



OPS-1-10

Operational Procedures for Metadata Analysis

OPERATIONAL POLICY

Canada

Table of Contents

1. Introduction.....	3
1.1 Objective.....	3
1.2 Authority.....	3
1.3 Context.....	4
1.4 Policy Statement	4
1.5 Application.....	5
2. Metadata Analysis [REDACTED].....	6
2.1 Sources for [REDACTED].....	6
2.2 Unknown Nationality [REDACTED].....	6
2.3 Process Summary.....	6
2.4 FI Test.....	7
2.5 Completing the Intelligence Branch Approval Form.....	8
2.6 Scope for Approval.....	8
2.7 Approval Process	9
2.8 Limitations on Activities.....	10
2.9 Use of Results	10
2.10 Reporting.....	11
2.11 Dissemination	12
2.12 Tracking and Retention Requirements.....	12
3. Metadata Analysis [REDACTED].....	13
3.1 [REDACTED].....	13
3.2 Sources for [REDACTED].....	13
3.3 Approval Process for [REDACTED].....	13
3.4 Analysis Conducted from [REDACTED] Metadata Repositories	14
3.5 Reporting.....	14
3.6 Dissemination	14
3.7 Tracking and Retention Requirements.....	14
4. Roles and Responsibilities	15
4.1 Roles and Responsibilities	15
5. Additional Information	18
5.1 Responsibility for these Procedures.....	18
5.2 References.....	18
5.3 Amendments	19
5.4 Review	19
5.5 Enquiries	19
6. Definitions.....	20

6.1 Canadian	20
6.2 Canadian Identity Information (CII).....	20
6.3 Contact Chaining	20
6.4 Foreign Intelligence (FI).....	21
6.5 [REDACTED]	21
6.6 [REDACTED]	21
6.7 Metadata.....	21
6.8 Metadata Analysis.....	21
6.9 Second Parties.....	21
ANNEX 1: Flowchart for Metadata Analysis [REDACTED]	23
ANNEX 2: Approval Form to Conduct Metadata Analysis [REDACTED]	23
ANNEX 3: Approval Form to Conduct Metadata Analysis [REDACTED]	25

1. Introduction

1.1 Objective

These procedures provide direction on the process CSE and CFIOG analysts must follow when conducting metadata analysis, pursuant to paragraph 273.64(1)(a) of the *National Defence Act* (NDA) (known as “Mandate A”) in pursuit of Foreign Intelligence (FI), [REDACTED]

For the purpose of these procedures, [REDACTED]
[REDACTED]
[REDACTED]

This includes, but is not limited to
[REDACTED]

IRRELEVANT

1.2 Authority

For the purpose of these procedures, CSE metadata analysis is conducted under the authority of:

- a) the *National Defence Act*, paragraph 273.64(1)(a), and
 - b) the *Ministerial Directive on the Collection and Use of Metadata*, March 2005.
-

1.3 Context

One of the key reasons for conducting metadata analysis, which includes various types of SIGINT development activities such as contact chaining [REDACTED] is FI target discovery. Metadata analysis is used to generate foreign leads and drive the pursuit of foreign targets.

In most cases, metadata analysis is [REDACTED]. However, in some instances where other SIGINT development avenues have already been considered, [REDACTED] metadata analysis [REDACTED] (including those encountered during the analysis of [REDACTED]), may be the only available option for conducting target discovery activities where there are reasonable grounds to believe that this activity may provide FI.

Because privacy measures must be applied to metadata [REDACTED]

[REDACTED]

[REDACTED]

1.4 Policy Statement

Metadata analysis conducted under CSE's Mandate A, [REDACTED] must:

- comply with relevant laws of Canada, including the *Charter of Rights and Freedoms*, the *Privacy Act*, the *Criminal Code* and the NDA;
- comply with all relevant Ministerial Directives, including:
 - the *Ministerial Directive on the Privacy of Canadians*,
 - the *Ministerial Directive on the Collection and Use of Metadata*, and
 - the *Ministerial Directive on CSE's Accountability Framework*;
- be conducted only in accordance with these procedures;
- never be conducted for the purpose of obtaining, producing or disseminating intelligence about a Canadian located anywhere or any person located in Canada;
- be subject to measures to protect the privacy of Canadians;
- be aimed at providing FI to the Government of Canada (GC) linked to GC FI priorities through application of the FI test defined in paragraph 2.4; and
- be carried out only with the knowledge and express approval of CSE management.

1.5 Application These procedures apply to CSE and CFIOG staff as well as any other parties involved in metadata analysis activities conducted under the authorities listed in paragraph 1.2, including secondees, integrees and contractors.

2. Metadata Analysis [REDACTED]

2.1 Sources for [REDACTED]

A [REDACTED] in metadata analysis may be provided to CSE by means of

- Departments or agencies of the GC (see paragraph 2.8), or
 - CSE IT Security activities, or
 - CSE/CFIOG SIGINT activities including metadata analysis (e.g. contact chaining [REDACTED] is encountered), or
 - Allied agencies.
-

2.2 Unknown Nationality [REDACTED]

In cases where the nationality or location of the person [REDACTED] is difficult or not possible to determine [REDACTED], the [REDACTED] should be treated as relating to a foreigner located outside Canada unless there are indications that it relates to a Canadian located anywhere or any person in Canada.

Conversely, the user [REDACTED] should be treated as Canadian unless there is strong evidence that the person is not a Canadian located anywhere or is not a person located in Canada.

2.3 Process Summary

The following is a summary of the process for conducting metadata analysis from [REDACTED] metadata repositories [REDACTED] (these steps are illustrated in a flowchart at Annex 1 and are explained in detail in the following paragraphs):

1. Determine whether the proposed metadata analysis is within the requirements outlined in these procedures.
 2. Complete the Intelligence Branch Approval Form at Annex 2.
 3. Obtain the appropriate approvals.
-

Continued on next page

2.3 Process Summary
(continued)

4. Conduct metadata analysis activities.
5. Attach the results of the metadata analysis activities to the Approval Form, including, but not limited to the following:
 - a. [REDACTED]
 - b. [REDACTED]
 - c. [REDACTED]
 - d. [REDACTED]

2.4 FI Test

A SIGINT (CSE/CFIOG) analyst who becomes aware of a [REDACTED] that could be a candidate for [REDACTED] metadata analysis must first apply the "FI test".

The following questions must be addressed prior to initiating the approval process for metadata analysis [REDACTED] with the answers to these questions forming part of the rationale contained in the Intelligence Branch Approval Form at Annex 2.

Step	Considerations	If the answer is...	Then...
1	Are there reasonable grounds to believe that the analysis [REDACTED] will provide information or intelligence about the capabilities, intentions or activities of foreign actors?	YES	Analyst provides detailed rationale, using the Approval Form, as to why the [REDACTED] will likely lead to FI; go to step 2.
		NO	Do not proceed with metadata analysis.
2	Will the expected FI satisfy a priority of the National SIGINT Priorities List (NSPL), and correspond to a formal Government of Canada Requirement (GCR)?	YES	Include pertinent GCR number on Approval Form.
		NO	Do not proceed with metadata analysis.
3	Have other avenues of FI target development been considered?	YES	Submit completed Approval Form (see paragraph 2.7). Note: Details of FI target development considerations must be included in the Approval Form (under Analyst Intentions and Justifications, point 4).
		NO	Do not proceed with metadata analysis.

**2.5 Completing
the Intelligence
Branch
Approval Form**

Before seeking approval, the analyst must ensure that the form includes:

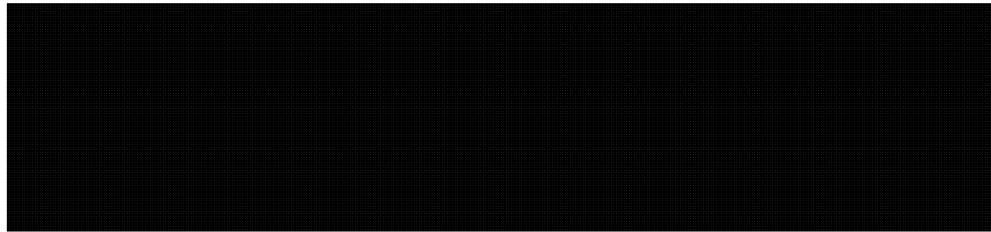
1. The GCR and NSPL priority the analysis is expected to satisfy;
2. The [REDACTED] metadata analysis is to be conducted [REDACTED] may be approved by a single authorization provided that [REDACTED] A separate justification is required [REDACTED]
3. The specific source of each [REDACTED] listed (i.e. GC information, SIGINT research, CSE IT Security, etc.); and
4. A detailed rationale outlining why the requester has reasonable grounds to believe that the activity will lead to FI.

**2.6 Scope for
Approval**

When granted, approval is valid for [REDACTED] days with no limitation on the number of activities that can be conducted during this period as long as the justification for doing so continues to be relevant for FI purposes.

Furthermore, the pool of metadata that can be searched is limited to that which has been collected up to and including the date of the written approval by Director General, Intelligence (DGI).

Once approval is received and provided it is within the approved time limit, an analyst can take reasonable steps to adjust the parameters of the activity (e.g. date range) to obtain satisfactory results.



2.7 Approval Process

Metadata analysis may be initiated [REDACTED] only after [REDACTED] has reviewed the request, and DGI has approved it.

In deciding whether a request should be approved, DGI must

- take into consideration all the relevant circumstances,
- be satisfied that the activity meets all the requirements of these procedures, and
- be satisfied that the activity may reasonably be expected to provide FI.

The approval process may be terminated at any stage by anyone in the chain, if they believe the answer to one of the considerations in paragraph 2.4 is “no”, or if they have other serious concerns. The Directorate of Legal Services (DLS) may be consulted for advice at any time in the process, as necessary.

Step	Who Does It	Activity
1	SIGINT (CSE/CFIOG) analyst	Submits the completed Intelligence Branch Approval Form to DGI Supervisor (CFIOG should submit these forms to [REDACTED])
2	DGI Supervisor	Reviews request and forwards to DGI Manager
3	DGI Manager	<ul style="list-style-type: none"> • Reviews request • Recommends to approve or deny, and • Forwards to DGI Director, only if approved
4	DGI Director*	<ul style="list-style-type: none"> • Reviews request • Recommends to approve or deny, and • Forwards to [REDACTED] only if approved
5	[REDACTED]	<ul style="list-style-type: none"> • Reviews request, • Recommends to approve or deny, • If recommendation is to approve, forwards request to DGI for final approval, and • If denied, [REDACTED] will initiate a discussion with DGI and then, if required, escalate for final decision
6	DGI *	Approves (or denies) request

* In the absence of Directors, [REDACTED] or DGI, anyone acting officially in this position, or a higher management level may act as approval authority. No downward delegation is permitted.

2.8 Limitations on Activities

The following limitations apply to metadata analysis activities [REDACTED]

1. [REDACTED]

2. If the metadata analysis [REDACTED]

If ...	Chains [REDACTED]	Then ...
[REDACTED]	[REDACTED]	Stop the chain
		Continue the chain
[REDACTED]	[REDACTED]	[REDACTED]

3. [REDACTED]

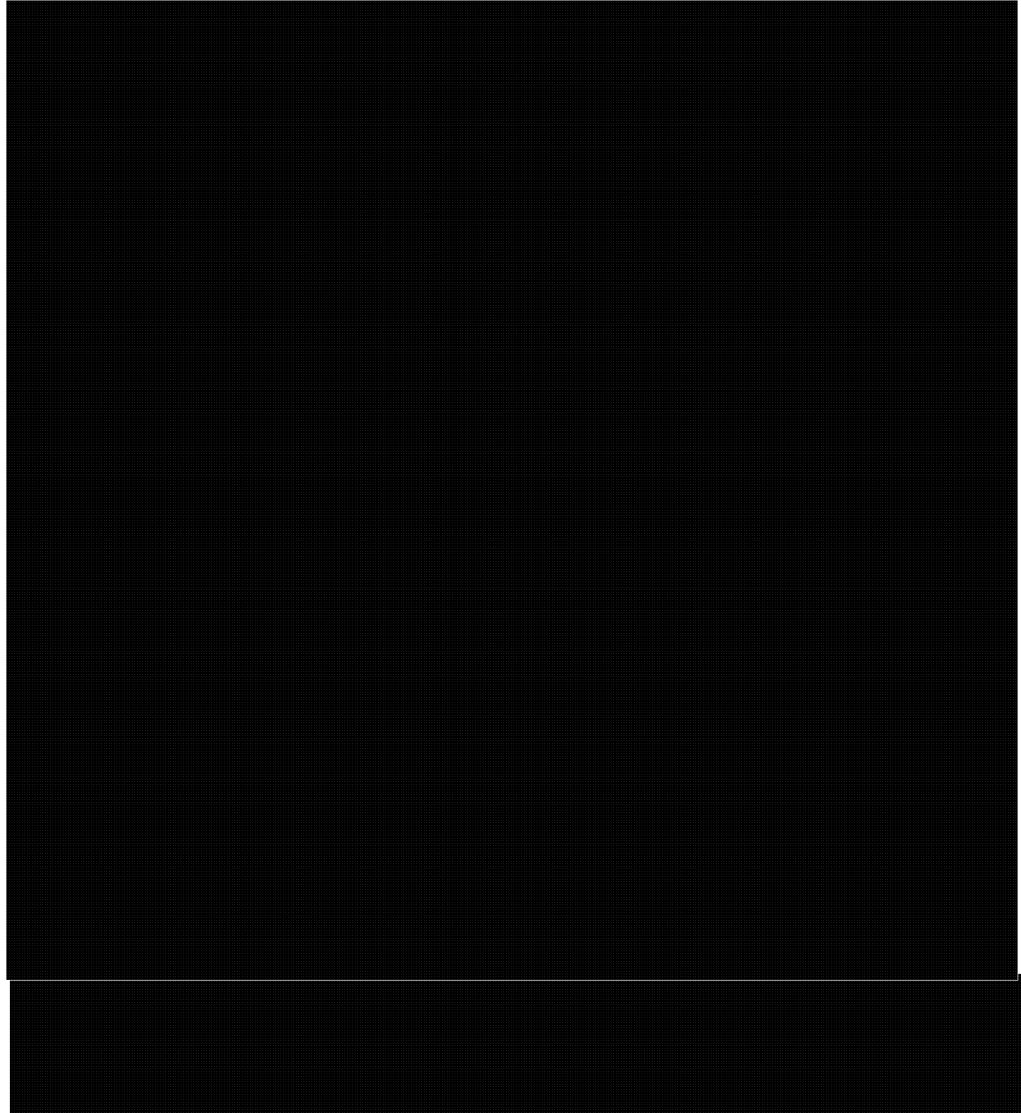
2.9 Use of Results

Results of metadata analysis activities must be attached to the Approval Form at Annex 2. (See paragraph 2.3)

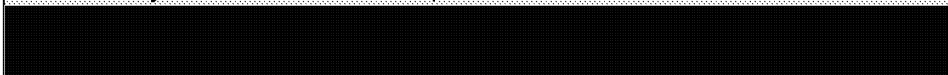
Visual charts and working aids prepared in the context of metadata analysis executed pursuant to these procedures may be kept for [REDACTED] following the sign off on the *Approval Form to Conduct Metadata Analysis* [REDACTED] unless the results of the analysis are used to produce a foreign intelligence report. In cases where the results are used in a foreign intelligence report, visual charts and working aids must be treated in accordance with OPS 1-11, *Retention Schedules for SIGINT Data*. In cases where the visual charts or working aids must be destroyed, the Approval Form at Annex 2 must be annotated accordingly.

[REDACTED] resulting from metadata analysis activities [REDACTED] in accordance with OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities*.

- 2.10 Reporting** The following limitations apply to the reporting of results from metadata analysis activities:



- DLS may be consulted as required



- CCSE (or person officially acting in that capacity) is the report release authority, and
- CSE/Operational Policy is notified of any such report issued.

Continued on next page

**2.10 Reporting
(continued)**

3. A client who has the lawful authority to [REDACTED] and produces an appropriate rationale, may request and receive that information at the discretion of Operational Policy. On a case by case basis, Operational Policy may consult with DLS or DGPC.
4. Visual charts and working aids prepared in the context of metadata analysis executed pursuant to these procedures are for CSE internal use only or for legal consultation with the Department of Justice and may not be further shared.
5. SIGINT reports based on metadata analysis must adhere to existing procedures including:
 - OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities*
 - OPS-1-1, *Release of Suppressed Information from SIGINT Reports*
 - OPS-1-7, *SIGINT Naming Procedures*
 - CSOI-4-1, *SIGINT Reporting*

**2.11
Dissemination**

SIGINT reporting derived from metadata analysis [REDACTED] may be disseminated to Canadian recipients and Second Parties (excluding reporting that includes [REDACTED] see paragraph 2.10) with the minimum classification of SECRET//COMINT, with distribution determined on a case-by-case basis.

**2.12 Tracking
and Retention
Requirements**

Intelligence Branch Approval Forms (and any related documentation where necessary, such as e-mails) must be retained centrally by the Manager of each section within DGI for tracking purposes. Because these forms contain [REDACTED] they must be securely stored with access limited to the relevant team (see OPS-1-11, *Retention Schedules for SIGINT data*).

3. Metadata Analysis [REDACTED]

3.1 [REDACTED]

3.2 [REDACTED]

[REDACTED]

[REDACTED]

3.3 Approval Process for [REDACTED]

A SIGINT (CSE/CFIOG) analyst [REDACTED] for metadata analysis must first apply the “FI test” outlined in paragraph 2.4. If all of the considerations are met, the analyst must complete the Intelligence Branch Approval Form at Annex 3.

The Approval Form is to be reviewed by a DGI Supervisor and forwarded to a DGI Manager for approval. [REDACTED]

[REDACTED]

**3.4 Analysis
Conducted from
Metadata
Repositories**

Metadata analysis [REDACTED] conducted from [REDACTED] **metadata repositories** requires the prior approval of a DGI Manager. No downward delegation for such approvals is permitted.

Metadata analysis [REDACTED] conducted from [REDACTED] **metadata repositories** must only be conducted in accordance with [REDACTED] policies. For example, [REDACTED]

[REDACTED]

3.5 Reporting

SIGINT reports based on metadata analysis [REDACTED] must respect the same limitations as those listed in paragraph 2.8 [REDACTED]

[REDACTED]

**3.6
Dissemination**

SIGINT reporting derived from metadata analysis [REDACTED] [REDACTED] may be disseminated to Canadian recipients and Second Parties with the minimum classification of SECRET//COMINT, with distribution determined on a case-by-case basis.

**3.7 Tracking
and Retention
Requirements**

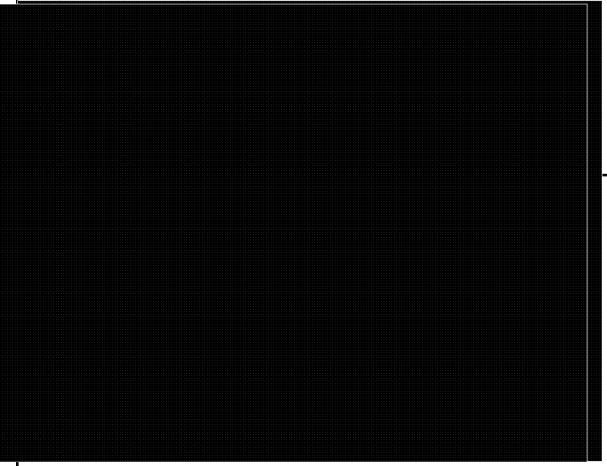

All forms must be retained and securely stored centrally by the Manager of each section within DGI, with access limited to the relevant team.

See OPS-1-11, *Retention Schedules for SIGINT Data*.

4. Roles and Responsibilities

4.1 Roles and Responsibilities

This table summarizes the key roles and responsibilities for conducting metadata analysis activities under Mandate A.

Who	Roles
CCSE	
DC SIGINT	
DGI	<ul style="list-style-type: none">• Consulting DLS as required Approving or denying requests for metadata analysis 

Effective Date: 25 June 2010

	<ul style="list-style-type: none"> • Reviewing requests for metadata analysis [REDACTED] and recommending approval or denial to DGI • If recommending approval, forwarding request to DGI for final approval, • If denying, initiating a discussion with DGI and then, if required, escalating for final decision • Seeking legal advice when required • For instances when metadata analysis [REDACTED] <p>[REDACTED]</p> <ul style="list-style-type: none"> • With [REDACTED] assessing the FI value [REDACTED] • Consulting DLS as required, and • [REDACTED]
Directorate of Legal Services*	Providing legal advice, when requested
DGI Directors	<ul style="list-style-type: none"> • Reviewing requests for metadata analysis [REDACTED] and recommending approval or denial to [REDACTED] • Seeking legal advice when required
DGI Managers	<ul style="list-style-type: none"> • Reviewing and approving or denying requests for metadata analysis [REDACTED] • Reviewing requests for metadata analysis [REDACTED] and recommending approval or denial to DGI Directors • Quarterly, reviewing Approval Forms for metadata analysis [REDACTED] to ensure continued FI relevance • Ensuring Approval Forms are retained centrally with limited access to the relevant team
DGI Supervisors	Reviewing requests for metadata analysis [REDACTED]
SIGINT (CSE/CFIOG) analysts	Completing the Approval Forms and seeking approval to use [REDACTED]

* CFIOG personnel will consult DLS by raising any issues in coordination with CSE DGI Directors through their managers. DGI Directors will assess whether DLS advice is required.

5. Additional Information

5.1 Responsibility for these Procedures

The following table outlines the responsibilities with respect to these procedures.

Who	Responsibilities
CCSE	Approving these procedures
DC SIGINT	Recommending these procedures
DGPC	Recommending these procedures
General Counsel, DLS	Reviewing these procedures to ensure they comply with the law
All CSE and CFIOG Managers involved in metadata analysis activities	Ensuring their staff have read, understood and comply with these procedures
Manager, Operational Policy	<ul style="list-style-type: none"> Revising these procedures when required Responding to questions concerning these procedures
CSE and CFIOG staff involved in metadata analysis activities	Reading, understanding and complying with these procedures

5.2 References

- *National Defence Act*
- *Ministerial Directive on the Privacy of Canadians*, June 2001
- *Ministerial Directive on the Collection and Use of Metadata*, March 2005.
- *Ministerial Directive on CSE's Accountability Framework*, June 2001
- OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities*
- OPS-1-1, *Release of Suppressed Information from SIGINT Reports*
- OPS-1-7, *SIGINT Naming Procedures*
- OPS-1-8, *Active Monitoring of Operations to Ensure Legal Compliance and the Protection of the Privacy of Canadians*
- OPS-1-11, *Retention Schedules for SIGINT Data*
- CSOI-4-1, *SIGINT Reporting*

-
- 5.3 Amendments** Situations may arise where amendments to these procedures may be required because of changing or unforeseen circumstances. The procedures in effect will be announced to staff and will be posted on the Operational Policy website.
-
- 5.4 Review** Metadata analysis activities are subject to management monitoring (see OPS-1-8, *Active Monitoring of Operations to Ensure Legal Compliance and the Protection of the Privacy of Canadians*), audit and review by various government review bodies, including, but not limited to, the CSE Commissioner and the Privacy Commissioner.
-
- 5.5 Enquiries** Questions related to these procedures should be directed to operational managers, who in turn will contact Operational Policy staff (e-mail [REDACTED] when necessary).
-

6. Definitions

6.1 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 (IRPA)*, 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; IRPA)

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.

6.2 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, e-mail addresses, and passport numbers.

6.3 Contact Chaining

Contact chaining means the method developed to enable the analysis, from information derived from metadata, of communications activities or patterns to build a profile of communications contacts of various foreign entities of interest in relation to the intelligence priorities of the Government of Canada, including the number of contacts to or from these entities, the frequency of these contacts, the number of times contacts were attempted or made, the time period over which these contacts were attempted or made as well as other activities aimed at mapping the communications of targeted foreign entities and their networks.

6.4 Foreign Intelligence (FI)

Foreign intelligence is information or intelligence about the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group, as they relate to international affairs, defence or security.

6.5**6.6****6.7 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.

Ministerial Directive on the Collection and Use of Metadata, March 2005

6.8 Metadata Analysis

Metadata analysis includes various types of SIGINT Development activities conducted against metadata, including contact chaining [REDACTED]

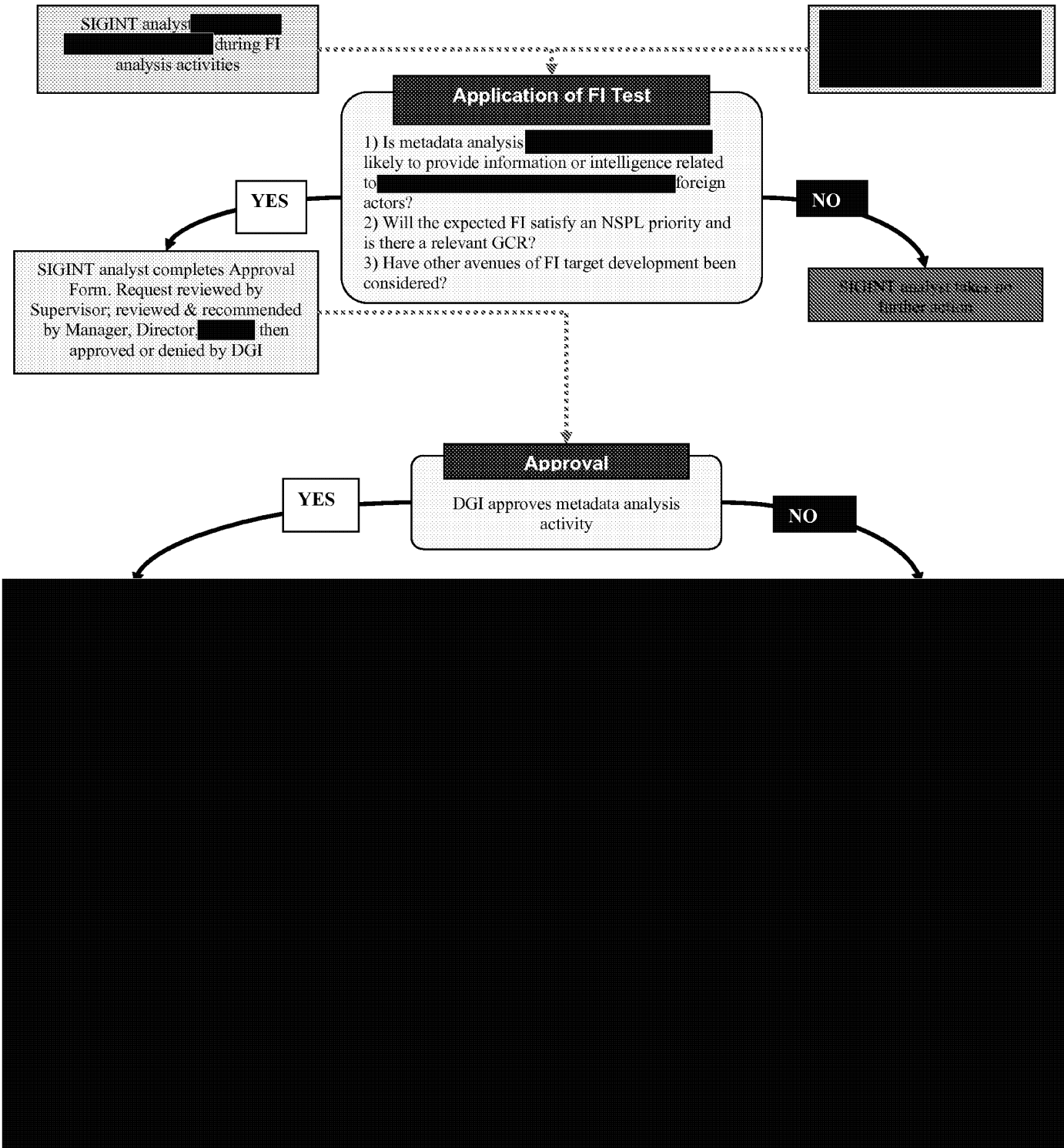
6.9 Second Parties

Second Parties refer to CSE's SIGINT counterparts and include: 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).

Effective Date: 25 June 2010

ANNEX 1: Flowchart for Metadata Analysis

This flowchart cannot supersede the test of these procedures. In case of inconsistencies between this chart and the body of these procedures, the latter shall prevail.





COMMUNICATIONS SECURITY ESTABLISHMENT
INTELLIGENCE BRANCH APPROVAL FORM

**ANNEX 2: Approval Form to Conduct Metadata
Analysis** [REDACTED]

[REDACTED]

1) Analyst intentions:

2) Expectation of foreign intelligence:

3) Foreign intelligence priority and objectives:

4) Foreign intelligence target development considerations (what other options have been considered?):

COMMUNICATIONS SECURITY ESTABLISHMENT
INTELLIGENCE BRANCH APPROVAL FORM



**ANNEX 3: Approval Form to Conduct Metadata
Analysis** [REDACTED]

[REDACTED]

- 1) Analyst intentions:
- 2) Expectation of foreign intelligence:
- 3) Foreign intelligence priority and objectives:
- 4) Foreign intelligence target development considerations (what other options have been considered) :