



CSEC IT Security Operational Instructions ITSOI-1-2

Data Handling in Cyber Defence Activities

IT Security

Canada

Table of Contents

1.	Introduction	3
2.	Data Types	3
3.	Marking and Labelling Requirements	5
4.	Private Communications	6
5.	Data Retention and Deletion	8
6.	Additional Information	9
7.	Promulgation	11

1. Introduction

1.1 Objective These instructions provide direction in the handling of data obtained by CSEC during cyber defence activities conducted under part (b) of CSEC's mandate, including those conducted under Ministerial Authorization (MA), and non-MA cyber defence activities using Data Provided by a System Owner (DPSO).

1.2 Application These instructions apply to CSEC personnel and any other parties, including secondees, contractors and integrees, involved in conducting or supporting cyber defence activities.

2. Data Types

2.1 Data For cyber defence activities conducted under part (b) of CSE's mandate, "data" refers to [REDACTED] obtained from computer systems or networks of importance to the Government of Canada (GC); it includes content and associated metadata.

"Raw data" refers to data that has not been determined to be relevant or essential (i.e., it has not been used or retained).

2.2 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 (for example, the subject line).



Note: The descriptions of data types noted in 2.3 to 2.6 apply only to cyber defence activities conducted under part (b) of CSEC's mandate.

2.3 "Detached" Metadata In certain situations, metadata may be automatically separated from associated content so that there is no requirement to consider it a private communication, regardless of its source (i.e., there is no essentiality test, nor a Ministerial reporting requirement). Such metadata (known as detached metadata) is

considered relevant, and may be retained for up to [REDACTED] (for longer retention, or to share with Second Parties, the detached metadata must be marked as used or retained).

Contact IPOC for guidance on determining what types of metadata may be considered detached, and under what conditions.

2.4 Identifying Metadata

“Identifying metadata” is metadata that could identify one or both communicants, or the communication itself (e.g., “from”, “to” fields of an email, or an IP address linked to the communication). If obtained from, or associated with, content from a private communication, **identifying metadata must be treated as a private communication** if it is used or retained (including being subject to an essentiality test, and Ministerial reporting requirements).

In consultation with IPOC, identifying metadata may qualify to become detached metadata. In such situations, the detached metadata is no longer “identifying metadata”, and would not be considered a private communication.

2.5 Technical Metadata

Technical metadata is metadata that does not identify either of the communicants or the communication itself (e.g., email protocol version, operating system, statistical information).

Technical metadata

- **is not treated as a private communication, and**
- **is not subject to use and retention requirements.**

For example, when a recognized private communication is tunnelled in another protocol but the tunnel is distinct from the recognized private communication itself, then the tunnel is considered to be technical metadata.

2.6 Derivative Information

Derivative information is produced or discovered as a result of executing a malicious code (e.g., running a malicious attachment in a virtual environment). Derivative information contains no data and is therefore **not subject to use or retention requirements**. It is the decision of analysts whether or not to retain the original data (see paragraph 3.2). This includes DPSO activities, where derivative information obtained from executing malicious code, which was originally embedded in a private communication attachment, may be used for part “b” of CSEC’s mandate without having to obtain the recipient’s consent.

As with other data types, use of derivative information must be for the purpose of fulfilling part (b) of CSEC’s mandate; it is subject to the reporting process described in ITSOI-1-4.

Examples:

- a malicious 'beaconing to' IP address uncovered after executing malware
- machine activity or patterns observed as a result of executing malware

3. Marking and Labelling Requirements

3.1 Overview

Accurate data marking is required in order to fulfil MA and/or client arrangement conditions related to retention and disposition, as well as to determine appropriate report approval levels (see OPS-1 for approval levels).

3.2 Labelling

Data (including detached metadata) obtained during cyber defence activities must be marked with:

- a client identifier;
- a date/time stamp indicating when the data was copied or obtained by CSEC; and
- the authority under which the data was obtained.

Data that is used and retained must also be marked as relevant and, for private communications obtained under MA, essential (essentiality must be based on a documented rationale).

In addition to the above, DPSO must be marked to show whether it is

- a private communication,
- a private communication with recipient consent to share, or
- other data.

Data markings must be preserved for the lifespan of the data at CSEC.



Note: DPSO submitted to CSEC under OPS-1-15 (e.g., email sent to [REDACTED]) is incidentally copied by MA sensors at CSE. If such DPSO is encountered in MA collection, analysts must contact CTEC in order to determine what, if anything, may be done with the data under OPS-1-14.

In situations where CTEC has identified sensitive DPSO, contact IPOC for guidance.

3.3 Changes to Data Markings

Not marked as private communication: If data that has been used and retained is later determined to be a private communication, the essentiality test and correct labels must be applied. This must be reported to the relevant manager in the Cyber Defence Branch, as well as to IPOC. Reports resulting from the data

must be cancelled and re-issued (with appropriate sign-off level); see ITSOI-1-4, and statistics related to private communications (an MA requirement) must be amended (see Note in 4.4).

Marked as private communication: Non-private communication data marked as a private communication must have the correct label applied (in order to ensure an accurate count of private communications used or retained). IPOC must be informed in order to ensure statistics (related to private communications) are accurate. No further action is required.

3.4 Hardware

The receipt of hardware (e.g., USB, hard drive, CD) provided as part of DPSO activities must be logged for tracking purposes (including serial numbers, if applicable). The hardware itself must be labelled for tracking purposes, with the log included in the relevant client file. CSEC is accountable for all DPSO hardware in its possession; hardware is disposed of in accordance with client instructions.

Data obtained from hardware is subject to conditions imposed by the requestor (see paragraph 5.1)

Logs provided by clients are disposed of in accordance with client instructions.

4. Private Communications

4.1 Key Elements of a Private Communication

Within the context of cyber defence activities, the key elements of a private communication are as follows:

- private communications involve the transmission or exchange of information between two or more human beings;
- at least one of the communicants must be physically located in Canada (this is the case for all communications obtained during CSEC's collection activities, including cyber defence activities); and
- private communications are captured in transit. Data at rest is not considered a private communication.

Identifying metadata (unless it is detached, as per paragraph 2.4) and email attachments taken from a private communication are treated as private communications; they are subject to essentiality tests and Ministerial reporting requirements. See paragraph 4.2 for examples of what does not constitute a private communication.

For cyber defence operations under MA, the determination of whether data is a private communication is made at the same time as the decision to use and retain the data. For DPSO, the requestor makes the determination.

4.2 Interpretation

Determining what constitutes a private communication is not always straightforward. The following examples are not private communications:

- results from executing malware taken from a private communication (this is derivative information - see paragraph 2.6; the malware itself is a private communication, and may be retained only if essential to do so.)
- signatures created from a private communication (derivative information); the original private communication may be retained, if essential
- firewall logs
- automated (machine-generated) messages, such as “out of office” responses – the originator (a machine) has no expectation of privacy. A private communication must have a human originator and a human recipient. This applies even if the automatic message contains extracts from the original message, such as a subject line.
- data obtained from a hard drive.

The distinction between “data at rest” and “data in transit” is not always clear; IPOC should be consulted if there is doubt.

4.3 Essentiality

Private communications obtained during cyber defence operations under MA may only be used or retained if essential to identify, isolate or prevent harm to GC computer systems or networks.

Private communication obtained under MA may be essential if they:

- have one or more significant characteristics similar to malicious activities of concern previously seen in cyber defence activities;
- provide an indication that a computer system is or may be attempting to, or succeeding in affecting the confidentiality, integrity, and/or availability of GC computer systems or networks;
- characterize the normal behaviour of a computer system or network, or a part of it, for the purpose of identifying deviation from this normal behaviour which could be indicative of possible malicious activity against GC computer systems or networks;
- can be used to improve or create a cyber defence capability.

Essentiality may be determined for other reasons; the rationale must be recorded.

Once the data is no longer essential, it may be deleted (see paragraph 5.2).

Private communications provided to CSEC by a system owner or requestor (DPSO) may only be used or retained if essential for the protection of the specific system, unless consent to share has been given by the originator or

recipient.

4.4 Counting

As an MA requirement, CSEC must count all recognized private communications retained during cyber defence operations under MA, as follows:

- every individual email retained will be counted as one recognized private communication, even if that email contains email attachments (retained email attachments are counted if the source email itself is not retained).
- if data from many identical emails is used or retained, the count must reflect the number of emails from which data was obtained.
 - for example, identical emails containing malicious attachments are sent to two individuals. If the “to” metadata from both emails is retained, count as two private communications used and retained.
- for other types of data recognized as private communications, every individual recognized data flow (or IP packet for non-flow data) retained will be counted as one recognized private communication.

The total count of recognized private communications that have been retained must be calculated on a per client basis for the MA under which the data was obtained. When requested by IPOC, a record of the count must be generated by a supervisor in the Cyber Defence Branch.



Note: The total number of private communications reported to the Minister must not be altered (for example, do not alter the count of private communications or delete a private communication once it has been accounted for in a report to the Minister), without first informing IPOC. IPOC will ensure that any changes to the reported total for an MA period are reflected in subsequent reports to the Minister.

5. Data Retention and Deletion

5.1 Raw Data

- Raw data obtained under MA operations must be deleted within [REDACTED] of the date it was copied, unless marked for retention.
- DPSO is subject to conditions imposed by the requestor; unless retention is approved, raw data must be deleted within [REDACTED] of completion of the requested assistance.
- Under MA operations, a client may direct that raw data obtained from their systems and networks be deleted (for example, if the client

terminates the operation). Raw data must be deleted within [REDACTED] of the client request; analysis is not permitted on the raw data, and the data must not be used or retained.

5.2 Data Retention

- Raw data may be marked as used or retained (if relevant or essential), for analysis purposes without having to be included in a cyber defence report (see ITSOI-1-4 for definition). Supervisors (or higher levels) may approve the deletion of data that has been used or retained (but not used in a report) if it no longer merits further retention from an operational perspective. Inform IPOC of any such deletions (to ensure statistics are accurate).
- Data used in a report must be retained for as long as the report is retained. Report retention is also subject to CSEC schedules.
- Detached metadata (see paragraph 2.3) is relevant for up to [REDACTED]. If there is a requirement to retain the information beyond [REDACTED] or share the information with Second Parties, it must be marked as used or retained. Otherwise it must be deleted.
- Metadata used only to generate statistics or to show trends is not considered to be used or retained; no retention is required.

5.3 Compliance

Supervisors in the Cyber Defence Branch are responsible for

- ensuring automated deletion processes are functioning properly, and
- ensuring staff delete raw data that is not accessible by automated deletion processes (e.g., stored on a desktop).

IPOC will send quarterly verification reminders to those authorized to conduct or support cyber defence activities.

6. Additional Information

6.1 Accountability

This table establishes the areas of responsibilities as they relate to these instructions.

Who	What
Deputy Chief, IT Security	<ul style="list-style-type: none"> • Approving these instructions
Director, Program Management and Oversight	<ul style="list-style-type: none"> • Recommending these instructions for approval • Revising these instructions as necessary • Monitoring compliance with these instructions • Communicating guidance to those authorized to conduct cyber defence activities regarding any revisions to these instructions

Manager, Corporate and Operational Policy	<ul style="list-style-type: none">• Reviewing these instructions to ensure compliance with CSEC policy
--	--

-
- 6.2 References**
- OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC's 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*
 - *Instructions for Commencing and Ceasing Cyber Defence Operations (IPOC Working Aid)*
 - ITSOI-1-3, *Accessing and Sharing Cyber Defence Data*
 - ITSOI-1-4, *Report Management in Cyber Defence Activities*
-

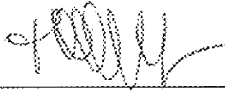
6.3 Enquiries Questions relating to these instructions should be directed to supervisors in the Cyber Defence Branch, who in turn will contact IPOC as required.

7. Promulgation

I hereby approve Operational Instructions ITSOI-1-2, *Data Handling in Cyber Defence Activities*.

These instructions are effective on June 28, 2013.
(Date)

Approved

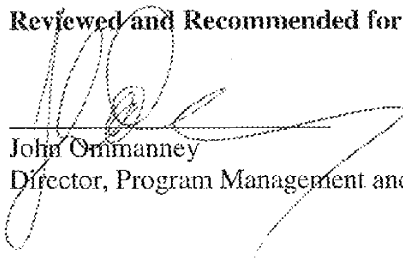


Toni Moffa
Deputy Chief, IT Security

28 June 2013

Date

Reviewed and Recommended for Approval



John Ommanney
Director, Program Management and Oversight

June 27/13

Date