Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

CSEC IT Security Operational Instructions: ITSOI-1-3

Accessing and Sharing Cyber Defence Data

IT Security

Canada

Table of Contents

1. Introduction 3

2. Access to Cyber Defence Data 3

3. Sharing Data 5

4. Additional Information 6

6. Promulgation 7

1. Introduction

1.1 Objective

These instructions provide direction concerning access to and sharing 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.

Terminology

1.3 Access

For these instructions, "access" refers specifically to raw data that is available to those within CSEC who are authorized to conduct or support cyber defence activities.

1.4 Sharing

For these instructions, "sharing" refers to data that has been used or retained, which may be made available to cyber defence counterparts within the Second Party cryptologic community.

2. Access to Raw Data

2.1 Definitions

For cyber defence activities, "data" refers to [redacted] obtained from computer systems or networks of importance to the Government of Canada (GC); it includes content and 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 General Principles

Access to raw data must be strictly controlled and limited to those authorized to conduct or support cyber defence activities, as per OPS-1-14[1] (raw data may also be accessed by CSEC personnel involved with oversight or compliance, as well as by review bodies such as the CSE Commissioner's Office).

[1] Raw DPSO data may be provided to CSIS and the RCMP in certain situations; see OPS-1-15.

Second Party cyber defence counterparts may not access raw data (data that has been used or retained may be shared with Second Parties - see section 3).

Detached Metadata (as described in ITSOI-1-2) is, for the purpose of these instructions, subject to the same conditions as raw data; it may only be accessed by those authorized to conduct or support cyber defence activities.

2.3 Authority to Conduct or Support Cyber Defence Activities

Personnel responsible for conducting or supporting cyber defence activities (primarily analysts in the Cyber Defence Branch) are in designated or temporary positions that are justified and approved yearly by DG Cyber Defence Branch. Access to raw data is granted without further justification provided they have read relevant policies and successfully completed the policy knowledge quiz. Those conducting or supporting cyber defence activities may query, use, retain and manipulate raw data.

Others in IT Security or SIGINT may also seek the approval of DG Cyber Defence for access to raw data if they will be conducting or supporting cyber defence activities. Temporary access may be granted to those involved in research and development (e.g., Second Party personnel attending cyber defence workshops).

Requests must be supported by the relevant Cyber Defence Branch manager, and include an operational justification. Prior to being authorized, individuals must read relevant policies and complete the policy knowledge quiz.

Note: Access to systems containing MA and DPSO raw data is limited to those authorized to conduct or support cyber defence activities, and those involved with oversight and compliance activities. CIO system administrators may have incidental access to raw data while performing their duties.
Any access to these systems must be logged; logs must be backed up.

2.4 ITS Access to SIGINT Data

ITS personnel may be given access to raw SIGINT data, in accordance with CSOI-5-3. IPOC should be consulted for further details and/or assistance in gaining access.

2.5 SIGINT "Triaging"

OPS-1-14 and OPS-1-15 allow raw data to be passed (by those authorized to conduct or support cyber defence activities) to individuals in SIGINT who are not authorized to conduct or support cyber defence activities, in order to seek assistance in determining whether the data is relevant or essential.

> **Attention:** personnel providing raw data to SIGINT for triaging are responsible for ensuring recipients are aware of their responsibilities with respect to use and handling of the data.

3. Sharing Data

3.1 General Principles

Second Parties are not authorized to access to raw data. However, they may access data that has been used or retained, for example in ITS Cyber Knowledge Bases (CKBs) such as the Malware Repository.

The purpose of sharing used or retained data with Second Party counterparts is to

- increase analytic coverage and efficiency,
- allow analytic collaboration, training, and R&D,
- allow CSE to receive data from Second Parties in return, and
- help protect Second Party infrastructures, which are interconnected with Canadian infrastructures of importance.

Conditions:

- Access controls must be in place to ensure only authorized users can access the data
- Users must be aware of any limitations concerning use of the data (caveats may be used within CKBs)
- Statistics on the amount of used or retained data shared via CKBs, including results from signatures which produce output that is automatically used or retained, must be available for review purposes (see ITSOI-1-1, paragraph 4.4).

Cyber Defence Branch managers are responsible for approving use of and access to IT Security CKBs. IPOC must be consulted prior to each new scenario involving the sharing of data with Second Parties.

Data sharing within ITS CKBs is not subject to OPS-1 report sign-off authorities.

3.2 Sharing CII

Canadian Identity Information (CII) contained within IT Security CBKs must not be accessible by Second Parties. However, it may be possible to share the CII unsuppressed if the CII is being used by a malicious foreign actor. IPOC must be consulted prior to each new scenario involving the sharing of unsuppressed CII with Second Party counterparts (in accordance with OPS-1, paragraph 4.7).

4. Additional Information

4.1 Accountability

Who	Responsibility
DC IT Security	○ Approving these instructions
Director, Program Management and Oversight	○ 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	○ Reviewing these instructions to ensure compliance with CSEC policy

5.2 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*

○ ITSOI-1-2, *Data Handling in Cyber Defence Activities*

○ ITSOI-1-4, *Report Management in Cyber Defence Activities*

5.3 Amendment Process

Situations may arise where amendments to these instructions are required because of changing or unforeseen circumstances. Such amendments will be communicated to relevant staff.

5.4 Enquiries

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

6. Promulgation

I hereby approve Operational Instructions ITSOI-1-3, *Access and Sharing Cyber Defence Data.*

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

Approved

28 June 2013

Toni Moffa
Deputy Chief IT Security

Date

Reviewed and Recommended for Approval

June 28/13

John Ommanney
Director, Program Management and Oversight

Date