Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

OPS-1

PROTECTING THE PRIVACY OF CANADIANS AND ENSURING LEGAL COMPLIANCE IN THE CONDUCT OF CSEC ACTIVITIES

OPERATIONAL POLICY

Canada

s.15(1)

Table of Contents

1. OVERVIEW 2
Legal Authorities 3
2. SIGINT AUTHORITIES AND TARGETING 7
Authority to Intercept – NDA, paragraph 273.64 (1)(a) (MANDATE A) 7
Authority to Intercept – Section 16 of the *CSIS Act* (MANDATE C) 11
3. USE, RETENTION AND DISSEMINATION OF SIGINT 14
Foreign Intelligence Reporting 19
SIGINT Report Release Authorities 20
SIGINT Retention and Dissemination 22
4. IT SECURITY 24
Protecting the Privacy of Canadians in Activities carried out under "Mandate B" 24
Use, Retention and Dissemination 25
5. 29
6. REVIEW 30
7. ADDITIONAL INFORMATION 32
8. DEFINITIONS 35
Annex 1 – Personal Information 41
Annex 2 – 43

1. OVERVIEW

1.1 Scope

This policy establishes baseline measures to protect the privacy of Canadians in the use and retention of intercepted information and ensure compliance of CSEC activities with the relevant laws of Canada, including Part V.1 of the *National Defence Act* (NDA). Detailed requirements are found in activity-specific policy instruments.

FYI: With respect to CSEC's legislated mandate under paragraph 273.64(1)(c) of the NDA (Mandate C), this policy only address CSEC support to section 16 of the *CSIS Act*. See paragraph 1.9.

This document supersedes OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities*, dated 11 March 2010, which should be destroyed.

1.2 Policy

CSEC must:

- act in strict compliance with all relevant laws of Canada including the NDA, the *CSIS Act,* the *Charter of Rights and Freedoms*, the *Privacy Act,* the *Criminal Code* and the *Financial Administration Act*, and
- only undertake activities that are within its mandate, consistent with ministerial direction and, if an authorization is required under section 273.65 of the NDA, consistent with the authorization (section 273.66 of the NDA).

1.3 Application

This policy applies to CSEC staff and any other parties who conduct activities under CSEC authorities, including secondees, and contractors.

Legal Authorities

1.4 CSEC's Mandate

CSEC is mandated to:

a) acquire and use information from the global information infrastructure (GII) for the purpose of providing foreign intelligence, in accordance with Government of Canada (GC) intelligence priorities;
b) provide advice, guidance and services, to help ensure the protection of electronic information and of information infrastructures of importance to the GC; and
c) provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties.

These are commonly referred to as Mandate A, Mandate B, and Mandate C, respectively.

1.5 Mandate Limitations

In respect of Mandates A and B, the activities undertaken by CSEC must:

- not be directed at Canadians or any person in Canada, and
- be subject to measures to protect the privacy of Canadians in the use and retention of intercepted information.

In respect of Mandate C, the activities carried out by CSEC are subject to any limitations imposed by law on assisting federal law enforcement and security agencies in the performance of their duties.

1.6 Authority to Intercept Private Communications

SIGINT: The interception of private communications for the purpose of providing foreign intelligence must only be conducted under the provisions of either:

- subsection 273.65(1) of the NDA (with a Ministerial Authorization (MA)), which authorizes CSEC to intercept private communications for the sole purpose of providing foreign intelligence in accordance with the GC's intelligence priorities
- sections 12 and 16 of the *CSIS Act* (with a judicial warrant), or
- any other lawful (that is, judicial) authority that supports a law enforcement or security agency's request for Mandate C assistance.

IT Security: Subsection 273.65(3) of the NDA authorizes CSEC to obtain an MA to intercept private communications for the sole purpose of protecting 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*

1.7 MA Requirements

SIGINT and IT Security activities conducted under an MA must satisfy conditions stated in subsections 273.65(2) and (4) of the NDA, respectively (conditions are addressed at the time a new MA is requested), and may also be subject to additional measures that the Minister considers advisable to protect the privacy of Canadians, pursuant to subsection 273.65(5) of the NDA.

1.8 Cyber Defence Activities Without an MA

IT Security may conduct cyber defence activities without an MA.

For cyber defence activities without an MA, CSEC relies on owners of computer systems or networks ("system owners") to acquire data from their systems, including private communications, which is related to a perceived cyber incident. System owners provide this data and other information, directly or indirectly, to CSEC for further analysis.

Continued on next page

1.8 Cyber Defence Activities Without an MA (continued)

Legal Provisions for the Acquisition of Private Communications by System Owners

Paragraph 184(2)(e) of the *Criminal Code* provides an exemption from criminal liability for persons who perform duties related to the management or protection of computer systems (that is, system owners) who may acquire private communications if the acquisition is necessary for such purposes.

Under section 161 of the *Financial Administration Act* (FAA), those responsible for managing or protecting GC computer systems or networks are authorized to take measures, including acquiring private communications, if the acquisition is necessary for such purposes.

Legal Provisions for the Disclosure of Private Communications to CSEC

According to section 193 of the *Criminal Code*, a system owner may disclose to CSEC all or part of a private communication, but only if the disclosure is necessary for the protection or management of the owner's computer systems. This restricts CSEC's ability to share this data with others.

Note: Section 193 of the *Criminal Code* allows any person to disclose a private communication to CSIS or the RCMP to allow those departments to fulfill their respective mandates. This means that CSEC, with the system owner's consent, may lawfully share such communications with CSIS or the RCMP.

Another method to lawfully disclose private communications involves the express and informed consent of the originator, or recipient, of a private communication. That is, if either party to the communication voluntarily discloses the communication to CSEC, CSEC may use and retain this communication in accordance with the given consent.

s.15(1)

1.9 Assistance to Law Enforcement and Security Agencies

With respect to CSEC's legislated mandate under paragraph 273.64(1)(c) of the NDA (Mandate C), this policy only addresses section 16 of the *CSIS Act*. For direction on other aspects of Mandate C, including the provision of technical and operational assistance to federal law enforcement and security agencies, the following offices must be consulted:

- Cyber Defence Support Office (CDSO) - for IT Security-related requests, or
- Director, SIGINT - for SIGINT-related requests.

These offices will in turn engage Operational Policy as necessary.

2. SIGINT AUTHORITIES AND TARGETING

Authority to Intercept – NDA, paragraph 273.64 (1)(a) (MANDATE A)

2.1 Context

Pursuant to its mandate under sub-section 273.64(1) of the NDA, CSEC requires explicit authorities as outlined below.

2.2 Authority for Foreign Intelligence Interception

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

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*

2.3 Conditions and Criteria for Foreign Intelligence MA and Approval Process

Pursuant to sub-section 273.65(1) of the NDA, the Minister of National Defence ("the Minister") may, for the sole purpose of obtaining foreign intelligence, authorize CSEC in writing to intercept private communications in relation to an activity or class of activities specified in the MA.

According to sub-section 273.65(2) of the NDA, the Minister may only issue an MA for foreign intelligence interception if satisfied that:

Continued on next page

2.3 Conditions and Criteria for Foreign Intelligence MA and Approval Process (continued)

a) the interception will be directed at foreign entities located outside Canada
b) the information could not reasonably be obtained by other means
c) the expected foreign intelligence value of the information that would be derived from the interception justifies it, and
d) satisfactory measures are in place to protect the privacy of Canadians and those measures ensure that private communications will only be used or retained if they are essential to international affairs, defence or security.

CSEC provides information as part of the documentation required for the MA approval process to satisfy the Minister that these conditions are met.

The MA would also contain any conditions that the Minister considers advisable for the purpose of protecting the privacy of Canadians, including additional measures to restrict the use and retention of, the access to, and the form and manner of disclosure of, information derived from the private communications. The MA would be in force for a period no longer than one year. (NDA, sub-section 273.68(1))

2.4 Process for Obtaining MAs under NDA sub-section 273.65(1)

The process for obtaining MAs is set out in ORG-2-1, *Procedures for Obtaining and Enabling Access to Ministerial Directives and Ministerial Authorizations.*

2.5 Authorities for

For information on these specific activities, see

- OPS-1-13, *Procedures for* *Activities*, and
- OPS-3-1, *Procedures for*

Activities

2.6 Limits on Targeting

All activities must be:

- directed at foreign entities located outside Canada
- consistent with GC intelligence priorities, and
- subject to annual review to ensure that they are consistent with GC intelligence priorities.

FYI: For more detail, see CSOI-4-4, *Targeting*

2.7

2.8

Continued on next page

2.8

s.15(1)
s.21(1)(a)
s.21(1)(b)

(continued)

2.9

Authority to Intercept – Section 16 of the *CSIS Act* (MANDATE C)

2.10 Authority

Section 16 of the *CSIS Act* authorizes CSIS to collect within Canada information or intelligence relating to the capabilities, intentions or activities of foreign states, persons or corporations. This collection, which must relate to Canada's international affairs or defence,

and following Federal Court authorization.

In accordance with the *CSIS Act* and the *CSE-CSIS Section 16 MOU*, CSEC acts as a cooperating agency, providing CSIS with operational support in the form of , technical or personnel assistance for the collection and processing of information acquired pursuant to a federal judicial warrant.

SIGINT Programs coordinates input from operational CSEC elements and consults with the Directorate of Legal Services (DLS) as appropriate.

2.11 Limits on Targeting

2.12 Verification Requirements

CSIS has a legal obligation to ensure that its activities conducted pursuant to section 16 of the *CSIS Act* are within the law.

s.15(1)
s.21(1)(a)
s.21(1)(b)

(MANDATE A)

2.13

As a result of the beneficial sharing arrangements with its SIGINT allies,

2.14 Limits on Targeting

See paragraph 2.6.

2.15

See paragraph 2.7.

Other Acquisition Activities

2.16 Other Activity

The Operational Policy Section must be consulted prior to conducting any acquisition or collection activity not addressed in the above sections. The Operational Policy Section will consult with DLS, as required.

s.15(1)
s.21(1)(a)
s.21(1)(b)

3. USE, RETENTION AND DISSEMINATION OF SIGINT

3.1 General

CSEC has adopted measures to protect the privacy of Canadians in the use, retention and dissemination of intercepted information. The use, retention and dissemination of:

- private communications
- communications of Canadians located outside Canada, or
- information about Canadians

will be strictly controlled as outlined below.

3.2 *Privacy Act* and Personal Information

Any personal information, including that of non-Canadians, is subject to the use and retention conditions set out in this policy and to the *Privacy Act* right to access and exemption provisions. (See Annex 1 for a definition of personal information.)

If any personal information has been used for an administrative purpose (decision-making process directly affecting an individual), then the *Privacy Act* requires that the personal information be retained for two years.

3.3 Criteria for Use and Retention of Intercept (Mandate A)

All intercept to be used in the production of SIGINT reports (acquired through CSEC SIGINT collection must be clearly related to GC intelligence priorities.

Continued on next page

3.3 Criteria for Use and Retention of Intercept (Mandate A)

s.15(1)
s.21(1)(a)
s.21(1)(b)

(continued)

3.4 Deletion of Intercept (Mandate A)

Continued on next page

s.15(1)
s.21(1)(a)
s.21(1)(b)

3.4 Deletion of Intercept (Mandate A) (continued)

3.5 Solicitor-Client Communications (Mandate A)

communication directly related to the seeking, formulating or giving of legal advice 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 a lawyer, notary, barrister or solicitor ("solicitor-client communication"):

Continued on next page

3.5
Solicitor-Client Communications (Mandate A)
(continued)

3.6 In accordance with the *Ministerial Directive on the*

(Mandate A)

FYI: For additional information see OPS-1-10, *Procedures for*

s.15(1)
s.21(1)(a)
s.21(1)(b)

3.7 Section 16 (Mandate C)

Information about Canadians

For information collected pursuant to section 16 of the *CSIS Act*, CSEC must comply with the condition common to all section 16 warrants related to protecting the privacy of Canadians. It states that "information about Canadians" must be destroyed unless it:

- relates to activities which would constitute a threat to the security of Canada as defined in section 2 of the *Act*
- could be used in the prevention, investigation or prosecution of an alleged indictable offence, or
-

Other Warrant Conditions

In considering section 16 warrants, the Federal Court judge may impose additional conditions as deemed necessary. CSEC must comply with these conditions.

(see OPS-4-3).

3.8 Section 16

(Mandate C)

Foreign Intelligence Reporting

3.9 Focus of SIGINT Reports

Canadian SIGINT reports must be written with a view to providing clients with foreign intelligence based on GC priorities.

3.10 Information about Canadians in SIGINT Reports

Information about Canadians must only be included in SIGINT reports if it meets one of the three criteria in paragraph 3.3.

For details , see OPS-1-7, *SIGINT Procedures*.

Note:

See the SIGINT Report Release Authorities table in paragraph 3.13.

3.11 :

(see OPS-1-7).

For details, see OPS-1-1, *Procedures for* .

SIGINT Report Release Authorities

3.12 Senior Management Approval

The release of SIGINT reports

-
-
-

generally requires approval by a senior CSEC manager

CSEC legislation and the *Ministerial Directive on the Privacy of Canadians* both require that CSEC safeguard the privacy of Canadians in the conduct of its activities. Senior manager approval provides an added level of assurance that Canadian privacy rights are being respected. The following table identifies the types of reports that require senior manager approval.

3.13 SIGINT Report Release Authorities Table

The following table sets out Report Release Authorities for SIGINT reports.

Attention: Recommend and Approval Authorities must be delegated in writing.

SIGINT Report Release Authorities

If the report is [redacted] ..	then the Category is ...	and requires signatures to Recommend:	Authorize:
A CSEC-collected **private communication**[3]	OPS-1	Director[2] from	CCSEC delegated to DC SIGINT[1]
private communication	OPS-1	Manager[2] (e.g.	CCSEC delegated to DC SIGINT[1]
A CSEC-collected communication containing **information about Canadians**[3] and the report includes information about Canadians	OPS-1	Manager[2] (e.g.	DC SIGINT delegated to
A CSEC-collected **communication**	OPS-1	Director[2] from	CCSEC delegated to DC SIGINT[1]

[1] In the absence of DC SIGINT, any other person officially acting in this position, the CCSEC or anyone officially acting as the CCSEC may act as release authority.

[2] In the absence of referenced senior managers, any other person officially acting in the referenced positions, or a higher management level may act as recommend and/or release authority. Downward delegation is not permitted.

[3]

s.15(1)
s.16(2)(c)

3.14 Labeling and Tracking of SIGINT Reports

provides a means of labeling and keeping track of SIGINT reports, in particular those that relate to the privacy of Canadians. The previous table identifies the labels (that is, the Category) that must be used for SIGINT end-product and technical reports. Proper labeling allows CSEC to provide the required statistics to the Minister (relating to private communications and for the CSEC collection programs conducted under the authority of an MA for foreign intelligence purposes (Mandate A).

SIGINT Retention and Dissemination

3.15 Storage of Intercept

Intercept used in reports or retained as background information where that intercept is:

-
-
-

must be securely stored. Hard copies of such intercept must be kept to a minimum and must be stored in a locked container when not in use;

3.16 Retention Period for CSEC Collection

CSEC may retain foreign intelligence reports indefinitely. For information about traffic retention, see OPS-1-11, *Retention Schedules for SIGINT Data.*

3.17 Retention Period for Section 16 Material

CSEC and CSIS have agreed to destruction procedures for warranted intercept pursuant to warrant conditions. For more information, see OPS-1-11. For retention and handling of from Section 16 material, see paragraph 3.8.

3.18 Collected Under Mandate A

The *Ministerial Directive on the* provides direction regarding collection, use and sharing of collected by CSEC under foreign intelligence acquisition programs. See OPS-1-11 for more information about retention.

s.15(1)
s.16(2)(c)

3.19 **CSEC SIGINT Collection**

. CSEC collection managers must ensure that these comply with and are consistent with CSEC's legislated mandate, MDs and any conditions stated in an MA. In addition, DC SIGINT may impose further limitations for national sensitivity reasons.

Section 16

Existing procedures are to be followed regarding the sharing of section 16 intercept. In some cases,

For further details, see OPS-4-3.

3.20 Sharing with IT Security

related to the protection of electronic information or information infrastructures of importance to the GC may be shared with the IT Security program, in accordance with SIGINT policy.

4. IT SECURITY

Protecting the Privacy of Canadians in Activities carried out under "Mandate B"

4.1 Context

The following measures are intended to protect the privacy of Canadians in the conduct of CSEC IT Security cyber defence activities, as required by

- sub-section 273.64(2) of the NDA, and
- the *Ministerial Directive on the Privacy of Canadians*, June 2001, and
- any relevant MA in force.

Cyber defence activities conducted under an MA are limited to computer systems and networks owned or operated on behalf of a federal institution.

Further measures to protect the privacy of Canadians are contained in relevant activity-specific policy instruments.

4.2 Precondition: Consent

Before conducting cyber defence activities on a federal institution's computer systems or networks, with or without an MA, CSEC requires that institution's consent (or for non MA activities, be satisfied that the system owner has given consent if the requesting federal institution is an intermediary).

4.3 Requirement for a Ministerial Authorization

An MA must be in force prior to the start of, and throughout, any cyber defence activity that may involve CSEC interception of a private communication.

Proposed new methods, or changes to existing non-MA methods that may result in that method intercepting a private communication, must undergo an MA requirement determination by CDSO (in consultations with DLS, as required).

4.4 Annual Confirmation

Persons conducting cyber defence activities must confirm yearly that they have read and understood this policy, as well as relevant legal authorities and policy instruments related to their specific cyber defence activities.

4.5

Use, Retention and Dissemination

4.6 Information Requiring Protection

In the course of conducting cyber defence activities, the following information must be accorded privacy protection:

Private Communications, including those
- intercepted under MA, and
- intercepted and disclosed under a system owner's authority (or any reference to the existence of that private communication), and

Information about Canadians, which includes
- any personal information about a Canadian, or
- any information about a Canadian corporation.

4.7

Cyber defence reports may include

to providing advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the GC.

4.8 *Privacy Act* and Personal Information

Any personal information, including that retained as a result of these activities must be accounted for in CSEC's Personal Information Bank for cyber protection.

Personal information obtained during cyber defence activities must not be used for administrative purposes by CSEC.

4.9 Relevancy of Information	that is relevant to ensuring the protection of electronic information and of information infrastructures of importance to the GC.
4.10	
4.11 Access to and Storage of Information	All information obtained or produced by CSEC during cyber defence activities must be securely stored, with limited access.
4.12 Retention Schedules	Retention and disposition schedules for data and other information must be established for each cyber defence activity, in accordance with: • The *Library and Archives of Canada Act* • MAs (for those activities requiring an MA), and • MoUs or other formal agreements with federal institutions.
4.13 Release Authority for	DGPC is the release authority for from cyber defence activity reports. This authority is delegated to the Operational Policy Section, except in cases of (authority remains with DGPC), or for exemptions (DC ITS and DGPC).

s.15(1)
s.21(1)(a)
s.21(1)(b)

4.14 Reports Having Multiple Sources

Reports containing information obtained under different authorities (for example, cyber defence activities under MA, as well as activities without an MA) are subject to dissemination restrictions detailed in activity-specific policy instruments, as well as the release levels noted in the following paragraphs.

If the release levels (and recommendation levels) are different for each source (for example, due to the presence of or in one of the sources), the higher level must sign.

4.15 Report Release Authorities

The following table sets out report release levels for dissemination of cyber defence reports beyond CSEC. See activity-specific policy instruments for guidance on access to cyber defence reports within CSEC.

Cyber Defence Report Release Authorities

Report Type	Dissemination (beyond CSEC)	Recommen-dation level	Approval level
All reports	To the federal institution from which the information was obtained (with no further dissemination)	Operational Supervisor	Operational Manager (or higher)
Reports containing	the federal institution from which the information was obtained		
Reports containing	the federal institution from which the information was obtained	Director	DC ITS, delegated to DG level
Reports containing		Director General	Chief, delegated to DC ITS

Continued on nest page

s.15(1)
s.21(1)(a)
s.21(1)(b)

4.15 Report Release Authorities (continued)

In the absence of the recommend or approval authorities, any other person officially acting in the referenced position or a higher management level (within the same authority hierarchy) may act as recommend or approval authority.

Note: For cyber defence activities without an MA, the federal institution that requested assistance

See activity-specific policy instruments for details on

6. REVIEW

6.1 Review

CSEC activities, including relevant policies and procedures, are subject to internal monitoring for policy compliance, audit and review by various government review bodies, including, but not limited to, the Office of the CSE Commissioner and the Privacy Commissioner.

6.2 CSE Commissioner

Pursuant to section 273.63 of the NDA, the CSE Commissioner plays a key role in providing independent review of CSEC activities. The Commissioner's mandate is to:

- review CSEC activities to ensure that they are lawful, including a review of CSEC activities conducted under MAs
- carry out investigations where necessary in response to a complaint
- report annually to the Minister, and
- inform the Minister and the Attorney General of Canada of any CSEC activity that the Commissioner believes may not be in compliance with the law.

In pursuing his/her mandate, the CSE Commissioner shall have full access to all CSEC staff, documentation (except for Cabinet documents) and materials. CSEC staff is obliged to cooperate fully with the CSE Commissioner and his staff. However, any requests for copies of legal opinions require prior consultation with DLS given the solicitor-client privilege.

6.3 External Review: Information Requirements

CSEC staff must ensure that all relevant information and documentation is entered into corporate systems of record (for example, CERRID, . When information is requested by external reviewers, CSEC is better placed to demonstrate evidence of its legal and policy compliance when it is able to retrieve and make available records that:

- demonstrate compliance with authorities and any associated conditions or constraints (for example, legal, MD, MA, policy, etc.) that could have lawfulness or privacy implications
- record management decisions and rationales, especially those related to operations, legal, and policy

Continued on next page

s.15(1)

6.3 External Review: Information Requirements (continued)

- provide a record of management decisions
- confirm that supervisors are monitoring compliance with conditions established in authority documents, and
- demonstrate CSEC's identification of any non-compliance issues and associated corrective actions (for example,

7. ADDITIONAL INFORMATION

7.1 Responsibility for This Policy

This table indicates responsibilities with respect to this policy.

Who	Responsibility
DC SIGINT	• Approving revisions to Chapters 1, 2, 3, 5, 6, 7 and 8 of this policy • Applying this policy • Seeking legal advice, as required
DC IT Security	• Approving revisions to Chapters 1, 4, 5, 6, 7 and 8 of this policy • Applying this policy • Seeking legal advice, as required
DGPC	• Recommending this policy for approval • Seeking legal advice, as required
General Counsel, Directorate of Legal Services	• Providing legal advice, when requested • Reviewing this policy and advising on its compliance with the law
Operational Policy Section	• Revising this policy • Answering questions regarding this policy • Seeking legal advice, as required
All CSEC Managers	• Ensuring their staff: o read this policy at least once per year, and o understand and comply with this policy
All CSEC staff and any other parties acting under CSEC authorities	Reading, understanding and complying with this policy

s.15(1)
s.16(2)(c)

7.2 References

- *National Defence Act*, Part V.1
- *Criminal Code of Canada*
- *CSIS Act*
- *Financial Administration Act*
- *Library and Archives of Canada Act*
- *Privacy Act*
- *Ministerial Directive on CSE's Accountability Framework*, June 2001
- *Ministerial Directive on the* March 2005
- *Ministerial Directive on the Privacy of Canadians*, June 2001
- CSE/CSIS MOU on Section 16
- OPS-1-1, *Procedures for the*
- OPS-1-6, *Operational Procedures for*
- OPS-1-7, *SIGINT Procedures*
- OPS-1-10, *Procedures for*
- OPS-1-11, *Retention Schedules for SIGINT Data*
- OPS-1-13, *Procedures for*
- OPS-3-1, *Procedures for*
- OPS-4-3, *Procedures*
- ORG-2-1, *Procedures for Obtaining and Enabling Access to Ministerial Directives and Ministerial Authorizations*
- ORG-2-2, *Procedures for Handling Documents Related to CSE Activities Conducted Under a Ministerial Authorization*
- CSOI-4-1, *SIGINT Reporting*
- CSOI-4-2,
- CSOI-4-4, *Targeting*

7.3 Enquiries

All questions related to this policy should be directed to operational Managers, who in turn will contact Operational Policy staff when necessary.

7.4 Amendments

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

7.5 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 subsections 273.65(1) or 273.65(3) of the NDA.

s.15(1)
s.16(2)(c)

8. DEFINITIONS

8.1 Canadian

"Canadian" refers to

a) a Canadian citizen, or
b) a person who has acquired the status of permanent resident under the *Immigration and Refugee Protection Act* 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, section 273.61)

For the purposes of this policy, "Canadian organizations" are also accorded the same protection as Canadian citizens and corporations.

A Canadian organization is an unincorporated association, such as a political party, a religious group, or an unincorporated business headquartered in Canada.

8.2

8.3

8.4 CSEC SIGINT Collection

For the purposes of these policy, CSEC SIGINT collection refers to acquisition conducted by CSEC, when required, pursuant to paragraph 273.64(1)(a) of the NDA. It includes, but is not limited to:

-
-
-
-
-
-

CSEC SIGINT collection does not include (acquired by CSEC under paragraph 273.64(1)(a) of the NDA, or (conducted under paragraph 273.64(1)(c) of the NDA).

8.5 Cyber Defence Activities

Cyber defence activities are conducted in order to identify, isolate or prevent harm to Government of Canada computer systems or networks of importance to the Government of Canada.

8.6 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).

8.7 Foreign

In the context of the NDA and the *Canadian Security Intelligence Service Act (CSIS Act)*, "foreign" refers to non-Canadian.

8.8 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)

8.9 Global Information Infrastructure (GII)

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. (NDA, section 273.61)

s.15(1)
s.16(2)(c)

8.10 "In Canada"

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

8.11 Information about Canadians

For the purposes of this document, information about Canadians has two meanings.

In the context of section 16 of the *CSIS Act*, "information about Canadians" is defined in warrants as information contained in any communication intercepted pursuant to the warrant, or information obtained that relates to a person who is a Canadian citizen, a permanent resident within the meaning of the IRPA, or a corporation incorporated by or under an Act of Parliament or of the legislature of a province.

Each time it is referred to in this document in the Section 16 context, the term will appear in quotations as follows: 'information about Canadians'.

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

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

8.12

8.13

8.14 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

- sub-section 273.65(1) of the NDA for the sole purpose of obtaining foreign intelligence, or
- sub-section 273.65(3) of the NDA for the sole purpose of protecting the computer systems or networks of the GC.

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.

8.15

8.16 Personal Information

Personal information is defined in the *Privacy Act* as "information about an identifiable individual that is recorded in any form". See Annex 1 for the complete definition.

8.17 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)

8.18 Second Party Second Party refers to CSEC's counterparts: the US National Security Agency (NSA), the UK Government Communications Headquarters (GCHQ), Australia's Defence Signals Directorate (DSD), and New Zealand's Government Communications Security Bureau (GCSB).

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

8.20

8.21

(see Annex 2).

8.22 SIGINT Reports Reports that are based on SIGINT and linked to a GC intelligence requirement (GCR). They include, but are not limited to:

- (See CSOI 4-1, *SIGINT Reporting.*)
-
-

Continued on next page

8.22 SIGINT Reports (continued)

•

•

•

(See CSOI-4-2,

8.23 Solicitor-Client Communications

For the purpose of these policy, 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.

8.24

FYI: For SIGINT reports, see OPS-1-7, *SIGINT*
For IT Security cyber defence reports, see OPS-1-6,

8.25 Targeting

To single out for collection or interception purposes.

Annex 1 – 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

(*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.

---

s.15(1)
s.16(2)(c)
s.21(1)(a)
s.21(1)(b)

Annex 2 –

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

s.15(1)
s.16(2)(c)

OPS-3-1

Procedures for

OPERATIONAL POLICY

Canada

s.15(1)
s.16(2)(c)

Table of Contents

1. Introduction 3
Policy Scope and Application 3
Activity Description 4
Legal Authorities 5
2. Mandate A: Legal and Policy Requirements 6
3. Mandate A: Approval Processes for Activities 9
Activities 10
Activities 12
4. Mandate C: Legal and Policy Requirements 13
5. Mandate C: Approval Processes for Activities 15
..... 15
..... 16
6. Rules for the Use and Retention 17
Targeting and Collection 17
Reporting 19
Data Use, Retention and Storage 20
Sharing Information 21
7. Roles and Responsibilities 23
8. Additional Information 25
9. Definitions 28
Annex 1 - 32
Annex 2 – Personal Information 34

s.15(1)
s.16(2)(c)

1. Introduction

Policy Scope and Application

1.1 Scope

CSEC can conduct 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 ("Mandate A"), 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 ("Mandate C").

These procedures govern CSEC's activities conducted under both Mandate A and Mandate C. This document supersedes OPS-3-1, *Procedures for Activities*, dated 23 December 2009, which should be destroyed.

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 activities
- set out the approval processes for conducting the various levels of activity
- set out the accountability trail for these activities
- provide direction to personnel regarding the handling of data, and
- document the activities authorized

1.3 Policy

Mandate A activities 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 *Ministerial Authorization* [MA] *on Activities* in force
- comply with all relevant Ministerial Directives, including the *Ministerial Directive on the Privacy of Canadians*, the *Ministerial Directive on the* the *Ministerial Directive on the*

Continued on next page

1.3 Policy (continued)

and the *Ministerial Directive on CSE's Accountability Framework*

-
-
- 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.

Mandate C activities are subject to limitations imposed by law on the requesting agency.

1.4 Application

These procedures apply to:

- CSEC staff
- staff, and
- any other parties who conduct activities under the authorities listed in this chapter, including secondees, and contractors.

Activity Description

1.5 What is

Continued on next page

1.5 What is

(continued)

1.6 Who is Permitted to Conduct Activities?

Standard Operating Procedures (SOPs).

1.7

Legal Authorities

1.8 Authorities for Mandate A Activities

CSEC conducts Mandate A activities under the authority of:

- the NDA
- the *Ministerial Directive on* (January 2002), and
- the *Ministerial Directive on* (March 2005).

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.

1.9 Authorities for Mandate C Activities

CSEC conducts Mandate C activities under the authority of:

- the NDA, and
- all laws governing the activities of the organization that CSEC is assisting.

---

2. Mandate A: Legal and Policy Requirements

2.1 Protecting the Privacy of Canadians

In accordance with paragraphs 273.64(2)(a) and (b) of the NDA, the communications of Canadians located anywhere must not be targeted, and CSEC must have measures in place to protect the privacy of Canadians.

2.2 Targeting Conditions

All Mandate A activities must be directed at foreign entities (for example, a person, group or association) located outside Canada, and must be linked to GC intelligence priorities. That is, the purpose of these activities is to obtain information of foreign intelligence value to Canada.

2.3

2.4

2.5 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 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

2.6 Informing the Minister

Information Relating to Private Communications and Solicitor-Client Communications

CSEC must record the following information and send a report to the Minister,

Continued on next page

2.6 Informing the Minister (continued)

Annual Reporting

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

2.7 Proposals

The table below outlines the process to be followed

Step	Who Does It	Activity
1	Team Member	Prepares proposal
2	Manager,	Reviews and recommends or rejects the proposal
3	Director,	Approves or denies the proposal (in consultation with DLS, as necessary)

2.8 Record Keeping

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

The Manager must also track the approval process for new proposals.

3. Mandate A: Approval Processes for Activities

3.1 Introduction

This chapter outlines the approval processes for Mandate A.

Activities

Step	Who Does It	Activity
1	Team Member	Prepares proposal for activity in accordance with the SOPs
2	Manager,	• Reviews and approves the activity • Reviews and recommends the activity
3	Director,	Reviews and approves the activity

s.15(1)
s.16(2)(c)

Activities

Step	Who Does It	Activity
Stage 1: Proposal		
1	Team Member	Drafts an operational proposal for the Manager, in accordance with the SOPs, which will include at a minimum: • details of the proposed operation, including the • a description of methods or measures taken to comply with the direction in these procedures, and • a rationale-based assessment of the
Stage 2: Recommendation to proceed		
2		**If the activity is ...** / **Then Recommend Authority is...** Manager, Director, DC SIGINT
Stage 3: Approval		
3		**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: The Director, may consult with DLS at any stage.

s.15(1)

3.2 Delegation of Recommend Authority

In the absence of the Recommend 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 Authority.

3.3 Delegation of Approval Authority for Activities

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

3. 4 Delegation of Approval Authority for Activities

Approval Authorities for activities must be delegated at the discretion of the CCSEC. The table below lays out alternate Approval Authorities in the absence of the regular Approval Authority.

In the absence of ...	Approval Authority is delegated to ...
Director,	• Director General, , or • any Executive officially designated to carry out the duties of DG (in extenuating circumstances, CCSEC may officially designate someone to carry out the duties of DG)
DC SIGINT	• CCSEC, or • any senior Executive officially designated to carry out the duties of CCSEC
CCSEC	Any Executive officially designated to carry out the duties of CCSEC

Activities

Step	Who Does It	Activity
1	Team Member	• Drafts a proposal (or an operational proposal for the Manager, in accordance with the SOPs, which will include at a minimum: • details of the proposed operation, including • a description of methods or measures used to comply with the direction in these procedures, and • a rationale-based assessment • Prepares a separate operational security plan in accordance with policies, procedures and the SOPs
2	Director,	In consultation with DG , recommends for review
3	DC SIGINT	In consultation with CCSEC,
4	CCSEC	• Informs the National Security Advisor and consults with the Minister • Recommends proceeding or further internal review, as appropriate
5	National Security Advisor	Approves the operation

Note: The Director, may consult with DLS at any stage.

s.15(1)

4. Mandate C: Legal and Policy Requirements

4.1 Mandate C Limitations

In conducting Mandate C activities to assist LESAs, CSEC must comply with the requesting agency's authority to undertake the activity.

> **FYI:** For more information on CSEC support to LESAs, see OPS-4-1, *Procedures for CSE Support to Law Enforcement,* and OPS-4-2, *Procedures for Assisting CSIS Section 12 Activities*. For more information on CSEC support to CSIS under the provisions of Section 16 of the *CSIS Act*, see OPS-4-3, *Procedures*

4.2 Targeting Conditions

All Mandate C activities are conducted from Canada. These activities may be conducted

4.3 Written Request for Assistance

CSEC must only provide assistance to a LESA on receipt of a written request which refers specifically to the agency's authority to undertake the activity.

4.4

See the related paragraphs in OPS-4-3.

4.5

See the related paragraphs in OPS-4-3.

s.15(1)

4.6

4.7 Proposals for

See paragraph 2.7.

4.8 Record Keeping

See paragraph 2.8.

5. Mandate C: Approval Processes for Activities

5.1 Introduction

This chapter outlines the approval processes for Mandate C:

- activities conducted f , and
- activities conducted

Attention: The steps outlined below are not exhaustive. Other steps are required when processing Mandate C requests (for example, consultation with the Directorate of Legal Services). These additional steps are laid out in OPS-4-1 and OPS-4-2.

Activities

Step	Who Does It	Activity
1	LESA	Prepares and submits a request to SIGINT
2		Processes the request and forwards to Team
3	Team Member	Prepares proposal for activity in accordance with the SOPs
4	Manager,	• Reviews and approves the activity • Reviews and recommends
5	Director,	Reviews and approves the activity

Activities

Step	Who Does It	Activity
1	LESA	Prepares and submits a request to
2	Team Member	Drafts an operational proposal for the Manager, in accordance with the SOPs, which will include at a minimum: • a description of the proposed operation • name of assisted body • confirmation that it is a LESA and has the legal authority to undertake the activity, e.g. a warrant • a description of methods or measures taken to comply with the direction in these procedures, and •
3	Manager,	Reviews operational proposal and makes recommendation to the Director,
4	Director,	Approves operation, with LESA concurrence

5.2 Delegation of Recommend and Approval Authorities

See paragraphs 3.2, 3.3 and 3.4.

6. Rules for the Use and Retention

6.1 Introduction

This section outlines the rules for:

- targeting and collection
- handling collected traffic
- reporting
- using
- storage and retention, and
- sharing of information.

Targeting and Collection

6.2

(Mandate A)

6.3

6.4

(Mandate A)

6.5 See the related paragraph in OPS-1.

(Mandate A)

6.6 See the related paragraphs in OPS-1 for both Mandate A and Mandate C.

Reporting

6.7 Reporting

Mandate A

SIGINT reports based on traffic collected under Mandate A must adhere to existing policy instruments, including:

- OPS-1
- OPS-1-7, *SIGINT Procedures*
- OPS-5-3,
- OPS-5-5, *Procedures for*
- OPS-5-8,
- CSOI-4-1, *SIGINT Reporting.*

All other special handling or restricted distribution rules also apply.

Mandate C

Any reporting of Mandate C traffic must be done in accordance with the requester's instructions.

6.8 Report Classification

SIGINT reports based on collection must be classified at a minimum TOP SECRET//COMINT.

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

Operational Policy is the authority for releasing from SIGINT reports derived from collection. See OPS-1-1, *Procedures for*

Data Use, Retention and Storage

6.11 Using Data

6.12

(Mandate A)

FYI: For additional information see OPS-1-10, *Procedures for*

6.14 Data Retention	See the related paragraphs in OPS-1-11, *Retention Schedules for SIGINT Data*, for both Mandate A and Mandate C.
6.15 Storage of Traffic	See OPS-1 for details on storing information about Canadians. traffic where that traffic contains

Sharing Information

6.16 Reports

Mandate A

All current CSEC reporting procedures apply to sharing reports based on Mandate A activities (subject to all dissemination control markings or sharing restrictions contained in specific operational plans).

Mandate C

The CSIS-CSEC Liaison Officer must approve the release of reports derived from collection obtained pursuant to Section 16 of the *CSIS Act*.

For all other reports based on operations conducted under Mandate C, CSEC must seek the approval of the agency to which it is providing support.

6.17 Data

Mandate A

Traffic obtained from activities may be with the prior approval of the appropriate Managers in (that is, those Managers whose operations are directly supported by the activity).

Prior to providing the proposed must be satisfied that they are associated with:

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

Continued on next page

6.17 Data (continued)

Data acquired as a result of the as requested. CSEC must retain an archived copy of

These measures include:

- SIGINT reports, in accordance with the CSEC Policy, and
-

Mandate C

7. Roles and Responsibilities

7.1 Roles and Responsibilities

This table summarizes roles and responsibilities with respect to activities.

Who	Responsibility
Chief, CSEC	• Providing the Minister with the information listed in paragraph 2.6 • Approving activities conducted (Mandate A) • Informing the National Security Advisor and consulting with the Minister for ; (Mandate A) • Seeking legal advice when required
Deputy Chief, SIGINT	• Approving activities conducted from Canada (Mandate A) • (Mandate A) • Seeking legal advice when required
Director General,	Acting as the Director, when that Director is absent
Director,	• (see paragraph 2.4) • Approving: ○ ○ (Mandate A) ○ (Mandate A), and ○ activities (Mandate C) • Seeking legal advice when required

Continued on next page

s.15(1)

Who	Responsibility
Manager,	• Approving activities (Mandate A and Mandate C) • Maintaining a record of: o all activities to track the approval process, of the activity, and dates, and o the approval process for proposals
SIGINT	Providing guidance on what is considered to be as required

8. Additional Information

8.1 Accountability

The following table outlines the accountability structure with respect to these procedures.

Who	Responsibility
Deputy Chief, SIGINT	• Approving these procedures • Seeking legal advice, as required
• Director General, • Director General,	• Applying these procedures • Seeking legal advice, as required
Director General, Policy and Communications	• Approving these procedures • Seeking legal advice, as required
General Counsel, Directorate of Legal Services	• Providing legal advice, when requested • Reviewing these procedures and advising on their compliance with the law
Manager, Operational Policy	• Revising these procedures to ensure that they comply with the MA in force • Answering questions related to these procedures • Seeking legal advice, as required
CSEC and Managers who are involved in activities	Ensuring that their staff have read, understood and comply with these procedures
CSEC and any other parties who are involved in activities	Reading, understanding and complying with these procedures

s.15(1)
s.16(2)(c)

8.2 References

- *National Defence Act*
- *Ministerial Directive on* (14 January 2002)
- *Ministerial Directive on CSE's Accountability Framework* (June 2001)
- *Ministerial Directive on the* (March 2005)
- *Ministerial Directive on Privacy of Canadians* (June 2001)
- *Ministerial Authorization on* in force
- DFAIT/CSE Memorandum of Understanding (20 May 2002)
- MOU on section 16 of the CSIS Act ("Tri-Ministerial" MOU, August 1987)
- OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities*
- OPS-1-1, *Procedures for*
- OPS-1-7, *SIGINT Procedures*
- OPS-1-8, *Active Monitoring of Operations to Ensure Legal Compliance and Protection of the Privacy of Canadians*
- OPS-1-10, *Procedures for*
- OPS-1-11, *Retention Schedules for SIGINT Data*
- OPS-4-1, *Procedures for CSE Support to Law Enforcement*
- OPS-4-2, *Procedures for Assisting CSIS Section 12 Activities*
- OPS-4-3, *Procedures Related to the Section 16 Program*
- OPS-5-3, *Procedures*
- OPS-5-5, *Procedures for*
- OPS-5-8, *Handling Standards*
- 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*

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 Operational Policy website.

8.4 Enquiries

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

8.5 Review

The CSEC 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 government review bodies, including, but not limited to, the CSEC Commissioner and the Privacy Commissioner.

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 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, section 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.

9.2 Data

Data is traffic and bulk unselected metadata, and unknown data acquired from the Global Information Infrastructure (GII).

9.3 Entity

Entity means 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.

9.4 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

9.5 Foreign

In the context of the NDA and the *Canadian Security Intelligence Service Act (CSIS Act)*, "foreign" refers to non-Canadian.

9.6 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.

9.7 "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.

9.8 Information about Canadians

For the purpose of this document, information about Canadians has two meanings.

In the context of section 16 of the *CSIS Act*, "information about Canadians" is defined in warrants as information contained in any communication intercepted pursuant to the warrant, or information obtained that relates to a person who is a Canadian citizen, a permanent resident within the meaning of IRPA, or a corporation incorporated by or under an Act of Parliament or of the legislature of a province.

Each time it is referred to in this document in the Section 16 context, the term will appear in quotations as follows: "information about Canadians".

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

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

9.9

9.10

9.12 Ministerial Authorization (MA)

An MA is an authorization provided in writing by the Minister of National Defence (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.

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.

9.13 Personal Information

Personal Information means information that could be used to identify a person as defined in section 3 of the *Privacy Act*. For the definition of personal information, see Annex 2.

9.15 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)

9.16 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.

9.19 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.

9.20 Target

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

Annex 1 –

A1.1 The Rule

A1.2
Activity

s.15(1)

A1.3
Activity

A1.4
Activity

A1.5
Activity

A1.6
Activity

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

(*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.

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

s.15(1)
s.16(2)(c)

OPS-1-13

PROCEDURES FOR

OPERATIONAL POLICY

Canada

s.15(1)
s.16(2)(c)

Table of Contents

1. Introduction 3
Policy Scope and Application 3
Legal Authorities 5
2. Program: Description and Approval Process 7
3. Program: Description and Approval Process 12
4. Program: Description and Approval Process 14
5. Activities: Description and Approval Process 19
6. Data Collection: All Programs 22
Collection – Traffic 22
Collection – 24
7. Data Use and Retention: All Programs 25
Use – Traffic 25
Use – 27
Use – Data 28
Retention 29
8. Data Sharing: All Programs 30
9. Additional Information 33
10. Definitions 36
Annex 1 – Personal Information 45

1. Introduction

Policy Scope and Application

1.1 Scope

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

-
-
-
-

FYI: These procedures address activities conducted under Mandate A only. For activities conducted under 273.64(1)(c) of the NDA (Mandate C), see OPS-4-1, *Procedures for CSE Support to Law Enforcement*, and OPS-4-2, *Procedures for Assisting CSIS Section 12 Activities*. For information on CSEC's activities, see OPS-3-1.

1.2 Objective

The purpose of these procedures is to:

- document the approval processes for conducting these programs
- prescribe an accountability trail for these activities
- provide direction to those involved in these programs regarding the collection, use and retention of associated data acquired pursuant to Ministerial Directives (MDs) and Ministerial Authorizations (MAs), and

Continued on next page

1.2 Objective (continued)

- 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 Privacy of Canadians* (June 2001), and
  - OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities.*

1.3 Policy

All CSEC SIGINT described herein, aimed at acquiring foreign intelligence, 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 Privacy of Canadians*
  - *Ministerial Directive on the* (March 2005)
  - *Ministerial Directive on CSE's Accountability Framework* (June 2001), and
  - *Ministerial Directive,* (2004)
- 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.

---

s.15(1)
s.16(2)(c)

1.4 Application These procedures apply to CSEC and staff, secondees, contractors, 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:

1.5 Previous Procedures These procedures supersede OPS-1-13, *Procedures for* dated 23 December 2008, which should be destroyed.

Legal Authorities

1.6 Authorities CSEC conducts activities under the authority of:

- Mandate 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 [GC] intelligence priorities"
- the *Ministerial Directive on the* and
- a valid MA. Because the activities of each program that falls within these procedures may result in the interception of private communications, each program requires a discrete MA. An MA authorizes CSEC, 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.

1.7 Privacy Protection Measures

All activities conducted pursuant to Mandate A must:

a) not be directed at Canadians anywhere or any person in Canada, and
b) be subject to measures to protect the privacy of Canadians in the use and retention of intercepted information.

1.8 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).

1.9 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 7.1 for more information).

2. Program: Description and Approval Process

2.1 Description The Canadian program includes any activities conducted under CSEC authorities in the relevant MA, at:

2.2

s.15(1)
s.16(2)(c)
s.21(1)(a)
s.21(1)(b)

2.3 SIGINT Activities

Continued on next page

s.15(1)
s.16(2)(c)
s.21(1)(a)
s.21(1)(b)

2.3 SIGINT

Activities
(continued)

2.4 SIGINT

s.15(1)
s.16(2)(c)
s.21(1)(a)
s.21(1)(b)

2.5 Approval Process

The following table outlines the approval process for SIGINT Development and collection.

Step	Who Does It	Activity
1	•	Make an initial statement of the intelligence requirement, including associated GC Requirements (GCRs),
		Attention: must submit the requirement to for onward forwarding to
2		• Drafts an which includes the following information: ○ intelligence requirement/GCRs • Forwards to the Director,
3	Director,	Reviews and: • approves or rejects and returns to • for other recommends to proceed and forwards to the Director, or rejects and returns to (along with a rationale as to why it was rejected)

Continued on next page

s.15(1)
s.16(2)(c)
s.21(1)(a)
s.21(1)(b)

2.5 Approval Process *(continued)*

Step	Who Does It	Activity
4	Director,	Reviews and • approves or rejects and returns to • for other recommends to proceed or rejects and returns to . (along with a rationale as to why it was rejected)

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

2.6 Types of Approval: Annual vs Case-by-case

For steps 3 and 4 in the preceding table:

If the activity is related to...	Then ...
	approval is given annually
	approval is given on a case-by-case basis; however, each is reviewed annually to ensure that it is still valid and meets GC intelligence priorities

s.15(1)
s.16(2)(c)
s.21(1)(a)
s.21(1)(b)

3. Program: Description and Approval Process

3.1 Description

3.2 Approval Process

Step	Who Does It	Activity
1	• • CSEC staff	Make an initial statement of the intelligence requirement, including associated GCRs, to . **Attention:** must submit the requirement for onward forwarding to
2		

Continued on next page

s.15(1)
s.16(2)(c)
s.21(1)(a)
s.21(1)(b)

3.2 Approval Process *(continued)*

Step	Who Does It	Activity
3		• Drafts an which includes the following information: ○ intelligence requirements/GCRs ○ ○ ○ ○ • Forwards to the Director,
4	Director,	• Reviews and • Recommends to proceed and forwards to the Director, or rejects and returns to (along with a rationale as to why it was rejected).
5	Director,	Approves or denies

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

3.3 Types of Approval: Annual vs Case-by-case

For steps 4 and 5 in the preceding table:

If the activity is related to...	Then ...
	approval is given annually
	approval is given on a case-by-case basis for an indeterminate or fixed period of time; however, each is reviewed annually to ensure that it is still valid and meets GC intelligence priorities

s.15(1)
s.16(2)(c)
s.21(1)(a)
s.21(1)(b)

4. Program: Description and Approval Process

4.1 Description

4.2

4.3

4.4

Continued on next page

s.15(1)
s.16(2)(c)
s.21(1)(a)
s.21(1)(b)

4.4

(continued)

(see paragraph 4.7).

4.5

as described in paragraph 4.4.

4.6

4.7 Approvals

The responsibility for [redacted] approvals are shared as follows:

s.15(1)
s.16(2)(c)
s.21(1)(a)
s.21(1)(b)

s.15(1)
s.16(2)(c)
s.21(1)(a)
s.21(1)(b)

4.8

Approval Process

The following table outlines the approval process for

Step	Who Does It	Activity
1	• • CSEC SIGINT staff	Make an initial statement of the intelligence requirement, including associated GCRs, to **Attention:** must submit the requirement to for onward forwarding to
2		• Drafts an , which includes the following information: ○ intelligence requirement/GCRs ○ ○ ○ ○ ○ • Forwards to the Director,
3	Director,	• Reviews , and • Recommends to proceed and forwards to the Director, or rejects and returns to (along with a rationale as to why it was rejected)
4	Director,	Approves or denies .

Continued on next page

s.15(1)
s.16(2)(c)
s.21(1)(a)
s.21(1)(b)

4.8

Approval Process (continued)

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

4.9 Types of Approval:
Annual vs Case-by-case

For steps 3 and 4 in the preceding table:

If the activity is related to...	Then ...
	approval is given annually
	approval is given on a case-by-case basis; however, each is reviewed annually to ensure that it is still valid and meets GC intelligence priorities

s.15(1)
s.16(2)(c)
s.21(1)(a)
s.21(1)(b)

5. Activities: Description and Approval Process

5.1 Description

CSEC conduct foreign intelligence activities in support of both operations carried out by

5.2 Approval Process

Continued on next page

s.15(1)
s.21(1)(a)
s.21(1)(b)

5.2

Approval Process (continued)

The following table outlines the approval process for

Step	Who Does It	Activity
1	• CSEC staff • • •	Make an initial statement of the intelligence requirement, including associated GCRs, to **Attention:** (must submit the requirement to the for onward forwarding to
2		• Drafts an , which includes the following information: ○ intelligence requirement/GCRs ○ ○ ○ ○ ○ • Forwards to the Director,
3	Director,	• Reviews , and • Recommends to proceed and forwards :o the Director, or rejects and returns to (along with a rationale as to why it was rejected)
4	Director,	Approves or denies

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

5.3 Types of Approval: Annual vs Case-by-Case

For steps 3 and 4 in the preceding table:

If the activity is related to ...	Then ...
	approval is given annually
	approval is given on a case-by-case basis

s.15(1)
s.21(1)(a)
s.21(1)(b)

6. Data Collection: All Programs

Collection – Traffic

6.1 Targeting Rules: Canadians

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

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

are associated with a foreign intelligence entity located outside Canada, and relate to a GC intelligence priority.

Continued on next page

s.15(1)
s.16(2)(c)
s.21(1)(a)
s.21(1)(b)

6.1 Targeting Rules: Canadians *(continued)*

[redacted]

6.2

6.3 Targeting Rules: Second Parties

The relationship among the Five-Eyes SIGINT agencies is based on the [redacted] 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.

[redacted]

6.4

[redacted]

s.15(1)
s.16(2)(c)
s.21(1)(a)
s.21(1)(b)

Collection –

6.5 Collection
Rules

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*

7. Data Use and Retention: All Programs

Use – Traffic

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

Continued on next page

s.15(1)
s.16(2)(c)
s.21(1)(a)
s.21(1)(b)

7.1 SIGINT

(continued)

7.2 SIGINT Activity

7.3

7.4 Reporting

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

- OPS-1
- OPS-1-7, *SIGINT*
- OPS-5-3,
- OPS-5-5, *Procedures for*
- OPS-5-7, *Handling Standards*
- CSOI-4-1,

All other special handling or restricted distribution rules apply.

s.15(1)
s.16(2)(c)
s.21(1)(a)
s.21(1)(b)

7.5 Report Classification

The table below lists information regarding 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.

Collection	Minimum Classification
	SECRET//COMINT
	TOP SECRET//COMINT
	TOP SECRET//COMINT
	TOP SECRET//COMINT

7.6 Report Release Authorities

See OPS-1 for information on report release authorities.

7.7 Storage of Traffic

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

- private communication

7.8 Authority for Release of Information

Operational Policy is the authority for the release of information. See OPS-1-1, *Procedures for* for more information.

Use -

7.9

s.15(1)
s.16(2)(c)
s.21(1)(a)
s.21(1)(b)

7.10 Using must be used only for the following purposes:

For additional information on see OPS-1-10, *Procedures for*

7.11 Using in SIGINT Reports See paragraphs 7.4, 7.5 and 7.6.

Use – Data

7.12 Use of Data

Access to data must be authorized by the Director,

Retention

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

s.15(1)
s.16(2)(c)
s.21(1)(a)
s.21(1)(b)

8. All Programs

8.1

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:

s.15(1)
s.16(2)(c)
s.21(1)(a)
s.21(1)(b)

8.2

8.3

1

8.4 Subject to approval from the Director, SIGINT CSEC may

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

s.15(1)
s.21(1)(a)
s.21(1)(b)

8.5 Subject to approval from Operational Policy, CSEC may share

8.6

s.15(1)

9. Additional Information

9.1 Accountability

The following table outlines responsibilities with respect to these procedures.

Who	Responsibility
Deputy Chief, SIGINT	• Approving these procedures • Seeking legal advice, as required
Director General, Policy and Communications	• Approving these procedures • Seeking legal advice, as required
• •	• Applying these procedures • Seeking legal advice, as required
General Counsel, Directorate of Legal Services	• Providing legal advice, when requested • Reviewing these procedures and advising on their compliance with the law
Manager, Operational Policy	• Revising these procedures to ensure that they comply with the MAs in force • Answering questions related to these procedures • Seeking legal advice, as required
All CSEC managers who are involved in the SIGINT activities described herein	Ensuring their staff read, understand, and comply with these procedures
All CSEC staff (see paragraph 1.4) who are involved in the SIGINT activities described herein	Reading, understanding and complying with these procedures

s.15(1)
s.16(2)(c)

9.2 References

- *Charter of Rights and Freedoms*
- *Criminal Code*
- *National Defence Act*
- *Privacy Act*
- *Ministerial Directive on CSE's Accountability Framework* (June 2001)
- *Ministerial Directive on the* (March 2005)
- *Ministerial Directive on Privacy of Canadians* (June 2001)
- *Ministerial Directive* ' (2004)
- *Ministerial Authorization on* in force
- *Ministerial Authorization on* in force
- *Ministerial Authorization on* in force
- *Ministerial Authorization on Activities (* in force
- DFAIT/CSE Memorandum of Understanding (2009)
- OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities*
- OPS-1-1, *Procedures for*
- OPS-1-7, *SIGINT* *Procedures*
- OPS-1-8, *Active Monitoring of Operations to Ensure Legal Compliance and Protection of the Privacy of Canadians*
- OPS-1-10, *Procedures for*
- OPS-1-11, *Retention Schedules for SIGINT Data*
- OPS-3-1, *Procedures for*
- OPS-5-3, *Procedures*
- CSOI-4-1, *SIGINT Reporting*

9.3 Enquiries

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

9.4 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 Operational Policy website.

s.15(1)
s.16(2)(c)

9.5 Review	Canadian activities, including relevant policies and procedures, are 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 government review bodies, including, but not limited to, the CSEC Commissioner and the Privacy Commissioner.
9.6 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.

10. Definitions

10.1

10.2

10.3 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.

10.4 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.

10.5

s.15(1)
s.16(2)(c)

10.6	
10.7 Data	Data is defined as traffic acquired from the GII.
10.8	
10.9 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, paragraph 273.61)
10.10	

10.11 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	s.15(1) s.16(2)(c) s.21(1)(a) s.21(1)(b)
10.12 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, paragraph 273.61)	
10.13		
10.14		
10.15 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)	
10.16 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.	

10.17

10.18

10.19 Information about Canadians

Information about Canadians refers to:

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

10.20

10.21 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.

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.

s.15(1)
s.16(2)(c)

10.22

10.23 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.

10.24

For more information, see OPS-1, Annex 2.

10.25 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 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)

s.15(1)
s.16(2)(c)

10.26

10.27

10.28

10.29 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.

10.30 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).

10.31

10.32

s.15(1)
s.16(2)(c)

10.33

10.34

10.35 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.

10.36

10.37

s.15(1)
s.16(2)(c)

10.38

10.39

10.40

Annex 1 – 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

(*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.

Pages 126 to / à 143

are withheld pursuant to sections

sont retenues en vertu des articles

15(1), 21(1)(a), 21(1)(b)

of the Access to Information

de la Loi sur l'accès à l'information
Loi sur l'accès à l'information

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

CSEC SIGINT Operations Instruction

CSOI-4-3

Protecting the Privacy of Canadians in the Use and Retention of Material for SIGINT

Last Updated:
11 April 2011

s.15(1)

Table of Contents

1. INTRODUCTION 4
1.1 Objective 4
1.2 Authority 4
1.3 Context 5
1.4 References 6
1.5 Application 6
1.6 Accountability 7
1.7 Amendment Process 7
1.8 Inquiries 7
1.9 Review 8

2. HANDLING OF CPRI 9
2.1 Introduction 9
2.2 Severing of Data 9
2.3 Need-to-Know 9
2.4 "Clean Desk" Approach 9
2.5 Avoid Making Copies 10
2.6 10
2.7 EPR Sign-off 10
2.8 Retention and Storage of EPRs 10

3. HANDLING OF CPRI 12
3.1 Introduction 12
3.2 Avoid Making Copies 12
3.3 "Clean Desk" Approach 12
3.4 Need-to-Know 12
3.5 12
3.6 12
3.7 Sharing of SIGINT Information with GC Clients 13
3.8 Storage of 13
3.9 Section 16 Traffic 13
3.10 14
3.11 14
3.12 15
3.13 Open Source Intelligence 15

4. INTERNAL REVIEWS OF CPRI HOLDINGS 16
4.1 Biannual Reviews of All Holdings 16
4.2 Monthly Reviews of Traffic 17

s.15(1)

5. SUMMARY OF OPERATIONAL ROLES AND RESPONSIBILITIES 18
5.1 Overview 18

6. DEFINITIONS 20
6.1 Associated Material 20
6.2 Canadian 20
6.3 Canadian Identity Information (CII) 20
6.4 Canadian privacy-related Information (CPRI) 20
6.5 Canadian SIGINT Production Chain 20
6.6 Need-to-Know 21
6.7 Personal information 21
6.8 Open Source Intelligence 21
6.9 21

ANNEX 1 -- 22

CSOI-4-3 PROMULGATION 23

s.15(1)
s.16(2)(c)
s.21(1)(a)
s.21(1)(b)

1. Introduction

1.1 Objective

As per paragraph 273.64(2)(b) of the *National Defence Act* (NDA), CSEC is required to take active measures to protect the privacy of Canadians in the performance of its mandated activities. These instructions provide guidelines to be followed in order to protect Canadian privacy-related information (CPRI) that is encountered in the conduct of day-to-day SIGINT activities. For the purposes of this CSOI, CPRI refers to private communications, communications of a Canadian abroad or information about Canadians or Canadian Identity Information (CII).

These instructions supplement the measures within the *Ministerial Directive on the Privacy of Canadians* and in OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities*.

These instructions focus on the physical and electronic handling measures for CPRI obtained through the conduct of SIGINT activities and used:

•

These instructions also provide guidance on the handling of information obtained through information disclosures made to CSEC by Government of Canada (GC) clients.

1.2 Authority

This CSEC SIGINT Operations Instruction is issued under the authority of the CSEC Deputy Chief, SIGINT (DCSIGINT).

s.15(1)
s.21(1)(a)
s.21(1)(b)

1.3 Context

Given the complexity of the Global Information Infrastructure, CSEC will inevitably encounter CPRI while conducting its SIGINT activities. CSEC is committed to taking reasonable measures and implementing appropriate policies to protect the privacy of Canadians in the handling, retention, use and destruction of this material.

This CSOI shall be used in conjunction with the processes stipulated in CSEC's OPS documents. In the event of any discrepancies between this CSOI and the OPS documents, the OPS documents shall supersede this CSOI.

CPRI can only be retained for these reasons:

Measures to protect privacy are outlined in several operational policy (OPS) documents:

- OPS-1: *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities*
  - within SIGINT repositories
  - Section 16 warrant
    (OPS-1)
  - obtaining senior management report release approvals

- OPS-1-1: *Procedures of t*

- OPS-1-7: *SIGINT . Procedures*

- OPS-1-10: *Operational Procedures for*

- OPS-1-11: *Retention Schedules for SIGINT Data*
  - conforming to retention and storage guidelines

1.4 References

- *National Defence Act*
- Ministerial Directive, *Privacy of Canadians*, June 2001
- Ministerial Authorizations
- OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities*
- OPS-1-1, *Procedures for*
- OPS-1-7, *SIGINT Procedures*
- OPS-1-8, *Active Monitoring of Operations to Ensure Legal Compliance and the Protection of the Privacy of Canadians*
- OPS-1-10, *Operational Procedures for*
- OPS-1-11, *Retention Schedules for SIGINT Data*
- OPS-1-13, *Procedures for*
- OPS-3-1, *Procedures for*
- OPS-4-3, *Procedures*
- CSOI-4-1, *SIGINT Reporting*
- CSOI-4-4, *Targeting and Management*
- CSOI-5-3, *Canadian SIGINT*
- OPS-5-15, *Need-To-Know Guidelines*
- Standard Operating Procedures (SOP) for SIGINT Information Needs via _____@cse-cst.gc.ca

s.15(1)
s.16(2)(c)
s.21(1)(a)
s.21(1)(b)

1.5 Application

These instructions apply to all individuals and elements within the Canadian SIGINT including GC authorized to conduct SIGINT activities under the authority of CSEC DCSIGINT. This includes personnel operating under the authority of the

1.6 Accountability

The following table outlines responsibilities with respect to these instructions.

Who	Responsibility
Deputy Chief SIGINT	• Approving these instructions.
Director General SIGINT	• Recommending these instructions for approval.
Director SIGINT	• Promulgating and implementing these instructions. • Revising these instructions as required. • Seeking legal and/or policy advice if required. • Responding to questions concerning these instructions.
Director of Legal Services	• Provide advice on these instructions when requested by Director SIGINT
SIGINT Directors-General and Directors who are affected by these instructions	• Applying these instructions.
All CSEC managers and Supervisors and leaders who are affected by these instructions	• Ensuring that their staff has read, understood and complies with these instructions and any amendments to these instructions.
All CSEC staff and members who are affected by these instructions	• Reading, understanding and complying with these instructions and any amendments to these instructions.

1.7 Amendment Process

Situations may arise where amendments to these instructions may be required because of changing or unforeseen circumstances. All approved amendments will be announced to staff and will be posted on the SIGINT home page.

1.8 Inquiries

Questions related to these instructions should be directed to Operational Managers, who in turn will consult with SIGINT staff (e-mail: @cse-cst.gc.ca) when necessary.

1.9 Review

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

2. Handling of

2.1 Introduction

When preparing a report analysts and reviewers must follow these instructions in order to protect the privacy of Canadians.

For the purposes of this CSOI, EPRs include the following releasable SIGINT products:

2.2

2.3 Need-to-Know

Report drafts and associated material must only be reviewed and edited by individuals with a need-to-know, in accordance with OPS-5-15, *Need-to-Know Guidelines*.

2.4 "Clean Desk" Approach

A "clean desk" approach is to be adopted when dealing with a report in progress and its associated material. When analysts are away from their desks for an extended period (one hour or longer), the report and all associated material must be stored in a temporary holding folder out of sight--either in a drawer or in the overhead storage of the employee's workstation.

[2] Instructions for is in CSOI-4-1, Appendix H.

2.5 Avoid Making Copies

2.6

2.7 EPR Sign-off The sign-off sheet, EPR

2.8 Retention and Storage of EPRs Approved EPRs and their associated material must be stored in an approved security container :

[4]Specific instructions for are in CSOI-4-1, Appendix H.

3. Handling of

3.1 Introduction

This section provides instructions on the handling of obtained through the conduct of SIGINT activities or

3.2 Avoid Making Copies

As a general rule, copies of

Hardcopy material containing CPRI that is no longer required must be shredded in an approved shredder.

3.3 "Clean Desk" Approach

A "clean desk" approach should be adopted when dealing with should be out of sight when not in use.

3.4 Need-to-Know

Sharing is permitted on a need-to-know basis within the team (OPS-5-15)

3.5

3.6

3.7

3.8

3.9 Section 16 Traffic

Traffic obtained through the authority of Section 16 of the *CSIS Act* containing

---

[5] Memorandum, 23 July 2010, CERRID #588491,

Pages 157 to / à 158

are withheld pursuant to sections

sont retenues en vertu des articles

15(1), 21(1)(a), 21(1)(b)

of the Access to Information

de la Loi sur l'accès à l'information
Loi sur l'accès à l'information

4. Internal Reviews of Holdings

4.1 Biannual Reviews of All Holdings

On a biannual basis, Level IV Managers of operational areas must complete a review of all holdings and complete a "Confirmation of Review" (form located in Annex 1) and send the completed form to

Level IV Managers must review the following:

will retain operational area confirmations and notifications for use in other review activities, as required.

4.2 Monthly Reviews of Traffic

In addition to the biannual review, on a monthly basis Level IV Managers are responsible for ensuring traffic and meet the criteria for retention (see section 1.3).

Monthly, will send a report containing all traffic for the month to Level IV Managers. Level IV Managers must ensure that staff review the list of traffic items for retention.

Additionally, for any Level IV Managers must provide documentation to to demonstrate consultation with DLS (OPS-1, 3.5).

Level IV Managers are responsible for retaining the results of these monthly reviews for future audits or reviews.

5. Summary of Operational Roles and Responsibilities

5.1 Overview The following table provides an overview of roles and responsibilities with respect to these instructions.

Who	Responsibilities
SIGINT personnel	• Remain well-versed in OPS-1 and complete the OPS-1 on-line quiz annually. • Depending on position held, traffic, as per OPS-1. • Storing CPRI as required. • Maintain awareness of policies--changes/updates.
Level V Supervisor	• Ensure that analysts receive proper training regarding handling and storage of CPRI; e.g. OPS-1 briefing, and CSOI 4-3, *Protecting the Privacy of Canadians in the Use and Retention of Material for SIGINT.* • Ensure analysts are aware of policy changes/updates. • Ensure that CPRI retained by the team is properly stored and destroyed. • Ensure that analysts are reviewing, at least twice a year, retained material and revalidating the need for its retention and deleting it if no longer required.
Level IV Manager	• On a monthly basis review traffic Keep results of this review available for any audits or reviews and provide documentation on consultation with DLS • Establish hard copy and electronic storage systems to allow for biannual review. • Provide biannual reports to (see section 4.1).
SIGINT	• On a monthly basis review all traffic for retention and

	• Maintain copies of all review documents sent to Production Managers on a monthly basis for immediate access by review bodies. • Track and file emails received from Level IV Managers that confirm DLS consultation :

6. Definitions

6.1 Associated Material

6.2 Canadian

"Canadian" refers to:

a) a Canadian citizen;
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.

"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.

6.3 Canadian Identity Information (CII)

CII refers to information

* GC Institutions do not fall within this definition.

6.4 Canadian privacy-related Information (CPRI)

Canadian privacy-related information includes private communications, communications of a Canadian abroad or information about Canadians, Canadian corporations or Canadian organizations.

6.5

6.6 Need-to-Know

Need-to-know is a fundamental aspect of CSEC's information handling system, and 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 needs to see all of it.

6.7 Personal information

Personal information is defined in the *Privacy Act* as "information about an identifiable individual that is recorded in any form". See Annex 1 of OPS-1 for the complete definition.

6.8 Open Source Intelligence

Open Source Intelligence is any unclassified, publicly available information that can be found in a variety of different sources including print, television, radio and the internet.

6.9

ANNEX 1 -- Operational Area Biannual Confirmation of Review Activity Form

Review Date: _____

Operational Area: _____
Full name of operational area

Please check boxes to indicate that a review has been completed for the following:

Signing this document confirms that, for your operational area, the above have been reviewed to ensure that any Canadian privacy-related information (CPRI) being retained meets the criteria for retention as outlined in CSOI-4-3, section 1.3. Additionally, your signature confirms that access to CPRI is limited to those with a need-to-know. Moreover, you signature also confirms that any items no longer meeting this criteria have been deleted or destroyed.

Signature: _____

Print Name: _____

Title: _____

(The email template version (available from of this document can be emailed to or the signed hardcopy version of this document can be send to by internal mail.)

s.15(1)

CSOI-4-3 Promulgation

Reviewed and Recommended for Approval

I have reviewed and hereby recommend these instructions for approval.

14. AP. 2011
Date

Director General SIGINT Programs

Approved

I hereby approve CSOI-4-3: *Protecting the Privacy of Canadians in the Use and Retention of Material for SIGINT*. These instructions are effective immediately.

Shelly Bruce
Deputy Chief SIGINT

15 April 2011
Date