



CSE IT Security Operational Instructions: ITSOI-1-7

Data Disclosures to CSE For Part (b) Cyber Defence Activities

IT Security

Canada

Table of Contents

1. Introduction.....	3
2. Disclosure Activities.....	4
3. Roles and Responsibilities	7
4. Additional Information	7
5. Promulgation	9
Annex A: Disclosure Letter Example.....	10
Annex B.....	10

1. Introduction

1.1 Objective These instructions provide direction on receiving and using data disclosed to CSE/IT Security for cyber defence activities. As there may be personal information included in some disclosed data, CSE must have measures in place regulating the use and retention of that information, as required by subsection 273.64(2) of the *National Defence Act* (NDA).

Note: For these instructions, “data” refers specifically to information obtained from a computer system or network, and provided to CSE for cyber defence purposes.

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

1.3 Authorities In accordance with paragraph 273.64(1)(b) of the NDA, CSE may receive information disclosed by other entities including federal institutions¹, the private sector², and foreign governments, to help protect electronic information and information infrastructures of importance to the GC.

Use of Personal Information disclosed to CSE must be consistent with CSE’s Cyber Defence Personal Information Bank³. Disclosed data is considered to be transitory until it is used and retained by CSE, and must be disposed of once no longer of business value⁴.

1.4 Disclosure versus Request for Assistance Entities disclosing data to CSE do not expect assistance. If assistance is required, the data must be provided either under OPS-1-15 or as a request submitted under part (c) of CSE’s mandate (if requested by law enforcement or security agencies under their mandate and authority).

1.5 Limitations CSE’s use of data disclosed under part (b) is limited to activities that:

- provide advice, guidance and services to help ensure the protection of electronic information and of information

¹ Personal information may be disclosed by GC entities pursuant to paragraph 8(2)(a) of the *Privacy Act*.

² CSE may receive information from any private sector entity, not just those of importance to the GC. These entities may disclose personal information pursuant to sub-paragraph 7(3)(d)(ii) of the *Personal Information Protection and Electronic Documents Act*.

³ CSE PPU 007 - see cerriid [11081675](#).

⁴ See cerriid [827151](#)- IM-1-2 *Policy on the Management and Disposition of CSEC Corporate Transitory Information* (2.2).

infrastructures of importance to the Government of Canada;

- are not directed at Canadians or any person in Canada;
- are subject to measures to protect the privacy of Canadians; and
- are in strict compliance with all relevant laws of Canada and consistent with Ministerial Directives and Authorizations.

2. Disclosure Activities

2.1 Disclosure Requirements

Entities disclosing data to CSE for part (b) purposes (from outside CSE) must:

- confirm that CSE may use the data for part (b) purposes, and
- provide any relevant contextual information that would impact CSE's ability to use the data lawfully. For example, a law enforcement agency must note whether data provided to CSE contains intercepted private communications lawfully obtained under warrant and if so, any use conditions noted in the warrant.

A single statement covering these requirements may be used for one-time or occasional disclosures (see Annex A). For on-going disclosures, either CSE or the disclosing entity may request that a formal agreement be signed.

The documentation forms part of the corporate record that the Cyber Defence Branch is responsible for establishing and maintaining for review purposes.

2.2 Requested Limitations

Disclosing entities may request limitations on CSE's use and sharing of data. CSE will abide by these limitations except in extenuating circumstances; under these circumstances the relevant operational director must be consulted.

2.3 Raw SIGINT

The SIGINT program may disclose raw data to IT Security for cyber defence purposes, in accordance with:

- the Metadata MD (paragraph 7(4)), which notes that unaltered metadata may be disclosed to ITS cyber defence personnel for part (b) purposes
- the Intelligence Priorities Ministerial Directive 2014-16 (paragraph 2(c)), which stresses the importance of sharing cyber threat information within CSE for part (b) purposes, and
- OPS-1 (3.20), which states that SIGINT intercept and metadata may be shared with IT Security.

All SIGINT data disclosures must be done in accordance with SIGINT operational policy. Contact IPOC for assistance.

**2.4 Data
Labelling**

For data (and devices containing that data) disclosed to CSE for cyber defence purposes, the Cyber Defence Branch recipient must be able to identify:

- how the data came into CSE's possession (i.e. "Disclosed for part (b)");
- the data source⁵;
- the date the data and/or devices were provided; and
- special handling instructions (if any).

See Annex B for various data labelling examples.

**2.5 Relevancy
of Information**

CSE may only use and retain data disclosed for part (b) purposes if it is relevant to helping to protect information and information infrastructures of importance to the GC.

Disclosed data may only be shared beyond CSE once it has been used and retained (i.e. formally deemed to be relevant to part (b) of CSE's mandate).

**2.6 Data
Retention**

Data that has been used and retained is subject to the CSE/ITS Functional Retention Schedule⁶, established pursuant to *The Library and Archives Canada Act*.

**2.7 Data
Sharing and
Cyber Defence
Reporting**

Data that has been used and retained may be shared with the SIGINT program; it may also be shared beyond CSE, in accordance with relevant CSE policies and authorities, including the Ministerial Directive on the Privacy of Canadians.

Cyber defence reports based on disclosed data are subject to ITSOI-1-4; CII is subject to OPS-1-6 *Operational Procedures for Naming and Releasing Identities in Cyber Defence Reports*. Reports are approved by the relevant manager.

⁵ For example, a cerid number may be used to reference the entity's disclosure letter

⁶ See cerid 10635303, functional file number M.2.6.0-00.

2.8 Sensitive Information

The following are examples of sensitive information that might be encountered within disclosed data, and guidance on how to handle that information.

Information type	Guidance
Intercepted private communications (PC)	<ul style="list-style-type: none"> • If intercepted PC is encountered, CSE may only use and retain that data if a request is submitted in accordance with OPS-1-15 (DPSO), or under part (c); • Law enforcement or security agencies may only disclose PC for part (b) purposes if permitted by the warrant under which it was obtained, or other legislative authority.
Personal information (PI)	<ul style="list-style-type: none"> • CSE's use of personal information must be consistent with uses described in the cyber defence PIB⁷.
Indications of a criminal offence	<ul style="list-style-type: none"> • If not related to a cyber threat, the data must be brought to the attention of the relevant director; • The director may seek advice as required, prior to taking action.
Security intelligence (non-PC)	<ul style="list-style-type: none"> • Data may be passed to CSIS with the approval of the relevant director; • No use or retention is permitted if the data is not relevant to part (b).
Information having solicitor-client privilege ⁸	<ul style="list-style-type: none"> • Contact IPOC to determine what should be done with the data.

⁷ See CSEC PPU 007 (available on the external CSE website).

⁸ As described in 8.24 of OPS-1.

3. Roles and Responsibilities

3.1 Roles and Responsibilities

This table highlights key roles and responsibilities with respect to handling information disclosed to CSE for cyber defence purposes.

Who	Responsibility
Cyber Defence Branch personnel receiving data disclosed for part (b) purposes	<ul style="list-style-type: none"> Ensuring CSE has permission to use disclosed data for part (b) purposes. Ensuring disclosed data is appropriately labelled. Respecting data provider's requested conditions.
Cyber Defence Branch managers	<ul style="list-style-type: none"> Approving reports based on disclosed data.
Cyber Defence Branch directors	<ul style="list-style-type: none"> Determining appropriate action when data contains indications of criminal activity or security intelligence.
IPOC	<ul style="list-style-type: none"> Determining appropriate action when data subject to solicitor-client privilege is encountered.

4. Additional Information

4.1 Accountability

This table outlines the accountability with respect to these instructions.

Who	Responsibility
DC IT Security	<ul style="list-style-type: none"> Approving these instructions
DG Cyber Defence	<ul style="list-style-type: none"> Recommending these instructions for approval
Director, ITS 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 CSE policy

4.2 References

- *Privacy Act*
 - *National Defence Act*
 - *Personal Information Protection and Electronic Documents Act*
 - *Ministerial Directive Collection and Use of Metadata*
 - *Ministerial Directive Intelligence Priorities 2014-2016*
 - *Ministerial Directive Privacy of Canadians*
 - *OPS-1, Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE's Activities*
 - *OPS-1-6, Operational Procedures for Naming and Releasing Identities in Cyber Defence Reports*
 - *OPS-1-15, Operational Procedures for Cyber Defence Activities Using System Owner Data*
 - *IM-1-2 Policy on the Management and Disposition of CSEC Corporate Transitory Information* ITSOI-1-2, *Data Handling for Cyber Defence Activities*
 - *ITSOI-1-3, Accessing and Sharing Cyber Defence Data*
 - *ITSOI-1-4, Report Management in Cyber Defence Activities*
 - *ITSOI-1-6, Cyber Defence Activities: Compliance Monitoring*
-

4.3 Amendment Process

Situations may arise where amendments to these instructions are required because of changing or unforeseen circumstances. Such amendments will be drafted and promulgated in accordance with ORG-1-1.

4.4 Enquiries

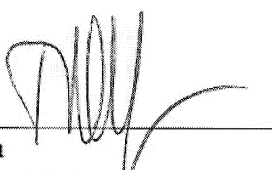
Questions related to these procedures should be directed to managers within the Cyber Defence Branch, who in turn will contact IPOC.

5. Promulgation

I hereby approve Operational Instructions ITSOI-1-7, *Information Disclosures to CSE for Part (b) Purposes*.

These instructions are effective on APRIL 29, 2015.
(Date)

Approved:


Toni Moffa
Deputy Chief IT Security

Apr 29/15
Date


Reviewed and Recommended for Approval:


Scott Jones
Director General, Cyber Defence Branch

APR 24 2015

Date

Reviewed and Recommended for Approval; report release authority (noted in paragraph 2.7) is approved, in accordance with OPS-1, 4.17:


Director, Program Management and Oversight

2015/04/21
Date

Reviewed:


Manager, Corporate and Operational Policy

15 April 2015
Date

Annex A: Disclosure Letter Example

(Classification: use PROTECTED B as default)

Dear [CSE contact]

In my role as [CIO, vice president, DG etc.], I have the authority to provide information lawfully acquired by, and under the control of [company, department], to CSE. CSE may use, share and retain any information provided by [company, department] for the purpose of helping to protect electronic information and information infrastructures of importance to the Government of Canada. Sharing may include domestic and international partners involved with cyber security, both in the public and private sector. CSE may retain this information for as long as is necessary [if not, state retention time]. [state additional restrictions if necessary].

This applies to all information provided to CSE by [company, department], unless otherwise noted.

[Save letter in cerrid; use number as reference for future disclosures]

Annex B

Examples of hardware and information labelling, identifying:

- Authority;
- Source;
- Reference to documented permissions and instructions;
- Date of intake; and
- Requested retention period.

1) Information disclosed from a GC department to CSE:

Part (b) disclosure / PS-CCIRC / #19526751 / 15 Feb 2014 / 1 year

2) Information from a private sector entity to CSE:

Part (b) disclosure / Anti-virus Company / #17710183 / 15 Feb 2014 / no limit

NOTE: Consider following the Smart Data initiatives and best practices.