

SECRET//SI



Communications
Security Establishment

Centre de la sécurité
des télécommunications



OPS-1 Awareness

Privacy and Lawfulness at CSE

CERRID 13185920

Canada¹



Objectives

By the end of this presentation you should understand:

- CSE's authorities and policy framework
- Ministerial Directives and Authorizations
- Key elements of OPS-1
- Select procedures in OPS-1 series
- How to apply elements of OPS-1 to your work



The *National Defence Act*

The *National Defence Act* mandates CSE to:

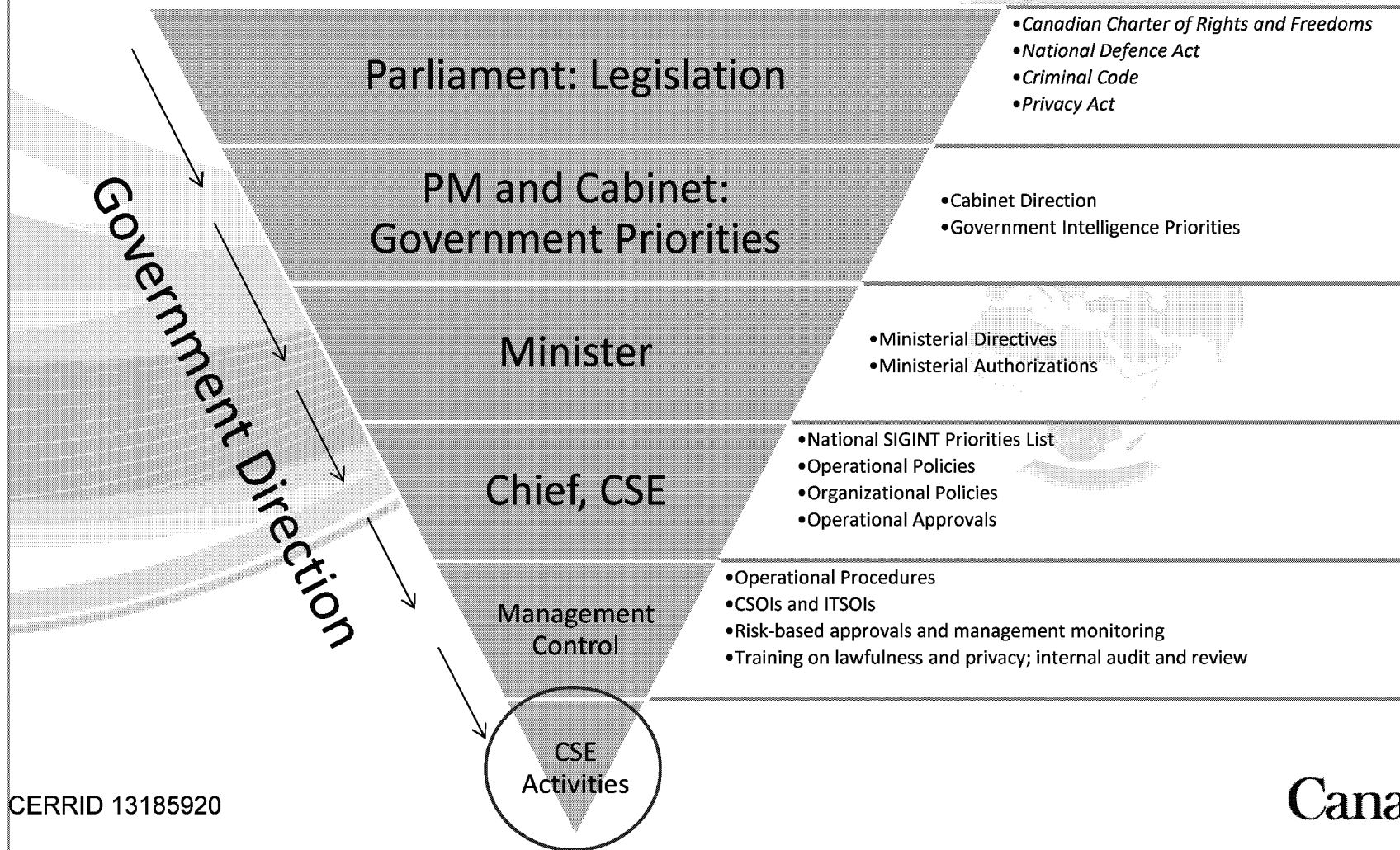
- a. Acquire and use information from the Global Information Infrastructure for the purpose of providing foreign intelligence, in accordance with GC intelligence priorities (*Foreign Intelligence, Part A*);
- b. Provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the GC (*Cyber protection, Part B*); and
- c. Provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties (*Assistance, Part C*)

CERRID 13185920

Canada³



CSE's Authorities and Direction



CERRID 13185920

Canada

4

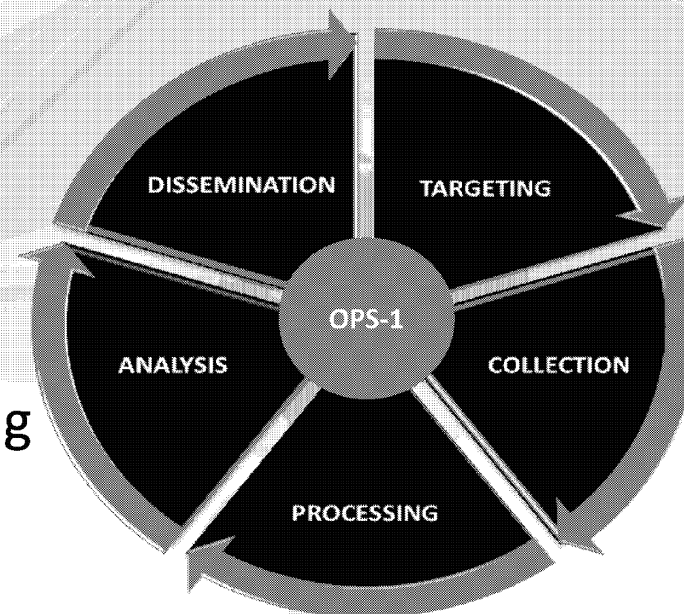


CSE Information Cycle and Policy Framework

CSE's operational policies translate legal requirements and government direction into policies that direct CSE's activities.

CSE's policies are organized according to the CSE information cycle.

There are privacy measures in place at each stage of the information cycle.



CERRID 13185920

Canada⁵



Value of OPS-1

OPS-1: Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities

- Is CSE's cornerstone policy and provides high-level guidance for CSE's mandated activities
- Presents the principles and rules CSE must follow to be legally compliant with the *National Defence Act*
- Interprets government direction which includes Ministerial directives and Ministerial authorizations
- Describes measures to protect the Privacy of Canadians

CERRID 13185920

Canada

6



Key Terms

Canadian

Private
Communication

Information
about a
Canadian

Canadian
Identity
Information (CII)

Solicitor-Client
Communication

CERRID 13185920

Canada⁷



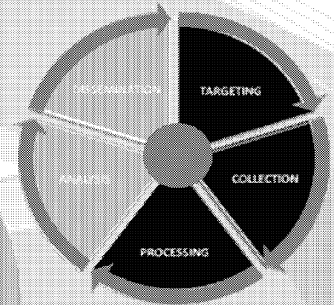
Targeting and Data Queries

Targeting : part (a) and part (c)

Data Query: part (b)

What's the difference?

What are the rules?



CERRID 13185920

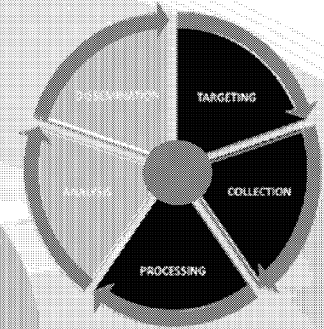


Collection and Processing

What information can I retain?

How do I track information requiring protection?

- Privacy Annotations
- Accountability Markings





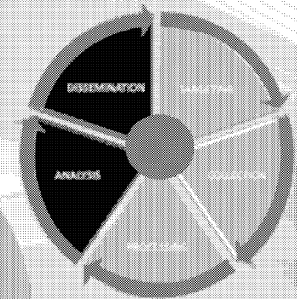
Collection and Processing

Privacy Annotation Hierarchy

**Private communication /
Solicitor-Client
communication**

**Communication of a
Canadian located outside
Canada**

**Traffic containing information about
Canadians**



CERRID 13185920

10

Canada



Targeting and Data Query Examples

Examples

Part (a) activity:

[REDACTED]

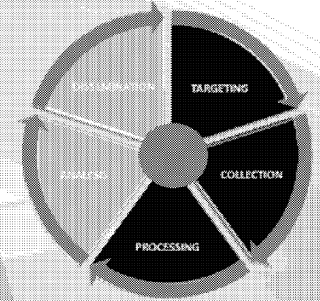
Part (a) activity:

[REDACTED]

Part (b) activity:

[REDACTED]

IRRELEVANT





Analysis

As an analyst, what can I report on?

What types of information must be suppressed in reports?

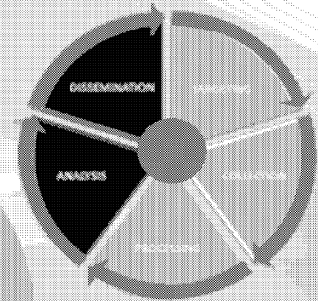


Analysis: Reporting

Examples:

Part (a) activity: You are [REDACTED] stealing from a convenience store in Ottawa. This information was obtained through a legitimate foreign selector. Can you report on this?

Part (b) activity: You are writing a cyber defence report which focuses on a Canadian domain name that has been assessed as belonging to a foreign national. You would like to include this information in your report, unsuppressed.



IRRELEVANT

13

CERRID 13185920

Canada

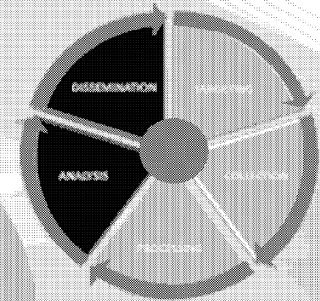


Dissemination

Releasing Reports with a Privacy Interest

- Management must sign off as the release authority for SIGINT (part a) and ITS (part b) reports based on:
 - A private communication,
 - A communication of a Canadian outside Canada, or
 - Communications containing information about Canadians or persons in Canada

• IRRELEVANT





MISTAKES HAPPEN!

Privacy Incidents

Privacy Incidents File (PIF)

- DG PC is the Privacy Officer for CSE
- DG PC tracks privacy incidents and ensures CSE demonstrates a commitment to protecting privacy, ensuring transparency and improving internal practices

Reporting an Incident

- Contact your supervisor



THE END

Please refer to the appropriate policies for in depth guidance regarding operational activities and for reporting release authorities.

CERRID 13185920

16
Canada