



OPS-1

**Protecting the Privacy of Canadians and
Ensuring Legal Compliance in the
Conduct of CSEC Activities**

OPERATIONAL POLICY

Canada

Table of Contents

1. OVERVIEW	2
Legal Authorities	3
2. SIGINT AUTHORITIES AND TARGETING	5
Authority to Intercept – NDA, paragraph 273.64 (1)(a) (part (a) of the Mandate)	5
Authority to Intercept – IRRELEVANT of the Mandate).....	9
3. USE, RETENTION AND DISSEMINATION OF SIGINT	11
Foreign Intelligence Reporting	16
SIGINT Report Release Authorities	17
SIGINT Retention and Dissemination	20
4. IT SECURITY	22
Protecting the privacy of Canadians in activities carried out under Part (b) of the Mandate	22
Use, Retention and Release.....	23
5. PRIVACY INCIDENTS REPORTING	27
6. REVIEW	29
7. ACCOUNTABILITY FOR OPS-1	31
8. DEFINITIONS.....	33
Annex 1 – Personal Information	39
Annex 2 – Business Information.....	41
Annex 3 – SIGINT Privacy Annotations and Accountability Markings	42

1. OVERVIEW

1.1 Scope

This policy establishes baseline measures to protect the privacy of Canadians in the use and retention of information intercepted by CSEC and to 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.

IRRELEVANT

This document supersedes OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities*, dated 1 December 2011, which should be destroyed.

1.2 Policy

CSEC must:

- act in strict compliance with all relevant laws of Canada including the NDA, the *Charter of Rights and Freedoms*, the *Privacy Act* (PA), 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 has been issued 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, intregrees and contractors.

Legal Authorities

1.4 CSEC's Mandate

CSEC's mandate as Canada's National Cryptologic Agency consists of three parts:

- 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 part (a), part (b), and part (c) of the Mandate, respectively.

1.5 CSEC Mandate Limitations

In respect of parts (a) and (b) of the Mandate, 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 part (c) of the Mandate, 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: Subsection 273.65(1) of the NDA permits the Minister to issue a Ministerial Authorization (MA) allowing CSEC to intercept private communications for the sole purpose of obtaining foreign intelligence in accordance with the GC's intelligence priorities.

IT Security: Subsection 273.65(3) of the NDA permits the Minister to issue an MA allowing CSEC 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. These activities may include analysis and mitigation support, tool deployment, or other services. Any interception of private communications that occurs as a result of these activities must be authorized by the interception authority set out in paragraph 184(2)(e) of the *Criminal Code*.

IRRELEVANT

2. SIGINT AUTHORITIES AND TARGETING

Authority to Intercept – NDA, paragraph 273.64 (1)(a) (part (a) of the Mandate)

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	<p>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.</p> <p>CSEC acquires telecommunications-related information used to identify, describe, manage or route all or part of the telecommunication, information referred to as "metadata", to gain a better understanding of the GII and identify new targets. This activity, also authorized under paragraph 273.64(1)(a) of the NDA, does not require an MA and is conducted in accordance with the <i>Ministerial Directive on the Collection and Use of Metadata</i>.</p>
2.3 Conditions and Criteria for Foreign Intelligence MA and Approval Process	<p>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.</p> <p>According to sub-section 273.65(2) of the NDA, the Minister may only issue an MA for foreign intelligence interception if satisfied that:</p>

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 Activity-Specific Procedures

For information on:

- [REDACTED] collection,
 - joint CSEC-GC activities, [REDACTED] collection [REDACTED]
 - interception in support of joint CSEC-CF activities, and
 - [REDACTED]
- see
- OPS-1-13, *Operational Procedures Related to Canadian [REDACTED] Collection Activities*, and
 - OPS-3-1, *Operational Procedures for [REDACTED] Activities*.

2.6 Limits on Targeting

All selectors and methods used in collection and acquisition in the integrated national cryptologic enterprise 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 and Selector Management*.

2.7 Inadvertent Targeting of Canadians or Persons in Canada

In the event that a Canadian or a person in Canada is inadvertently targeted, the following actions must be taken as soon as possible:

Step	Action
1	The selector must be de-targeted.
2	Any existing traffic resulting from that selector must be destroyed.
3	Any SIGINT reports based on the traffic must be cancelled.
4	CSEC's SIGINT Programs, Oversight and Compliance (SPOC) must be notified and apprised of the actions taken. SPOC, in turn, will notify the Corporate and Operational Policy Section of the incident and actions
5	The Corporate and Operational Policy Section must track these occurrences (see Chapter 5).

2.8 SIGINT Privacy Annotations and Verification Requirements

If analysts whose functions are directly related to the production of foreign intelligence reports recognize that SIGINT traffic is a private communication, a communication of Canadians located outside Canada, or contains information about Canadians, and which is not essential to international affairs, defence or security, then they must, upon recognition, annotate this traffic for deletion. Private communications and communications of Canadians located outside Canada deemed essential to international affairs, defence, or security must also be annotated appropriately. See Annex 3 for instructions on SIGINT Privacy Annotations.

Continued on next page

**2.8 SIGINT
Privacy
Annotations
and
Verification
Requirements
(continued)**

Should an analyst recognize traffic where:

- both the originator and the recipient of a communication are Canadians
- both the originator and recipient are located in Canada, or
- where one communicant is in Canada and the other is a Canadian abroad

and the traffic is not collected as a result of a legitimate foreign selector, then the traffic must be annotated for deletion. All associated selectors must be reviewed and both [REDACTED] and SPOC must be notified. SPOC will track all such incidents.

If analysts identify a foreign selector that continues to yield only private communications or communications of Canadians located outside Canada that are not essential to international affairs, defence or security, then the analyst must take appropriate remedial action, including notifying [REDACTED] and SPOC to have the selector removed or the targeting modified.

**2.9
Determining
Essentiality**

MAAs governing CSEC SIGINT interception activities state that a private communication will be considered essential to international affairs, defence or security only if it contains information that is clearly related to GC intelligence priorities. See the Foreign Intelligence Priorities (FIP) list, GC Requirements (GCRs), and the National SIGINT Priorities List (NSPL).



Note: This essentiality test related to traffic use and retention also applies to traffic from other collection sources used by CSEC in the production of foreign intelligence in accordance with part (a) of the Mandate (see paragraph 3.3). For information on determining the essentiality of including information about Canadians in reports, see paragraph 3.10.

Authority to Intercept – Section 16 of the *CSIS Act* (part (c) of the Mandate)

IRRELEVANT

Acquisition from Second Party Sources (part (a) of the Mandate)

2.12 Selection of Intercept

As a result of the beneficial sharing arrangements with its SIGINT allies, CSEC acquires a considerable amount of foreign intelligence [REDACTED] consistent with GC priorities from Second Parties. Second Parties conduct collection activities in pursuit of their own national interests and in accordance with their domestic laws.

[REDACTED]

2.13 Limits on Targeting

See paragraph 2.6.

2.14 SIGINT Privacy Annotations and Verification Requirements

See paragraph 2.7.

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 information intercepted by CSEC. 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** All personal information is subject to the use and retention conditions set out in this policy and to the PA right to access and exemption provisions. (See Annex 1 for a definition of personal information and refer to subsection 8(2)(a) and (b) of the PA for use and disclosure rights.)
- If any personal information has been used for an administrative purpose (decision-making process directly affecting an individual), then the PA requires that the personal information be retained for two years.
-
- 3.3 Criteria for Use and Retention of Intercept (part (a) of the Mandate)** All intercept to be used in the production of SIGINT reports (acquired through CSEC SIGINT collection or from Second Parties) must be clearly related to GC intelligence priorities.
- If during the course of scanning intercept, analysts
- identify a private communication, or a communication of a Canadian located outside Canada (an MA is a prerequisite for some programs), or
 - observe a communication that contains information about Canadians
- then this intercept may be retained if it:
- (a) is foreign intelligence as defined in the NDA using the following criteria:**
- 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
-

Continued on next page

3.3 Criteria for Use and Retention of Intercept
(part (a) of the Mandate)
(continued)

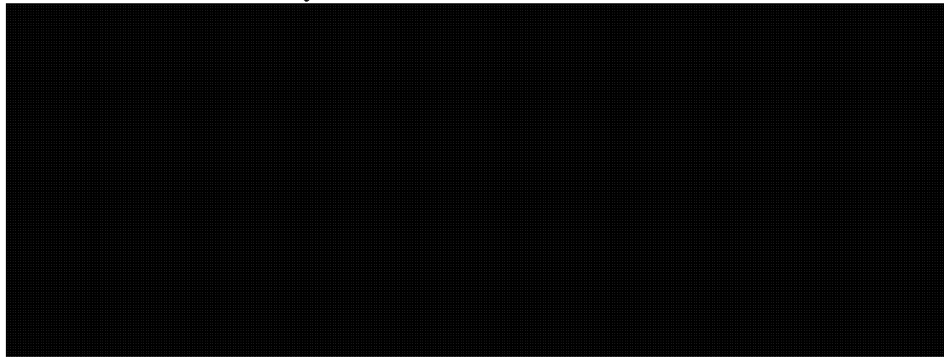
(b) is essential to protect the lives or safety of individuals of any nationality, using the following criteria:

- the information could be useful to federal agencies or other countries in preventing, identifying or investigating a potential threat against the life and safety of any individual in Canada or abroad

or,

(c) contains information on serious criminal activity relating to the security of Canada using the following criteria only:

- capabilities/intentions/activities of a foreign terrorist/terrorist group relating to international affairs, defence or security
- threats to the security of Canada



3.4 Deletion of Intercept (part (a) of the Mandate)

Information or intelligence that does not relate to one of the criteria listed in the previous paragraph must be annotated for deletion in traffic databases if recognized, and no hard copies shall be retained (see Annex 3). In cases where CSEC has intentionally created a copy (or copies) of a traffic item in several traffic databases, each copy must be annotated for deletion (see exemption below).

Continued on next page

3.4 Deletion of Intercept (part (a) of the Mandate)
(continued)

Exemptions: Duplicates of traffic items that have not been viewed are exempt from this requirement.

An exemption also occurs when:

- analysts deem the intercept to be of foreign intelligence value, and
- the intercept contains information about Canadians that does not relate to one of the above criteria, and
- this information cannot be easily severed from the foreign intelligence portions of the traffic.

Under such circumstances, and despite the presence of information about Canadians, the intercept may be retained in its entirety and stored according to this policy.

3.5 Handling Solicitor-Client Communications (part (a) of the Mandate)

In cases where an analyst recognizes 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"):

- a) The analyst shall annotate that communication for deletion unless the analyst believes it may contain foreign intelligence;
- b) If the analyst believes that a solicitor-client communication may contain foreign intelligence, then the analyst shall annotate that communication for retention and immediately bring the communication to the attention of his/her Director (via the reporting chain);
- c) The Director shall forthwith obtain legal advice from DLS on whether the continued retention and/or use of the solicitor-client communication would be in conformity with the laws of Canada, and not bring the administration of justice into disrepute;

Continued on next page

**3.5 Handling
Solicitor-Client
Communications
(part (a) of the
Mandate)**
(continued)

- d) Where legal advice has been obtained that the retention or use of a solicitor-client communication would be in conformity with the laws of Canada, and not bring the administration of justice into disrepute, CSEC may only use or retain the information derived from the solicitor-client communication in conformity with the legal advice received.

If the communication must be deleted, this must be carried out through the process by which analysts must annotate such communications, when recognized, as outlined in Annex 3.

**3.6 Searching
and Using
Metadata (part
(a) of the
Mandate)**

In accordance with the *Ministerial Directive on the Collection and Use of Metadata*, metadata may be searched for the purpose of providing any information or intelligence about the capabilities, intentions or activities of a foreign individual, state, organization, terrorist group or other such entities as they relate to international affairs, defence or security, including any information related to the protection of electronic information or information infrastructures of importance to the GC that may be used for CSEC part (b) purposes which includes sharing with the IT Security program.

Metadata must be used only for the following purposes:

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



FYI: For additional information on contact chaining, see OPS-1-10, *Operational Procedures for Metadata Analysis*

IRRELEVANT

3.8 IRRELEVANT

IRRELEVANT

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. When drafting such reports, CSEC/CFIOG production analysts must focus on the activities, capabilities and intentions of foreign intelligence targets. For example, if a report covers discussions between a foreign person and a Canadian, the emphasis must be placed on the foreign person's assessment of the discussion, not on the identity, statements or views of the Canadian.

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 on naming, see OPS-1-7, *Operational Procedures for Naming in SIGINT Reports*.



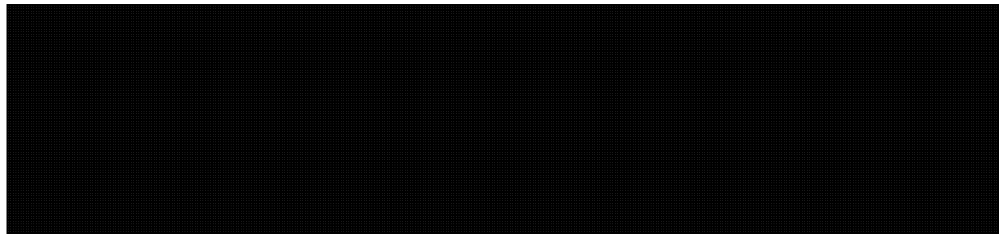
Note: The [REDACTED] must approve reports based on CSEC or Second Party collection sources that include information about Canadians. See the SIGINT Report Release Authorities table in paragraph 3.13.

3.11 Suppressed Information

When SIGINT analysts include Canadian identity information (CII) in a SIGINT report, this information must be suppressed and replaced with a generic term (see OPS-1-7).

Continued on next page

3.11 Suppressed Information (continued)



Analysts must input CII suppressed from SIGINT reports into the [REDACTED] database. Once this information is in the database, it is accessible only to the Corporate and Operational Policy Section and a limited number of system administration staff, as well as to report authors and others in the reporting chain (e.g., reviewers, editors, contributors, and releasers).

The [REDACTED] is the authority for the release of suppressed information. This authority in some cases is delegated in writing to the Corporate and Operational Policy Section, which responds to and tracks requests for suppressed information. Under certain circumstances, this authority is delegated in writing to [REDACTED] or trained individuals fulfilling the function of Client Relations Officers. For details, see OPS-1-1, *Procedures for Release of Suppressed Information from SIGINT Reports*.

SIGINT Report Release Authorities

3.12 Senior Management Approval

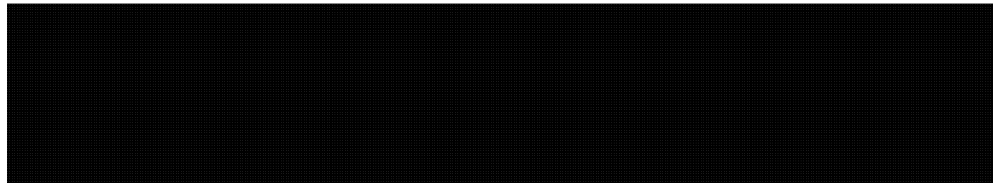
The release of SIGINT reports:

- based on a private communication
 - based on communications of a Canadian located outside Canada, or
 - containing information about Canadians
- generally requires approval by a senior CSEC manager¹ (see exemption below).

Continued on next page

¹ A senior manager is considered to be anyone over the level of Director; see the table in paragraph 3.13.

**3.12 Senior
Management
Approval**
(continued)



The NDA 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.

Continued on next page

<u>SIGINT Report Release Authorities</u>			
If the report is based on ...	then the Category is ...	and requires signatures to	
		Recommend:	Authorizes:
A CSEC-collected (under part (a) authority) private communication ³	OPS-1A	Director ² from [REDACTED]	CCSEC delegated to DC SIGINT ¹
A Second Party-acquired private communication or communication to which a Canadian located outside Canada is a party ³	OPS-1B	Manager ² (e.g. [REDACTED] from [REDACTED])	CCSEC delegated to DC SIGINT ¹
A CSEC-collected or Second Party-acquired communication or metadata containing information about Canadians ³ and the report includes information about Canadians	OPS-1C	Manager ² (e.g. [REDACTED])	DC SIGINT delegated to [REDACTED]
A CSEC-collected communication to which a Canadian located outside Canada is a party ³	OPS-1E	Director ² from [REDACTED]	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. In threat-to-life silent-hours situations, Managers may sign reports. DC SIGINT and [REDACTED] must sign the reports *post factum*.

³ Where contextual identification of a Canadian is possible, DGPC authorization via Corporate and Operational Policy is also required.

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 solicitor-client communications) for the CSEC collection programs conducted under the authority of an MA for foreign intelligence purposes (part (a) of the Mandate).

SIGINT Retention and Dissemination

3.15 Storage of Intercept

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

- a private communication
 - a communication of a Canadian located outside Canada, or
 - a communication containing information about Canadians
- 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; soft copies outside of traffic databases must be stored in electronic folders with limited access. See OPS-1-11, *Retention Schedules for SIGINT Data* for details.

3.16 Retention Period for CSEC Collection and Acquisition from Second Parties

CSEC may retain foreign intelligence reports indefinitely. For information about traffic retention, see OPS-1-11.

IRRELEVANT

3.18 Metadata Collected Under Part (a) of the Mandate

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

3.19 Sharing of Intercept with Second Parties**CSEC SIGINT Collection**

Where technically feasible, Second Parties, via CSEC collection managers, [REDACTED] acquiring communications of foreign entities located outside Canada [REDACTED] CSEC collection managers must ensure that these selectors 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.

Metadata

Subject to any conditions stated in the *MD on the Collection and Use of Metadata*, CSEC may share metadata acquired through its foreign intelligence acquisition programs with international allies to maximize its mandate activities as set out in the NDA, and strengthen Canada's partnerships abroad. Such sharing must be subject to strict conditions to protect the privacy of Canadians, consistent with these standards governing CSEC's other programs. For greater certainty, Canada's allies must not be granted access to metadata known to be associated with Canadians located anywhere or persons located in Canada unless it is altered prior to granting access in such a way as to render impossible the identification of the persons to whom the metadata relates.

IRRELEVANT

3.20 Sharing with IT Security

Subject to any conditions stated in the MDs or MAs, SIGINT intercept and metadata acquired in the execution of CSEC's foreign intelligence program related to cyber threats may be shared with the IT Security program. Appropriate SIGINT and Operational policies and procedures must be followed for any use of this intercept or metadata by the IT Security program.

4. IT SECURITY

Protecting the privacy of Canadians in activities carried out under Part (b) of the Mandate

4.1 Context	<p>The following measures are intended to protect the privacy of Canadians in the conduct of CSEC cyber defence activities, as required by:</p> <ul style="list-style-type: none"> • sub-section 273.64(2) of the NDA, • the most recent <i>Ministerial Directive on the Privacy of Canadians</i>, and • any relevant MA in force. <p>Cyber defence activities conducted under an MA are limited to computer systems and networks owned or operated on behalf of a federal institution.</p> <p>Further measures to protect the privacy of Canadians are contained in relevant activity-specific policy instruments.</p>
4.2 Precondition: Consent	<p>Before conducting cyber defence activities with or without an MA, CSEC requires the consent of a system owner, or must be satisfied that the system owner has given consent if the requesting institution is an intermediary.</p>
4.3 Requirement for a Ministerial Authorization	<p>An MA must be in force or CSEC must be operating under the authority of system owners and administrators pursuant to subsection 184(2)(e) of the <i>Criminal Code</i> prior to the start of, and throughout, any cyber defence activity that may involve the interception of a private communication.</p> <p>Proposed new activities, or changes to existing non-MA activities that may result in the interception of private communications, must be reviewed by IPOC (in consultation with DLS, as required).</p>
4.4 Annual Confirmation	<p>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.</p>

4.5 Criminal Activity

If, in CSEC's conduct of cyber defence activities, an indication of a *Criminal Code* offence is encountered, CSEC's response will be guided by the following Procedures:

- OPS-1-14, *Operational Procedures For Cyber Defence Operations Conducted Under Ministerial Authorization*, and
- OPS-1-15, *Operational Procedures for Cyber Defence Activities Using System Owner Data*.

Use, Retention and Release**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,
- intercepted and disclosed under a system owner's authority, and

Information about Canadians, which includes

- any personal information about a Canadian, or
- any business information about a Canadian corporation (as defined in section 20(1) of the *Access to Information Act*. See Annex 2.).

Information about Canadians is normally protected by suppressing details that may identify individuals or corporations in the context of personal or business information. Such details, whether suppressed or not, are referred to as "Canadian Identity Information" - CII.

4.7 Canadian Identity Information (CII)

CII is normally suppressed in cyber defence reporting. Unsuppressed CII may be included in reports if necessary for recipients to use CSEC mitigation advice to protect their own networks. Under certain circumstances, and in consultation with DLS on a case-by-case basis, reports may contain unsuppressed CII if that CII is being utilized by a malicious foreign actor. Contact IPOC for further details; IPOC may engage Corporate and Operational Policy, as required.

4.8 Relevancy of Information

CSEC must only use or retain data from a client's network that is relevant to CSEC's Mandate.

4.9 Essentiality – Private Communications in MA Operations	<p>A private communication may only be used or retained if essential to identify, isolate or prevent harm to GC computer systems or networks. Such information must be tracked in order to allow CSEC to fulfill Ministerial reporting requirements concerning use and retention.</p>
4.10 Access to and Storage of Information	<p>All information obtained or produced by CSEC during cyber defence activities must be safeguarded by appropriate access controls.</p> <p>Information obtained under part (b) authorities that is relevant, or in the case of a private communication, essential to identifying, isolating or preventing harm to GC computer systems or networks may be shared with, or made accessible to, Second Party counterparts. In some cases (see paragraph 4.7), there may not be a requirement to suppress CII obtained under part (b) authorities. IPOC and Corporate and Operational Policy must be consulted prior to sharing unsuppressed CII with Second Parties.</p> <p>Any information used in reporting going outside Second Party counterparts must be handled in accordance with formal arrangements with the Second Parties, e.g., action-on and suppressions.</p>
4.11 Retention Schedules	<p>Retention and disposition schedules for data and other information are set by CIO in accordance with:</p> <ul style="list-style-type: none"> • The <i>Library and Archives of Canada Act</i> • MAs (for those activities requiring an MA), and • MoUs or other formal agreements with federal institutions.
4.12 Release Authority for CII	<p>DGPC is the authority for releasing CII suppressed from cyber defence activity reports.</p>
4.13 Sharing with SIGINT	<p>Data from cyber defence activities may be shared with SIGINT in accordance with appropriate Corporate and Operational Policy and ITS Security policy instruments.</p>

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 release 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 CII or private communications in one of the sources), the higher level must sign.

4.15 Report Release Authorities

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

<u>Cyber Defence Report Release Authorities</u>			
Report Type	Release (beyond CSEC)	Recommendation level	Approval level
All reports	To the institution from which the information was obtained (with no further release)	Operational Supervisor	Operational Manager (or higher)
Reports containing <ul style="list-style-type: none"> • no CII (or CII allowed under paragraph 4.7), and • no private communications • private communications previously approved by DC ITS in other reports 	To any recipient, including or beyond the institution from which the information was obtained		
Reports containing suppressed CII but no private communications	To any recipient beyond the institution from which the information was obtained	Director	DG CDB
Reports containing private communications		Director General	DC ITS

Continued on next page

**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 institution that requested assistance must authorize release of reports to other recipients. Release of reports containing a private communication is limited.

See activity-specific policy instruments for details on whether report release beyond the institution that requested assistance is permitted.

**4.16 Release
Authorities for
Joint ITS-
SIGINT
Reporting**

The sign-off authority for reports based on data acquired under both IT Security and SIGINT authorities will be determined on a case-by-case basis, in consultation with IPOC and SPOC.

**4.17 Release
Authorities for
Other Sources**

Open Source

Reports based on open-source information are approved by operational managers; this may be delegated to operational supervisors.

IRRELEVANT

Other Sources

Release authorities for reports based on any other sources must be determined by the relevant Director, in consultation with IPOC and Corporate and Operational Policy.

5. PRIVACY INCIDENTS REPORTING

5.1 Privacy Incidents Reporting at CSEC


A privacy incident occurs when the privacy of a Canadian is put at risk in a manner that runs counter to, or is not provided for in, an operational policy. It is inevitable that, given the nature of CSEC operations, incidents related to privacy will occur. It is CSEC's responsibility to report and document those incidents in order to demonstrate compliance with its operational policies and legal requirements, and to prevent further incidents.

Examples of privacy incidents may include:

- inadvertently including CII in a SIGINT or a cyber defence report
- unknowingly targeting a Canadian or any person in Canada
- improper access controls on an electronic folder that contains a private communication that was intercepted under MA
- improper deletion of information or data that might include information about Canadians or CII, or
- an unforeseen technical error that makes a limited access database more widely accessible for a period of time.

CSEC has created a central record of privacy incidents to track and demonstrate CSEC's commitment to protecting privacy, improving internal practices, ensuring transparency, and enhancing public confidence in CSEC.

If an analyst in SIGINT or IT Security believes that a privacy incident has occurred, he or she must follow the steps in this table:

Step	Who	Action
1	Analyst	brings the incident to the attention of supervisor
2	Supervisor	<ul style="list-style-type: none"> • notifies the manager, director, and either IPOC or SPOC, as appropriate, as soon as possible • must consult with IPOC or SPOC to determine what immediate steps must be taken to investigate and address the situation <div>  Note: In DGPC, supervisors should notify and consult Corporate and Operational Policy. </div>

Continued on next page

SECRET//SI

OPS-1

Effective Date: 1 December 2012

Step	Who	Action
3	<ul style="list-style-type: none"> • SPOC • IPOC 	<ul style="list-style-type: none"> • notifies Corporate and Operational Policy of the incident and actions • provides summary of the incident and mitigation to the Manager, Corporate and Operational Policy, who maintains the central file for Director, Disclosure, Policy and Review (formerly Director, Corporate and Operational Policy) follow-on briefing or action, as appropriate

6. REVIEW

6.1 Review

CSEC activities are subject to internal and external review for policy compliance and lawfulness.

6.2 CSE Commissioner

Pursuant to section 273.63 of the NDA, the CSE Commissioner plays a key role in providing independent, external 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
- 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, and
- report annually to the Minister.

In executing the Commissioner's mandate, staff from the Office of the CSE Commissioner has access to CSEC staff, documentation and material (except those subject to Cabinet Confidence or to solicitor-client privilege). All requests from the Commissioner's staff are coordinated at CSEC by the External Review team (via email: [REDACTED])

6.3 External Review: Information Requirements

CSEC staff must ensure that all relevant documentation is entered into corporate system of record. 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 operational, legal, and policy issues
 - provide a record of management decisions
 - confirm that supervisors and managers 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, Privacy Incidents File).
-

SECRET//SI

OPS-1

Effective Date: 1 December 2012

IRRELEVANT

7. ACCOUNTABILITY FOR OPS-1

7.1 Accountability

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

Who	OPS-1 Responsibility
DC SIGINT	<ul style="list-style-type: none"> • Approve revisions to Chapters 1, 2, 3, 5, 6, 7 and 8
DC IT Security	<ul style="list-style-type: none"> • Approve revisions to Chapters 1, 4, 5, 6, 7 and 8
DGPC	<ul style="list-style-type: none"> • Recommend for approval
General Counsel, Directorate of Legal Services	<ul style="list-style-type: none"> • Provide legal advice, when requested • Review for legal compliance
Director, Disclosure, Policy and Review	<ul style="list-style-type: none"> • Review for consistency with the policy framework
Corporate and Operational Policy Section	<ul style="list-style-type: none"> • Revise • Respond to related questions

7.2 References

- *National Defence Act*, Part V.1
- *Access to Information Act*
- *Criminal Code of Canada*
- *CSIS Act*
- *Financial Administration Act*
- *Library and Archives of Canada Act*
- *Privacy Act*
- Most recent *Ministerial Directive on CSE's Accountability Framework*
- Most recent *Ministerial Directive on the Collection and Use of Metadata*
- Most recent *Ministerial Directive on the Privacy of Canadians*
- Most recent *Ministerial Directive on Assistance to Federal Law Enforcement and Security Agencies*
- OPS-1-1, *Procedures for the Release of Suppressed Information from SIGINT Reports*
- OPS-1-6, *Operational Procedures for Naming and Releasing Identities in Cyber Defence Reports*
- OPS-1-7, *Operational Procedures for Naming in SIGINT Reports*
- OPS-1-10, *Operational Procedures for Metadata Analysis* [REDACTED]

Continued on next page

7.2 References
(continued)

- OPS-1-11, *Retention Schedules for SIGINT Data*
- OPS-1-13, *Procedures for [REDACTED] Activities*
- OPS-1-14, *Operational Procedures For Cyber Defence Operations Conducted Under Ministerial Authorization*
- OPS-1-15, *Operational Procedures for Cyber Defence Activities Using System Owner Data*
- OPS-3-1, *Operational Procedures for [REDACTED] Activities*
- IRRELEVANT [REDACTED]
- 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, *Producing Gists for Indications and Warning Purposes*
- CSOI-4-4, *Targeting and Selector Management Using [REDACTED] National SIGINT Systems for Intelligence Reporting Purposes*

7.3 Enquiries

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

7.4 Amendments

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

7.5 Records Management

CSEC must 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.

8. DEFINITIONS

8.1 Business Information

Business information is information of, from, or about a Canadian company (incorporated under the laws of Canada or a province) the disclosure of which:

- could reasonably be expected to result in material financial loss or gain to, or could reasonably be expected to prejudice the competitive position of, the Canadian company, or
- could reasonably be expected to interfere with contractual or other negotiations of the Canadian company.

In some situations this may apply to GC entities (e.g., crown corporations, special operating agencies, etc.).

8.2 Canadian

“Canadian” refers to

- a) a Canadian citizen, or
 - b) a person who has acquired the status of permanent resident under the *Immigration and Refugee Protection Act (IRPA)* and who has not subsequently lost that status under that *Act*, or
 - c) a corporation incorporated under an Act of Parliament or of the legislature of a province.
- (NDA, section 273.61)

For the purposes of this policy, “Canadian organizations” are also considered to be Canadian.

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

8.3 Canadian Identity Information (CII)

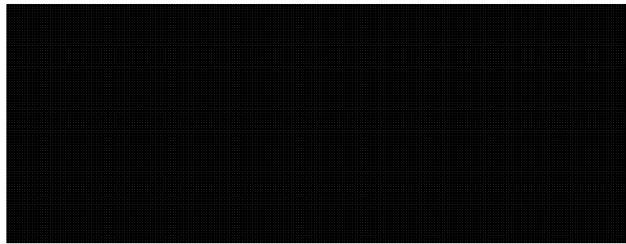
CII refers to information that may be used to identify a Canadian person, organization, or corporation, in the context of personal or business information. CII includes, but is not limited to, names, phone numbers, email addresses, IP addresses, and passport numbers.

8.4 Contact Chaining

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

8.5 CSEC SIGINT Collection

For the purposes of these policy, CSEC SIGINT collection refers to acquisition conducted by CSEC, with the assistance of the CFIOG, [REDACTED] or others 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 Second Party collection (acquired by CSEC under paragraph 273.64(1)(a) of the NDA, or [REDACTED] (conducted under paragraph 273.64(1)(c) of the NDA).

8.6 Cyber Defence Activities

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

8.7 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).

8.8 Foreign

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

8.9 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)
8.10 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)
8.11 “In Canada”	Canada’s territory, internal waters, territorial sea (i.e., up to the 12 nautical mile limit), and the associated airspace.
8.12 Information about Canadians	<p>For the purposes of this document, information about Canadians has two meanings. IRRELEVANT</p> <p>IRRELEVANT</p> <p>IRRELEVANT the term “information about Canadians” refers to:</p> <ul style="list-style-type: none"> • any personal information about a Canadian, or • business information about a Canadian corporation (as defined in section 20(1) of the <i>Access to Information Act</i> (see Annex 2)).
8.13 Integree	An integree is a person seconded to CSEC from one of CSEC’s cryptologic partner organizations.
8.14 Metadata	Metadata is defined as information associated with a telecommunication to identify, describe, manage or route that telecommunication or any part of it as well as the means by which it was transmitted, but excludes any information or part of information which could reveal the purport of a telecommunication, or the whole or any part of its content.

8.15 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.

8.16 Network Analysis and Prioritization

Network Analysis and Prioritization refers to the method developed to understand the GII, from information derived from metadata, in order to identify and determine telecommunication links of interest to achieve the GC foreign intelligence priorities. This method involves the acquisition of metadata, [REDACTED]

[REDACTED]

8.17 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.

8.18 Private Communication

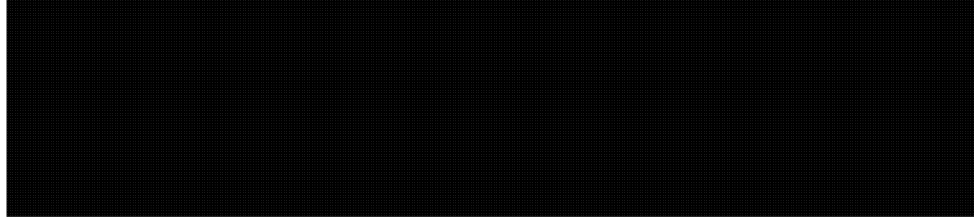
A private communication is “any oral communication, or any telecommunication, that is made by an originator who is in Canada or is intended by an originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it 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)

8.19 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).
8.20 Seconded	A secondeed 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.
8.21 Selectors	Selectors are terms identifying a SIGINT target that may include a name, [REDACTED] IP or e-mail address, facsimile or telephone number, or other alphanumeric character stream [REDACTED] for the purpose of identifying traffic that relates to national foreign intelligence requirements and isolating it for further processing.
8.22 SIGINT Privacy Annotations	SIGINT Privacy Annotations are markings applied to SIGINT traffic in traffic repositories for the purpose of identifying private communications, communications of Canadians located outside Canada, solicitor-client communications, and information about Canadians to be retained or deleted. It is the responsibility of analysts whose functions are directly related to the production of SIGINT reports to annotate appropriately SIGINT traffic that is recognized as falling into one of the categories described above (see Annex 3).
8.23 SIGINT Reports	<p>Reports that are based on SIGINT and linked to a GC intelligence requirement (GCR). They include, but are not limited to:</p> <ul style="list-style-type: none"> • Advance Reports: informal, partially vetted SIGINT end-product containing information that requires further analysis; they are intended as vehicles for timely reporting of highly perishable intelligence. (See CSOI 4-1, <i>SIGINT Reporting</i>.) • End-products (a.k.a. SIGINT end-product; end-product reports): issued in response to a GCR. End-products conform to established reporting standards. • Technical SIGINT Reports, such as Cryptologic/Communications Information Reports (CIR) and [REDACTED]: they are usually issued solely to SIGINT producers, and intended to aid in the further collection of SIGINT.

Continued on next page

8.23 SIGINT Reports
(continued)

- Gists, which consist of raw and often unassessed SIGINT: relate to indications and warnings in connection with certain SIGINT targets. They are serialized and released using [REDACTED] (See CSOI-4-2, *Producing Gists for Indications and Warning Purposes*.)



8.24 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.

8.25 Suppressed Information

Suppressed information is defined as information excluded from a SIGINT end-product or technical report or an IT Security cyber defence report because it may reveal the identity of a Canadian or US/UK/AUS/NZ entity. Suppressed information is stored in a limited-access database or system and is replaced in the report by a generic term.

Information that is suppressed includes, but is not limited to, personal identifiers such as names, passport information, [REDACTED] email addresses, phone numbers and IP addresses, [REDACTED]



	<p>FYI: For SIGINT reports, see OPS-1-7, <i>SIGINT Naming Procedures</i>. For IT Security cyber defence reports, see OPS-1-6, <i>Operational Procedures for Naming and Releasing Identities in Cyber Defence Reports</i>.</p>
---	--

8.26 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,

Effective Date: 1 December 2012

- (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.

Annex 2 – Business Information

Definition of Business Information in the *Access to Information Act*

20. (1) ... the head of a government institution shall refuse to disclose any record requested under this Act that contains

- (a) trade secrets of a third party²;
- (b) financial, commercial, scientific or technical information that is confidential information supplied to a government institution by a third party and is treated consistently in a confidential manner by the third party;
- (c) information the disclosure of which could reasonably be expected to result in material financial loss or gain to, or could reasonably be expected to prejudice the competitive position of, a third party, or;
- (d) information the disclosure of which could reasonably be expected to interfere with contractual or other negotiations of a third party.

² In this instance “third party” refers to a business or corporation vs. the accepted CSEC usage of “non-Five-Eyes”.

Annex 3 – SIGINT Privacy Annotations and Accountability Markings

SIGINT Privacy Annotations are to be applied only to traffic from CSEC and Second Party collection (part “a” of the Mandate) sources. See OPS-3-1 for details related to [REDACTED] traffic and SIGINT Privacy Annotations.

Note: In cases where CSEC has intentionally created a copy (or copies) of a traffic item in several traffic databases, each copy must be annotated. Duplicates that have not been viewed are exempt from this requirement.

Location	If one communicant is physically located in Canada ¹		If one communicant is a Canadian ² physically located outside Canada		Both communicants are foreigners located outside Canada, but the communication contains information about a Canadian ^{2,3}		Recognized one-end Canadian e-mails [REDACTED]
Source	[REDACTED]						
Essentiality	Contains FI essential to international affairs, defence or security of Canada	Not essential// annotate for deletion	Contains FI essential to international affairs, defence or security of Canada	Not essential// annotate for deletion	Contains FI essential to international affairs, defence or security of Canada	Not essential// annotate for deletion	Contains FI essential to international affairs, defence or security of Canada
Annotation	INCA	INCAN	OUCA	OUCAN	(None required)	IACN	AM

See next page for Annotations for Solicitor-Client communications

¹ This is a private communication, with geography being the determining factor (i.e., one of the communicants must be located in Canada. See paragraph 8.18 for the definition. Should an analyst recognize traffic where both the originator and the recipient are Canadians, or are both in Canada, or where one communicant is in Canada and the other is a Canadian located outside Canada, the traffic must be annotated for deletion. All associated selectors must be reviewed and SPOC [REDACTED] must be notified; see paragraph 2.8.

² See paragraph 8.2 for the definition of a Canadian.

³ There is no requirement to maintain statistics on these communications; however, for privacy reasons, those communications that do not contain FI essential to international affairs, defence or the security of Canada are to be annotated for deletion

⁴ Although this marking is not required under any MA, for accountability purposes, [REDACTED] one-end Canadian e-mail [REDACTED] must be marked.

SOLICITOR-CLIENT ANNOTATIONS⁵

Location	If one communicant is physically located in Canada ⁵		If one communicant is a Canadian ⁵ physically located outside Canada	
Source				
Essentiality	Contains FI essential to international affairs, defence or security of Canada	Not essential// annotate for deletion	Contains FI essential to international affairs, defence or security of Canada	Not essential// annotate for deletion
Annotation	INCAS	INCASN	OUCAS	OUCASN

⁵ See paragraphs 3.5 and 3.8 for definition and handling instructions related to solicitor-client communications