



OPS-3-1

Operational Procedures for [REDACTED]

Activities

OPERATIONAL POLICY

Canada

Table of Contents

1. Introduction.....	3
Policy Scope and Application.....	3
Activity Description.....	5
Legal Authorities	5
2. Legal and Policy Requirements for Operations Conducted Under Part (a) of the Mandate..	7
3. Approval Processes for ██████████ Activities Conducted Under Part (a) of the Mandate.....	11
██████████ Activities Conducted ██████████	11
██████████ Activities Conducted ██████████	12
██████████ Activities Conducted ██████████	13
4. IRRELEVANT	14
IRRELEVANT	16
██████████ Activities	16
██████████ Activities	17
6. Rules for the Use and Retention of ██████████ Data	18
Targeting and Collection.....	18
Reporting.....	20
Data Use, Retention and Storage	21
Sharing Information	22
7. Roles and Responsibilities	24
8. Accountability for OPS-3-1	26
9. Definitions.....	28
Annex 1 – ██████████	32
Annex 2 – Personal Information	34

1. Introduction

Policy Scope and Application

1.1 Scope

CSEC conducts [REDACTED] activities under:

- paragraph 273.64(1)(a) of the *National Defence Act* (NDA) to acquire and provide foreign intelligence in accordance with Government of Canada (GC) intelligence priorities (part (a) of the Mandate), or
- paragraph 273.64(1)(c) of the NDA to support federal law enforcement and security agencies (LESAs) in the performance of their lawful duties (part (c) of the Mandate).

These procedures govern CSEC's [REDACTED] activities conducted under both parts (a) and (c) of the Mandate. This document supersedes OPS-3-1, *Procedures for [REDACTED] Activities*, dated 14 January 2011.

1.2 Objective

The purpose of these procedures is to:

- outline measures to ensure legal compliance and protect the privacy of Canadians in the conduct of [REDACTED] activities
 - set out the approval processes for conducting the [REDACTED] activity
 - set out the accountability trail for these activities
 - provide direction to personnel regarding the handling of [REDACTED] data, and
 - document the activities authorized at each [REDACTED]
-

1.3 Policy

[REDACTED] activities conducted under part (a) of CSEC's Mandate must:

- comply with all relevant laws of Canada, including the *Charter of Rights and Freedoms*, the *Privacy Act*, the *Criminal Code* and the NDA
 - comply with the most recent *Ministerial Authorization* (MA) on [REDACTED] Activities
-

Continued on next page

1.3 Policy
(continued)

- comply with all relevant and most recent Ministerial Directives, including the *Ministerial Directive on the Privacy of Canadians*, the *Ministerial Directive on [REDACTED] Operations*, the *Ministerial Directive on the Collection and Use of Metadata* and the *Ministerial Directive on CSE's Accountability Framework*
- [REDACTED]
- [REDACTED]
- comply with all relevant policies and procedures
- be subject to measures to protect the privacy of Canadians, including those prescribed in OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities*, and
- be carried out only with the knowledge and approval of CSEC management.

[REDACTED] activities conducted under part (c) of the Mandate are subject to limitations imposed by law on the requesting agency and the most recent *Ministerial Directive on Assistance to Federal Law Enforcement and Security Agencies*.

1.4 Application

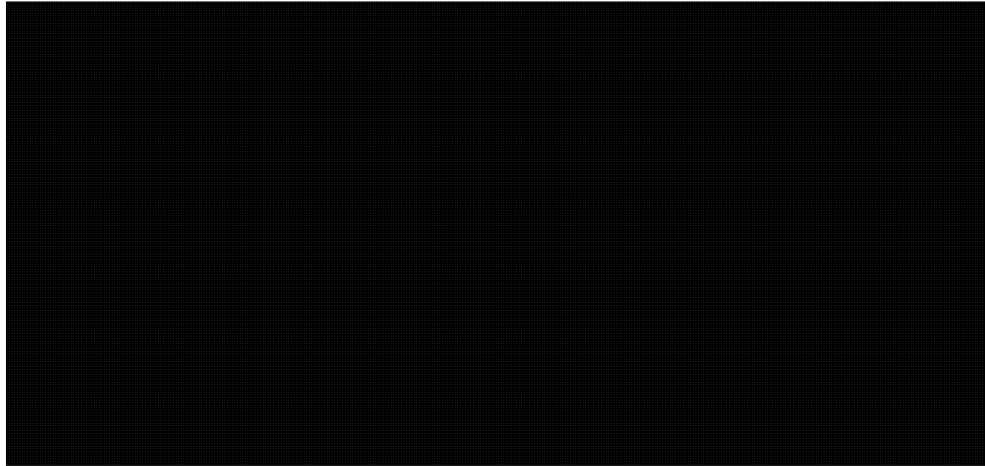
These procedures apply to:

- CSEC staff
 - Canadian Forces Information Operations Group (CFIOG) staff, and
 - any other parties who conduct [REDACTED] activities under the authorities listed in this chapter, including secondees, integrees and contractors.
-

Activity Description

1.5 What is

██████████



1.6 Who is Permitted to Conduct Activities?



██████████ Standard Operating Procedures (SOPs).

1.7 ECI Control Sensitive aspects of ██████████ activities are controlled under the appropriate ECI programs.

Legal Authorities

1.8 Authorities for ██████████ Activities under part (a) of CSEC's Mandate

CSEC conducts part (a) ██████████ activities under the authority of:

- the NDA
- the most recent *Ministerial Directive on ██████████ Operations*, and
- the most recent *Ministerial Directive on the Collection and Use of Metadata*.

Continued on next page

TOP SECRET//SI

OPS-3-1

Effective Date: 11 December 2012

**1.8 Authorities
for [REDACTED]
Activities under
part (a) of
CSEC's
Mandate
(continued)**

Because [REDACTED] activities may result in the interception of private communications, an MA is also required. The MA, authorized under section 273.65(1) of the NDA, enables CSEC to intercept private communications without violating the *Criminal Code*. Private communications may be intercepted solely for the purpose of obtaining foreign intelligence in accordance with GC intelligence priorities.

IRRELEVANT

**2.4 MA
Conditions and
Requirements**

The NDA requires that prior to issuing an MA, the Minister of National Defence (“the Minister”) must be satisfied that the following conditions have been met:

- the interception will be directed at foreign entities located outside Canada
- the information cannot reasonably be obtained by other means
- the expected foreign intelligence value of the information 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 (see OPS-1 for information on essentiality).

The Minister also requires special handling of solicitor-client communications (see the related paragraph in OPS-1).

**2.5 Informing
the Minister**

Information Relating to Private Communications and Solicitor-Client Communications

CSEC must record the following information regarding its usage of [REDACTED] data, and send a report to the Minister, within four months following the expiration of the MA or at any time upon request:

- the number of recognized, intercepted private communications that were used or retained because they were essential to international affairs, defence or security
 - the number of recognized, intercepted solicitor-client communications that were used or retained because they were essential to international affairs, defence or security, and their retention conformed with received legal advice
 - 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.
-

Continued on next page

**2.5 Informing
the Minister
(continued)**

Information Relating to Marking [REDACTED]

The Chief, CSEC (CCSEC) will provide annual statistics to the Minister regarding the number of recognized one-end Canadian emails [REDACTED]
[REDACTED]
acquired through the [REDACTED] program and retained by CSEC because they are essential to international affairs, defense or security.

Serious Issues

The CCSEC must report to the Minister when any serious issue arises in the implementation of the MA, including but not limited to a sustained substantial decrease in the value of this source of foreign intelligence, or any sustained major increase in recognized private communications or solicitor client communications. Where there is no such issue, the CCSEC must insert in the accountability report an explicit statement to this effect.

Annual Reporting

The CCSEC must report annually to the Minister on [REDACTED] activities. This is done as part of the *CSEC Annual Report to the Minister of National Defence*.

**2.6 Proposals
for New [REDACTED]
Techniques or
Capabilities**

The table below outlines the process to be followed when new [REDACTED] techniques or capabilities require approval. These responsibilities may be performed by anyone officially delegated to carry out the duties of that position.

**2.6 Proposals
for New [REDACTED]
Techniques or
Capabilities
(continued)**

Step	Who Does It	Activity
1	[REDACTED] Team Member	Prepares proposal for a new [REDACTED] technique or capability
2	Manager, [REDACTED] [REDACTED]	Reviews and recommends the proposal
3	Director, [REDACTED]	Approves the proposal

 **Note:** Consultation with DLS and Director SIGINT Program Requirements (SPR) may occur at any stage.

**2.7 Record
Keeping**

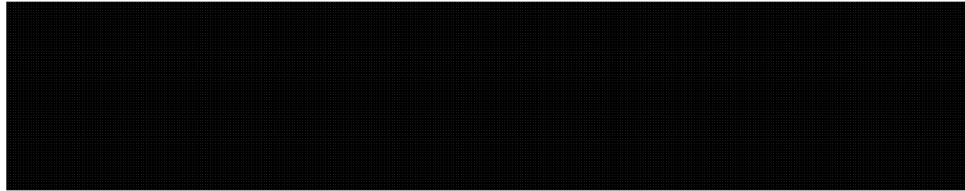
The Manager, [REDACTED] must maintain a record of all [REDACTED] operational activities to track the approval process, [REDACTED] and outcome of the activity, and dates.

The Manager, [REDACTED] and Manager, [REDACTED] must track the approval process for new [REDACTED] techniques or capability proposals.

3. Approval Processes for [REDACTED] Activities Conducted Under Part (a) of the Mandate

3.1 Introduction


This chapter outlines the approval processes for activities conducted under part (a) of the Mandate.




[REDACTED] Activities Conducted [REDACTED]

Step	Who Does It	Activity
1	[REDACTED] Team Member	Prepares proposal for [REDACTED] activity in accordance with the [REDACTED] SOPs
2	Manager, [REDACTED] [REDACTED]	<ul style="list-style-type: none">• Reviews and recommends the activity if the [REDACTED] associated with the [REDACTED]• Reviews and approves the activity if the [REDACTED] [REDACTED]
3	Director, [REDACTED]	Reviews and approves the activity if the [REDACTED] [REDACTED]


Activities Conducted

Step	Who Does It	Activity						
Stage 1: Proposal								
1	██████ Team Member	Prepares an operational proposal for the Manager, ██████████ in accordance with the ███████ SOPs						
Stage 2: Recommendation to proceed								
2	<table><tr><th>If the activity is ...</th><th>Then Recommend Authority is...</th></tr><tr><td rowspan="3">██████████</td><td>Manager, ██████████</td></tr><tr><td>Director, ███████</td></tr><tr><td>DC SIGINT</td></tr></table>		If the activity is ...	Then Recommend Authority is...	██████████	Manager, ██████████	Director, ███████	DC SIGINT
If the activity is ...	Then Recommend Authority is...							
██████████	Manager, ██████████							
	Director, ███████							
	DC SIGINT							
Stage 3: Approval								
3	<table><tr><th>If the activity is ...</th><th>Then Approval Authority is ...</th></tr><tr><td rowspan="3">██████████</td><td>Director, ███████</td></tr><tr><td>DC SIGINT</td></tr><tr><td>CCSEC or any senior executive officially designated to carry out the duties of CCSEC</td></tr></table> <div>Note: The CCSEC must consult with the Minister before approving any particularly sensitive ███████ operations or those that carry significant risk.</div>		If the activity is ...	Then Approval Authority is ...	██████████	Director, ███████	DC SIGINT	CCSEC or any senior executive officially designated to carry out the duties of CCSEC
If the activity is ...	Then Approval Authority is ...							
██████████	Director, ███████							
	DC SIGINT							
	CCSEC or any senior executive officially designated to carry out the duties of CCSEC							

**Note:** Any level of management may consult with DLS and Director, SPR at any stage.

Activities Conducted

Step	Who Does It	Activity
1	Team Member	<ul style="list-style-type: none"> Prepares an operational proposal for the Manager, in accordance with the SOPs Prepares a separate operational security plan in accordance with policies, procedures and the SOPs
2	Director,	<ul style="list-style-type: none"> In consultation with reviews and recommends the proposal
3	DC SIGINT	<ul style="list-style-type: none"> Complies with the terms of the most recent and may consult with other external department(s) (as required) Recommends the proposal for review
4	CCSEC	<ul style="list-style-type: none"> Approves the operation, if appropriate Consults with the Minister if the operation is particularly sensitive or carries a significant risk Informs the National Security Advisor, as necessary Reviews and recommends the proposal
5	The Minister	<ul style="list-style-type: none"> Approves the operation, if required due to sensitivity or significant risk

 **Note:** Consultation with DLS and Director, SPR may occur at any stage.

3.2 Delegation of Recommend or Approve Authority

In the absence of the Recommend or Approve Authority for any activities, anyone officially designated to carry out the duties of that position, or the next *higher* management level, may act as Recommend or Approve Authority.

IRRELEVANT

IRRELEVANT

IRRELEVANT

IRRELEVANT

6. Rules for the Use and Retention of [REDACTED] Data

6.1 Introduction

This section outlines the rules for:

- targeting and collection
 - handling collected traffic (annotations, essentiality and solicitor-client communications)
 - reporting
 - using metadata
 - storage and retention, and
 - sharing of information.
-

Targeting and Collection

6.2 Applying Selection Criteria for Collection/ Targeting (under part (a) of CSEC's Mandate)

CSEC maintains a list of selection criteria [REDACTED] [REDACTED] These criteria are obtained from a number of sources, including but not limited to:

- open source information
- analysis of previously acquired SIGINT, and
- information provided by various GC departments and agencies as well as allied agencies.

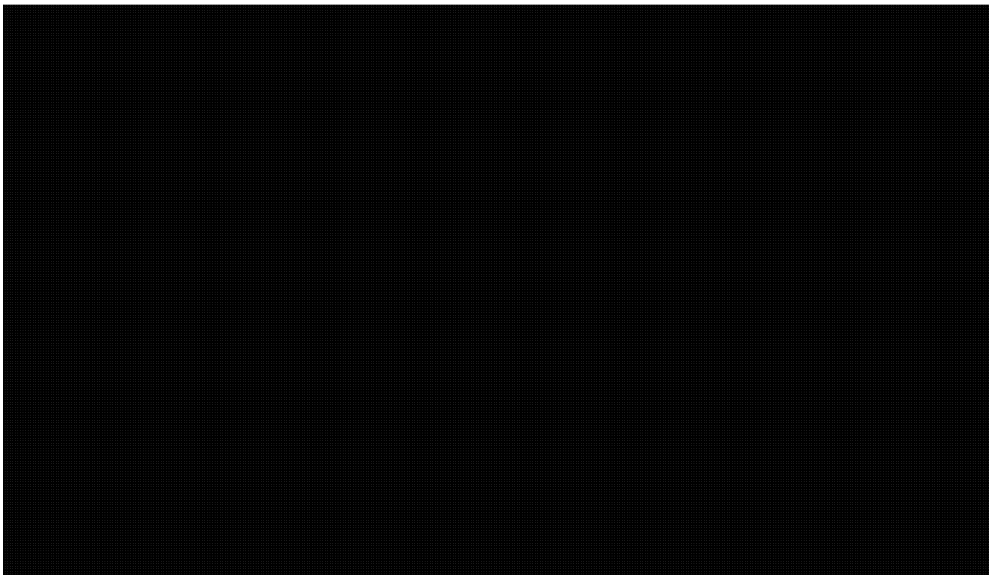
Before any [REDACTED] activities can be conducted, CSEC personnel must be satisfied, based on all the information that CSEC has available to it at the time, that the proposed selection criteria are associated with a foreign entity located outside Canada, and that they relate to a GC intelligence priority.

6.3 Applying Privacy Annotations (under part (a) of CSEC's Mandate)


Foreign intelligence analysts must apply privacy annotations to recognized private communications, solicitor-client communications, and communications of Canadians located outside Canada. These communications must be annotated for destruction unless the information is essential to international affairs, defence or security. If the data contains information about Canadians, however, it must be annotated for deletion (IACN) when the information does not meet the essentiality test.

Continued on next page

6.3 Applying Privacy Annotations (under part (a) of CSEC's Mandate) (continued)



CSEC traffic databases generate the statistics required for the Minister (relating to private communications and solicitor-client communications) based on such privacy annotations.

**Note:** Solicitor-Client Privilege

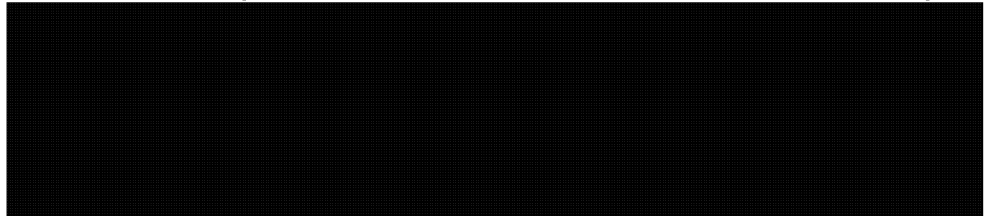
Solicitor-Client Privilege

Solicitor-Client Privilege

Contact SIGINT Programs Oversight and Compliance (SPOC) for guidance on when a private communication is intercepted in the context of a specific [REDACTED] operation.

6.4 Accountability Markings (AM)

Although there is no legal requirement to annotate the number of [REDACTED] emails acquired under the [REDACTED] MA, CCSEC has committed to report on the number of recognized one-end Canadian emails [REDACTED] [REDACTED] acquired through the [REDACTED] program and retained by CSEC because they are essential to international affairs, defence or security.



6.5 Determining Essentiality (Part (a) of the Mandate) See the related paragraph in OPS-1.

6.6 Handling of Solicitor-Client Communications See the related paragraphs in OPS-1 for both parts (a) and (c) of CSEC's Mandate.

Reporting

6.7 Reporting Under Part (a) of the Mandate

SIGINT reports based on [REDACTED] traffic collected under part (a) of CSEC's Mandate must adhere to existing policy instruments, including:

- OPS-1
- OPS-1-7, *Operational Procedures for Naming in SIGINT Reports*
- OPS-5-3, *Write-to-Release (WTR) Procedures* (see Note)
- CSSS-104, *GAMMA Handling Standards*, and
- CSOI-4-1, *SIGINT Reporting*.

All other special handling or restricted distribution rules also apply.



Note: [REDACTED] traffic is eligible for WTR reporting (in consultation with the Manager, [REDACTED]) provided that the information does not fall into one of the categories listed in the WTR Exemption List.

Under Part (c) of the Mandate

IRRELEVANT

**6.8 Report
Classification**

SIGINT reports based on [REDACTED] collection must be classified at a minimum TOP SECRET//SI.

Additional sub-control system markings or dissemination control markings may be added as needed.

**6.9 Report
Release
Authorities**

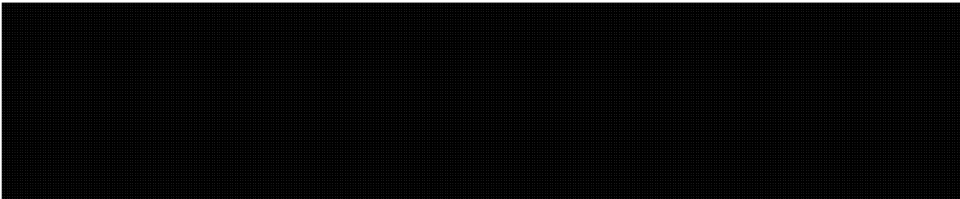
See the related paragraphs in OPS-1.

**6.10 Authority
for the Release
of Suppressed
Information**

Corporate and Operational Policy (formerly Operational Policy) is the authority for releasing suppressed identities from SIGINT reports derived from [REDACTED] collection. See OPS-1-1, *Procedures for Release of Suppressed Information from SIGINT Reports*, for more information.

Data Use, Retention and Storage

**6.11 Using
Unknown Data**



**6.12 Searching
Metadata
(Under Part (a)
of CSEC's
Mandate)**

CSEC may search any metadata acquired for the purpose of providing any information or intelligence about the capabilities, intentions or activities of a foreign individual, state, organization, terrorist group or other such entities as they relate to international affairs, defence or security, including any information to monitor or identify patterns of malicious cyber activities.

6.13 Using Metadata

Metadata must be used only for the following purposes:

- contact chaining
- network analysis and prioritization, or
- identifying new targets and target-associated selectors, which can be used:
 - at any time to intercept foreign communications (both ends foreign)
 - to intercept private communications strictly where a duly issued MA is in effect, and in exact compliance with that MA, or
 - to monitor or identify patterns of malicious cyber activities.



FYI: For additional information on contact chaining, see OPS-1-10, *Procedures for Metadata Analysis* [REDACTED] and CSOI-4-5, *Procedures for Metadata Analysis Using a* [REDACTED] (in draft).

6.14 Data Retention

See the related paragraphs in OPS-1-11, *Retention Schedules for SIGINT Data*, for both parts (a) **IRRELE** of the Mandate.

6.15 Storage of [REDACTED] Traffic

See OPS-1 for details on storing [REDACTED] traffic where that traffic contains information about Canadians.

Sharing Information

6.16 Reports

Reporting Under Part (a) of the Mandate

All current CSEC reporting procedures apply to sharing reports based on [REDACTED] activities under part (a) of the Mandate (subject to all dissemination control markings or sharing restrictions contained in specific [REDACTED] operational plans).

Continued on next page

6.16 Reports
(continued)

Reporting Under Part (c) of the Mandate

IRRELEVANT

6.17 Data

Sharing Under Part (a) of the Mandate

Traffic obtained from [REDACTED] activities may be shared with Second Parties with the approval of appropriate Managers in [REDACTED] (that is, those Managers whose operations are directly supported by the [REDACTED] activity). This approval for sharing is to be indicated by the use of appropriate dissemination control markings which are established at the time of an operation's approval. If such approval is received, Second Parties may submit selection criteria to [REDACTED]

Prior to providing the proposed selection criteria to [REDACTED] [REDACTED] must be satisfied that they are associated with:

- foreign entities located outside Canada, and
- GC intelligence priorities.

Data acquired as a result of the selectors [REDACTED] to Second Parties as requested. Second Parties have measures in place to protect the privacy of Canadians in the handling and reporting of foreign intelligence that contains information about Canadians. CSEC must retain an archived copy of all data forwarded to Second Parties.

Sharing Under Part (c) of the Mandate

IRRELEVANT

7. Roles and Responsibilities

7.1 Roles and Responsibilities

This table summarizes roles and responsibilities with respect to [REDACTED] activities.

Who	Responsibility
The Minister	<ul style="list-style-type: none"> Approving a [REDACTED] from [REDACTED] as required
Chief, CSEC	<ul style="list-style-type: none"> Providing the Minister with the information listed in paragraph 2.5 Approving [REDACTED] activities conducted [REDACTED] (under part (a) of the Mandate) Approving [REDACTED] activities [REDACTED] if appropriate Consulting the Minister about [REDACTED] activities [REDACTED] (under part (a) of the Mandate) Advising the NSA, as necessary
Deputy Chief, SIGINT	<ul style="list-style-type: none"> Approving [REDACTED] activities conducted [REDACTED] (under part (a) of the Mandate) [REDACTED] required) for [REDACTED] activities conducted [REDACTED] (under part (a) of the Mandate)
Directorate of Legal Services	<ul style="list-style-type: none"> Providing legal advice and guidance, as requested
Director General, [REDACTED]	<ul style="list-style-type: none"> Acting as the Director, [REDACTED] Approval Authority, when that Director is absent

Continued on next page

TOP SECRET//SI
OPS-3-1
Effective Date: 11 December 2012

Who	Responsibility
Director, [REDACTED] [REDACTED]	<ul style="list-style-type: none"> Informing [REDACTED] activities [REDACTED] (see paragraph 2.3) Approving: <ul style="list-style-type: none"> new [REDACTED] techniques or capabilities, as required [REDACTED] activities [REDACTED] (under part (a) of the Mandate) [REDACTED] activities conducted [REDACTED] (under part (a) of the Mandate), and [REDACTED] activities [REDACTED] and [REDACTED] activities [REDACTED] IRRELEVANT
Manager, [REDACTED] [REDACTED]	<ul style="list-style-type: none"> Approving [REDACTED] activities [REDACTED] (under both parts (a) IRRELEVANT of the Mandate) Maintaining a record of all [REDACTED] activities to track the approval process, [REDACTED] of the activity, and dates
Manager, [REDACTED] [REDACTED]	<ul style="list-style-type: none"> Maintaining a record of the approval process for new [REDACTED] techniques and capabilities
Director, SPR SIGINT Programs Oversight and Compliance	<ul style="list-style-type: none"> Providing guidance, as required

8. Accountability for OPS-3-1

8.1 Accountability

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

Who	Responsibility
Deputy Chief, SIGINT	Approves
Director General, Policy and Communications	Recommends for approval
General Counsel, Directorate of Legal Services	Reviews to ensure compliance with the law
Director, Disclosure, Policy and Review (formerly, Corporate and Operational Policy)	Reviews for consistency with the policy framework
Corporate and Operational Policy	<ul style="list-style-type: none"> Revises Answers questions
SIGINT Requirements	Contributes SIGINT-specific information from relevant operational areas during revisions

8.2 References

- National Defence Act*
- Most recent *Ministerial Directive on* [REDACTED] *Operations*
- Most recent *Ministerial Directive on CSE's Accountability Framework*
- Most recent *Ministerial Directive on the Collection and Use of Metadata*
- Most recent *Ministerial Directive on Privacy of Canadians*
- Most recent *Ministerial Directive on Assistance to Federal Law Enforcement and Security Agencies*
- Ministerial Authorization on* [REDACTED] *in force*
- Most recent [REDACTED]
- 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*

Continued on next page

8.2 References
(continued)

- OPS-1-8, *Active Monitoring of Operations to Ensure Legal Compliance and Protection of the Privacy of Canadians*
- OPS-1-10, *Procedures for Metadata Analysis* [REDACTED]
- OPS-1-11, *Retention Schedules for SIGINT Data*

IRRELEVANT

- OPS-4-3, *Procedures Related to the Section 16 Program*
- OPS-5-3, *Write-to-Release Procedures*
- CSSS-104, *GAMMA Handling Standards*
- CSOI-4-5, *Procedures for Metadata Analysis* [REDACTED]
- ORG-2-2, *Procedures for Creation and Management of Corporate Files Related to CSE Activities Conducted Under a Ministerial Authorization*
- CSOI-4-1, *SIGINT Reporting*
- [REDACTED] Standard Operating Procedures

8.3 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.

8.4 Enquiries

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

8.5 Review

The CSEC [REDACTED] program, including relevant policies and procedures, is subject to active monitoring (see OPS-1-8, *Active Monitoring of Operations to Ensure Legal Compliance and Protection of the Privacy of Canadians*), audit and review by various internal and external review bodies.

8.6 Records Management

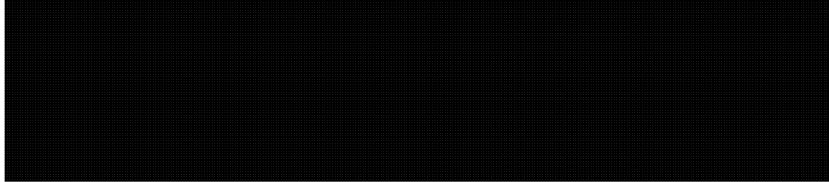
See ORG-2-2, *Procedures for Creation and Management of Corporate Files Related to CSE Activities Conducted Under a Ministerial Authorization* for information on the requirement to establish and maintain a separate corporate file for each activity or class of activities undertaken under the authority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

9. Definitions

9.1 Accountability Markings (AM)	Markings applied by analysts to recognized one-end Canadian emails [REDACTED] [REDACTED] acquired through the [REDACTED] program, and retained by CSEC because they are essential to international affairs, defence or security.
9.2 Canadian	<p>“Canadian” refers to</p> <ul style="list-style-type: none">a) a Canadian citizen, orb) a person who has acquired the status of permanent resident under the <i>Immigration and Refugee Protection Act</i>, and who has not subsequently lost that status under that <i>Act</i>, orc) a corporation incorporated under an Act of Parliament or of the legislature of a province. <p>(NDA, section 273.61)</p> <p>For the purpose of these procedures, “Canadian organizations” are also accorded the same protection as Canadian citizens and corporations.</p> <p>A Canadian organization is an unincorporated association, such as a political party, a religious group, or an unincorporated business headquartered in Canada.</p>
9.3 Data	Traffic, bulk unselected metadata, and unknown data acquired from the Global Information Infrastructure (GII).
9.4 Entity	A person, group, trust, partnership or fund or an unincorporated association or organization and includes a state or a political subdivision or agency of a state.
9.5 Essential	In reference to an intercepted private communication, this refers to a communication that provides information that responds to the intelligence priorities of the GC in relation to international affairs, defence or security.

**9.6
Exceptionally
Controlled
Information
(ECI)**

A sub-control system of the Special Intelligence (SI) control system that provides additional protection for very sensitive SIGINT activities. The sensitivity of an activity can relate to



9.7 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, CSEC treats SIGINT allies (i.e. the US, UK, Australia and New Zealand) as non-foreign.

**9.8 Foreign
Intelligence**

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.

**9.9 “In
Canada”**

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

**9.10
Information
about
Canadians**

Information about Canadians has two meanings.

IRRELEVANT

In all other contexts, the term information about Canadians refers to:

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

9.11 Integree	A person seconded to CSEC from one of CSEC's cryptologic partner organizations.
9.12 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, or the whole or any part of its content.
9.13 Ministerial Authorization (MA)	<p>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</p> <ul style="list-style-type: none"> • 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. <p>When such an authorization is in force, Part VI of the <i>Criminal Code</i> does not apply in relation to an interception of a private communication, or in relation to a communication so intercepted.</p>
9.14 Personal Information	Information that could be used to identify a person as defined in section 3 of the <i>Privacy Act</i> . For the definition of personal information, see Annex 2.
9.15 Privacy Annotations	Markings applied to SIGINT traffic in traffic repositories for the purpose of identifying 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 the categories described above. See OPS-1, Annex 2 for more information.

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

9.17 Seconded

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.

9.18 Selection Criteria

Measures that are used to identify targets [REDACTED] whose data is to be selected for forwarding to CSEC. These criteria are obtained from a number of sources, including but not limited to open source information, analysis of previously acquired SIGINT, and information provided by various departments and agencies of the GC, as well as allied agencies.

9.19 [REDACTED]

[REDACTED]

9.20 Solicitor-Client Communication

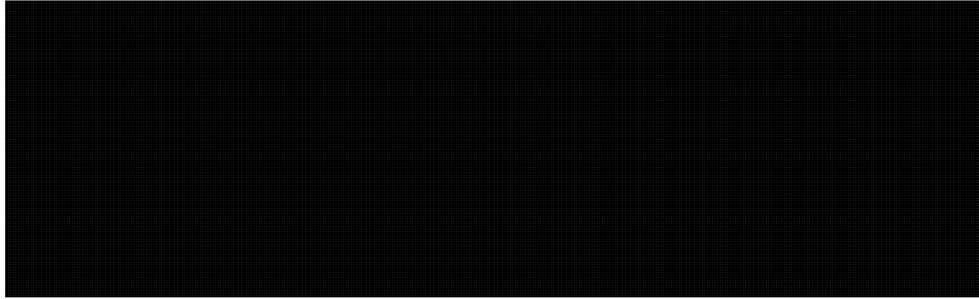
For the purposes of these procedures, a solicitor-client communication means any communication that is directly related to the seeking, formulating or giving of legal advice or legal assistance between a client and a person authorized to practice as a lawyer or a notary in the province of Quebec or as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

9.21 Target

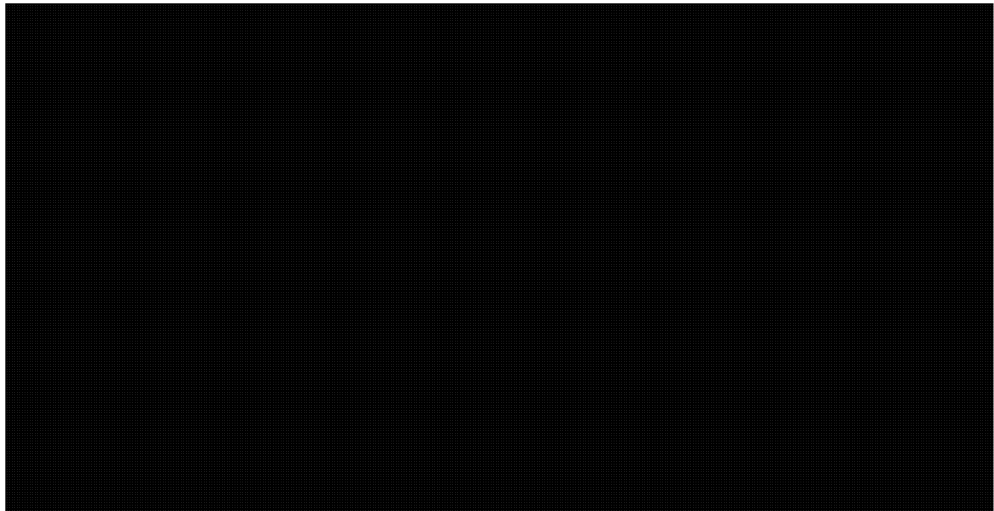
To target (v.) means to single out for collection or interception purposes.

Annex 1 – [REDACTED]

A1.1 The Rule



A1.2 [REDACTED] Activity



A1.3 [REDACTED] Activity



Continued on next page

A1.3 [REDACTED]
Activity
(continued)

[REDACTED]

A1.4 [REDACTED]
Activity

[REDACTED]

A1.5 [REDACTED]
Activity

[REDACTED]

A1.6 [REDACTED]
Activity

[REDACTED]

Annex 2 – Personal Information

Definition of Personal Information in the *Privacy Act*

"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

TOP SECRET//SI

OPS-3-1

Effective Date: 11 December 2012

(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.