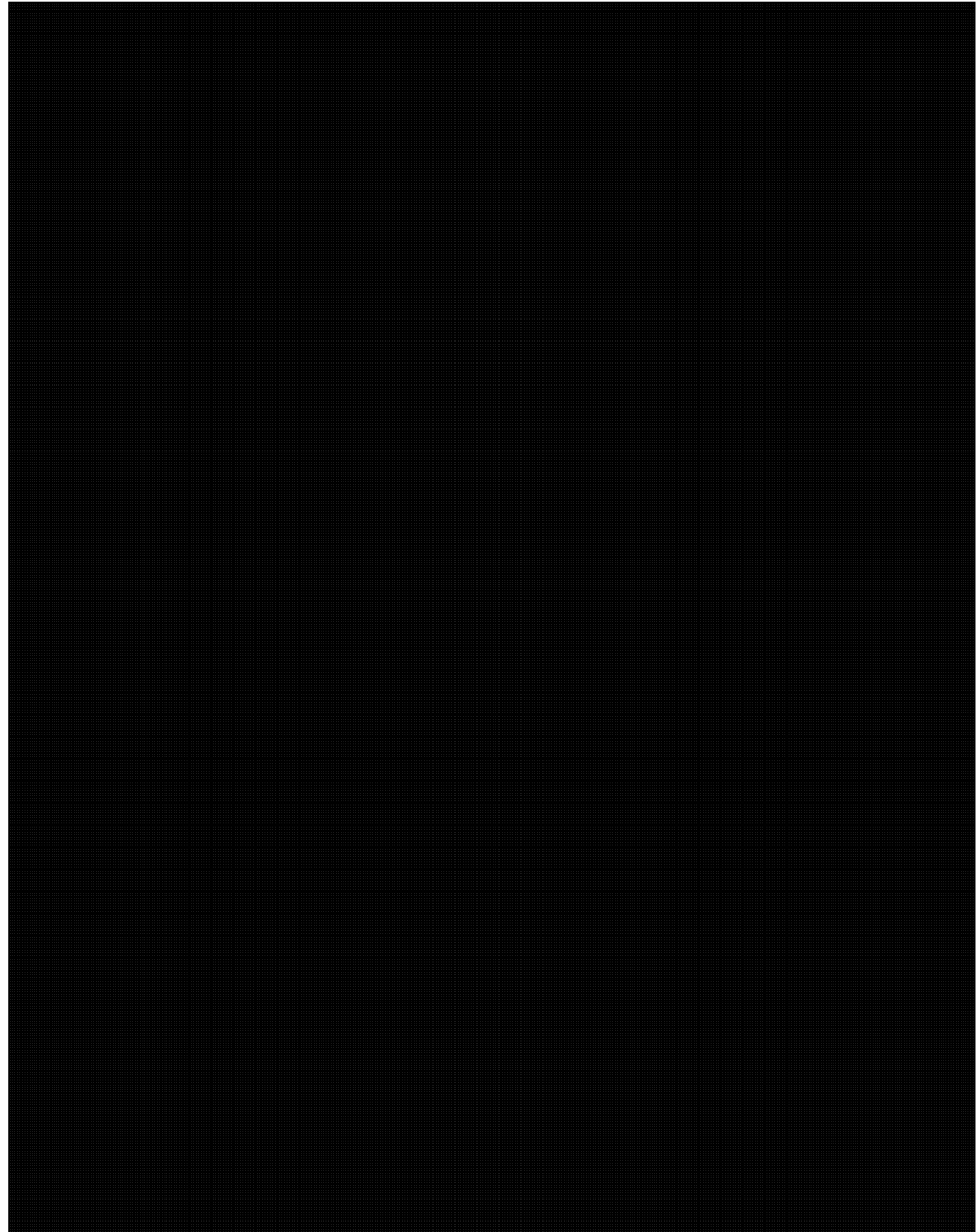
[REDACTED]

Continued on next page

2.3 [REDACTED]
(continued)

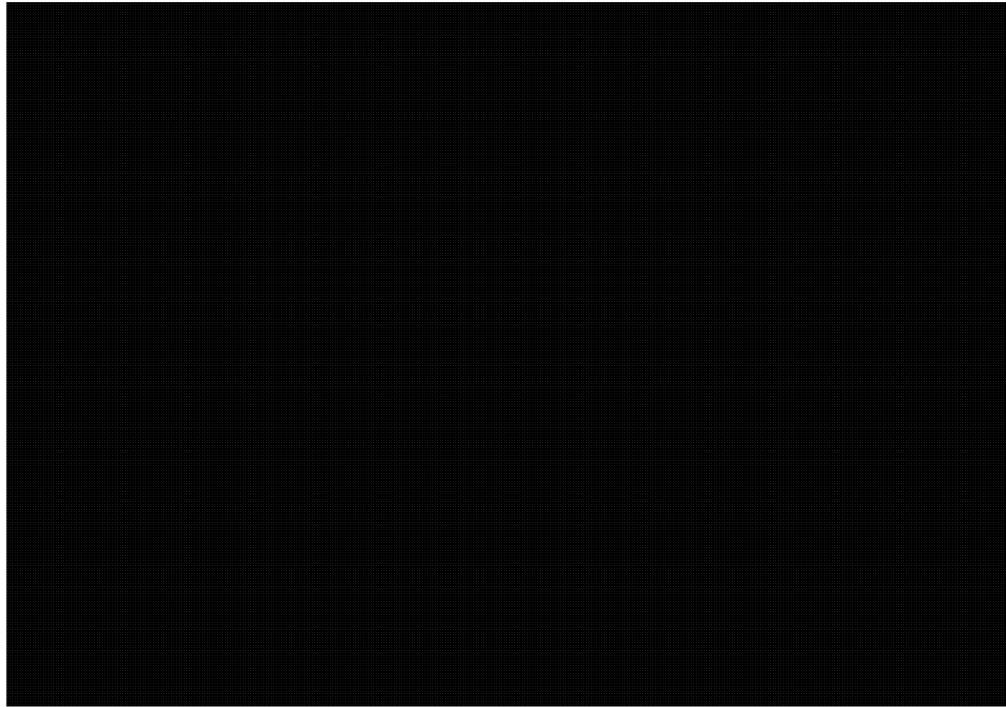


2.4 [REDACTED]
SIGINT
Development
Activities

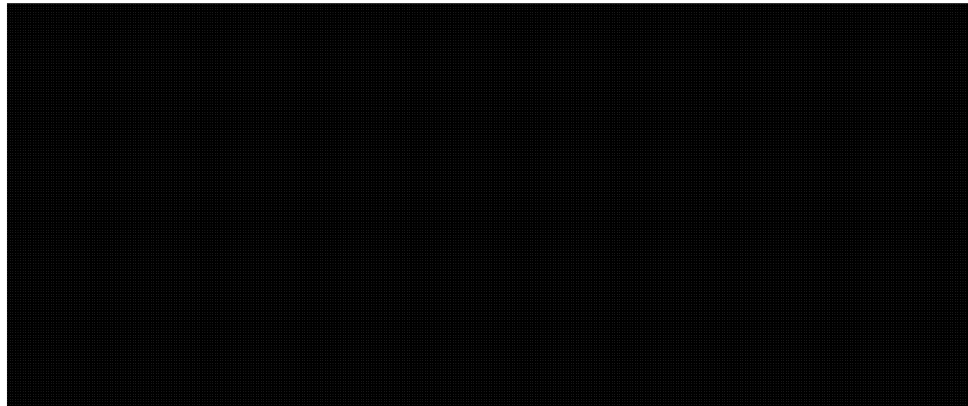


Continued on next page

2.4 [REDACTED]
SIGINT
Development
Activities
(continued)



2.5 [REDACTED]
SIGINT
Development:
Metadata



[REDACTED]

2.6 [REDACTED]

**Program
Description**

[REDACTED]

[REDACTED] is protected
under ECI [REDACTED]

[REDACTED]

2.7 [REDACTED]

**Program
Description**

[REDACTED]

2.8 [REDACTED]

**Program
Activities**

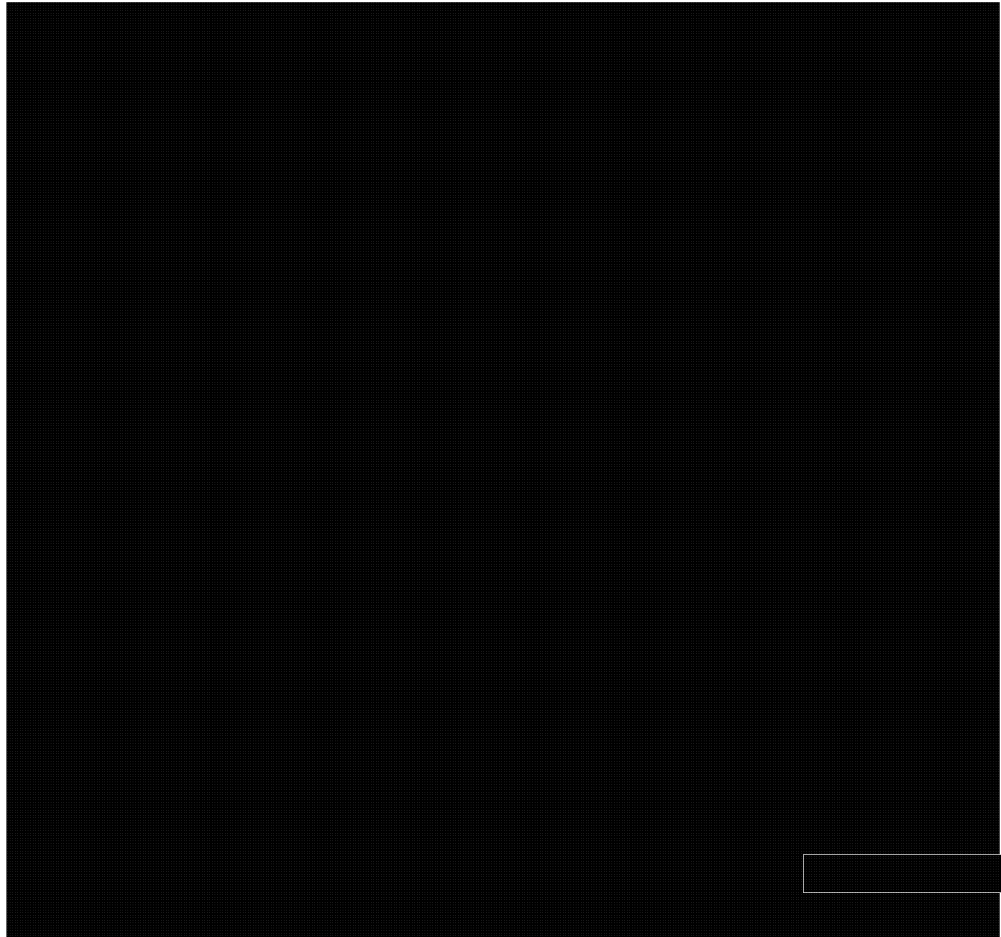
[REDACTED]

2.9 [REDACTED]

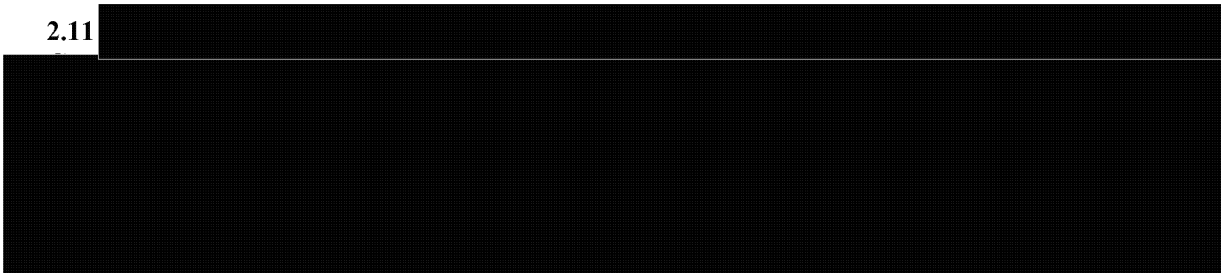
[REDACTED]

[REDACTED]

2.10



2.11

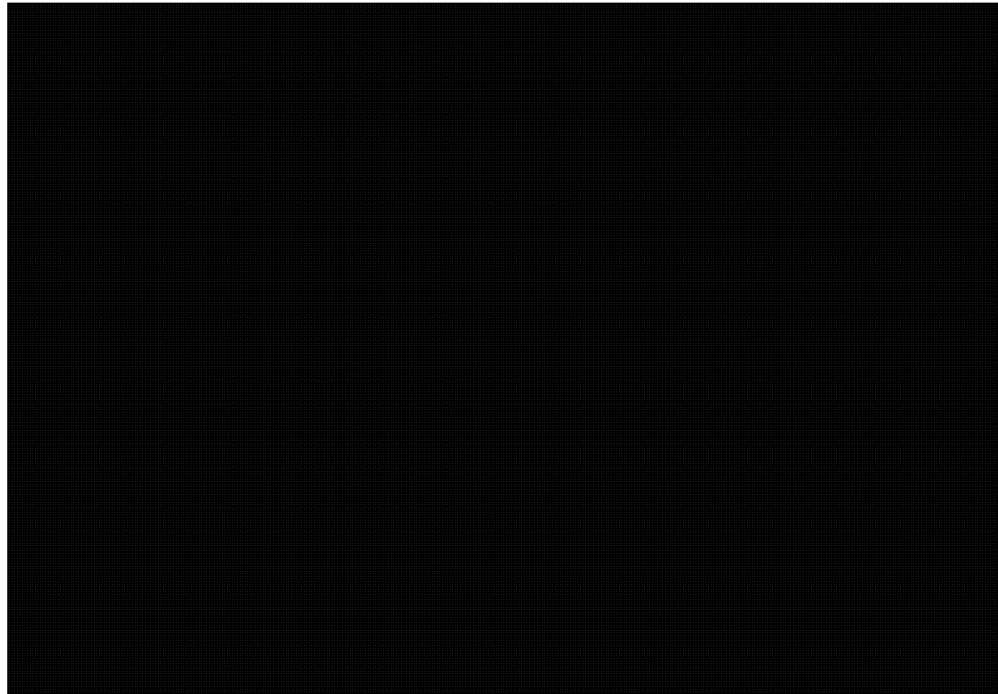


2.12

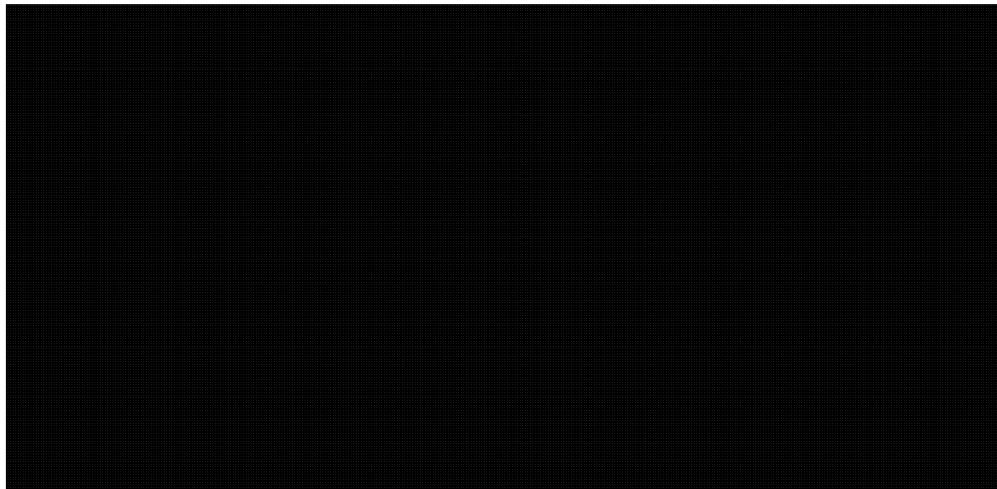




2.13
Description of



2.14
Activities



3. APPROVAL PROCESS FOR [REDACTED] COLLECTION ACTIVITIES

3.1 Introduction

This chapter describes the approval process for all CSEC [REDACTED] collection activities.

3.2 Approval Process - all programs

The approval process for conducting [REDACTED] collection activity, including, where applicable, [REDACTED] and SIGINT Development, is normally initiated by the submission to [REDACTED] of an intelligence requirement by CSEC SIGINT staff or CFIOG staff. Approval to conduct [REDACTED] collection activity aimed at responding to the intelligence requirement is then requested through the submission to [REDACTED] of an Activity Authorization Request (AAR), unless it can be conducted under an existing approval. Director, SIGINT Requirements is responsible to promulgate detailed guidance on the AAR approval process, subject to the provisions of these procedures. (The detailed guidance can be found on the SPOC website, under "Quick References".)

All [REDACTED] collection activities must be reviewed and approved by both the Director, SIGINT Requirements and Director, [REDACTED]. Approval can be given on either an annual or a case-by-case basis, in accordance with detailed guidance promulgated by the Director, SIGINT Requirements.

In the absence of the Director, SIGINT Requirements or the Director, [REDACTED], anyone acting officially in these positions or at a higher management level may act as approval authority. No downward delegation is permitted.

3.3 Additional Approvals Required for [REDACTED]

- the Minister of National Defence

The Director, SIGINT Requirements is responsible to promulgate detailed guidance regarding these additional approvals and the process for requesting them.

**3.4 Additional
Approvals
Required for**
[REDACTED]

All [REDACTED] require approval by senior CSEC officials. The Director, SIGINT Requirements is responsible to promulgate detailed guidance regarding these additional approvals and the process for requesting them.

4. DATA COLLECTION - ALL PROGRAMS

Collection – Traffic

4.1 Targeting Rules: Canadians

Collection must not be directed against Canadians located anywhere, or against anyone located in Canada.

Selectors

For targeting purposes, selectors must meet the definition of the term “metadata” in the *Ministerial Directive on the Collection and Use of Metadata*.

Consequently, a selector can only be used to collect a communication where CSEC is satisfied that it is foreign and relates to the external component of the communication – that is, a foreign telephone number, internet protocol (IP) address or e-mail address, etc. [REDACTED]

[REDACTED]

Selectors are obtained from a number of sources including, but not limited to:

- open source information
- analysis of previous SIGINT collection, and
- information provided by SIGINT clients, allies and partner intelligence agencies (e.g. HUMINT).

Targeting

Prior to any targeting and before collection systems are tasked to collect communications, CSEC personnel must be satisfied, based on all the information that CSEC has available to it at the time, that the proposed selectors are associated with a foreign entity located outside Canada, and relate to a GC intelligence priority. Once satisfied of this, analysts may submit selectors to [REDACTED] for targeting.


[REDACTED] staff must review submitted selectors prior to forwarding them to the collection system(s). Once [REDACTED] staff has validated that the selector is properly formatted, directed at a foreign entity located outside of Canada, and that it is related to a GC intelligence priority, the selector is forwarded to the collection system(s).

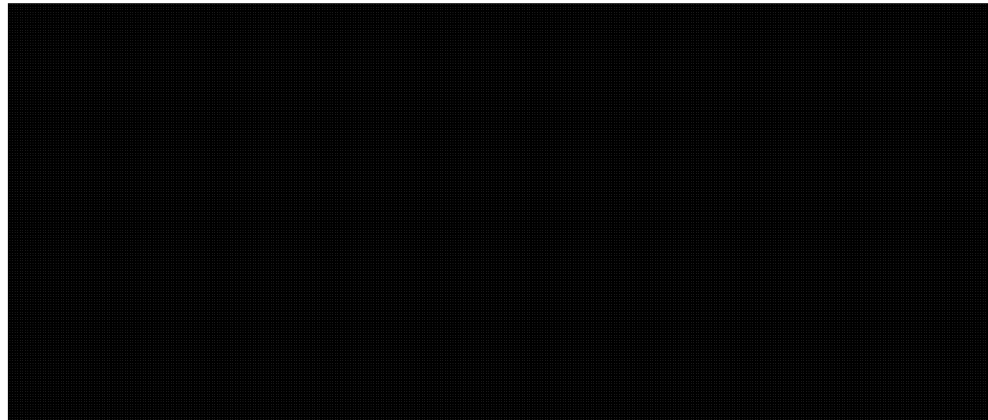
4.2 Inadvertent Targeting of Canadians

Refer to OPS-1 for the actions to be taken in the event that a Canadian anywhere or anyone located in Canada is inadvertently targeted, or in the unlikely event that communications having both the originator and the recipient in Canada are intercepted.

4.3 Targeting Rules: Second Parties

The relationship among the Five-Eyes SIGINT agencies is based on the *Canada-U.S. COMINT Agreement*, the *British-U.S. Communication Intelligence Agreement*, and other conventions where the agencies recognize each other's state sovereignty and show respect for each other's laws by pledging not to target one another's communications.



4.4 Cyber Threat Detection

Collection – Metadata

4.5 Collection Rules

CSEC acquires telecommunications-related information used to identify, describe, manage or route all or part of the telecommunication (“metadata”), to gain a better understanding of the global information infrastructure (GII) and identify new targets.

This activity, also authorized under paragraph 273.64(1)(a) of the NDA, does not require an MA and is conducted in accordance with the *Ministerial Directive on the Collection and Use of Metadata*.

5. DATA USE AND RETENTION – ALL PROGRAMS

Use – Traffic

5.1 SIGINT Privacy Annotations

CSEC must record the following information and send a report to the Minister, within four months of the expiration of an MA or at any time upon request:

- the number of recognized, intercepted private communications that are used or retained on the basis that they are essential to international affairs, defence or security
- the number of recognized, intercepted solicitor-client communications that are used or retained on the basis that they are essential to international affairs, defence or security, and are in conformity with the legal advice received
- the number of intelligence reports produced from the information derived from recognized, intercepted private communications, and
- the foreign intelligence value of these reports, as they relate to international affairs, defence or security.

CSEC traffic databases have been designed to generate the required statistics (regarding both private communications and solicitor-client communications) based on the privacy annotations, which must be made by analysts whose functions are directly related to the production of foreign intelligence reports.

Privacy measures require that, in addition to private communications and solicitor-client communications, communications of Canadians located outside Canada and communications that contain information about Canadians anywhere also be annotated for destruction by analysts unless the information is essential to international affairs, defence or security. (See OPS-1 for determining essentiality and for handling solicitor-client communications.)

5.2

[REDACTED]

5.3 ECI Control

[REDACTED]

5.4 Reporting

SIGINT reports based on traffic collected by these programs must adhere to existing policy instruments, including:

- OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities*
- OPS-1-7, *Operational Procedures for Naming in SIGINT Reports*
- OPS-5-3, *Write-to-Release (WTR) Procedures*
- CSSS-104, *GAMMA Handling Standards* (in draft)
- CSOI-4-1, *SIGINT Reporting*

All other special handling or restricted distribution rules apply.



Attention: Traffic derived from [REDACTED] collection is eligible for WTR reporting provided that the information does not fall into one of the categories listed in the WTR Exemption List.

5.5 Report Classification

The table below specifies the minimum classification of SIGINT reports based on traffic collected by these programs. Additional sub-control system markings and dissemination control markings may be added as needed.

	Minimum Classification
	SECRET//SI
	TOP SECRET//SI
	TOP SECRET//SI
	TOP SECRET//SI

5.6 Report Release Authorities

See OPS-1 for information on report release authorities.

5.7 Storage of Traffic

See OPS-1 for details on storing traffic that is a:

- private communication
- communication of a Canadian located outside of Canada, or
- communication containing information about Canadians located anywhere.

5.8 Authority for Release of Suppressed Information

Corporate and Operational Policy (D2) is the authority for the release of suppressed information. See OPS-1-1, *Procedures for Release of Suppressed Information from SIGINT Reports*, for more information.

Use – Metadata**5.9 Searching Metadata**

CSEC may search any metadata acquired in the execution of its foreign intelligence acquisition programs for the purpose of providing any information or intelligence about the capabilities, intentions or activities of foreign entities as they relate to international affairs, defence or security. This may include any information related to protecting electronic information or information infrastructures of importance to the GC.

5.10 Using Metadata

Metadata must be used only for the following purposes:

- contact chaining
- network analysis and prioritization
- identifying new targets and target-associated selectors, which can be used:
 - at any time to intercept foreign communications (both ends foreign), or
 - to intercept private communications strictly where a duly issued MA is in effect, and in exact compliance with that MA
- monitoring or identifying patterns of foreign malicious cyber activities to provide indications and warnings of actual or potential intrusions directed against infrastructures of importance to the GC.

For additional information on contact chaining, see OPS-1-10, *Procedures for Metadata Analysis* [REDACTED]

5.11 Using Metadata in Reports

See paragraphs 5.4, 5.5 and 5.6 of these procedures for guidance on the use of metadata in reports.

Use – Unknown Data

5.12 Use of Unknown Data

Samples of unknown data may be copied and sent to [REDACTED] where it is technically analyzed in a strictly controlled environment to make it intelligible to persons or systems. If the data is successfully processed, metadata may be extracted and retained in accordance with these procedures; [REDACTED] (subject to the targeting rules in paragraph 4.1), and any results obtained may be retained and handled in accordance with these procedures.

Access to unknown data must be authorized by the Director, [REDACTED] and must be limited to those conducting the signals and network analysis as well as decryption. When analysis assistance is required, the Manager, SIGINT Programs Oversight and Compliance (SPOC) may authorize the sharing of unknown data with SIGINT counterparts at CSEC and Second Parties.

TOP SECRET//SI//Canadian Eyes Only

OPS-1-13

Effective Date: 5 December 2012

Retention

5.13 Retention See OPS-1-11, *Retention Schedules for SIGINT Data*.

6. DATA SHARING - ALL PROGRAMS

6.1 Sharing Data with Second Parties

[REDACTED] Second Parties may submit selectors to [REDACTED]. These selectors are subject to the targeting rules in paragraph 4.1.

Data acquired as a result of such targeting [REDACTED] to Second Parties as requested. CSEC must retain an archived copy of all data forwarded to Second Parties.

[REDACTED]

Second Parties have implemented measures to protect the privacy of Canadians in the handling and reporting of foreign intelligence that relate to private communications, communications of Canadians located outside Canada, and information about Canadians anywhere. These measures include:

- suppression of Canadian identity information in SIGINT reports, in accordance with CSEC naming procedures, and
- consultation with CSEC prior to release of sensitive reports containing information about Canadians.

[REDACTED]

**6.2 Sharing
Metadata with
Second Parties**

As part of normal data exchanges with Second Parties, [REDACTED] may share [REDACTED] metadata provided that all metadata known to be associated with Canadians located anywhere or persons located in Canada is altered by CSEC prior to sharing so that it is impossible to identify individuals to whom the information relates. Disclosure of any unaltered versions of metadata are subject to specific requests to Corporate and Operational Policy, and such requests shall be granted strictly in accordance with criteria outlined in CSEC's operational procedures. CSEC must retain an archived copy of all metadata forwarded to Second Parties.

[REDACTED]



Attention: Sharing [REDACTED] metadata and traffic with Second Parties is subject to the terms and conditions of the Five-Eyes [REDACTED] agreement.

**6.3 Sharing
Metadata with
Second Parties:**

[REDACTED] may be forwarded to Second Parties provided that all metadata known to be associated with Canadians located anywhere or persons located in Canada is altered by CSEC prior to sharing so that it is impossible to identify individuals to whom the information relates. [REDACTED]

[REDACTED]

[REDACTED]

6.4

Subject to approval from the Director, SIGINT Requirements, CSEC may [REDACTED]

[REDACTED]

Related handling instructions will be issued on a case-by-case basis.

TOP SECRET//SI//Canadian Eyes Only

OPS-1-13

Effective Date: 5 December 2012

6.5



7. ACCOUNTABILITY FOR OPS-1-13

7.1 Accountability

This table outlines the accountabilities for revising, reviewing, recommending and approving this document.

Who	Responsibility
Deputy Chief, SIGINT	<ul style="list-style-type: none"> Approves
Director General, Policy and Communications	<ul style="list-style-type: none"> Approves
General Counsel, Directorate of Legal Services	<ul style="list-style-type: none"> Reviews to ensure compliance with the law
Director, Disclosure, Policy and Review	<ul style="list-style-type: none"> Reviews for consistency with the policy framework
Manager, Corporate and Operational Policy	<ul style="list-style-type: none"> Revises Answers questions

7.2 References

- National Defence Act*
- Privacy Act*
- Ministerial Directive on CSE's Accountability Framework*
- Ministerial Directive on the Collection and Use of Metadata* (November 2011)
- Ministerial Directive on Privacy of Canadians*
- Ministerial Directive "Integrated SIGINT Operational Model"* (2004)
- Ministerial Authorization on CSE [REDACTED] Collection Activities* in force
- Ministerial Authorization on [REDACTED]* in force
- [REDACTED] (2009)
- OPS-1, Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities*
- OPS-1-1, Procedures for Release of Suppressed Information from SIGINT Reports*
- OPS-1-7, Operational Procedures for Naming in SIGINT Reports*
- OPS-1-8, Operational Procedures for Policy Compliance Monitoring to Ensure Legal Compliance and the Protection of the Privacy of Canadians*
- OPS-1-10, Procedures for Metadata Analysis [REDACTED]*

Continued on next page

7.2 References
(continued)

- OPS-1-11, *Retention Schedules for SIGINT Data*
- OPS-2-1, *Operational Procedures for Sanitizations and Actions-On*
- OPS-3-1, *Operational Procedures for [REDACTED] Activities*
- OPS-5-3, *Write-to-Release Procedures*
- CSOI-4-1, *SIGINT Reporting*
- CSOI-4-4, *Targeting and Selector Management Using [REDACTED] National SIGINT Systems For Intelligence Reporting Purposes*

7.3 Enquiries

Questions related to these procedures should be directed to operational managers, who in turn will contact Corporate and Operational Policy staff when necessary.

7.4 Amendments

Situations may arise where amendments to these procedures are required because of changing or unforeseen circumstances. Such amendments will be communicated to relevant staff, and will be posted on the Corporate and Operational Policy website.

7.5 Review

Canadian [REDACTED] activities, including relevant policies and procedures, are subject to policy compliance monitoring (see OPS-1-8, *Operational Procedures for Policy Compliance Monitoring to Ensure Legal Compliance and the Protection of the Privacy of Canadians*), and to audit or review by DGAEE and various external review bodies.

7.6 Records Management

See ORG-2-2, *Procedures for Handling Documents Related to CSE Activities Conducted Under a Ministerial Authorization*, for information on the requirement to establish and maintain a separate corporate file for each activity or class of activities undertaken under the authority of an MA issued pursuant to subsection 273.65(1) of the NDA.

8. Definitions

8.1 Activity Authorization Request (AAR)

An AAR is a proposal for [REDACTED], SIGINT Development or collection connected to the [REDACTED] collection programs. It is prepared by [REDACTED] based on a request and an intelligence requirement received from CFIOG, CSEC staff, or a Second Party. It includes the following information:

- intelligence requirement/GCRs
- collection source [REDACTED] as applicable, against which the activity will take place
- target details, if available
- targeting and collection handling procedures
- [REDACTED] options, and
- sponsoring element(s).

8.2

8.3 British-U.S. Communication Intelligence Agreement

The *British-U.S. Communication Intelligence Agreement* (dated 1946) governs the relations of the two parties in Communication Intelligence (COMINT) matters relating to the exchange of foreign communications products, information on methods and techniques, third party agreements, and dissemination and security.

8.4 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*, 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.

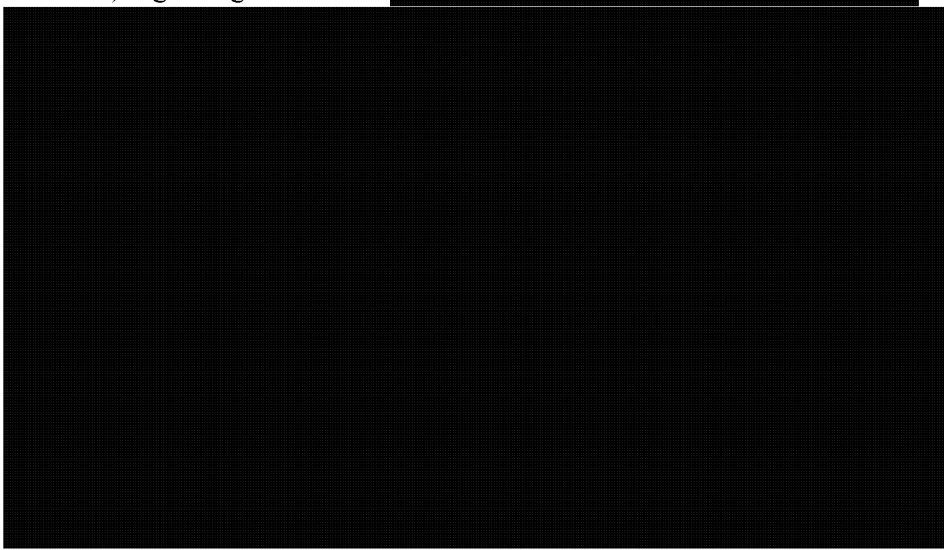
(NDA, paragraph 273.61)

For the purpose 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.

**8.5 Canada-US
COMINT
Agreement**

In 1949, the *Canada-U.S. COMINT Agreement* established the relationship between the Canadian Communications Research Committee (now known as CSEC) and the United States Communication Intelligence Board (now known as NSA) regarding COMINT. [REDACTED]



8.6 Collection For the purposes of these procedures, collection has two meanings. With respect to private communications, collection is the process of acquiring data [REDACTED] With respect to all other communications, collection is the process of acquiring data [REDACTED] and subsequently forwarding it to the traffic repository.

8.7 Contact Chaining Contact chaining means the method developed to enable the analysis, from information derived from metadata, of communications activities or patterns to build a profile of communications contacts of various foreign entities of interest in relation to the foreign intelligence priorities of the GC, including the number of contacts to or from these entities, the frequency of these contacts, the number of times contacts were attempted or made, the time period over which these contacts were attempted or made as well as other activities aimed at mapping the communications of foreign entities and their networks.

8.8 Data Data is defined as traffic and bulk unselected metadata, and unknown data acquired from the GII.

8.9 Dictionary For the purpose of these procedures, a dictionary is [REDACTED] based on approved keywords (selectors).

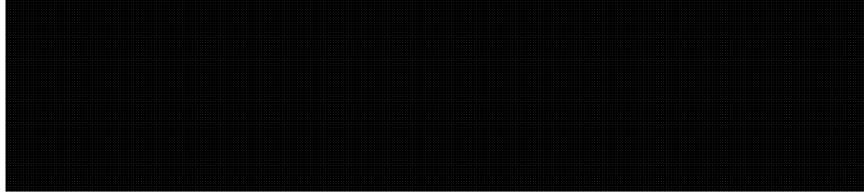
8.10 Entity An entity is a person, group, trust, partnership, or fund or an unincorporated association or organization and includes a state or political subdivision or agency of a state. (NDA, section 273.61)

8.11

[REDACTED]

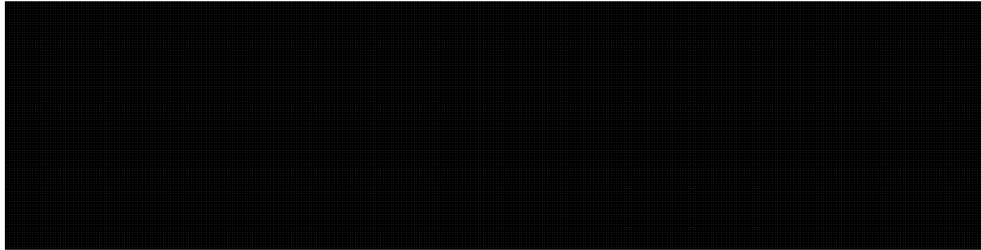
**8.12
Exceptionally
Controlled
Information
(ECI)**

ECI is a sub-control system of the COMINT control system that provides additional protection for very sensitive SIGINT operations. The operations' sensitivity can relate to



**8.13 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. (NDA, section 273.61)

8.14

8.15

**8.16 Global
Information
Infrastructure
(GII)**

The 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 or networks. (NDA, section 273.61)

8.17 In Canada

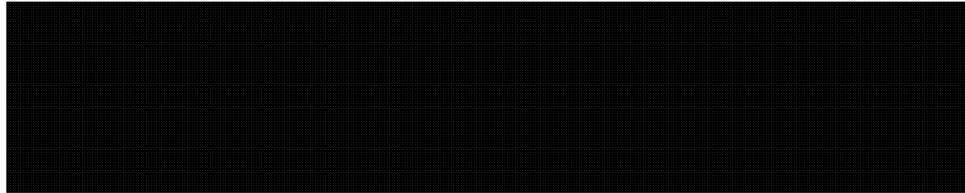
"In Canada" refers to Canada's territory, internal waters, territorial sea (i.e. up to the 12 nautical mile limit), and the associated airspace.

**8.18
Information
about
Canadians**

Information about Canadians includes:

- any personal information about a Canadian, or
- any business information about a Canadian corporation.

8.19



8.20 Integree

An integree is a person seconded to CSEC from one of CSEC's cryptologic partner organizations.

**8.21
Interception**

For the purposes of these procedures, interception occurs when a private communication is selected from a [REDACTED] and is forwarded to the traffic repository.

8.22 Metadata

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.

**8.23 Ministerial
Authorization
(MA)**

An MA is an authorization provided in writing by the Minister of National Defence (the Minister) to CSEC to ensure that CSEC is not in contravention of the law if, in the process of conducting its foreign intelligence or IT security operations, it should intercept private communications. MAs may be granted in relation to an activity or class of activities specified in the authorization pursuant to

- subsection 273.65(1) of the NDA for the sole purpose of obtaining foreign intelligence, or
- subsection 273.65(3) of the NDA for the sole purpose of protecting the computer systems or networks of the GC from mischief, unauthorized use or interference, in the circumstances specified in paragraph 184(2)(c) of the criminal code.

When such an authorization is in force, Part VI of the *Criminal Code* does not apply in relation to an interception of a private communication, or in relation to a communication so intercepted.

8.24 Network Analysis and Prioritization

Network analysis and prioritization means the method developed to understand the GII from information derived from metadata, in order to identify and determine telecommunication links of interest to achieve the GC's foreign intelligence priorities. This method involves

- the acquisition of metadata
- the identification of [REDACTED]
- the determination of the [REDACTED]

- [REDACTED]
 - [REDACTED]
-

8.25 Personal Information

Personal information means information that can be used to identify a person as defined in section 3 of the *Privacy Act*. For the definition of personal information, see Annex 1.

8.26 Privacy Annotations

Privacy annotations are markings applied to SIGINT traffic in traffic repositories to identify private communications, communications of Canadians located outside Canada, solicitor-client communications, and information about Canadians to be retained or deleted. 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 of these categories. For more information, see OPS-1, Annex 2.

8.27 Private Communication

A private communication is:

“Any oral communication, or any telecommunication, that is made by an originator who is in Canada or is intended by the originator to be received by a person 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)

8.28 [REDACTED]

[REDACTED]

[REDACTED]

8.29 [REDACTED]

[REDACTED]

[REDACTED]

8.30 [REDACTED]

[REDACTED]

[REDACTED]

8.31 Secondee

A secondee is an individual who is temporarily moved from another GC or private organization to CSEC, and who at the end of the assignment returns to the originating organization.

8.32 Second Parties

Second Parties refer to CSEC's SIGINT counterparts (SIGINT partners) and include: the US National Security Agency (NSA), the UK Government Communications Headquarters (GCHQ), Australia's Defense Signals Directorate (DSD), and New Zealand's Government Communications Security Bureau (GCSB).

8.33 Selectors

Selectors are terms that 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.

8.34 SIGINT Development

SIGINT Development is aimed at [REDACTED]

[REDACTED]

8.35

[REDACTED]

[REDACTED]

8.36

[REDACTED]

[REDACTED]

8.37 Solicitor-Client Communication

For the purposes of these procedures, a solicitor-client communication means any communication that is directly related to the seeking, formulating or giving of legal advice or legal assistance between a client and a person authorized to practice as a lawyer or a notary in the province of Quebec or as a barrister or solicitor in any territory or other province of Canada, or any person employed in the office of such lawyer, notary, barrister or solicitor.

8.38

[REDACTED]

[REDACTED]

8.39

[REDACTED]

[REDACTED]

8.40 [REDACTED]

8.41 [REDACTED]

8.42 Unknown Data

Unknown data is data that is unrecognized by a collection system and therefore cannot be processed for the purpose of extracting metadata or content without additional analysis or processing to render it readable.

Annex 1 – Personal Information

Definition of Personal Information in the *Privacy Act* (s. 3)

"Personal information" means information about an identifiable individual that is recorded in any form including, without restricting the generality of the foregoing,

- (a) information relating to the race, national or ethnic origin, colour, religion, age or marital status of the individual,
- (b) information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,
- (c) any identifying number, symbol or other particular assigned to the individual,
- (d) the address, fingerprints or blood type of the individual,
- (e) the personal opinions or views of the individual except where they are about another individual or about a proposal for a grant, an award or a prize to be made to another individual by a government institution or a part of a government institution specified in the regulations,
- (f) correspondence sent to a government institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to such correspondence that would reveal the contents of the original correspondence,
- (g) the views or opinions of another individual about the individual,
- (h) the views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the individual by an institution or a part of an institution referred to in paragraph (e), but excluding the name of the other individual where it appears with the views or opinions of the other individual, and
- (i) the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual,

but, for the purposes of sections 7, 8 and 26 and section 19 of the *Access to Information Act*, does not include

- (j) information about an individual who is or was an officer or employee of a government institution that relates to the position or functions of the individual including,

- (i) the fact that the individual is or was an officer or employee of the government institution,
- (ii) the title, business address and telephone number of the individual,
- (iii) the classification, salary range and responsibilities of the position held by the individual,
- (iv) the name of the individual on a document prepared by the individual in the course of employment, and
- (v) the personal opinions or views of the individual given in the course of employment,

(k) information about an individual who is or was performing services under contract for a government institution that relates to the services performed, including the terms of the contract, the name of the individual and the opinions or views of the individual given in the course of the performance of those services,

(l) information relating to any discretionary benefit of a financial nature, including the granting of a licence or permit, conferred on an individual, including the name of the individual and the exact nature of the benefit, and

(m) information about an individual who has been dead for more than twenty years.