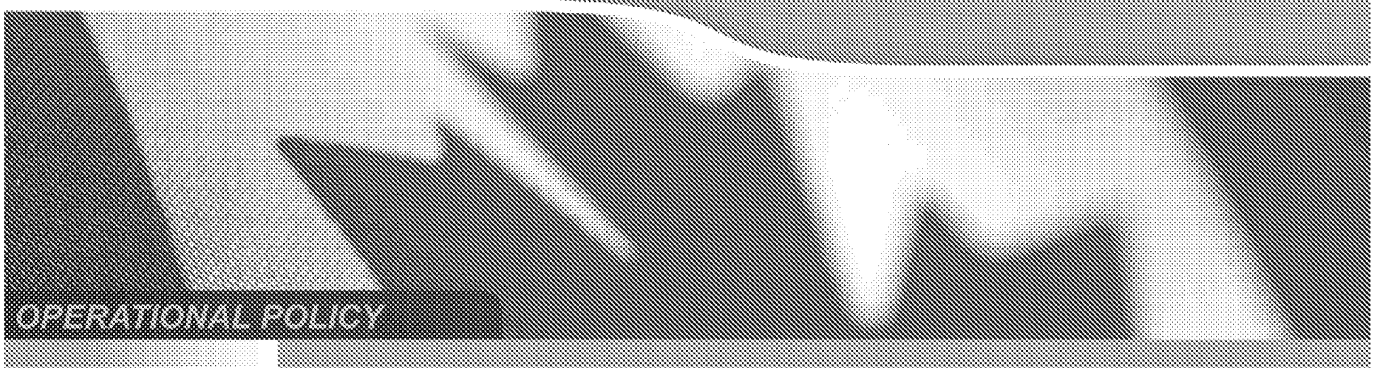
Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

OPS-1-6

OPERATIONAL PROCEDURES FOR NAMING AND RELEASING IDENTITIES IN CYBER DEFENCE REPORTS



Canada

Table of Contents

1. Procedures for Naming in CSEC Cyber Defence Reports

1.1 Objective

The purpose of the procedures set out in this chapter is to provide direction to personnel regarding the naming of Canadians, as well as US, UK, Australian and New Zealand (US/UK/AUS/NZ) entities, in CSEC cyber defence reports issued under paragraph 273.64(1)(b) of the *National Defence Act* (NDA) and resulting from cyber defence activities.

Exemption: These procedures do not apply to reports issued in accordance with OPS-1-12, *Active Network Security Testing*.

1.2 Policy

CSEC must protect the privacy of Canadians in the conduct of its operational activities in accordance with

- the NDA
- the *Ministerial Directive on the Privacy of Canadians*
- the *Privacy Act,* and
- OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the conduct of CSEC Activities.*

In cyber defence activities, one way this is achieved is by suppressing Canadian identity information (CII) in cyber defence reports that may reveal the identity of:

- Canadian persons, or
- Canadian corporations and organizations.

CII includes, but is not limited to, names, phone numbers, email addresses, IP addresses, and passport numbers.

For US/UK/AUS/NZ identities, CSEC's policy is to honour the naming rules of Second Party partners.

1.3 Application

The following staff must read, understand and comply with these procedures:

- CSEC staff, and
- any other parties, including secondees, integrees, and contractors

who are involved in the production and release of reports governed by these procedures.

1.4 Including CII

CII may be included in a cyber defence report only if it is relevant, or essential if it includes data containing a recognized private communication, to identifying, isolating or preventing harm to a federal institution's computer systems or networks.

1.5 When Must CII be Suppressed?

The following table sets out when CII must be suppressed from cyber defence reports. See paragraph 1.6 for information regarding naming exemptions.

If the report is to be disseminated to...	Then suppress and replace with a generic term...
the federal institution from which the information was obtained	N/A (No suppression required)
other federal institutions (including CSEC's Information Protection Centre)	**all CII,** except where • inclusion is relevant, or essential if it includes data containing a recognized private communication, for each recipient to use CSEC mitigation advice to protect their own networks, or • a naming exemption has been approved (see paragraph 1.6).
• Other CSEC areas (beyond the Cyber Defence Team) • Second Parties	**all CII**, except where a naming exemption has been approved (see paragraph 1.6).

1.6 Naming Exemption

CII may be included in cyber defence reports without suppression with the prior approval of the Director General, Policy and Communications (DGPC) and the Deputy Chief, Information Technology Security (DC, IT Security). This approval can be either on a case-by-case basis or for a series of reports in support of time-sensitive operations and where the information is essential to identifying, isolating or preventing harm to a federal institution's computer systems or networks.

IT Security operational elements must inform Operational Policy of all instances where CII is included in cyber defence reports under these circumstances so that the approvals and released CII can be tracked for audit and review purposes.

1.7 Naming Federal Institutions

The identities of a federal institution's employees must be suppressed. This includes the identities of Canadian users in a federal institution's email address (for example, "namedCanadian@international.gc.ca"), IP address or other electronic identifier.

The name of federal institutions, including domain names associated with their e-mail addresses (for example, the information following the "@" sign of an e-mail address, such as "@cse-cst.gc.ca"), websites (for example, www.cse-cst.gc.ca) or IP addresses that identify federal institutions (and cannot be linked to an individual), may be included in cyber defence reports without suppression. However, a decision not to include such details in cyber defence reports disseminated beyond the federal institution from which the information was obtained may be based on other criteria, such as national sensitivities.

1.8 Use of Generic Terms

Generic terms such as "a Canadian IP address" or "a Canadian e-mail address" must be used in cases where CII must be suppressed. To avoid confusion, the same generic term must be used throughout the report to describe the same entity (for example, "Canadian IP address 1).

1.9 Unknown Nationality

In cases where CII must be suppressed, and there is doubt as to whether the CII is associated with a Canadian, generic terms such as "a possible Canadian IP address" or a "probable Canadian IP address" must be used.

1.10 US/UK/AUS/NZ Identities	US/UK/AUS/NZ identity information must be suppressed from cyber defence reports in accordance with Second Party policies.
1.11 Naming Violations	Operational Policy and Cyber Defence Support Office (CDSO) personnel must be notified in cases where a CSEC cyber defence report has been issued containing Canadian or US/UK/AUS/NZ identity information that should have been suppressed in accordance with these procedures or Second Party policies, or not included at all. In these cases, the Cyber Defence Team must cancel and reissue a corrected version of the report. Operational Policy must track these incidents, including corrective action taken, in the Privacy Incidents File.
1.12 Cyber Defence Report Release	Cyber defence reports containing CII, in suppressed or unsuppressed form, must be approved for release by CSEC senior management in accordance with OPS-1.

2. Procedures for the Release of Identity Information Suppressed from Cyber Defence Reports

2.1 Objective

The purpose of the procedures set out in this chapter is to provide direction to personnel regarding the storage and release of identity information suppressed from CSEC cyber defence reports.

2.2 Policy

The release of identity information suppressed from cyber defence reports must comply with

- the NDA
- the *Ministerial Directive on the Privacy of Canadians*
- the *Privacy Act,* and
- OPS-1.

2.3 Application

These procedures apply to CSEC staff and any other parties who conduct activities under CSEC authorities, and who are involved in requesting, releasing, and storing information suppressed from cyber defence reports.

2.4 What is Suppressed Information?

For the purpose of these procedures, suppressed information is defined as information that is excluded from a cyber defence report and replaced by a generic term because it may reveal the identity of a Canadian or US/UK/AUS/NZ entity.

2.5 Access to/Storage of Suppressed Information

Information suppressed from cyber defence reports must be stored in a system with access limited to the Cyber Defence Team and others in the report editing and approval chain, system administration staff, Operational Policy and others as provided for by legislation.

2.6 Authority For Release of Suppressed Information

CSEC relies on paragraphs 8(2)(a) and 8(2)(b) of the *Privacy Act* together with the authority listed in paragraph 273.64(1)(b) of the NDA when disclosing personal information about Canadians referenced in its cyber defence reports.

CSEC's DGPC is the authority for releasing information suppressed from CSEC cyber defence reports. For all domestic releases, this authority has been delegated in writing to the Operational Policy Section. DGPC must approve foreign releases (see paragraph 2.12) before they occur.

2.7 Who May Request Suppressed Information

Requests for information suppressed from CSEC cyber defence reports may be made by:

- Canadian (domestic) requesters: federal institutions or CSEC personnel (that is, SIGINT, CIO and other IT Security personnel), or
- Second Party personnel on behalf of their clients (foreign) via Operational Policy's Second Party counterparts.

Release to Canadian Requesters

2.8 Submitting Requests

Canadian requesters must submit requests to CSEC's Operational Policy Section using the "*Request for Release of Identity Information Suppressed From CSEC Cyber Defence Reports*" form at Annex 1.

Requesters must complete fields A through G.

2.9 Criterion and Additional Conditions for Release

The key criterion for the release of identity information suppressed from cyber defence reports is whether the release of the information is relevant, or essential if it includes data containing a recognized private communication, to identify, isolate or prevent harm to a federal institution's computer systems or networks.

Continued on next page

2.9 Criterion and Additional Conditions for Release (continued)

Once this criterion has been met, Operational Policy staff must ensure that the following conditions are also met prior to releasing the information:

- the requester requires the information in the exercise of the mandate of their institution or of their responsibilities in the said institution
- the released information will be under the control of that institution, and
- the requesting institution will handle the information in accordance with the *Access to Information Act* and the *Privacy Act*.

Foreign Requests for CII Suppressed from Cyber Defence Reports

2.10 Description of the Foreign Release Process

The following table describes the foreign release process for CII suppressed from cyber defence reports.

Note: Requesting agencies include Second Party or federal institutions who may request on behalf of a foreign counterpart (for example, CSIS who wants to pass CII to the CIA).

Continued on next page

Stage	Who does it	Action
1	Requesting Agency	Forwards a detailed request to CSEC's Operational Policy Section. (See paragraph 2.11)
2	Operational Policy staff	Review the request, and **If the request is...** / **Then staff will...** incomplete: ask requesting agency for additional information. complete: • research/gather information related to the request (see paragraph 2.13) • forward a request assessment and recommendation (see paragraph 2.13) to the Manager, Operational Policy.
3	Manager, Operational Policy	Provides to DGPC (via Director, Corporate and Operational Policy) recommendation to approve or deny the request.
4	DGPC	• Reviews recommendation • If necessary, consults with CCSEC who may consult with the National Security Advisor and counterparts at Canadian partner agencies • Approves or denies the request
5	Operational Policy staff	• Replies to Requesting Agency • Retains request and all related documentation for accounting purposes

2.11 Information Required for Foreign Release Requests

The request for release of suppressed information must include the following:

- Requesting agency (for example. NSA, [redacted]
- Report serial number
- Information requested
- Priority (e.g. Urgent, Routine)
- Rationale (see paragraph 2.12 for further details), and

Continued on next page

2.11 Information Required for Foreign Release Requests (continued)

- A description of how the information will be used, once acquired, and
- Any possible action to be taken against the Canadian linked to the CII.

2.12 Rationale

Suppressed information may only be released if it is relevant, or essential if it includes data containing a recognized private communication, to protecting a federal institution's computer systems or networks.

2.13 Request Assessment and Recommendation

Once a foreign release request is received, Operational Policy must prepare a Request Assessment and Recommendation for review by the Manager, Operational Policy as part of the process described in paragraph 2.10.

The Assessment must include the following information:

a) Requesting agency
b) Report serial number
c) Information requested
d) CII
e) Priority
f) Rationale provided by requesting agency
g) Assessment of Rationale: Does it meet criteria for release i.e. is the release of the information relevant or essential to help protect a federal institution's computer systems or networks.
h) Consultations: List who was consulted as part of the assessment process (for example, the Report author or other members of the Cyber Defence Team).
i) Authority: Was the information obtained by CSEC under an MA or under the authority of the federal institution requesting assistance?
j) Possible implications for the Canadian linked to the CII or Canadian interests: What is the potential impact, including the privacy impact on the Canadian if the information is released?
k) Equities: Are there any equities issues (e.g. SIGINT equities)?
l) Proposed form of words/caveat for reply (see paragraph 2.14)
m) Recommendation (to approve or deny release)

2.14 Reply

Operational Policy must use the following form of words when replying to requests for foreign release of CII suppressed from cyber defence reports.

CSEC approves the release of [CII and minimization phrase] in report [serial] solely to [agency name] at the [classification level] for the purposes described in your request. No further action may be taken with regards to this information without the prior approval of CSEC/Operational Policy. CSEC requests that the Canadian Identity Information be protected in accordance with your own procedures for the handling of national identities. Furthermore, this information may not be used in affidavits, court proceedings, or for any other legal or judicial purpose without the prior approval of the Chief, CSEC. Questions are to be directed to CSEC/Operational Policy.

Foreign Requests for US/UK/AUS/NZ Identity Information Suppressed from CSEC Cyber Defence Reports

2.15 US/UK/AUS/NZ Identity Information

All requests for US/UK/AUS/NZ identity information suppressed from CSEC cyber defence reports must be handled by Operational Policy.

If Second Parties request one of their own national identities suppressed from a CSEC cyber defence report, then Operational Policy [redacted]

In the absence of other inter-agency arrangements, if Second Parties request the identity of another allied national (for example, NSA requests the identity of a UK IP address suppressed from a CSEC cyber defence report), then Operational Policy must seek the concurrence of the other allied agency (in the example above, GCHQ), prior to releasing the identity.

3. Information About These Procedures

3.1 Accountability

This table outlines accountability for revising, reviewing, recommending and approving these procedures.

Who	What
DC IT Security	Approves revisions to Chapters 1, 3 and 4 of these procedures
DGPC	Approves revisions to Chapters 2, 3 and 4, and Annex 1, of these procedures
General Counsel, Directorate of Legal Services	• Reviews these procedures to ensure they comply with the law • Provides legal advice, when requested
Operational Policy	Revises these procedures as required

3.2 References

- *National Defence Act*, part V.1
- *Privacy Act*
- *Ministerial Directive on the Privacy of Canadians*, June 2001
- OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities*
- OPS-1-14, *Operational Procedures for Computer Defence Operations Conducted under Ministerial Authorization*

3.3 Amendment Process

Situations may arise where amendments to these procedures are required because of changing or unforeseen circumstances. Such amendments will be communicated to staff and will be posted on the Operational Policy website.

3.4 Enquiries

Direct any questions about these procedures to CSEC Supervisors and Managers, who in turn, will contact Operational Policy staff (e-mail [redacted] as necessary.

4. Definitions

4.1 Action-on

Action-on is any action, or decision to act, taken on the basis of COMINT information, which might jeopardize the COMINT source. Action-on usually involves a sanitization.

4.2 Canadian

"Canadian" refers to

- a Canadian citizen, or
- a person who has acquired the status of permanent resident under the *Immigration and Refugee Protection Act* and who has not subsequently lost that status under that Act, or
- a corporation incorporated under an Act of Parliament or of the legislature of a province.

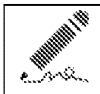
(NDA, section 273.61)

For the purpose 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 Canadian Identity Information (CII)

CII refers to information that may be used to identify a Canadian person, organization, or corporation, including, but not limited to names, phone numbers, email addresses, IP addresses, and passport numbers.

	**Note:** The names of federal institutions and their IP addresses (that cannot be linked to an employee of the institution) are not considered CII.

4.4 Cyber Defence Reports

Cyber defence reports include but are not limited to reports issued as a result of ANST, cyber defence operations and cyber defence support.

4.5 Cyber Defence Team	The Cyber Defence Team is a multi-disciplinary team consisting of persons involved in conducting or supporting cyber defence activities under the relevant authorities.
4.6 Entity	An entity is a person, group, trust, partnership, or fund or an unincorporated association or organization and includes a state or political subdivision or agency of a state.
4.7 Federal Institution	These procedures use the term "federal institution" as defined in subsection 3(1) of the *Official Languages Act*.
4.8 Information about Canadians	Information about Canadians refers to: • any personal information about a Canadian, or • any information about a Canadian corporation.
4.9 Integree	An integree is a person seconded to CSEC from one of CSEC's cryptologic partner organizations.
4.10 Personal Information	Personal information is defined in the *Privacy Act* as "information about an identifiable individual that is recorded in any form". See OPS-1, Annex 1 for the complete definition.
4.11 Privacy Incidents File (PIF)	The PIF is a central record of privacy incidents to track and demonstrate CSEC's commitment to protecting privacy, improve our own practices, ensure transparency, and enhance public confidence in CSEC. The reporting and tracking of privacy incidents is one of the measures in place to ensure legal compliance and enhances the overall privacy protection framework.

4.12 Second Parties	Second Parties refers to CSEC's counterparts: 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).
4.13 Secondee	A secondee is an individual who is temporarily moved from another GC or private or organization to CSEC, and who at the end of the assignment returns to the originating organization.
4.14 Suppressed Information	Suppressed information is defined as information excluded from a SIGINT end product or technical report or an IT Security cyber defence report because it may reveal the identity of a Canadian or US/UK/AUS/NZ entity. Suppressed information is stored in a limited access database or system and is 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]

Annex 1: Request for Release of Identity Information Suppressed From Cyber Defence Reports Form (for Canadian Requesters)

SECRET//Canadian Eyes Only (or higher when completed)

Instructions: Sections A-G to be completed by Requester
Section H to be completed by CSEC's Operational Policy

A. Requester Name	B. Requester Title and Federal Institution
C. Report Serial Number	D. Date of Request /Priority
E. Information Requested	
F. Rationale for Request ➢ Explain: o Why the suppressed information is required, and o How it relates to protecting a federal institution's computer systems or networks.	
G. Please indicate what action, if any, is being contemplated based on this information.	
H. Suppressed Information *Released by:* *Comments:* **CSEC relies on paragraphs 8(2)(a) and 8(2)(b) of the *Privacy Act* together with the authority found in paragraph 273.64(1)(b) of the *National Defence Act* when disclosing personal information about Canadians referenced in its reports. This information is provided on the understanding that the requesting federal institution requires this information to either assist CSEC in the protection of, or for the purpose of protecting, electronic information or information infrastructures of importance to the Government of Canada.** **The information contained in this form may not be used in affidavits, court proceedings or for any other legal or judicial purposes without prior approval of CSEC. It is to be used for mitigation purposes only. Any other use requires the prior approval of CSEC.**	