

CONFIDENTIAL//COMINT
OPS-1-11
Effective date: 31 October 2007



OPS-1-11
Retention Schedules for
SIGINT Data

CONFIDENTIAL//COMINT
OPS-1-11
Effective date: 31 October 2007

Table of Contents

1. Introduction	3
2. Retention Schedules	5
3. Additional Information	12
4. Definitions	15
Annex 1	22

s.15(1) - DEF

CONFIDENTIAL//COMINT
OPS-1-11
Effective date: 31 October 2007

1. Introduction

1.1 Objective The objective of these procedures is to provide direction to staff on retention schedules for SIGINT data

These procedures supersede the existing OPS-1-11, dated 11 March 2004, which should be destroyed.

1.2 Authorities The existing legal and policy instruments that determine SIGINT data retention schedules are as follows:

- The laws of Canada including the *National Defence Act*, Part V.1, and the *Privacy Act*;
 - Judicial warrants;
 - *Ministerial Directive on the Collection and Use of Metadata* (March 2005); and
 - CSE policies and procedures governing SIGINT activities, including OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities*.
-

1.3 The Library and Archives of Canada Act CSE is not required to retain or schedule the destruction of SIGINT data records to comply with the *Library and Archives of Canada Act* since SIGINT data are considered to be transitory records. These should only be retained as long as is reasonably necessary.

1.4 Application These procedures apply to:

- CSE staff,
- CFIOG staff, and
- any other parties, including secondees, [REDACTED] and contractors, who conduct activities under CSE authority and who handle SIGINT data.

CONFIDENTIAL//COMINT
OPS-1-11
Effective date: 31 October 2007

**1.5 Policy
Statement**

SIGINT data may be retained by CSE only when required to fulfill CSE's mandate. Traffic requiring [REDACTED] must be appropriately [REDACTED] and stored in accordance with OPS-1.

s.15(1) - DEF

CONFIDENTIAL//COMINT
OPS-1-11
Effective date: 31 October 2007

2. Retention Schedules

2.1 The retention schedules outlined in these procedures deal with SIGINT data
Scope acquired from Canadian [REDACTED] sources.

2.2 There are five operational requirements that justify the retention of SIGINT
Justification data.
for Retention

Operational Requirements	Description
[REDACTED]	

2.3 General Guidelines

Retention schedules must be:

- standardized as much as possible;
- applied to all SIGINT data regardless of media and/or location (hard copy, personal or group accounts, and/or electronic data repositories); and
- consistent with the [REDACTED] on the retention of metadata imposed by Ministerial Directive.

2.4 Handling of Traffic Used in SIGINT Reports

[REDACTED] When a production element runs out of space for report files, the oldest files must be shipped to [REDACTED] for permanent retention ([REDACTED])

Electronic copies of traffic used in SIGINT reports may be retained in traffic repositories as outlined in these procedures.

For traffic used in SIGINT reports containing information about Canadians:

[REDACTED]

All traffic containing information about Canadians must be handled in accordance with OPS-1.

For details on the retention schedule for suppressed information see OPS-1-1, *Procedures for the Release of Suppressed Information from SIGINT Reports*.

2.5

[REDACTED]

[REDACTED]

will be replaced by a CSE SIGINT Operations Instruction (CSOI). Until then, any questions should be directed to D2, Operational Policy.

s.15(1) - DEF

CONFIDENTIAL//COMINT
OPS-1-11
 Effective date: 31 October 2007

2.6 Traffic Retained in Traffic Repositories

In general and where the maximum retention period is [redacted] traffic should be retained in accessible online traffic repositories for [redacted] at which point it may be archived for the remainder of the [redacted] [redacted] it must be deleted from the archives.

2.7 SIGINT Data Acquired under 273.64 (1) (a) of the NDA (Mandate "A")

The retention schedules for Canadian [redacted] SIGINT data have been established for the purpose of satisfying the requirements relating to retention as laid out in paragraphs 273.64(2)(b) and 273.65(2)(d) of the *National Defence Act*, by Ministerial Directive, and in CSE's operational requirements.

Canadian [redacted] (Mandate "A")	Mode	If the data is...	Then the retention period will be...
	[redacted]	a recognized: <ul style="list-style-type: none"> • private communication, [redacted] • communication of a Canadian located outside Canada, or • communication that contains information about Canadians, where the information is essential to international affairs, defence, or security 	[redacted] Pursuant to Ministerial Authorization, advice from DLS is required to retain communications which constitute [redacted] [redacted]

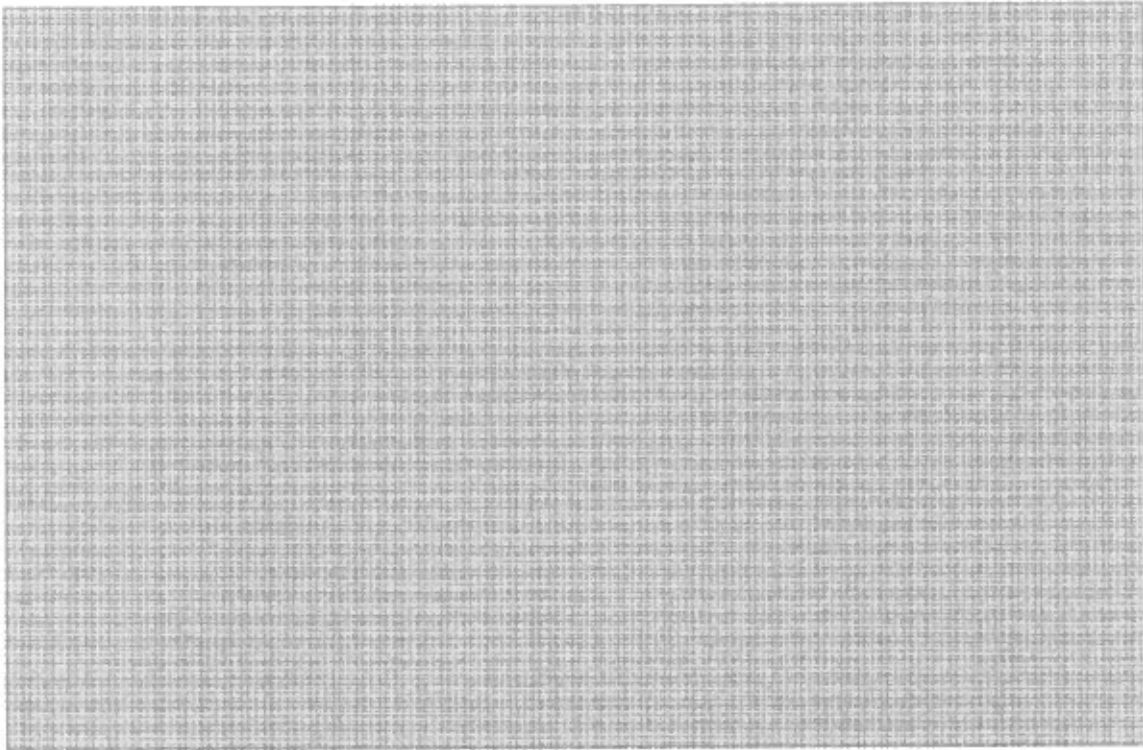
s.15(1) - DEF

CONFIDENTIAL//COMINT
OPS-1-11
Effective date: 31 October 2007

	<p>a recognized</p> <ul style="list-style-type: none">• private communication, <p>[REDACTED]</p> <ul style="list-style-type: none">• communication of a Canadian located outside Canada, or• communication that contains information about Canadians, where the information is not essential to international affairs, defence, or security	[REDACTED]
	<p>a communication where:</p> <ul style="list-style-type: none">• both the originator and the recipient are Canadians, or• both the originator and recipient are located in Canada, or• where one communicant is in Canada and the other is a Canadian abroad	
	<p>All other including <u>non-assessed traffic</u></p>	
[REDACTED]	[REDACTED]	
Metadata	[REDACTED]	
	<p>Collected under a Ministerial Directive (MD)</p>	<p>[REDACTED] at the discretion of the Minister of National Defence</p>

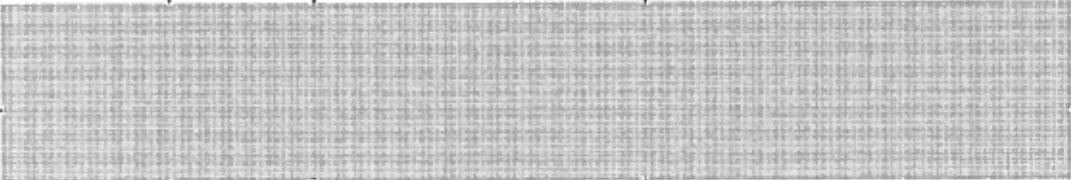
s.15(1) - DEF

CONFIDENTIAL//COMINT
OPS-1-11
Effective date: 31 October 2007



**2.9 Data
Acquired
under 273.64
(1) (c) of the
NDA
(Mandate "C")**

Data acquired pursuant to CSE's Mandate "C" may be retained according to the following schedules. These schedules reflect warrant conditions, CSIS-CSE agreements, and CSE operational requirements (see paragraph 2.8 for exceptions).



s.15(1) - DEF

CONFIDENTIAL//COMINT
OPS-1-11
Effective date: 31 October 2007

	[Redacted]	
	[Redacted]	[Redacted]
Section 12		
<u>Assistance to Other Federal Law Enforcement and Security Agencies</u>		



s.15(1) - DEF

CONFIDENTIAL//COMINT
OPS-1-11
Effective date: 31 October 2007

2.10

[Redacted]

[Redacted]

[Redacted]

[Redacted]

CONFIDENTIAL//COMINT
 OPS-1-11
 Effective date: 31 October 2007

3. Additional Information

3.1 **Accountability** The following table outlines responsibilities of various CSE elements with respect to these procedures.

Who	Responsibility
Deputy Chief, SIGINT	<ul style="list-style-type: none"> • Approving these procedures • Applying these procedures • Seeking legal advice, if required
Director General, Policy and Communications	<ul style="list-style-type: none"> • Approving these procedures • Seeking legal advice, if required
General Counsel, Directorate of Legal Services (DLS)	<ul style="list-style-type: none"> • Providing legal advice, when requested • Reviewing these procedures to ensure they comply with the law
Manager, Operational Policy	<ul style="list-style-type: none"> • Revising these procedures when required • Responding to queries about these procedures • Seeking legal advice, if required
CSE and CFIOG Operational Managers who handle SIGINT data	<ul style="list-style-type: none"> • Ensuring their staff has read, understood, and is complying with these procedures
CSE and CFIOG Operational Staff who handle SIGINT data	<ul style="list-style-type: none"> • Reading, understanding and complying with these procedures

s.15(1) - DEF

s.16(2)(c)

CONFIDENTIAL//COMINT
OPS-1-11
Effective date: 31 October 2007

- 3.2 References**
- *National Defence Act*, Part V.1
 - *Ministerial Directive on CSE's Accountability Framework*, June 2001
 - *Ministerial Directive on Privacy of Canadians*, June 2001
 - *Ministerial Directive on the Collection and Use of Metadata*, March 2005
 - *Ministerial Authorization on [REDACTED]* (December 2006)
 - *Library and Archives of Canada Act*
 - *Privacy Act*
 - *MOU on Section 16 of the CSIS Act ("Tri-Ministerial" MOU, August 1987)*
 - *CSE/CSIS Section 16 MOU (1 November 1990)*
 - *OPS-1, Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities*
 - *OPS-1-1, Procedures for the Release of Suppressed Information from SIGINT Reports*
 - *OPS-1-6, Canadian [REDACTED] Procedures*
 - *OPS-1-7, SIGINT Naming Procedures*
 - *OPS-1-8, Active Management Monitoring of Operations to Ensure the Privacy of Canadians*
 - *OPS-3-1, Procedures for [REDACTED]*
 - *OPS-3-5, [REDACTED] Procedures*
 - *OPS-3-7, [REDACTED] Procedures*
 - *ORG-2-2, Procedures for Handling Documents Related to CSE Activities Conducted Under a Ministerial Authorization*
 - *CSOI-4-1, SIGINT Reporting*
 - *CSOI-4-3, [REDACTED] Handling and Storage of Privacy Information*

Existing policy instruments related to Section 16 are currently under revision. For details or assistance, please contact D2, Operational Policy.

**3.3
Amendment
Process**

Situations may arise where amendments to these procedures are required because of changing or unforeseen circumstances. All revisions of these procedures will be announced to CSE staff, and will be posted on the Operational Policy website at [REDACTED]

3.4 Enquiries

Questions related to these procedures should be directed to your operational manager, who in turn will contact Operational Policy staff ([REDACTED]) when necessary.

CONFIDENTIAL//COMINT
OPS-1-11
Effective date: 31 October 2007

3.5 Review

All CSE activities, including relevant policies and procedures, are subject to management monitoring (see OPS-1-8, *Management Monitoring and Policy Review Procedures to Ensure the Privacy of Canadians*), audit, and review by various government review bodies, including, but not limited to the CSE Commissioner and the Privacy Commissioner.

s.15(1) - DEF

CONFIDENTIAL//COMINT
OPS-1-11
Effective date: 31 October 2007

4. Definitions

4.1 Analyst



4.2 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*, S.C. 2001, c. 27, 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.

(*National Defence Act*, R.S.C., 1985, c. N-5 (NDA), section 273.61;
Immigration and Refugee Protection Act)

For the purposes 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.

4.3



4.4



s.15(1) - DEF

CONFIDENTIAL//COMINT
OPS-1-11
Effective date: 31 October 2007

4.5
[Redacted]

[Redacted]

4.6 Criminal Intelligence (CI)

Criminal intelligence is information that may be used in the investigation or prosecution of an alleged contravention of any federal or provincial law in Canada (CSE-CSIS Section 16 MOU).

4.7 Data

[Redacted] metadata, [Redacted] acquired from the Global Information Infrastructure (GII).

4.8

[Redacted]

4.9

[Redacted]

[Redacted]

CONFIDENTIAL//COMINT
OPS-1-11
Effective date: 31 October 2007

4.10 Federal Law Enforcement and Security Agencies

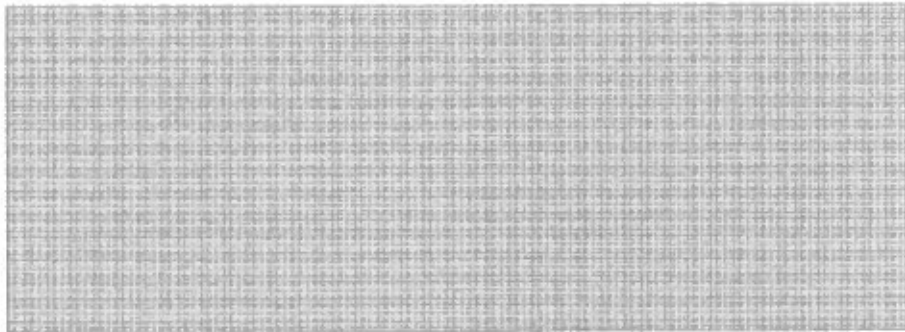
Federal law enforcement and security agencies include, in the first instance, the RCMP and CSIS, and, second, the other federal government departments and agencies with law and regulatory enforcement functions, including Canada Border Services Agency, Canada Revenue Agency, Citizenship and Immigration Canada, Health Canada, Environment Canada, Industry Canada, Transport Canada, the Canadian Food Inspection Agency, the Department of Fisheries and Oceans.

(Ministerial Directive on Support to Law Enforcement and National Security Agencies, June 2001)

4.11 Foreign Intelligence

Foreign intelligence (FI) 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. (*National Defence Act*, section 273.61)

4.12



4.13



4.14 Information about Canadians

For the purposes of this document, information about Canadians refers to:

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

s.15(1) - DEF


CONFIDENTIAL//COMINT
OPS-1-11
Effective date: 31 October 2007

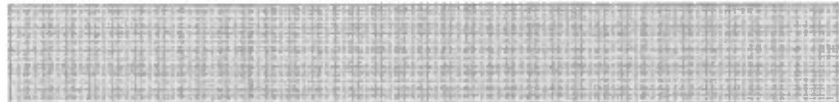
4.15 Metadata Metadata is defined as information associated with a telecommunication to identify, describe, manage or route that telecommunication or any part of it as well as the means by which it was transmitted, but excludes any information or part of information which could reveal the purport of a telecommunication, or the whole or any part of its content.
(Ministerial Directive on the Collection and Use of Metadata, March 2005)

4.16 Ministerial Authorization (MA) A Ministerial Authorization (MA) is an authorization provided in writing by the Minister of National Defence to CSE to ensure that CSE 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

- s.273.65(1) of the *National Defence Act (NDA)* for the sole purpose of obtaining foreign intelligence, or
- s.273.65(3) of the *NDA* for the sole purpose of protecting the computer systems or networks of the Government of Canada

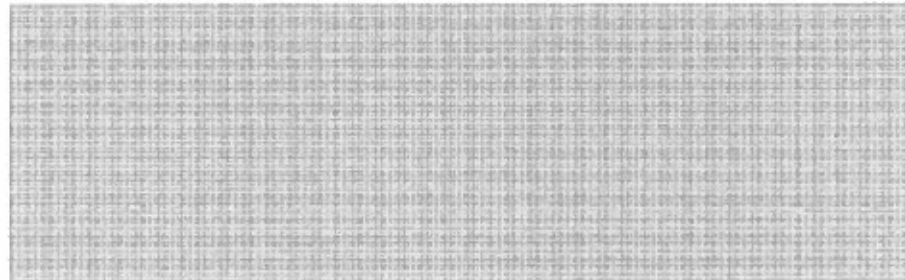
When such an authorization is in force, Part VI of the *Criminal Code* does not apply in relation to an interception of a private communication, or in relation to a communication so intercepted.

4.17 



4.18 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 complete definition, see Annex I.

4.19 



CONFIDENTIAL//COMINT
OPS-1-11
Effective date: 31 October 2007

4.20 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)

4.21

[Redacted]

[Redacted]

4.22 Records

Includes any correspondence, memorandum, book, plan, map, drawing, diagram, pictorial or graphic work, photograph, film, microform, sound recording, videotape, machine readable record, and any other documentary material, regardless of physical form or characteristics, and any copy thereof.

4.23 Retention Schedules

The time allotted for retaining a record or specific types of records within an organization. Retention schedules reflect all legal, policy and operational requirements levied against an organization and its holdings.

4.24

[Redacted]

s.15(1) - DEF

CONFIDENTIAL//COMINT
OPS-1-11
Effective date: 31 October 2007

4.25 [REDACTED]

[REDACTED]

4.26 Security Intelligence (SI)

Security intelligence is information relating to threats to the security of Canada as defined in Section 2 of the *CSIS Act*.

4.27 Selectors

[REDACTED]

4.28 [REDACTED]

[REDACTED]

4.29 [REDACTED]

[REDACTED]

4.30 Suppressed Information

Suppressed information is defined as information excluded from a SIGINT end-product or technical report because it may reveal the identity of a Canadian or [REDACTED] Suppressed information is stored in a [REDACTED] and is in most cases replaced in the report by a generic term.

Suppressed information includes, but is not limited to, personal identifiers such [REDACTED]

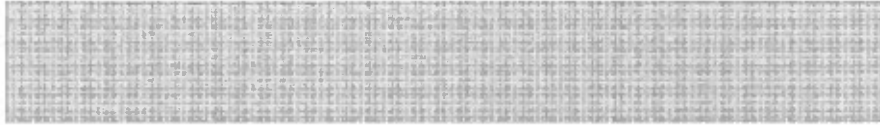
[REDACTED]

Note: See OPS-1-7, *SIGINT Naming Procedures*, for details regarding suppression, including exceptions.

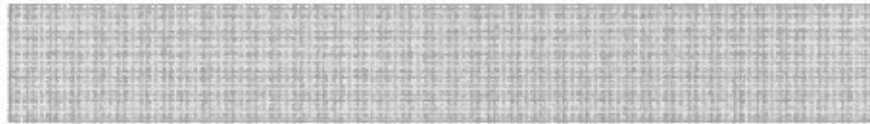
s.15(1) - DEF

CONFIDENTIAL//COMINT
OPS-1-11
Effective date: 31 October 2007

4.31



4.32 Traffic



4.33
Transitory
Records

These are records that are required only for a limited time to ensure the completion of a routine action or the preparation of a subsequent record.-

4.34



CONFIDENTIAL//COMINT
OPS-1-11
Effective date: 31 October 2007

Annex 1

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

**CONFIDENTIAL//COMINT
OPS-1-11**

Effective date: 31 October 2007

- (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.**