OPS-1-11

Retention Schedules for SIGINT Data

CERRID #787403-v1

Table of Contents

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, integrees, and contractors,

who conduct activities under CSE authority and who handle SIGINT data.

1.5 Policy Statement	SIGINT data may be retained by CSE only when required to fulfill CSE's mandate. Traffic requiring privacy annotations must be appropriately annotated and stored in accordance with OPS-1.

2. Retention Schedules

2.1 Scope

The retention schedules outlined in these procedures deal with SIGINT data acquired from Canadian and Second Party sources.

2.2 Justification for Retention

There are five operational requirements that justify the retention of SIGINT data.

Operational Requirements	Description
Target continuity	[redacted]
Target research and development	
Processing requirements	
Data management	The retention of some SIGINT data may contribute (in whole or part) to managing other traffic and metadata.
Disaster recovery	Regular backups of CSE repositories are performed to avoid permanent loss of SIGINT data in the event of a disaster.

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] limit on the retention of metadata imposed by Ministerial Directive.

2.4 Handling of Traffic Used in SIGINT Reports

Hard copies of traffic used in SIGINT reporting must be retained [redacted] with its corresponding report. When a production element runs out of space for report files, the oldest files must be shipped to Information Holding Services for permanent retention (see [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:

- If the information about Canadians **is essential** to understanding the Foreign Intelligence (FI), the traffic may be retained in its entirety.

- If the information about Canadians **is not essential** to understanding the FI, the traffic may be retained if, where technically possible, all information identifying Canadians is suppressed or deleted.

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 SIGINT Data Retained in Target-Knowledge Databases

Traffic or information extracted from SIGINT data, identified as foreign intelligence, may be retained in CSE target-knowledge databases as long as is operationally required or for as long as the information remains current. OPS-5-13, *Procedures for Incorporating Information into the Target Profile Builder*, will be replaced by a CSE SIGINT Operations Instruction (CSOI). Until then, any questions should be directed to D2, Operational Policy.

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] After [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 and Second Party 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 and Second Party Sources (Mandate "A")	Mode	If the data is…	Then the retention period will be…
	[redacted] Fax	a recognized: • private communication, • Solicitor-Client communication, • 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] Upon recognition in traffic databases, analysts must apply appropriate privacy annotations (see OPS-1, Annex 2), and must retain any material that has been used in reports in secure containers, as specified in CSOI 4-3. Pursuant to Ministerial Authorization, advice from DLS is required to retain communications which constitute Solicitor-Client communication.

	a recognized : • private communication, • Solicitor-Client communication, • 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] Upon recognition in traffic databases, analysts must apply appropriate privacy annotations for deletion of the material (see OPS-1 Annex 2); traffic will then automatically be deleted from the traffic databases **after the** [redacted]
	a communication where: • 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	This type of communications is retained only until such time as it is recognized as such in traffic databases by an analyst. Upon such recognition, analysts must annotate for deletion, and Mission Operations must be notified so they can review the relevant selectors. (See OPS-1, paragraph 4.6)
	All other including non-assessed traffic	Up to [redacted]
Cipher Decrypts Unknown data		Up to [redacted]
Metadata		Up to [redacted]
	Collected under a Ministerial Directive (MD)	[redacted] Longer than [redacted] at the discretion of the Minister of National Defence

Note: The retention period for traffic and metadata begins from the time the material becomes readable in any one or more of the existing traffic repositories. In the case of unknown data, the retention period will begin from the time of collection. Optimal delivery of data to appropriate repositories is [redacted] of collection/processing. If there is a large backlog situation, however, it may take [redacted] for traffic to reach a repository after it has been processed and rendered readable.

2.8 Retention of Canadian and Second Party Collection Beyond Outlined Retention Periods

Traffic used to populate target knowledge databases and/or files with target-related information and/or technical details may be kept for longer periods as required to support current and future technical operations.

To facilitate research and development efforts, and on a case-by-case basis, and weighing any privacy interests involved here, traffic collected by CSE and Second Parties may also be retained for longer than the indicated retention period. This traffic must be deleted at the completion of the project for which it was initially retained.

Except for metadata or a solicitor-client communication, approval to retain this material beyond the timeframe indicated in paragraph 2.7 must be sought from a Director on the recommendation of the Manager, SIGINT Oversight and Compliance.

IRRELEVANT

IRRELEVANT

IRRELEVANT

IRRELEVANT

IRRELEVANT

[redacted]

[redacted]

[redacted]

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	• Approving these procedures • Applying these procedures • Seeking legal advice, if required
Director General, Policy and Communications	• Approving these procedures • Seeking legal advice, if required
General Counsel, Directorate of Legal Services (DLS)	• Providing legal advice, when requested • Reviewing these procedures to ensure they comply with the law
Manager, Operational Policy	• 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	• Ensuring their staff has read, understood, and is complying with these procedures
CSE and CFIOG Operational Staff who handle SIGINT data	• Reading, understanding and complying with these procedures

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*

IRRELEVANT

- 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] *Operations*
- 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, *DGI Handling and Storage of Privacy Information*

IRRELEVANT

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 (e-mail [redacted] when necessary.

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.

4. Definitions

4.1 Analyst An analyst is someone whose function is directly related to the production of Foreign Intelligence (FI).

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 [redacted]

4.4 Cipher Cipher is unintelligible traffic that has no meaning but may be understood with the application of a decryption process. Cipher may hold [redacted]

4.5 Computer [redacted]

4.6 IRRELEVANT

IRRELEVANT

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

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

4.9 [redacted]

4.10 IRRELEVANT

IRRELEVANT

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 [redacted]

4.13 [redacted]

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.

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 Non-Assessed Traffic

Non-assessed traffic has not been viewed or evaluated in any way by an analyst.

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 1.

4.19 Privacy Annotations

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 the categories described above. See OPS-1 Annex 2.

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]

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]

4.25 Second Parties Second Parties refer to CSE's SIGINT counterparts, and include: 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).

4.26 IRRELEVANT

IRRELEVANT

4.27 Selectors Selectors are terms that may include a name, [redacted] IP or e-mail address, facsimile or telephone number, or other alphanumeric character stream [redacted] for the purpose of identifying traffic that relates to national foreign intelligence requirements and isolating it for further processing.

4.28 Solicitor-Client Communications A solicitor-client communication means any communication of a confidential character 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 their office, that is directly related to the seeking, formulating or giving of legal advice or legal assistance.

4.29 [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 Second Party entity. Suppressed information is stored in a limited-access database and is in most cases replaced in the report by a generic term.

Suppressed information includes, but is not limited to, personal identifiers such as names, passport information, [redacted] email addresses, phone numbers and IP addresses, [redacted]

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

4.31	[redacted]
4.32 Traffic	Traffic is defined as content or payload of a communication or [redacted] plus the associated metadata acquired from the Global Information Infrastructure.
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 Unknown Data	Unknown Data is data unrecognized by a collection system and therefore unable to be processed for the purpose of extracting metadata or content without additional analysis or processing to render it readable.

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

(*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.