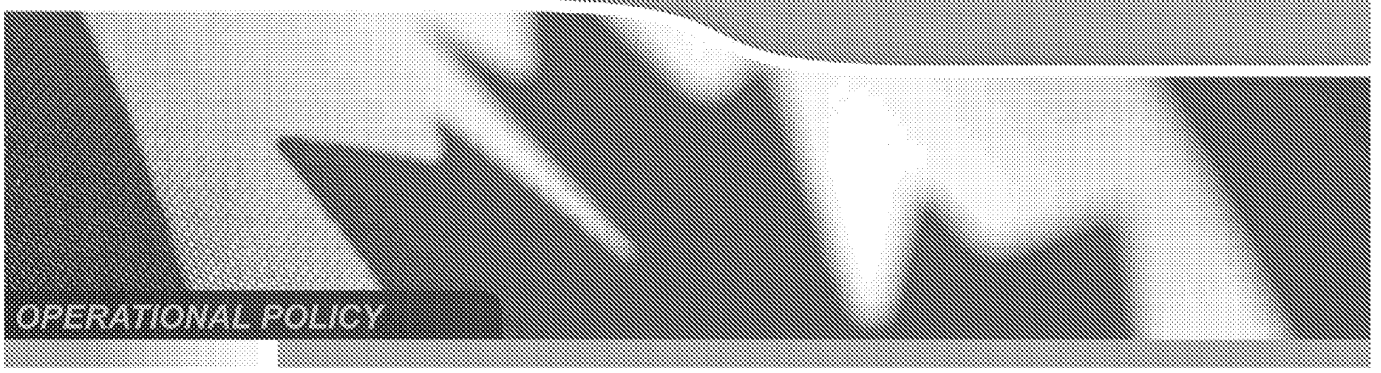
Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

OPS-1-14

Operational Procedures for Cyber Defence Operations Conducted Under Ministerial Authorization



Canada

Table of Contents

1. Introduction

Policy Scope and Application

1.1 Scope

These procedures govern CSEC cyber defence operations conducted under the authority of the National Defence Act (NDA) and a Ministerial Authorization (MA).

This document supersedes OPS-1-14, Operational Procedures for Cyber Defence Operations Conducted Under Ministerial Authorization, dated 1 December 2011.

1.2 Objective

These procedures:

- set out mandatory measures to protect the privacy of Canadians during cyber defence operations, and
- provide direction regarding
  - sharing and handling information
  - preparing for cyber defence operations
  - handling and disseminating CSEC cyber defence reports, and
  - retention and disposition schedules.

1.3 Policy

Cyber defence operations must:

- comply with the relevant laws of Canada, including the Charter of Rights and Freedoms, the Criminal Code, the Privacy Act, and the NDA
- comply with all relevant Ministerial Directives, including the the most recent Ministerial Directive on the Privacy of Canadians and the most recent Ministerial Directive on CSE's Accountability Framework
- comply with the Ministerial Authorization for Protection of Government of Canada Computer Systems and Networks ("cyber defence operations MA") in force

Continued on next page

1.3 Policy (continued)

- respect the conditions specified in arrangements signed with the federal institution ("the client")
- be subject to measures to protect the privacy of Canadians, prescribed in
  - OPS-1, Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities, and
  - paragraphs 273.64(2)(b) and 273.65(4)(e) of the NDA
- comply with these procedures, and other related IT Security policy instruments and documentation
- be carried out with awareness and approval of responsible authorities

In addition, cyber defence operations are subject to internal and external review for policy compliance and lawfulness.

1.4 Application

These procedures apply to CSEC personnel and any others, including secondees, contractors and integrees, involved in conducting or supporting cyber defence operations under the authorities noted in this Chapter.

Activity Description

1.5 What are Cyber Defence Operations?

Cyber defence operations provide advice, guidance and services to persons in possession or control of Government of Canada (GC) computer systems or networks, and all of the electronic information contained therein. Clients must request cyber defence operations.

Cyber defence operations use many different tools and databases that perform highly specialized functions; some tools may take automated action on a malicious threat as soon as it is detected.

1.6 Who is Authorized to Conduct Cyber Defence Operations?

Cyber defence operations must only be conducted or supported by CSEC personnel, secondees, contractors, or integrees who are authorized by the Director General (DG), Cyber Defence and who have acknowledged the legal and policy requirements for cyber defence operations. The Director, Program Management and Oversight (PMO) is accountable for the list of those authorized to conduct or support cyber defence operations. This responsibility is delegated to IT Security Program Oversight & Compliance (IPOC).

Legal Framework

1.7 Authorities

Cyber defence operations are conducted under the authority of:

- the NDA, paragraph 273.64(1)(b) (part (b) of the Mandate) "to provide advice, guidance, and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada"

and

- an MA in force prior to the start of and throughout cyber defence operations, issued pursuant to subsection 273.65(3) of the NDA.

FYI: MAs are issued for the sole purpose of protecting GC computer systems or networks from mischief, unauthorized use or interference, in the circumstances specified in paragraph 184(2)(c) of the *Criminal Code*, in relation to an activity or class of activities specified in the authorization.

All activities conducted pursuant to part (b) of the Mandate

- must not be directed at Canadians or any person in Canada (see ITSOI-1-1, Data Handling in Cyber Defence Activities, for further information on criteria for not directing activities at Canadians), and
- must be subject to measures to protect the privacy of Canadians in the use and retention of intercepted information.

2. Requirements for Cyber Defence Operations

Pre-Cyber Defence Operation Requirements

2.1 Required Approvals and Notifications

Prior to conducting cyber defence operations, CSEC requires:

- a letter of request from the client
- a written arrangement with the client consenting to operations (client arrangement), and
- approval by the Deputy Chief, IT Security (DC ITS).

CSEC must notify the Minister of its receipt of a letter of request, signed by the appropriate client authority, prior to deploying tools or services that risk intercepting private communications (for each MA, only one notification is required per client, not one per tool). CSEC must confirm that the Minister has received this notification.

These documents form part of the corporate record that the Cyber Defence Branch is responsible for establishing and maintaining.

Tool Deployment Requirements

2.2 Requirements for Tool or Service Deployment

The following are required to deploy a tool or service (which may consist of several tools):

1. IPOC policy compliance verification for the tool or service
2. a concept of operations (CONOP) describing the tool or service, its proposed use on the client's system, and any potential risks in running the tools; the CONOP must be provided to the client
3. documented client consent to the deployment.

These documents form part of the corporate record which the Cyber Defence Branch is responsible for establishing and maintaining.

Changes to existing services or tools may also require compliance verification and documented client consent; contact IPOC for further information.

Privacy of Canadians

2.3 Types of Information Requiring Privacy Protection Measures

Private communications and Canadian Identity Information (CII) are information types that require privacy protection measures.

See OPS-1 for an explanation of privacy protection measures.

2.4 Accounting for Personal Information Bank (PI)

To comply with its obligations under the Privacy Act regarding personal information, CSEC must account for all personal information during cyber defence operations. These are retained in a Personal Information Bank (PIB), specifically, PIB DND PPU 007.

MA Reporting Requirements

2.5 Reporting to the Minister and Other CSEC Obligations

Statistics Relating to Private Communications

The cyber defence operations MA requires that CSEC record and report to the Minister, for each client, after expiration of the MA or at any time upon request the total number of recognized private communications used or retained pursuant to the MA.

Review of Recognized Private Communications

IT Security (Director, PMO) must report on the number of recognized private communications used or retained, twice annually to the CCSEC and quarterly to the DC ITS.

3. Data Handling

3.1 Types of Retained Data

This chapter outlines the basic requirements for the handling of data and metadata. (For definitions of these types of information, see Chapter 8.)

Relevance and Essentiality

3.2 Relevancy and Essentiality of Data

Data must only be used and retained if it is relevant to providing advice, guidance, and services to help ensure the protection of electronic information and of information infrastructures of importance to the GC. In addition, private communications must be determined to be essential to identify, isolate or prevent harm to GC computer systems or networks, and may only be used (which includes sharing) and retained if both relevant (as above) and essential.

Confirmation of relevancy and essentiality may be done through automated [redacted] or human [redacted] processes.

Once the data is determined to be relevant, and essential in the case of a recognized private communication, tags must be applied prior to use and retention (this can be an automated process).

Note: Once private communications have been determined to be "essential", no further reconfirmation of essentiality is required for any further use.

3.3 Relevancy of Metadata

Metadata, as described in paragraph 8.10 is relevant since IT Security requires a pool of this type of data to conduct the statistical analysis required for situational awareness as well as the discovery efforts to detect new threats against the GC.

3.4 Data Under CSEC Control

Data that has not been used or retained (i.e., not determined to be relevant and/or essential) must be handled in accordance with the client arrangement and Chapter 5 of these procedures.

Data that has been used or retained is considered to be under CSEC's control. Specifically this data may be used beyond the client arrangement and cyber defence operations MA expiry dates. See Chapter 5 for information on retention and disposition schedules.

3.5 Private Communication Scope

Under Part VI of the Criminal Code, a communication must be intercepted while "in transit" to be considered a private communication. While all intercepted private communications must be handled in accordance with OPS-1, the scope of what constitutes a private communication is not always clear. The legal distinction between "data-at-rest" and "data-in-transit" can be complex when using [redacted] network capture. IPOC should be consulted whenever there is doubt. IPOC may seek advice from the Directorate of Legal Services (DLS) as needed.

For further instructions on use and retention of derivative information (see Chapter 8 for a definition), see ITSOI-1-1, Data Handling in Cyber Defence Activities.

Sharing and Access

3.6 Access to Cyber Defence Data

Access to data from cyber defence operations by CSEC personnel is limited those who are authorized to conduct or support such operations. These personnel must complete an annual policy quiz (IPOC maintains records relating to compliance with this requirement), and be authorized by the DG, Cyber Defence. Access by other persons requires DG Cyber Defence approval.

Raw data is not shared beyond CSEC.

Continued on next page

3.6 Access to Cyber Defence Data (continued)

Data that has been identified as relevant or essential:

- may be shared with 5-Eyes counterparts [redacted] since this in turn, will augment CSEC's ability to protect the GC. Access must be limited through access controls only to those in the cryptologic community who work on cyber defence analysis. This data is subject to suppression requirements (see paragraph 4.2).
- must be in the form of a report in order to be shared outside CSEC and the five-eyes

Attention: See ITSOI-1-3, *Accessing and Sharing Cyber Defence Data.*

Restrictions on Use

3.7 Triaging

In determining whether data should be used or retained (i.e., it has not been determined to be relevant or essential), it may be passed to personnel in SIGINT who are not authorized to conduct or support cyber defence operations, in order to seek their assistance in determining the operational significance of the data for cyber purposes. Such "triaging" is performed on the understanding that SIGINT will not use or retain the data.

Consult IPOC for requirements and restrictions on sharing data with individuals in SIGINT who are not authorized to conduct or support cyber defence operations.

3.8 Data Indicating a Criminal Offence

If, during a cyber defence operation, personnel authorized to conduct or support cyber defence operations find indications of a possible Criminal Code offence that is unrelated to a cyber threat, the incident must be brought to the attention of the relevant Director in the Cyber Defence Branch. The Director may seek advice from DLS, as needed, prior to informing the client. The client has responsibility with respect to follow-on action. The Director must also notify DG, Cyber Defence and DC ITS of the incident.

Continued on next page

3.8 Data Indicating a Criminal Offence (continued)

Warning: All details concerning any such discovery must be controlled and shared on a strict "need-to-know" basis.

4. CSEC Cyber Defence Reports

Report Writing

4.1 Focus

Reports must focus on providing advice and guidance to help protect computer systems or networks of the GC or to help ensure the protection of electronic information and of information infrastructures of importance to the GC.

4.2 Suppressing Identity Information

Identity information is suppressed in accordance with operational procedures. See OPS-1-6 and OPS-1-7 for details.

4.3 Caveats

Where applicable, reports must contain a caveat that

- notes any restrictions in the use of the reported information, and
- sets out the recipient's obligations with respect to follow-on action (this caveat should appear on the cover page).

Publication and Distribution

4.4 Release Authorities

Report Release Authorities must review and approve reports prior to release, as set out in OPS-1.

In addition to ensuring that privacy measures have been properly applied, Report Release Authorities are responsible for confirming caveats, ensuring the proposed distribution is appropriate, identifying reports that may affect intelligence sources or methods, and consulting those responsible for the intelligence assets prior to report release.

4.5 Rationale for Sharing Reports

Reports may be shared for the purpose of helping to protect electronic information and information infrastructures of importance to the GC. In order to include a private communication in a report, doing so must be essential to identify, isolate, or prevent harm to GC computer systems or networks. The Report Release Authority must confirm essentiality prior to approving release of the report.

Post-Publication Requests

4.6 Releasing Identity Information

Corporate and Operational Policy (formerly Operational Policy) is the authority for releasing suppressed Canadian or US/UK/AUS/NZ identities.

Warning: Anyone outside Corporate and Operational Policy who releases suppressed identity information is committing a privacy violation.

4.7 Sharing Beyond 5-Eyes

Corporate and Operational Policy must approve any sharing of information to countries beyond the 5-Eyes.

5. Retention and Disposition Schedules

5.1 General Principles

Those authorized to conduct or support cyber defence operations must apply retention and disposition schedules to all data, regardless of media or location (e.g., hard copy, personal or group accounts, or electronic repositories).

Control of the data will determine schedules as follows:

Data Type	Length of Retention	Condition
Data that has not been used or retained	[redacted]	Must be deleted according to the CDO MA in force
Metadata	Up to [redacted]	Must be deleted when no longer relevant
Data or metadata that has been used or retained	As per CSEC retention and disposition schedules	Stored in an approved CSEC repository

Attention: The above schedules for data under client control do not apply in the event the arrangement is

- suspended, or
- terminated ahead of its expiry date, or
- the MA expires and a new MA is not approved.

See paragraph 5.2 for instructions.

5.2 Data Disposition Schedule in the Event of Suspension or Termination of the Client Arrangement

In the event that the client terminates a cyber defence operation, upon notification of the termination, those authorized to conduct or support cyber defence operations must immediately cease

- copying data
- intercepting data
- selecting data, and
- analyzing selected data, except for that which is already under CSEC control.

This table sets out the disposition schedule for these events.

If the data has been...	Then the deletion period will be...
copied, selected, or intercepted only	up to [redacted] from notification of suspension (where termination is planned) or termination of the arrangement, or [redacted] from date copied, whichever comes first
used or retained	in accordance with CSEC retention and disposition schedules

5.3 Technical Client Information

CSEC may retain technical client information (see definition in Chapter 8) in accordance with the client arrangement.

6. Roles and Responsibilities for Cyber Defence Operations

6.1 Roles and Responsibilities

This table describes the key roles and responsibilities with respect to the cyber defence operations.

Who	What
Chief, CSEC (CCSEC)	• Notifying the Minister that CSEC has received a letter of request for cyber defence assistance (only if CSEC plans to conduct cyber defence operations where tools or services risk intercepting private communications) • Providing the Minister with the documentation listed in paragraph 2.5
Deputy Chief, IT Security (DC ITS)	• Signing client arrangements on behalf of CSEC • Authorizing the start of cyber defence operations
Directorate of Legal Services (DLS)	• Providing legal advice, including legal briefings, as required
Director General, Cyber Defence (DG, Cyber Defence)	• Authorizing personnel to conduct or support cyber defence operations • Informing the Director, PMO of those authorized to conduct or support cyber defence operations • Approving access within CSEC to data (for other than those authorized to conduct or support cyber defence operations)
Director, Program Management and Oversight (PMO)	• Confirming to the DC, ITS that all prerequisites noted in paragraph 2.1 have been fulfilled and operations can commence • Providing reports on the number of private communications used and retained, as required in paragraph 2.5 • Coordinating the resolution of policy and legal issues on behalf of the Cyber Defence Branch • Acting as the accountability authority for the list of personnel authorized to conduct or support cyber defence operations
Director, Cyber Threat Evaluation Centre (CTEC)	• Informing IPOC of receipt of client letter of request, as noted in paragraph 2.1

Continued on next page

Who	What
Director, Strategic Policy	• Preparing MA request package • Informing the Chief, CSEC of receipt of a letter of request from a federal institution • Confirming that the Minister has received notification as per paragraph 2.1 • Fulfilling Ministerial reporting requirements
Director, Disclosure, Policy and Review (formerly Corporate and Operational Policy)	• Providing operational policy advice and guidance
Manager, Corporate and Operational Policy	• Managing the review and approval of requests to share information with countries beyond the 5-Eyes (see OPS-2-1, Operational Procedures for Sanitizations and Actions-On) • Managing the review and approval of release of suppressed identities
Managers in the Cyber Defence Branch	• Ensuring those authorized to conduct or support cyber defence operations comply with the MA, client arrangements, and all relevant policy instruments • Ensuring that all required records are contained in the cyber defence activities corporate record
Operational Supervisors in the Cyber Defence Branch	• Providing technical direction and guidance to personnel authorized to conduct or support cyber defence operations • Ensuring destruction of all data in accordance with the MA, the client arrangements, and Chapter 5 of these procedures
Those authorized to support cyber defence operations	• Complying with the MA, client arrangements, and all relevant policy instruments and documentation
IPOC	• Maintaining a list of personnel authorized to conduct or support cyber defence operations, and validating it annually • Informing Strategic Policy that CSEC has received a letter of request • Providing policy advice to operations, and consulting Director General, Policy and Communications (DGPC), Corporate and Operational Policy and DLS as necessary

7. Accountability for OPS-1-14

7.1 Accountability

This table outlines accountabilities for revising, reviewing, recommending and approving this document.

Who	What
DG ITC	Approves
DGPC	Recommends
General Counsel, DLS	• Reviews for legal compliance • Provides legal advice
Director, Disclosure, Policy and Review	Reviews for consistency with the policy framework
Corporate and Operational Policy	Revises, in consultation with IPOC

7.2 References

- National Defence Act, part V.1
- Privacy Act
- the most recent Ministerial Directive on the Privacy of Canadians
- the most recent Ministerial Directive on CSE*'s Accountability* Framework
- Cyber Defence Operations MA in force
- OPS-1, Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities
- OPS-1-6, Operational Procedures for Naming and Releasing Identities in Cyber Defence Reports
- OPS-1-7, Operational Procedures for Naming in SIGINT Reports
- OPS-2-1, Operational Procedures for Sanitizations and Actions-On
- ITSOI-1-1, Data Handling in Cyber Defence Activities
- ITSOI-1-2, Report Management in Cyber Defence Activities
- ITSOI-1-3, Accessing and Sharing Cyber Defence Data
- ITSOI-1-4, Data Querying and Signatures in Cyber Defence Operations

7.3 Amendment Process	Situations may arise where amendments to these procedures are required because of changing or unforeseen circumstances. Such amendments will be communicated to relevant personnel, and will be posted on the Corporate and Operational Policy website.
7.4 Enquiries	Questions related to these procedures are to be addressed to operational managers, who in turn will contact IPOC. IPOC will consult Corporate and Operational Policy, as required.

8. Definitions

8.1 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)

"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.

8.2 Canadian Identity Information (CII)

CII refers to information that may be used to identify a Canadian person, organization, or corporation in the context of personal or business information. CII includes, but is not limited to, names, phone numbers, email addresses, IP addresses, and passport numbers.

Note: GC institutions do not fall within the definition of CII, thus federal institution names or IP addresses (that cannot be linked to an individual) do not require suppression.

8.3 Client

For cyber defence operations conducted under an MA, a client must:

- be a federal institution, in accordance with subsection 273.65(9) of the NDA, and
- control the computers and/or networks on which cyber defence operations will be conducted.

8.4 Cyber Defence Reports	Reports may include, but are not limited to: • mitigation advice • information requests • detection information (including signatures) • advisories • profiling • cataloguing of malicious code. Report formats may vary, e.g., formalized reporting, and data sharing by email.
8.5 Data	For the purpose of these procedures, data is defined as [redacted] obtained from the computer systems or networks of importance to the GC (this includes content and associated metadata). Raw data refers to data that has not been determined to be relevant or essential.
8.6 Derivative Information	Any information produced or discovered as a result of an analytic process. While analysis may involve data, derivative information contains no data.
8.7 Information	Information in cyber defence operations includes data and metadata.
8.8 Information about Canadians	Information about Canadians refers to: • any personal information about a Canadian, or • business information about a Canadian corporation.
8.9 Integree	An integree is a person seconded to CSEC from one of CSEC's cryptologic partner organizations.
8.10 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.

Continued on next page

8.10 Metadata (continued)	For the purposes of cyber defence operations, "metadata" has been separated from associated data before being made available to a human analyst (detached metadata).
8.11 Ministerial Authorization	A Ministerial Authorization (MA) is an authorization provided in writing by the Minister of National Defence (Minister) to CSEC to ensure that CSEC is not in contravention of the law if, in the process of conducting its foreign intelligence (SIGINT) or IT Security operations, it should intercept private communications. MAs may be issued in relation to an activity or class of activities specified in the authorization pursuant to • subsection 273.65(1) of the NDA for the sole purpose of obtaining foreign intelligence, or • subsection 273.65(3) of the NDA for the sole purpose of protecting the computer systems or networks of the GC. When such an authorization is in force, Part VI of the Criminal Code does not apply in relation to an interception of a private communication, or in relation to a communication so intercepted.
8.12 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.
8.13 Private Communication	A private communication is "any oral communication, or any telecommunication, that is made by an originator who is in Canada or is intended by an originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it, and includes any radio-based telephone communication that is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it". (Criminal Code, section 183)

8.14 Recognized Private Communication	A "recognized private communication" includes a recognized private communication in whole or in part, or metadata associated with a recognized private communication that can identify one or both communicants or the communication itself.
8.15 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).
8.16 Secondee	A secondee is an individual who is temporarily moved from another GC or private organization to CSEC, and who at the end of the assignment returns to the originating organization.
8.17 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] numbers, email addresses, phone numbers and IP addresses, [redacted]
8.18 [redacted]	[redacted]