



CSEC IT Security Operational Instructions: ITSOI-1-4

Report Management in Cyber Defence Activities

IT Security

Canada

Table of Contents

1. Introduction.....	3
2. Cyber Defence Reporting	3
3. Re-issuing Reports	8
4. Additional Information	9
5. Promulgation	11
Annex A – Report Caveats	12
Annex B – Cyber Defence Report Release Authorities	13

1. Introduction

1.1 Objective These operational instructions provide direction concerning reports produced 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 integreees, involved in conducting or supporting cyber defence activities.

2. Cyber Defence Reporting

2.1 General Principles During the course of cyber defence activities, several different types of reports may be generated by those authorized to conduct cyber defence activities.

Reports and data used in the creation of the reports are official CSEC records, subject to requirements set forth in the *Access to Information Act*, the *Privacy Act*, and the *Library and Archives of Canada Act*.

2.2 Definition of "Report" A report, in the context of cyber defence activities conducted under part (b) of CSEC's mandate, refers to information prepared by those authorized to conduct or support cyber defence activities, which has been approved for distribution beyond CSEC and Second Party cyber defence counterparts (reports may also be sent to Second Party recipients for analytic collaboration, training, research and development, or for situational awareness).

2.3 Report Types Report formats may vary and can include a variety of vehicles, from traditional narrative reports to email. Report series, formats and classifications are determined by CTEC and written by analysts within the Cyber Defence Branch.

For distribution methods that do not fit the definition of "report", contact IPOC to determine approval levels and compliance requirements.

**2.4 Report
Access**

All reports, regardless of the report format or type, must be stored on accredited systems and retained in accordance with CSEC retention and disposition schedules (which are the responsibility of CIO).

Access to reporting systems, as well as databases containing reports, may be granted to anyone at CSEC authorized to conduct or support cyber defence activities. Access may also be granted on a case by case basis through, IPOC, for purposes of supporting part (b) of CSEC's mandate; an appropriate rationale must be provided to IPOC.

**2.5 Time-
sensitive
Reports
("Tippers")**

In order to prevent or mitigate a cyber incident, reports often must be passed to a client immediately (i.e., cyber defence tippers). Tippers may be pre-approved for release by the operational manager, provided they:

- are issued only to the client from which the information was obtained, under MA (this may also include SSC, as the system owner)
- only contain enough information to allow the recipient to perform mitigation. This may include
 - o domains,
 - o IPs,
 - o email header information
- include only mitigation advice, such as:
 - o "block domain/IP (x)"
 - o "unplug from your network the machine matching timestamp and IP (x)", and/or
 - o "remove traces of email (x) from your departmental mail servers", and
- contain standard caveats warning against further action.

There is no requirement to obtain post-release manager approval. Any proposed tipper that does not meet the above conditions must be approved at the manager level prior to release.

For compliance purposes:

- The granting of pre-approval for these tippers must be retained
 - Supervisor approval for each release is required, and must be retained
 - A copy of the tipper must be retained
 - IPOC will review tippers as part of compliance monitoring.
-

**2.6 Use of
SIGINT**

Data provided to the IT Security program from SIGINT sources may be used for:

- Cyber defence activities under part (b) of the mandate
- Triage and correlation
- Situational awareness

The SIGINT program will stipulate handling instructions for reporting

their information, including classification and what action, if any, may be undertaken.

IPOC should be consulted if instructions have not been provided.

**2.7 Forwarding
Second Party
Non-classified
Reports**

With the approval of a Cyber Defence Branch supervisor (or higher), non-classified¹ reports from Second Parties without any restrictive caveats may be sent to:

- Other government departments, as required;
- Public Safety - CCIRC (which may in turn forward the reports to information infrastructures of importance to the Government of Canada).

A record of the distribution, including recipients, must be kept.

**2.8 Forwarding
Second Party
Classified
Reports**

Classified Second Party cyber defence reports normally contain specific handling instructions that outline what usage, including dissemination, may be undertaken on the basis of the reports without prior consultation, and at what classification. For usage not addressed by handling instructions, those authorized to conduct or support cyber defence activities must first consult the relevant Second Party (the consultation must be documented).

In cases where Canadian or Second Party identities are involved, contact IPOC to determine whether suppression is required.

Factors to consider prior to forwarding classified Second Party reports include:

- limitations outlined in the handling instructions
- equity issues
- tradecraft sensitivities
- requisite clearance and storage capability of the intended recipient(s).

Forwarding classified Second Party reports requires the approval of a Cyber Defence Branch supervisor (or higher). A record of the distribution, including recipients, must be kept.

**2.9 Use of
Cyber Defence
Reports**

Classified or Protected cyber defence reports must carry a caveat, describing how the reported information may be used, and obligations regarding other uses. See Annex A for an example of a caveat that might be used. Other caveats relating to the report's source, sensitivity, and distribution may also be included, if necessary.

¹ "Non-classified" refers to information that is not "confidential", "secret" or "top secret". Non-classified includes Protected A, B, or C, as well as second party markings such as For Official Use Only, or Restricted.

IPOC must be informed of any proposed usage that goes beyond permitted mitigation (e.g., the recipient wants to distribute information beyond their department). IPOC in turn will inform DGPC (Disclosure, Policy and Review) as necessary, for example if the proposed usage may result in:

- information being disclosed in a legal proceeding
- CII (that had originally been suppressed) being distributed beyond the recipient's department
- information being sent to [REDACTED]

2.10 Equities

Authorities responsible for recommending and approving cyber defence reports must ensure that reports which might impact equities (e.g., SIGINT and/or Second Party equities) have been identified and appropriate consultations have taken place prior to report release.

CTEC is responsible for managing equities in reporting on behalf of the Cyber Defence Branch.

2.11 CII

For reports distributed beyond the federal institution from which the data was obtained, and beyond CSEC, unsuppressed Canadian Identity Information (CII) may be included if:

- the information is necessary in order for recipients to use CSEC mitigation advice to protect their own networks, or
- on a case by case basis, CII has been compromised by, or is the target of, a malicious foreign actor (contact IPOC for details).

Otherwise, CII must be suppressed.

Domain names and websites associated with federal institutions, as well as the name of the federal institution, are not CII. If in doubt, consult a supervisor in the Cyber Defence Branch, who may in turn contact IPOC as necessary.

Reports containing suppressed identities must be made accessible to Corporate and Operational Policy (D2) staff to manage requests for suppressed identities.

2.12 Second Party Identities

IT Security treats Second Party identifying information in accordance with their respective policies. Identities must be linked to malicious cyber activity.

Most Second Party identifiers must be suppressed when reported, however various Second Party policies allow for some exceptions. For more information, contact IPOC.

If IT Security discovers an intrusion that affects one of the other Second Party partner nations, identities (of that Second Party) related to that intrusion may be included in a report and sent to the affected partner,

unsuppressed. For example, [REDACTED]

2.13 Second Party Reports Containing Unsuppressed CII

CSEC may receive unsuppressed CII from Second Party counterparts (if CSEC is the only recipient), on the understanding that the CII will be suppressed in reports issued to other recipients. If the CII is emailed directly to IT Security, Corporate and Operational Policy must be informed.

2.14 Report Release Authority

See OPS-1 Cyber Defence Report Release Authorities - also attached in Annex B

2.15 Recommend/Release Authority Considerations

Cyber Defence Recommend and Release Authorities responsible for recommending and approving release should consider the following before signing:

- Does the report contain private communications? If so, is reporting essential to protect the GC?
- Does the report contain Canadian or Second Party Identity Information? If so, is it necessary to include that information? Should the information be suppressed or unsuppressed?
- Is the proposed distribution justified?
- Based on the above, are the "recommend for release" and the "report approval" levels consistent with OPS-1 requirements?
- Is the report classification appropriate?
- If the report contains information provided by the SIGINT program, has the appropriate consultation taken place and been documented?
- If the report contains information received from a Second Party, or reveals a Second Party's tradecraft or equity, is the approval of that Second Party required?

2.16 Report Release Documentation

Details concerning the release of cyber defence reports must be recorded in a corporate repository and be accessible for future audit and review.

The report details must contain the following information:

- unique report identifying number
- list of recipients
- the data source(s) (e.g., MA, DPSO, Second Parties, Open Source)
- recommendation and approval
- whether the report contains CII (either suppressed or unsuppressed)
- whether the report contains private communications.

3. Cancelling and Re-issuing Reports

3.1 Report Cancellation

While reports may be corrected to address minor errors, Cyber Defence Branch supervisors must cancel a report when:

- a re-evaluation of the status of the original data is required. For example, data is later determined to be a portion of a private communication, in which case a higher level of approval is required. In such cases, data must be noted as being an essential private communication. (Note that a cancellation is not required if a higher sign-off level than required approves a report, although data markings and statistics related to private communications would require correction) – inform IPOC of changes to data markings;
- a significant portion of the report is found to be incorrect;
- it is nationally sensitive (e.g., it should have been CEO);
- it is under-classified (i.e., the classification of the original report was lower than required, or one or more caveats were omitted); or
- it inadvertently discloses a Canadian or Second Party identity that should not have been included or that should have been suppressed (IPOC must be notified of the potential privacy incident, and in turn will inform D2 of a confirmed privacy incident).

Reports may also be cancelled for other reasons, as determined by supervisors in the Cyber Defence Branch.

Cancelled reports must be removed from all holdings except the client file (held by CTEC). The supervisor must send a destruction notice to all recipients of such cancelled reports. The rationale for cancelling the report and the steps taken to do so must be documented and added to the client file. A new report may be issued depending on the circumstances, as determined by the relevant supervisor in the Cyber Defence Branch.

IPOC must be informed of any report cancellations. In addition, IPOC must be notified if there are any suspected privacy incident(s). IPOC will inform Operational Policy (D2) of a confirmed privacy incident.

3.2 Report Corrections and Re-issues

A report may be corrected and re-issued when:

- part of its contents are found to be incorrect because of new information or a re-evaluation of the original data;
- it contains significant typographical or spelling errors;
- it is over-classified (i.e., the classification of one or more portions of the original report was higher than required, or one or more unnecessary caveats were included), preventing potential users from accessing information they might need; or
- it has an incorrect dissemination control marking that is too restrictive,

e.g., it was issued CEO but should have been shared with one or more Second Parties; or

- it was sent to one or more incorrect recipients (the incorrect recipients must be asked to destroy the report. Follow-on action may include a security investigation, if required).

A re-issued report will have the same report serial number as the original, with the word "Correction" immediately following. A subsequent correction may be noted as "Correction 2"; if more than two corrections are required, a cancellation may be in order.

The corrected report will be added to the client file. A report re-issue will follow all of the steps required for a new report.

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
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

4.2 References

- OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC's Activities*
- OPS-1-6, *Operational Procedures for Naming and Releasing Identities in Cyber Defence Reports*
- 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 for Cyber Defence Activities*

4.3 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.
<hr/>	
4.4 Enquiries	Questions related to these procedures should be directed to managers within the Cyber Defence Branch, who in turn will contact IPOC.
<hr/>	

5. Promulgation

I hereby approve Operational Instructions ITSOI-1-4, *Report Management in Cyber Defence Activities*.

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

Approved

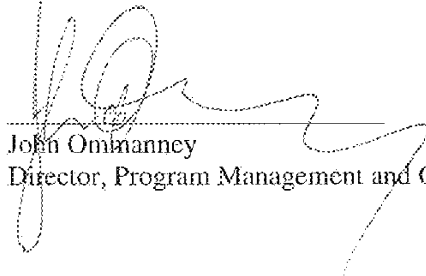


Toni Moffa
Deputy Chief IT Security

28 June 13

Date

Reviewed and Recommended for Approval



John Ommannney
Director, Program Management and Oversight

June 29/13
Date

Annex A – Sample Report Caveat

A.1 Example

Classified or Protected cyber defence reports must contain a caveat on the cover page. The following example may be used:

“This report contains details of entities, techniques or intrusion identifiers relating to malicious activities against information systems. Do not attempt to conduct open-source queries, probes or scans on the identities, techniques, domains, URLs, IP Addresses or other intrusion identifiers contained in this report. Such actions may tip hostile entities, harm information systems and/or produce false positives in security monitoring systems. Any proposed use beyond mitigation advice provided in this report must be approved by the originator of this report.”

Annex B – Cyber Defence Report Release Authorities (from OPS-1)

Cyber Defence Report Release Authorities			
Report Type	Release (beyond CII/C)	Recommendation level	Approval level
All reports	To the institution from which the information was obtained (with no further release)	Operational Supervisor	Operational Manager (or higher)
Reports containing <ul style="list-style-type: none"> • no CII (or CII allowed under paragraph 4.7 of OPS-1) • no private communications • private communications previously approved by DC ITS in other cyber defence reports 	To any recipient, including or beyond the institution from which the information was obtained		
Reports containing suppressed CII but no private communications	To any recipient beyond the institution from which the information was obtained	Director	DG CDB
Reports containing private communications		Director General	DC ITS
Open source	To any recipient	n/a	Operational Manager (may be delegated to supervisor)