

Communications Security  
Establishment Commissioner

The Honourable Charles D. Gonthier, C.C., Q.C.



Commissaire du Centre de la  
sécurité des télécommunications

L'honorable Charles D. Gonthier, C.C., c.r.

**TOP SECRET/COMINT/CEO**  
**(with attachment)**

09 January 2008

The Honourable Peter G. MacKay, P.C., M.P.  
Minister of National Defence  
101 Colonel By Drive  
Ottawa, Ontario  
K1A 0K2

Dear Mr. MacKay:

The purpose of this letter is to advise you of the results of a review by my office of CSE's metadata activities carried out under a ministerial directive (MD) dated March 9, 2005. The review focused on those metadata activities undertaken by CSE in support of its foreign intelligence mandate articulated in Part V.1, paragraph 273.64(1)(a) of the *National Defence Act (NDA)*, and referred thereafter as mandate (a), for the period April 1, 2005 to March 31, 2006.

The objective of the review was to assess CSE's compliance with the ministerial directive and with the laws of Canada, including the *NDA*, and also the *Privacy Act*, which governs the collection, use and disclosure of personal information. My office also set out to assess whether these metadata activities conformed with CSE's operational policies, procedures and practices. The review was undertaken under my general authority articulated in paragraph 273.63(2)(a) of the *NDA*.

By way of background, metadata can be broadly characterized as *data about data*. In the context of the ministerial directive under review, however, metadata is limited to a fairly narrow group of data that can generally be described as the routing or the transport information that is unique to the transmission of a particular telecommunication. In this context, it never includes the content of a communication, in whole or in part, or any information that could reveal its purport.

P.O. Box/C.P. 1984, Station "B"/Succursale «B»  
Ottawa, Canada  
K1P 5R5  
(613) 992-3044 Fax: (613) 992-4096

NOT REVIEWED

A0000383\_1-00939

CSE acquires, analyzes, retains and uses metadata from a variety of collection sources, including its own and those of its quinquartite SIGINT (signals intelligence) partners, i.e., the National Security Agency (NSA) of the United States, Government Communications Headquarters (GCHQ) of the United Kingdom, Defence Signals Directorate (DSD) of Australia and Government Communications Security Bureau (GCSB) of New Zealand. It also shares metadata with these partners. [REDACTED]

[REDACTED] Further, and subsequent to discussions with CSE, my office recognized that certain metadata activities are not limited to what is authorized under the metadata MD but must be considered in the context of ministerial authorizations.

This was my office's first examination of CSE's collection and use of metadata as governed by ministerial directive. Due to the complexity and breadth of the activities it authorizes, this is a preliminary report. As is my practice, I provided officials at CSE an opportunity to review and comment on this report, prior to finalizing and forwarding it to you. There was much discussion between CSE and my office regarding specific issues, several of which I describe briefly below. I believe that some of these will require further examination.

#### Legal issues

My office questions whether CSE appropriately undertook certain activities as principal under its (a) mandate rather than as agent under its (c) mandate. The activities in question involve developing a "contact chain" [REDACTED] which was provided to CSE by a federal law enforcement or security agency, to assist in identifying foreign links in support of an authorized investigation. CSE undertakes this activity under its (a) mandate. At first glance, it would appear to me that the use of the (c) mandate would be more appropriate. Discussions of this matter between my office and CSE will be pursued outside the framework of this report because it affects other areas currently under review by my officials.

My office has been advised that CSE is re-examining its metadata activities, particularly contact chaining, as well as its policy entitled OPS-1-10, *Procedures for Metadata Analysis* [REDACTED] I support this review, and depending on its outcome, my office may conduct a more in-depth examination of these activities.

NOT REVIEWED

A0000383\_2-00940

Lastly, since my office has now observed that some of CSE's analytic work using metadata may subsequently involve access to content authorized under an MA, and thus result in the acquisition and recognition of private communications by persons conducting the metadata activities, I believe that CSE must re-examine and re-assess its current position and practice that require that only those private communications recognized by intelligence analysts be accounted for. I suggest that those persons involved in the metadata activity known as network analysis and prioritization, as defined in the MD and as it applies to CSE's [REDACTED] program (which is conducted prior to the involvement of intelligence analysts) should also be responsible for accounting for all private communications they observe and handle.

#### Policy issues

CSE policy and procedures need to be amended, finalized and possibly augmented in order to better guide and support metadata activities undertaken for each method of collection. In particular, CSE has indicated that it is reviewing its use of terminology to ensure consistency and to avoid confusion.

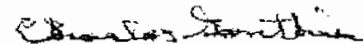
#### Corporate Records Management

I am of the opinion that CSE ought to be in a position to account for its metadata activities, up to and including any disclosures of Canadian identifiers made to clients and partners under the *Privacy Act*. Any future metadata reviews conducted by my office will pay particular attention to the documentation CSE is able to provide in order to facilitate an accurate assessment of its compliance with the authorities established in the *NDA*, the metadata MD, and related policies and procedures.

My report, attached, contains 15 findings and two recommendations dealing with the matters I have summarized for you in this letter.

I will continue to monitor the issues raised in the report. If you have any questions or comments, I will be pleased to discuss them with you at your convenience.

Yours sincerely,



Charles D. Gonthier

c.c. Mr. John Adams, Chief, CSE  
Ms. Margaret Bloodworth, National Security Advisor, PCO  
Mr. Robert Fonberg, Deputy Minister, National Defence

NOT REVIEWED

A0000383\_3-00941

**TOP SECRET/COMINT/CEO**

**OCSEC Review of the  
*Ministerial Directive, Communications Security Establishment,  
Collection and Use of Metadata, March 9, 2005***

**January 2008**

**NOT REVIEWED**

**A0000384\_1-00942**

---

## I. AUTHORITIES

This report was prepared on behalf of the Communications Security Establishment (CSE) Commissioner under his general authority articulated in Part V.1, paragraph 273.63(2)(a) of the *National Defence Act* (NDA).

## II. INTRODUCTION

On March 9, 2005, the Minister of National Defence signed a ministerial directive (MD)<sup>1</sup> to the Chief CSE describing how the Minister expects CSE to collect, use and destroy metadata<sup>2</sup> acquired in support of its foreign intelligence acquisition programs (mandate (a)), as well as for its computer systems and networks protection programs (mandate (b)) as they relate to malicious cyber activity. Included in the MD is a statement that activities undertaken pursuant to the MD are subject to review by the CSE Commissioner.<sup>3</sup> This is OCSEC's first such review. A copy of the MD can be found at Annex A.

CSE acquires, analyzes, retains and uses metadata from a variety of collection sources, including its own and those of its SIGINT partners.<sup>4</sup> It also shares metadata with its SIGINT partners. [REDACTED]

(see Annex B).

## III. OBJECTIVES

For this first metadata review, our objective was to identify and understand the nature of CSE's metadata activities and to assess their compliance with the ministerial directive and with the laws of Canada, including the *NDA*, and also the *Privacy Act*, which governs the collection, use and disclosure of personal information. We also set out to assess whether these activities conformed with CSE's own operational policies, procedures and practices.

## IV. SCOPE

In scoping out this review, OCSEC chose to focus on only those metadata activities undertaken by CSE in support of its foreign intelligence mandate (mandate (a)) and which did not require a ministerial authorization (MA), for the period April 1, 2005 to March 31, 2006. However, subsequent to discussions with CSE respecting the draft report's observations and findings, OCSEC recognized that certain metadata activities are

---

<sup>1</sup>Ministerial Directive [MD], *Communications Security Establishment, Collection and Use of Metadata*, dated March 9, 2005. See copy at Annex A.

<sup>2</sup>"Metadata" is defined below in Section IX – Background.

<sup>3</sup>Ministerial directive, paragraph 10.

<sup>4</sup>CSE's SIGINT partners are: the U.S. National Security Agency (NSA), the U.K. Government Communications Headquarters (GCHQ), the Australian Defence Signals Directorate (DSD), and the New Zealand Government Communications Security Bureau (GCSB).

not limited to what is authorized under the metadata MD and must also be considered in the context of MAs. Therefore, this was taken into consideration, as appropriate, in revising the report.

## V. LINES OF ENQUIRY

This review included the following lines of enquiry:

- (a) the legal authorities and guidance governing metadata activities;
- (b) how metadata activities are determined, scoped and planned;
- (c) how they are conducted and managed;
- (d) how acquired metadata is retained, used and shared; and
- (e) how acquired Canadian identities are retained, used, shared and protected.

## VI. CRITERIA

We assessed CSE compliance against the criteria (expectations) that CSE would:

- 1) conduct its metadata activities based on :
  - a) whether the activity was within its legislative mandate and complied with the ministerial directive;
  - b) legal analysis and guidance on, for example, specific metadata activities described in the MD, metadata collection methods and sources, metadata [REDACTED] versus collection and interception;
  - c) assessment(s) of whether the activity would produce metadata of foreign intelligence value; and
  - d) foreign intelligence priorities of the Government of Canada (specifically, those provided to CSE by its GoC clients);
- 2) have approved plans, a methodology and processes that guided its activities and were consistent with its legislative mandate and the ministerial directive;
- 3) have processes to identify, and measures to protect, metadata that identified Canadians;
- 4) have formal procedures that guided metadata activities, including the acquisition, retention, use and reporting of metadata, consistent with the *NDA* and the MD;
- 5) have the means to record, track, and account for disclosures of metadata that identified Canadians; and
- 6) have the means to determine if its metadata activities had been conducted as per its mandate, the ministerial directive and approved procedures.

NOT REVIEWED

A0000384\_3-00944

---

## VII. LIMITATIONS OF THE REVIEW

Soon after commencing our review, it became evident that most of CSE's collection methods or programs involved the [REDACTED] collection, retention and use of metadata. As a result, we limited the focus of this first metadata review to generally identifying CSE's mandate (a) metadata activities, understanding CSE's own legal framework for conducting these activities, determining when and if metadata could identify or be used to identify Canadians and persons in Canada, and observing, where possible, some metadata acquisition.

The majority of our observations and findings are based on our review of two principal metadata activities. The first is known as network analysis and prioritization. For this activity, we focussed our attention on CSE's [REDACTED] collection [REDACTED] program. We did not examine similar activities undertaken in two CSE collection programs known as [REDACTED]

The second principal metadata activity is known as contact chaining. This review is preliminary and OCSEC will determine at a later date whether an in-depth review of contact chaining is necessary as we have been advised by CSE that it is currently examining this activity.

## VIII. METHODOLOGY

A variety of documentation was examined, beginning with the 2005 ministerial directive, followed by policies and procedures, and then legal guidance issued to CSE by the Department of Justice (DoJ). We consulted CSE managers and personnel responsible for metadata activities, and received several briefings during the review. CSE provided both verbal and written answers to our questions.

We obtained a briefing and an on-site demonstration of network analysis and prioritization. While this activity area is common to every CSE collection method or program, the activities we observed fell within CSE's [REDACTED] collection program and were identified as [REDACTED] and signals intelligence development (SIGINT development). We also examined a selection of requests for contact chains [REDACTED] received by CSE from its Government of Canada (GoC) clients. We paid particular attention to those CSE policies and practices instituted to protect the privacy of Canadians in the acquisition, use and sharing of metadata.

---

## IX. BACKGROUND

### What is Metadata?

There are many different definitions in the public domain of what constitutes metadata. According to CSE, over [REDACTED] different types of data have been identified under the rubric of metadata. Basically, metadata is *data about data*. In the context of the ministerial directive under review, however, metadata is limited to a fairly narrow group of data that can generally be described as the routing or the transport information that is unique to the transmission of a particular telecommunication. In this context, it never includes the content of a communication, in whole or in part, or any information that could reveal its purport.<sup>5</sup>

In our briefings, CSE identified the following examples of metadata it collects:

- E-mail addresses
- IP addresses
- [REDACTED]
- Phone numbers
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

### What is a Metadata Activity?

The ministerial directive of March 9, 2005 identifies two distinct categories of activities: network analysis and prioritization, and contact chaining, which are defined below. The MD also sets out general guidelines for CSE's collection, use and destruction of metadata.

Network Analysis and Prioritization is best understood as research and development activities involving the analysis of telecommunications metadata that is acquired at the initial stages of any CSE foreign intelligence collection activity. According to the MD definition, it means:

The method developed to understand the global information infrastructure, from information derived from metadata, in order to identify and determine telecommunication links of interest to achieve the Government of Canada

---

<sup>5</sup> The ministerial directive of March 9, 2005 defines metadata 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."



foreign intelligence priorities. This method involves the acquisition of metadata, the identification of [REDACTED], the determination of the [REDACTED] the determination of the [REDACTED]

[REDACTED]

We learned that network analysis and prioritization is undertaken for each of CSE's [REDACTED] collection programs, which include [REDACTED]

[REDACTED] As noted above, we met with individuals responsible for operating [REDACTED] where metadata is analyzed, and were given an on-site, on-line demonstration. We were shown two separate [REDACTED] activities that relate to network analysis and prioritization: [REDACTED] and signals intelligence development (SIGINT development).

Contact Chaining involves the use and analysis of metadata, [REDACTED] to identify and document the communications activities or patterns of entities of potential foreign intelligence interest.

The MD defines contact chaining as:

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 foreign 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.

By *chaining* [REDACTED]

[REDACTED]

[REDACTED] will also benefit intelligence analysis efforts.

<sup>6</sup> OPS-1-10, *Procedures for Metadata Analysis* [REDACTED]

[REDACTED]

We learned that CSE may also [REDACTED] contact chain [REDACTED]

CSE's GoC clients, such as the Canadian Security Intelligence Service (CSIS) or the Royal Canadian Mounted Police (RCMP), may provide Canadian identifiers to CSE. These identifiers, such as a phone number or an e-mail address, are obtained by the GoC clients, most often, as part of an ongoing security or law enforcement investigation in Canada. CSE may [REDACTED]

Solicitor-Client Privilege

During the period April 1, 2005 to March 31, 2006, CSE received [REDACTED] requests from three of its GoC clients: CSIS, the RCMP and Foreign Affairs Canada. We were provided documentation for [REDACTED] of the [REDACTED]. For the most part, in the requests reviewed, the client provided the identifier to CSE and requested that it provide them with any information it may have or receive that relates to the identifier. Annex C contains more detailed information on this subject.

In order to comply with legal guidance provided by the DoJ,<sup>10</sup> [REDACTED]

Solicitor-Client Privilege

<sup>7</sup> See draft procedures known as OPS-1-10, *Procedures for Metadata Analysis* [REDACTED]

[REDACTED] June 2006.

<sup>8</sup> Legal opinion provided to the Chief of CSE by counsel, Justice Canada dated October 1, 2003 entitled

Solicitor-Client Privilege

<sup>9</sup> Documentation for the remaining [REDACTED] was not available.

<sup>10</sup> Legal opinion provided to the Chief of CSE by the Deputy Minister of Justice and Deputy Attorney

General of Canada dated June 6, 2005 [REDACTED]

Solicitor-Client Privilege

[REDACTED] and legal opinion provided to the

Chief of CSE by CSE's Legal Services Unit dated January 23, 2004 entitled [REDACTED]

Solicitor-Client Privilege

<sup>11</sup> Solicitor-Client Privilege

Solicitor-Client Privilege

<sup>12</sup> Evidence of the DoJ interpretation is also found in a statement made in his correspondence to the

Minister of National Defence in February 2004 when the former Chief, CSE indicated that [REDACTED]

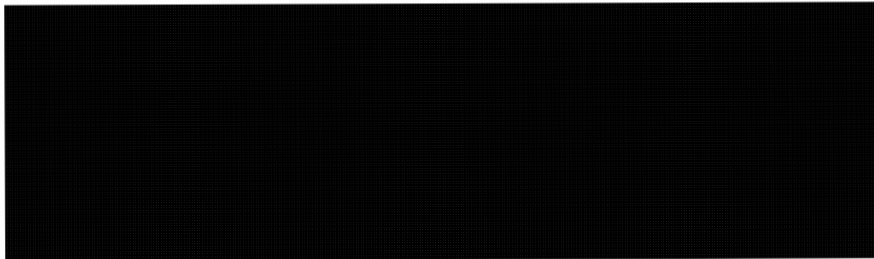
Solicitor-Client Privilege

Solicitor-Client Privilege

[REDACTED] (See page 6 of February 23, 2004 correspondence from CSE Chief to the Minister in his application seeking both an MA and an MD (metadata) in relation to the collection activity known as [REDACTED])

### How Metadata is Obtained

The accessing and processing of data, including metadata, is at the very root of CSE's signals intelligence (SIGINT) acquisition mandate. In order for us to understand metadata acquisition, the sequence of SIGINT acquisition was described to us during a meeting with CSE officials on February 26, 2007 using the following terminology: [REDACTED] acquire, collect, and intercept. These terms are not defined in the *National Defence Act*, the ministerial directive, or in CSE's operational policies and procedures. However, based on the information provided to us by CSE, we understand their meaning is as follows.

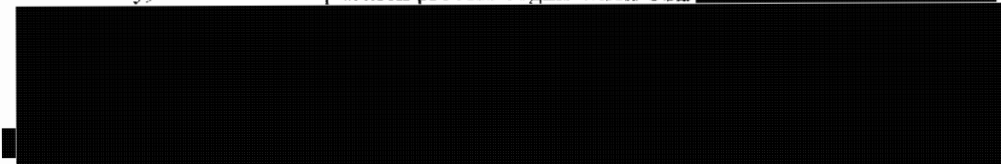


**Acquire/Collect:** *Used synonymously to indicate interception.*<sup>13</sup>

During our review, we learned that through its [REDACTED] of data as described above, CSE does in fact acquire both the metadata and the content of all accessible communications traffic. However, according to DoJ, [REDACTED] Solicitor-Client Privilege

Solicitor-Client Privilege

Essentially, the SIGINT acquisition process begins when CSE [REDACTED]



At the same time, selectors associated with specific targets of foreign intelligence interest are applied and, [REDACTED] the metadata and content of these selected communications are [REDACTED]

[REDACTED] This is referred to as metadata acquired from selected communications. It should be noted that this latter

<sup>13</sup>The MD does not distinguish between these various terms and, in his general and broad direction to CSE, the Minister has adopted the terms *acquired* and *acquisition*.

<sup>14</sup>Legal opinion relating to [REDACTED] Solicitor-Client Privilege

Solicitor-Client Privilege

targeting process, which includes the interception of communications content, is performed under ministerial authorization. See Annex D for more details.

We learned that CSE's points of access to telecommunications make available both a variety and a tremendous volume of data. However, according to CSE, it intentionally directs its efforts at those telecommunications links where there is an expectation that communications of foreign intelligence interest will be present in the data.<sup>15</sup> CSE's knowledge is based on information received from a variety of unclassified and classified sources, as well as on what it has learned from its own network analysis and prioritization efforts, as described above.

#### Access to Metadata

As described above, CSE [REDACTED] and collects metadata from its own foreign intelligence collection systems and programs.<sup>16</sup> It resides, and may be accessed, via various compartments within the [REDACTED] database. What is known as DNR (dialed number recognition) metadata is shared with its SIGINT partners in the U.S., the U.K., Australia and New Zealand. The [REDACTED] signed jointly in [REDACTED] (Annex B). CSE informs us that "the sharing of DNR metadata is subject to minimization (altering or disguising) of any Canadian identifiers as per the conditions of the MD on Collection and Use of Metadata".<sup>17</sup> DNR metadata generally refers to phone and fax communications.

The [REDACTED] recognizes that the acquisition and analysis of metadata is critical to the generation of valuable intelligence. [REDACTED] metadata repositories. Access is through a database known as [REDACTED]

In spite of the [REDACTED] however, CSE does not yet share its digital network intelligence (DNI) metadata for reasons of privacy and "due to the difficulty and complexity of developing an automated solution to minimize Canadian identifiers as per the conditions of the MD on Collection and Use of Metadata".<sup>18</sup> This privacy measure is discussed again later in the report.

<sup>15</sup> In the case of [REDACTED] this expectation is documented in *Activity Authorization Requests*, which serve as CSE's official tasking of communications [REDACTED] resources [REDACTED] These are referred to later on in the report.

<sup>16</sup> CSE also has access to some metadata obtained via its SIGINT partners.

<sup>17</sup> CSE comments on "OCSEC Draft Review Report of the Ministerial Directive on the Collection and Use of Metadata" at page 3, sent by e-mail to OCSEC Director of Operations from CSE on September 25, 2007.

<sup>18</sup> *Ibid.*

---

## X. FINDINGS

The findings documented below were derived from:

- documentation received from CSE, including PowerPoint presentations, legal opinions, and partial contact chaining records;
- briefings and discussions held with CSE personnel at various levels;
- the demonstration of [REDACTED] and SIGINT development activities undertaken by Canadian Forces personnel at Leitrim, one of CSE's [REDACTED] collection sites; and
- answers received from CSE to verbal and written questions.

To reiterate, the metadata activities identified in the MD and known as network analysis and prioritization, as it applies to [REDACTED] collection, and contact chaining, were the two areas of focus for this initial metadata review. The criteria used to assess the activities were that CSE would:

- 1) conduct its metadata activities based on :
  - a) whether the activity was within its legislative mandate and complied with the ministerial directive;
  - b) legal analysis and guidance on, for example, specific metadata activities described in the MD, metadata collection methods and sources, metadata [REDACTED] versus collection and interception;
  - c) assessment(s) of whether the activity would produce metadata of foreign intelligence value; and
  - d) foreign intelligence priorities of the Government of Canada (specifically, those provided to CSE by its GoC clients);
- 2) have approved plans, a methodology and processes that guided its activities and were consistent with its legislative mandate and the ministerial directive;
- 3) have processes to identify, and measures to protect, metadata that identified Canadians;
- 4) have formal procedures that guided metadata activities, including the acquisition, retention, use and reporting of metadata, consistent with the *NDA* and the MD;
- 5) have the means to record, track, and account for disclosures of metadata that identified Canadians; and
- 6) have the means to determine if its metadata activities had been conducted as per its mandate, the ministerial directive and approved procedures.

NOT REVIEWED

A0000384\_10-00951

---

Criterion 1 a):

*CSE conducted its metadata activities based on:*

*(a) whether the activity was within its legislative mandate and complied with the ministerial directive.*

The National Defence Act

Solicitor-Client Privilege

CSE derives its legislative authority to collect and use metadata for foreign intelligence purposes from its mandate found at paragraph 273.64(1)(a) of the *National Defence Act* (mandate (a)):

**273.64(1)** The mandate of the Communications Security Establishment is

- (a) to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence priorities;

Metadata is one type of information acquired from the global information infrastructure during the SIGINT collection process, as envisaged by this authority.

The Ministerial Directive

The MD defines metadata, guides its collection and use for network analysis and prioritization and contact chaining, and directs CSE, among other things, to share metadata with international allies.

In his direction to CSE, the Minister has also outlined four (4) steps CSE must take during the conduct of its metadata activities in order to protect the privacy of Canadians.<sup>20</sup>

**Step (1)** states that metadata known to be associated with Canadians anywhere or with persons in Canada must be altered in CSE reports to render impossible the identification of the persons to whom the metadata relates. (We noted that the phrase "CSE reports" was not further described in the MD.)

**Step (2)** states that CSE's Operational Policy division must be satisfied that certain criteria, "outlined in CSE Operational Procedures," are met before disclosing unaltered versions of metadata.

---

Solicitor-Client Privilege

<sup>20</sup>Ministerial directive, page 2, paragraph 7.

---

**Step (3)** places limits on access to unaltered metadata in CSE's repositories to only SIGINT operational staff and their supervisors, Operational Policy staff and system administration staff of CSE.

And finally, **Step (4)** places limits on access by CSE's allies to metadata of Canadians or persons in Canada only if it has been altered to render impossible the identification of the persons to whom the metadata relates.

For our review of CSE's compliance with steps (1) and (2), we asked CSE to provide us with any reports completed during the review period that related directly to contact chaining and which involved the use of [REDACTED]. We could anticipate that some of these reports would include metadata that had been minimized as described in step (1) above, and that the Operational Policy division might have received requests for disclosure of the unaltered versions (as per step (2)). We asked for an accounting of all requests made during our review period, including the number of requests, the type of metadata requested, and to whom it was released (see Annex C).

***Finding no. 1: MD Step (2)***

The Operational Policy division was unable to provide us with documentation that specifically tracked its disclosures of unaltered metadata in relation to CSE reporting based on contact chains.

**Details:**

From our reading of Step (2) as set out in the MD, we expected that CSE would have linked and tracked any disclosures of Canadian metadata identifiers back to the following:

- the original client request for a contact chain or information related to a [REDACTED] furnished by the client;
- the resulting contact chain; and,
- the resulting CSE report, if any, that contained derivative suppressed Canadian metadata identifiers and which led to the request for disclosure.

However, we found that this is not the case.

We were advised that while the Operational Policy division does process and track "ident" releases, which includes metadata releases, they do not "distinguish between 'metadata' (info used to identify, describe, manage or route a telecom) and other Canadian identifying information that happens to be a phone number or e-mail address for example".<sup>21</sup>

---

<sup>21</sup> Source: E-mail dated April 3, 2007, from Manager, Operational Policy (D2) to External Review and Policy Compliance (D3) staff and forwarded from External Review and Policy Compliance (D3) staff on

Further, we learned that when a client requests an e-mail address that has been suppressed in a given report, the Operational Policy division does not know and does not try to determine or track “whether the analyst got that e-mail address from the traffic ‘metadata’ or whether that e-mail address was part of the traffic ‘content’”.<sup>22</sup>

As a result, it is not possible to draw a line between a metadata activity such as contact chaining, a derivative report containing a suppressed Canadian (metadata) identifier and the disclosure of that metadata to a client.

**Observation no. 1:**

CSE should be able to draw a clear line between a foreign intelligence priority, a metadata activity such as contact chaining, a derivative report containing a suppressed Canadian (metadata) identifier and the disclosure of that metadata to a client. In addition, and in those instances where a disclosure is made, CSE should be able to provide all of the following information: the identity of the client department, the client’s authority and need to know the information, and the *Privacy Act* authority under which it was released.<sup>23</sup>

OCSEC may, as part of a future metadata review, assess the extent to which [REDACTED] contact chain have been suppressed in EPRs and/or subsequently released to a client, and examine any such cases for compliance with paragraph 7, Step (2) of the MD.

**Finding no. 2: MD Step (3): Limits on Access at CSE**

CSE provided us with verbal assurance that access to CSE’s bulk metadata repository, [REDACTED] has been limited to certain personnel. Our follow-up inquiries did not reveal any further information on how such access is monitored or controlled, or how CSE assures itself and the Minister that it has complied with this direction.

**Finding no. 3: MD Step (4): Limits on Sharing with Allies**

We examined sample documents provided by CSE that showed that DNR metadata related to Canadian-registered phone numbers had been sufficiently minimized to render impossible the identification of the Canadians or persons in Canada to whom they belonged.

---

April 3, 2007 to OCSEC Senior Analyst, with the subject: “FW: Classified Report: OCSEC Review: Metadata MD – Some last minute follow-up issues.”

<sup>22</sup> *Ibid.*

<sup>23</sup> Reference: OCSEC’s Phase 2 review of CSE support to the RCMP, sent to the Minister of National Defence on 16 June 2006 and entitled: *Report to the CSE Commissioner on CSE’s Support to Law Enforcement: Royal Canadian Mounted Police (RCMP), Phase II: CSE Mandate (a)*. See page 16 of the report, which begins a discussion of CSE’s handling of personal information under its (a) mandate.



Details:

As part of our review, CSE provided us with two one-page printouts of sample DNR and DNI metadata. For copies, see Annex E. These printouts represented metadata that had been acquired during a period of [REDACTED] during our review period. As already stated, metadata is acquired in huge volumes.

The DNR metadata, which related to Canadian-registered phone numbers, had been minimized to render impossible the identification of the Canadians or persons in Canada to whom they belonged. The DNI metadata had not been minimized, but CSE advised us that it did not share DNI metadata with its allies at this time because it did not yet have a system to automatically minimize it. We understand, however, that CSE is engaged in the development of such a system under the project name, [REDACTED]. For more details, please see Criterion 3, page 24.

Criterion 1 b)

*CSE conducted its metadata activities based on:*

*(b) legal analysis and guidance on, for example, specific metadata activities described in the MD, metadata collection methods and sources, metadata [REDACTED] versus collection and interception.*

Our findings fall under three headings: Legal Opinions, Network Analysis and Prioritization, and Contact Chaining.

Legal Opinions:

We reviewed three DoJ legal opinions that relate to the activities contemplated by the metadata MD:

- opinion dated October 1, 2003 entitled: Solicitor-Client Privilege  
Solicitor-Client Privilege
- opinion dated January 1, 2004 entitled: Solicitor-Client Privilege  
Solicitor-Client Privilege and
- opinion dated June 6, 2005 that dealt with Solicitor-Client Privilege  
Solicitor-Client Privilege

We noted that these opinions dealt with several issues, including the Solicitor-Client Privilege  
Solicitor-Client Privilege

Solicitor-Client Privilege The January 2004 opinion dealt specifically with Solicitor-Client Privilege

NOT REVIEWED

A0000384\_14-00955

Solicitor-Client Privilege

**Observation no. 2:**

So while metadata is indeed “data about data”, we understand that it can be put towards uses that have the potential to encroach on the privacy of the individual. For this reason, the application of the *Criminal Code*, the *Charter* and other laws of Canada that relate to actions by an agent of the government that impact on Canadians and persons in Canada, and information about those persons that may be intentionally or incidentally acquired by an agent of the government, must be carefully and repeatedly examined and re-assessed, particularly as technologies and the derivative uses of metadata change.

An in-depth examination by OCSEC of the legal positions put forward by these three DoJ opinions was beyond the scope of this review exercise. We did, however, compare some of the positions they established with some of the metadata activities undertaken by CSE.

Network Analysis and Prioritization:

We understand that, because of the very nature of the work, some of CSE’s network analysis and prioritization activities go undocumented. However, we were able to briefly examine these activities during a real-time [REDACTED] and SIGINT development demonstration we received at Leitrim in November 2006. The demonstration was instructive.

(a) [REDACTED] and SIGINT Development Activities at Leitrim:

We note that paragraph 5 on page 31 of the January 2004 opinion states that:

Solicitor-Client Privilege

<sup>24</sup> The January 2004 opinion uses the phrase Solicitor-Client Privilege

Further, the last paragraph on page 17, which continues on page 18, states:

Solicitor-Client Privilege

We were able to observe both the [REDACTED] and the SIGINT development activity during our visit to Leitrim. These activities are undertaken pursuant to both the Metadata ministerial directive and the [REDACTED] ministerial authorization, as it is possible that a private communication could be intercepted.

Based on the demonstrations we were given, the operator was able to [REDACTED]  
[REDACTED] In response to a question, the operator indicated that, as a matter of course, he would receive [REDACTED]  
[REDACTED]  
[REDACTED] CSE's operational procedures indicate that these activities may include [REDACTED] and the acquisition of private communications.

This raised questions, Solicitor-Client Privilege

Solicitor-Client Privilege

Solicitor-Client Privilege

NOT REVIEWED

A0000384\_16-00957

Solicitor-Client Privilege

**Recommendation no. 1:**

**CSE should re-examine and re-assess its current position and practice that requires that only those private communications recognized by intelligence analysts be accounted for.**

Details:

Based on the June 2005 DoJ opinion, that states that Solicitor-Client Privilege

Solicitor-Client Privilege

Solicitor-Client Privilege we believe that those persons involved in network analysis and prioritization should also be responsible for accounting for all private communications they recognize and handle, as this would be considered "analysis" of the intercepted communications. CSE has advised, consistent with the conditions in the ██████ MA, that only analysts responsible for producing end product reports are capable of determining whether a private communication has foreign intelligence value. Therefore, CSE maintains that only those analysts can assess whether private communications should be retained or destroyed (and for accounting for those communications). Furthermore, CSE indicated that the collection equipment complicates the assessment process as it only permits that a recognized private communication be annotated for either retention or deletion. However, OCSEC maintains that during ██████ and SIGINT development activities, an operator who observes a private communication should be required to record the fact that a private communication was observed, even though the operator may not be in a position to assess the foreign intelligence value of the private communication.

An in-depth examination of CSE's ██████ SIGINT development, and ██████ practices to ensure conformity to OPS-1-6 and other relevant policies was beyond the scope of this review exercise. OCSEC may conduct a detailed review of ██████ activities in future.

<sup>25</sup> Legal opinion relating to Solicitor-Client Privilege

Solicitor-Client Privilege

---

(b) Contact Chaining:

An in-depth examination of CSE's contact chaining activities was beyond the scope of this preliminary review.

Page 6 of the January 2004 DoJ opinion deals with Solicitor-Client Privilege  
Solicitor-Client Privilege

The October 2003 DoJ opinion, which deals with Solicitor-Client Privilege  
Solicitor-Client Privilege

***Finding no. 4:***

We understand that CSE is currently reviewing its contact chaining activities, including contact chaining [REDACTED] and that CSE is re-drafting OPS-1-10 "to ensure that there is clarity in how contact chaining is to be done".<sup>27</sup> OCSEC supports this review and will monitor developments.

Details:

Depending on the outcome of CSE's re-examination of its contact chaining activities, OCSEC may conduct a more detailed review of contact chaining [REDACTED] to answer, among others, the following questions:

- Could contact chaining [REDACTED] be considered Solicitor-Client Privilege?
- Is CSE's (a) mandate the appropriate authority to conduct contact chaining [REDACTED] obtained from a federal law enforcement or security agency in the context of a criminal or national security investigation of a Canadian in Canada?
- Could a [REDACTED] contact chain be included in an end product report (as [REDACTED] information), and potentially released to CSE's clients?

---

<sup>26</sup> *Metadata Operations Under the National Defence Act*, *supra* note 10 at page 6. Contact chaining is differentiated from another metadata activity known as [REDACTED] which involves use of what is referred to as [REDACTED] metadata, i.e., [REDACTED]. This activity was not part of this review.

<sup>27</sup> *Supra*, note 17 at page 5.

---

Criteria 1 c) and d):

*CSE conducted its metadata activities based on:*

- c) assessment(s) of whether the activity would produce metadata of foreign intelligence value; and*
- d) foreign intelligence priorities of the Government of Canada (specifically, those provided to CSE by its GoC clients).*

We learned from CSE that its network analysis and prioritization, and its contact chaining activities, were either conceived on the basis of, and/or focussed on, the foreign intelligence priorities established annually by a committee of Ministers. In direct support of these priorities, we understand that CSE continues to update its National SIGINT Priorities List (NSPL),<sup>28</sup> which is generated in-house and which guide CSE's foreign intelligence metadata activities. CSE advised that the NSPL is also endorsed by senior Government of Canada clients and stakeholders external to CSE.

***Finding no. 5:***

Based on the statements and written documentation provided by CSE, network analysis and prioritization activities as defined in the metadata MD, and as they apply to CSE's [REDACTED] program, appear to be supported by an assessment of available information and a formal statement of why their planned efforts can be expected to result in access to foreign intelligence of value to, and in support of, foreign intelligence priorities.

***Finding no. 6:***

Based on our discussions with CSE, our previous knowledge of [REDACTED] acquisition activities, and on the brief examination of the network analysis and prioritization activities as demonstrated by Canadian Forces personnel at Leitrim, CSE's activities respecting metadata acquired from unselected communications appear to be guided by and support the foreign intelligence priorities of the Government of Canada.

Details:

*Network Analysis and Prioritization*

As we noted on page 9 of this report, CSE routinely accesses both a variety and a tremendous volume of telecommunications data in support of its metadata objectives. During this initial stage, CSE is not specifically targeting foreign entities *per se* – an entity being as defined at section 273.61 of the *NDA*:

---

<sup>28</sup> The NSPL is described in detail in the classified report entitled: *Report to the CSE Commissioner on an External Review of CSE [REDACTED] Activities Conducted Under Ministerial Authorization*, dated 28 February 2005, which was provided to the Minister of National Defence on the same date.

A person, group, trust, partnership or fund or an unincorporated association or organization and includes a state or a political subdivision or agency of a state.

CSE is, in fact, [REDACTED] all telecommunications data [REDACTED]. In the case of [REDACTED] communications, CSE's focus is, for example, on certain [REDACTED] [REDACTED] but CSE maintains that its focus is not indiscriminate. It intentionally directs its efforts at those telecommunications links where there is an expectation that communications of foreign intelligence interest will be present in the data. We were advised that this knowledge is based on information received from a variety of unclassified and classified sources, as well as on what they have learned from their own network analysis and prioritization efforts.

During a previous review of CSE's [REDACTED] activities,<sup>29</sup> OCSEC was provided with copies of what are called *Activity Authorization Requests*. Once completed and approved, these requests authorize either network analysis and prioritization activities [REDACTED] and SIGINT development activities) at CSE's [REDACTED] site located at Leitrim, or sustained foreign intelligence collection. Each authorization gives supporting reasons for the belief that foreign intelligence may be acquired as a result of the contemplated and documented [REDACTED] activity.

On this occasion, for our metadata review, we did not ask CSE to provide copies of any such authorizations, since this area of activity would have been covered by other OCSEC reviews of CSE's [REDACTED] activities conducted under ministerial authorization.

We can confirm, however, that some of the assessment information in *Activity Authorization Requests* includes the [REDACTED]

*Contact Chains* [REDACTED]

***Finding no. 7:***

Before CSE [REDACTED] contact chain [REDACTED] it must have reasonable grounds to believe that the planned searches to be conducted [REDACTED] [REDACTED] will yield foreign intelligence. This belief must be established by analyzing information, most of which is presented to CSE by the client, about the [REDACTED] entity of interest. For further details, please refer to Annex C.

<sup>29</sup> See the classified report entitled *A Report to the CSE Commissioner on an External Review of CSE [REDACTED] Activities Conducted under Ministerial Authorization*, dated 28 February, 2005.

Based on our review of [REDACTED] CSE contact chain approval request forms,<sup>30</sup> we can confirm that CSE linked the [REDACTED] supplied by clients to CSE's Government of Canada intelligence requirements (GCRs), and/or the National SIGINT Priorities List (NSPL).

Criterion 2:

*CSE had approved plans, a methodology and processes that guided its activities and were consistent with its legislative mandate and the ministerial directive.*

Our discussions indicated that CSE undertakes network analysis and prioritization, and contact chaining, within the context of its operational priorities established at the beginning of each year. These priorities are driven by GoC intelligence priorities and by complementary requirements of clients and partners. We did not receive any documentation during this review, however, that indicates that CSE drafts specific annual objectives for these two metadata activities as part of a formal annual planning document. CSE indicated that this is the case because these activities "...constitute key ongoing elements that support individual collection and analytic efforts directed against a wide variety of targets and issues".<sup>31</sup> The targets and issues are linked to the GoC intelligence priorities.

*Network Analysis and Prioritization* [REDACTED]

***Finding no. 8:***

CSE has not drafted any formal documentation to instruct [REDACTED] and SIGINT development activities undertaken in response to *Activity Authorization Requests*. There are no written methodology or process materials to guide personnel in ensuring compliance with the authorities of the *NDA* and the metadata MD. However, OPS-1-6 provides general guidance with regard to [REDACTED] activities.

Details:

[REDACTED] and SIGINT development activities are undertaken in response to written *Activity Authorization Requests*, which are generated within certain activity areas in SIGINT and issued to Leitrim, in the case of [REDACTED] metadata collection.

To our knowledge, however, there is no formal written documentation available for CSE personnel (or their Leitrim counterparts), that supports these requests and which articulates [REDACTED] or SIGINT development methodologies or processes. We believe this type of information should be available to personnel, possibly as formal standard operating procedures, so that they can assure themselves that the activities they

<sup>30</sup> CSE conducted [REDACTED] such chains but was only able to provide evidence of [REDACTED]

<sup>31</sup> *Supra* note 17 at page 5.



undertake, and that undoubtedly vary from time to time, comply with the law, ministerial directives and policy.

*Contact Chaining*

***Finding no. 9:***

During the period under review, CSE followed a process for receiving, reviewing and approving contact chains [REDACTED]. The process was formally documented in June 2006, in the form of the draft OPS-1-10 procedures. A more detailed discussion of our findings regarding OPS-1-10 can be found in Annex C.

Details:

We were provided with documentation that related to [REDACTED] of the [REDACTED] client requests to [REDACTED] contact chains [REDACTED] supplied by the client. In every instance, the documentation consisted of a "Selector identification and tracking approval form." All but [REDACTED] of these [REDACTED] were accompanied by a CSE addendum that:

- assessed whether a chain [REDACTED] could be expected to produce foreign intelligence;
- identified the foreign intelligence priority and objectives; and
- identified what measures CSE would take to protect privacy.

Some of the tracking approval forms [REDACTED] included copies of the original client request. One included both the client request and the resulting CSE reporting.

From this documentation, we can confirm that these requests were subject to a process of internal review and managerial approval. Not all documentation, however, was provided or available for our review. Please see section XI regarding corporate records keeping at page 30 for further discussion on this matter.

This preliminary examination did raise one other fundamental issue that has been identified in previous reviews and that will require further study.<sup>32</sup> CSE undertook these [REDACTED] contact chains using their mandate (a) authority (i.e. paragraph 273.64(1)(a) of the *NDA*). In each instance, the [REDACTED] chain was provided to CSE by the client. In all but one instance, the [REDACTED] related to national security and criminal investigations being conducted by CSIS and the RCMP in Canada.

<sup>32</sup> See in particular OCSEC's Phase 2 review of CSE support to the RCMP, sent to the Minister of National Defence on 16 June 2006 and entitled: *Report to the CSE Commissioner on CSE's Support to Law Enforcement: Royal Canadian Mounted Police (RCMP), Phase II: CSE Mandate (a)*.

CSE explained to us that the [REDACTED] Further, they reiterated that while the [REDACTED] becomes part of CSE's information holdings, it is never used for targeting purposes. Our examination of the [REDACTED] requests for chaining confirmed this approach.

However, we continue to question whether CSE's authority to undertake contact chains at the request of a federal law enforcement or security client to identify foreign links in support of an ongoing investigation in Canada, should be authorized under paragraph 273.64(1)(a) or paragraph 273.64(1)(c) of the *NDA* (also known as mandate (c)).

In each of these instances, CSE is commencing an activity at the specific request of its client using information supplied by the client. These [REDACTED] have not been acquired incidentally by CSE as part of its own foreign intelligence collection activities. Rather, they identify and represent persons, both in Canada and under lawful investigation by Canadian authorities, for activities deemed to constitute either a threat to the security of Canada and/or a criminal offence(s) under Canadian law. For these reasons, mandate (c) may be the more appropriate authority that should be used for this activity under these conditions.

During discussions on the draft report in November 2007, CSE indicated that its (c) mandate could be insufficient authority to enable it to use an identifier provided by law enforcement and security agencies. CSE indicated that "the default position is always mandate (a)".<sup>33</sup> CSE expressed the opinion that since the resultant information meets the criteria for foreign intelligence and is provided as such to the agencies, there is no need to consider whether it is a mandate (c) activity. CSE added that mandate (c) may not apply as it requires the use of the authorities of the requesting agencies and the agencies do not have the appropriate mandate [to collect foreign intelligence themselves], as the agencies' warrants/authorizations may not apply extraterritorially.<sup>34</sup> OCSEC is not convinced that such limitations would exist in all contact chaining cases examined as part of this review where the identifiers provided to CSE by the agencies related to Canadians who were the subjects of the agencies' investigations. Discussion of this matter will be pursued with CSE outside the framework of this report because it affects other areas currently under review by OCSEC.

<sup>33</sup> CSE "Comments on OCSEC 2<sup>nd</sup> Draft Review Report of the Ministerial Directive on the Collection and Use of Metadata" at page 6, sent by e-mail to OCSEC Director of Operations from CSE on December 6, 2007.

<sup>34</sup> *Ibid.*

---

**Recommendation no. 2:**

**CSE should re-examine and reassess the legislative authority used to conduct its contact chaining activities [REDACTED] particularly those supplied by federal law enforcement and security agencies engaged in ongoing criminal and national security investigations.**

**Criterion 3:**

*CSE had processes to identify, and measures to protect, metadata that identified Canadians.*

**Finding no. 10:**

From our discussions with CSE staff and our examination of the documentation they provided, we are satisfied that CSE's method of minimizing DNR metadata generated by communications equipment registered in Canada is an adequate means of protecting the identities of Canadians and persons in Canada.

Further, we can report that we have received assurances that CSE does not share any DNI metadata at this time and will not do so until an adequate means of minimizing such metadata, which would otherwise identify Canadians or persons in Canada, can be implemented.

**Details:**

As described above, CSE is able to recognize DNR metadata that relates to, for example, phone and fax numbers [REDACTED] The assignment of [REDACTED]

[REDACTED] Such Canadian identifying information, however, is used as the starting point for both the implementation and assessment of privacy measures.

CSE shares DNR metadata with SIGINT allies [REDACTED]

[REDACTED]

<sup>35</sup> [REDACTED] along with CSE's own [REDACTED] database, is a key tool used by intelligence analysts involved in contact chaining.

**Observation no. 3:**

The minimizing of DNR metadata as described above will safeguard the privacy of Canadians and persons in Canada who use digital communications equipment registered in Canada. We would expect that this would apply to the vast majority of Canadians. It will not apply, however, to [REDACTED]

**Criterion 4:**

*CSE had formal procedures that guided metadata activities, including acquisition, retention, use and reporting of metadata consistent with the NDA and MD authorities.*

According to CSE, the MD is the principal document guiding CSE's acquisition and use of metadata. For our review period from April 2005 to March 2006, this was complemented by OPS-3-5, entitled [REDACTED] *Procedures*, dated 9 March 2005. These procedures were available for those persons cleared for and involved in [REDACTED] activities, including those described in the metadata MD.

Other formal written guidance for personnel involved in metadata activities was introduced incrementally during the months that followed. By August 2005, OPS-1, CSE's principal policy on protecting privacy and ensuring lawfulness, was re-issued with revisions that included a definition of metadata as well as definitions for the principal activities described in the March 2005 metadata MD. By December 2005, and to coincide with applications for new SIGINT ministerial authorizations, two more procedures provided metadata guidance:

- OPS-1-6, *Canadian [REDACTED] procedures*, 23 December 2005 (update); and,
- OPS-3-7, [REDACTED] *procedures*, 23 December 2005 (new).

Subsequent to the period of review, in June 2006, CSE released draft procedures, OPS-1-10, entitled: *Procedures for Metadata Analysis [REDACTED]*. It was included as part of the review since it represented the sole guidance for contact chaining activity.

As part of our review, we examined these policies and procedures in more detail to determine how they guided metadata activities.

NOT REVIEWED

A0000384\_25-00966

---

OPS-1: Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities, dated 31 August 2005

***Finding no 11:***

OPS-1 does not include definitions of or any references to network analysis and prioritization or contact chaining, CSE's two key metadata activities. Also, OPS-1 has no reference to the two operational procedures (noted above) that deal with metadata. In addition, we verified that the most current version of OPS-1, dated December 2006, does not include any reference to OPS-1-10.<sup>36</sup> Given that OPS-1-10 is still in draft, and that it is the only formal guidance available to CSE employees, the fulfilment of Criteria 4 remains weak. (For discussion of OPS-1-10, please see Annex C).

Details:

OPS-1 includes the definition of metadata (as it appears in the MD), outlines metadata in relation to CSE's (b) mandate and its use for the protection of GoC computer systems and networks, and refers to metadata again in relation to both its mandate (b) and its mandate (a) SIGINT reporting and release authorities.

In the section of OPS-1 titled *Retention and Dissemination*, metadata is dealt with briefly at para. 6.15, *Metadata Collected Under Mandate A*. The reader is referred to the metadata MD which, according to OPS-1, "outlines rules regarding collection, use and sharing of metadata collected by CSE."

In relation to metadata retention, paragraph 6.15 directs readers to OPS-1-11, entitled *Retention Schedules for SIGINT Traffic*, dated 11 March 2004. According to OPS-1-11, metadata collected by CSE and by its SIGINT partners may be retained for [REDACTED].<sup>37</sup> In written answers to questions received from CSE dated December 6, 2006, we were advised that currently, DNR is being "manually monitored, with manual deletions being applied" to meet the destruction requirement. CSE plans to implement an automated destruction process [REDACTED].

Other Operational Procedures

***Finding no. 12:***

The [REDACTED] operational procedures do not provide adequate guidance respecting [REDACTED] or target development metadata activities.

---

<sup>36</sup> This statement remains true even upon examining the current December 2006 version of OPS-1.

<sup>37</sup> OPS-1-11, para. 2.4 *Traffic Acquired under Section 273.64(1)(a) of the NDA*.

---

Details:

As outlined above, the subject of metadata has been incorporated into the following operational procedures:

- a) OPS-1-6, *Canadian [REDACTED] Procedures*
- b) OPS-3-5, [REDACTED] *Procedures*; and,
- c) OPS-3-7, [REDACTED] *Procedures*.

These three deal specifically with foreign intelligence collection methods and programs, but were pertinent to our review since metadata activities form part of these methods and programs.<sup>38</sup> From our examination, we noted that each procedure includes definitions and standard (but limited) guidance on metadata activities identified as collection, use and retention.

Metadata Collection

The guidance given for metadata *collection* is noteworthy for it is identical in each procedure and consists of one sentence:

*Metadata may be collected for all telecommunications, including private communications.*

No other guidance for this activity is present in these documents. Further, in the absence of any definition, we had to question what "collected" was to mean in this particular context. From our reading of the documents, we concluded that "collected" should be read in its broadest sense so as to complement the authorities and activities of the metadata MD.

Metadata Use

Each of the three OPS documents has a brief paragraph called *Using Metadata*. It is similarly worded in each procedure and is a reiteration of paragraph 8 of the metadata MD (see Annex A).

Network Analysis and Prioritization

The MD definition of Network Analysis and Prioritization is included in the [REDACTED]  
[REDACTED] OPS documents.

[REDACTED]

---

The [REDACTED] procedures<sup>39</sup> have no discussion or identification of what activities would fall within the definition of network analysis and prioritization.

The [REDACTED] procedures deal with activities that would likely fall within the definition, i.e. those referred to as [REDACTED] Operations and SIGINT Development.<sup>40</sup> These activities are not linked or cross-referenced to the definition, however.

**Observation no. 4:**

Policies and procedures should be clarified to explain the differences between network analysis and prioritization, [REDACTED] and SIGINT development.

Contact Chaining

All three of these OPS procedures deal similarly with contact chaining. In each instance, the MD definition is included, and contact chaining is noted as a metadata use. There are no other rules or guidance given for this activity in these documents, even though these can involve the [REDACTED]

**Observation no. 5:**

It is our practice during reviews to examine CSE's policies and procedures which must both interpret and guide those activities provided for under the authority of the *NDA*. Paragraph 4 of the metadata MD directs CSE to "...apply procedures for the use and retention of metadata acquired through its program consistent with CSE's existing procedures to protect the privacy of Canadians." As outlined in the foregoing paragraphs, we have noted deficiencies in CSE's OPS-1 policy and its [REDACTED] procedures in relation to metadata activities as described in the March 2005 metadata MD.

Criterion 5:

*CSE had the means to record, track, and account for disclosures of metadata that identified Canadians.*

**Finding no. 13:**

Findings no. 2 and no. 3 on page 13 of this report also apply to this criterion. Also, please see the section on Corporate Records Management on page 30.

---

<sup>39</sup> Reference OPS-3-5 and OPS-3-7, respectively.

<sup>40</sup> Reference OPS-1-6, paragraphs 3.1 and 3.2, respectively.

CSE does record, track, and account for disclosures of information that identifies Canadians. It does not, however, link these disclosures, or attribute them, to those specific metadata activities it conducts pursuant to the authority and rules of the governing MD.

Criterion 6:

*CSE had the means to determine if its metadata activities had been conducted as per its mandate, ministerial directive and approved procedures.*

***Finding no. 14:***

We are satisfied that the CSE managers with whom we spoke understood their responsibilities under OPS-1-8, *Management Monitoring and Policy Review Procedures to Ensure Privacy of Canadians*<sup>41</sup>, and that they approached their daily work with the knowledge that their metadata activities must comply with law and policy.

Our inquiries did not result, however, in receipt of any written material created by CSE managers that indicate how they explicitly address or document their responsibilities as established in OPS-1-8.

Details:

In 2004, CSE issued a new directive known as OPS-1-8. OPS-1-8 deals with CSE management's review and accounting of, among other things, its SIGINT activities, including those known as metadata activities. There are at least four (4) separate references in the document related to management monitoring of the use of metadata. From these references, we wanted to understand:

- a) the monitoring and review of management controls on "directed-at" chaining activities (ref. para. 2.2);
- b) how SIGINT operational areas have developed and instituted management monitoring to ensure that operational policies on the use of metadata are respected on an on-going basis (ref. para. 4.4);
- c) how SIGINT operational areas have developed and instituted management monitoring to ensure retention schedules are followed for metadata used / retained (ref. para. 4.7); and
- d) how management monitoring ensures metadata activities are in compliance with policies and procedures, including activity proposals for [REDACTED] (ref. para. 2.1).

<sup>41</sup> Metadata is also dealt with in OPS-5-17, *Using [REDACTED] Information in SIGINT End-Product Reports and CFIOG/CFSOC Responses to Request for Information (RFIs)*, 16 April 2004. Our inquiries indicated, however, that it fell outside the purview of this review.



The wording of the policy directs SIGINT operational areas to “develop and institute Management Monitoring” to ensure that the above-noted areas comply with law and policy, including the *NDA*, the *Privacy Act* and OPS-1. Level 4 managers in SIGINT operational areas and in the Operational Policy division are responsible for management monitoring.

We are satisfied that the CSE managers with whom we spoke understood their responsibilities under OPS-1-8 and that they approached their daily work with the knowledge that their metadata activities must comply with law and policy. In addition, we know from previous reviews and discussions with CSE managers that the organization’s Audit, Evaluation and Ethics branch conducts periodic compliance assessments in different operational activity areas within CSE.

Our inquiries did not result, however, in receipt of any written material created by CSE managers that indicate how they explicitly address or document their responsibilities as established in OPS-1-8. In one written response received from CSE, we were advised that “In order to ensure the privacy of Canadians, the DGI management monitors the use of [REDACTED] by following the process set forth in OPS-1-10”.<sup>42</sup> We were not provided with any further information as to what is meant by “management monitors.”

## **XI. Corporate Record Keeping**

In the MD, the Minister has established a general framework for the collection and use of metadata which includes rules to which CSE must adhere. In addition, the Minister has advised CSE that metadata activities will be subject to review by the CSE Commissioner.

Records creation and retention is one means by which CSE can assure compliance with the metadata framework and can account for its activities as authorized.

During our review, we learned that some metadata activities are of such a nature that they do not always lead, or lend themselves, to the creation of records or documents that can be subsequently examined. This is particularly true of some of the [REDACTED] activities we observed at Leitrim that fall under the heading of network analysis and prioritization and deal with [REDACTED]

While we understand that some metadata analysis may not involve record keeping, the following two statements made by CSE in response to our requests for various documentation during our review raised questions:

Other than for those contact chaining activities [REDACTED]  
[REDACTED] there is no requirement to retain records of analytic work using metadata. If analytic work involving metadata is used in a report, a copy of

<sup>42</sup>Consistent with OCSEC’s review methodology, OPS-1-10 will be subject to further examination when future metadata reviews are undertaken.

---

that work (i.e., a contact chain) would be retained along with other materials used in the report.<sup>43</sup>

During our discussions, CSE confirmed that it does not as a matter of policy or practice maintain corporate records of those contact chaining activities [REDACTED]

[REDACTED] We were advised that some documentation may exist, but it is held at the discretion of individual employees and may be retained by them in their personal hard copy files, for example, or their CSE computers.

This does not allow for any systematic recording or retrieving of any contact chains. Further, it does not support CSE's ability to account for these activities, or for any activity, such as the identification of new foreign targets and selectors, which may result. It also does not allow for any subsequent review by the CSE Commissioner as is contemplated by the Minister in the MD governing CSE's metadata activities.

Lastly, we include one more statement made by CSE during this review and which raised questions:

Note that aside from chaining activities [REDACTED] there is no legal or policy requirement to retain records of analytic work using metadata.<sup>44</sup>

***Finding no. 15:***

We suggest that CSE consult GoC legislation and policies regarding corporate record keeping and information management and ensure that it is in compliance.

## **XII. CONCLUSION**

This was OCSEC's first examination of CSE's collection and use of metadata as governed by ministerial directive. Due to the complexity and breadth of the activities it authorizes, this preliminary report raises some questions which we believe require further examination.

---

<sup>43</sup> Response received from CSE dated December 6, 2006, page 2 in reference to OCSEC's document entitled "MD on Collection and Use of Metadata: Preliminary Questions", sent to CSE via e-mail on October 4, 2006.

<sup>44</sup> Response dated March 19, 2007 in e-mail from External Review and Policy Compliance (D3) staff to OCSEC Senior Analyst, Subject: "FW: OCSEC Review of Metadata MD / Meeting ... 26 Feb 2007."

---

Legal issues:

As has been documented above, some of CSE's metadata activities raise issues that make us question whether CSE is always in compliance with the limits established by the *National Defence Act* regarding the directing of CSE's mandate (a) activities. Further, this review has confirmed that metadata activities have the potential to encroach on the privacy of the individual, particularly those related to network analysis and prioritization and to contact chaining using metadata from unselected communications, [REDACTED]

We understand that CSE is re-examining its metadata activities, particularly contact chaining. This effort will support and inform future metadata reviews.

Any future OCSEC review will also likely examine and assess CSE's metadata activities in relation to mandate (b). While not a focus of this review, we did learn that all telecommunications data accessed via the global information infrastructure, which is [REDACTED] processed for foreign intelligence collection purposes, is also subject to processes designed to identify malicious cyber activity and protect the integrity of the collection system. These activities, which may also include the acquisition of private communications and a review of their content, are also conducted under the guidance of the metadata MD.

Since we have now observed that some of CSE's "analytic work using metadata"<sup>45</sup> involves the acquisition and recognition of private communications by persons conducting metadata activities, we believe that CSE should re-examine and re-assess its current position and practice that requires that only those private communications recognized by intelligence analysts be accounted for. We suggest that those persons involved in network analysis and prioritization should also be responsible for accounting for all private communications they recognize and handle.

Lastly, and further to this and previous reviews, CSE should re-examine its use and disclosure of personal information about Canadians in the context of mandate (a) of the *NDA*, and section 8 of the *Privacy Act*.

Policy issues:

CSE policy and procedures should be amended, finalized and perhaps augmented in order to guide and support metadata activities undertaken for each method of collection. In particular, OPS-1-10 should be finalized as soon as practicable and made available to all personnel engaged in contact chaining [REDACTED]

---

<sup>45</sup> See footnote 43.

---

Corporate Records Management:

CSE ought to be in a position to account for its metadata activities, up to and including any disclosures made to clients and partners under the *Privacy Act*.

Future metadata reviews will pay particular attention to the documentation CSE is able to provide in order to facilitate an accurate assessment of its compliance with the authorities established in the *NDA*, the metadata MD, and all related policies and procedures.

Our two (2) recommendations are repeated below:

**Recommendation no. 1:**

**CSE should re-examine and re-assess its current position and practice that requires that only those private communications recognized by intelligence analysts be accounted for.**

**Recommendation no. 2:**

**CSE should re-examine and re-assess the legislative authority used to conduct its contact chaining activities [REDACTED] particularly those supplied by federal law enforcement and security agencies engaged in ongoing criminal and national security investigations.**

NOT REVIEWED

A0000384\_33-00974

# Annex A

 NOT REVIEWED

A0000384\_34-00975

TOP SECRET COMINT

To: Chief, Communications Security Establishment

OCSEC- BCCST-
Original: 2800-9
Copies:
Rec. #: 221
Date: Feb 22, 2005

**MINISTERIAL DIRECTIVE  
COMMUNICATIONS SECURITY ESTABLISHMENT  
COLLECTION AND USE OF METADATA**

1. This Directive is issued under my authority pursuant to subsection 273.62 (3) of the *National Defence Act*.
2. For the purpose of the CSE foreign intelligence acquisition programs:
  - a) "*metadata*" means 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.
  - b) "*Network Analysis and Prioritization*" means the method developed to understand the global information infrastructure, from information derived from metadata, in order to identify and determine telecommunication links of interest to achieve the Government of Canada foreign intelligence priorities. This method involves the acquisition of metadata, the identification of [REDACTED] the determination of the [REDACTED] the determination of the [REDACTED]  
[REDACTED]
  - c) "*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 foreign 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 foreign entities and their networks.
3. CSE will collect and use metadata under foreign intelligence acquisition programs according to principles enunciated in this Ministerial Directive. Any amendment to this Ministerial Directive will require my personal approval.

4. CSE will apply procedures for the use and retention of metadata acquired through its program consistent with CSE's existing procedures to protect the privacy of Canadians.

In the fulfillment of its mandate as set out in paragraphs 273.64(1) (a) and (b) of the National Defence Act, CSE may search any metadata acquired in the execution of its foreign intelligence acquisition programs for the purpose of providing any information or intelligence about the capabilities, intentions or activities of a foreign individual, state, organization, terrorist group or other such entities, as they relate to international affairs, defence or security, including any information related to the protection of electronic information or information infrastructures of importance to the Government of Canada.

6. CSE will share metadata, acquired through its foreign intelligence acquisition program with international allies to maximize its mandate activities as set out in the National Defence Act, and strengthen Canada's partnerships abroad. Such sharing will be subject to strict conditions to protect the privacy of Canadians, consistent with these standards governing CSE's other programs.
7. CSE must take the following steps to protect the privacy of Canadians:
  - (1) Metadata that is known to be associated with Canadians anywhere or any person in Canada, and that is incidentally obtained as a result of the acquisition of metadata, must, when such metadata is reported in CSE reports, be altered in such a way as to render impossible the identification of the persons to whom the metadata relates.
  - (2) Disclosure of the unaltered version of metadata shall be subject to specific requests to the Operational Policy division, and such requests shall be granted strictly in accordance with criteria outlined in CSE's Operational Procedures.
  - (3) Access to unaltered metadata in the CSE metadata repositories (bulk metadata) shall be limited to SIGINT operational staff and their supervisors, Operational Policy staff and system administration staff of CSE.
  - (4) For greater certainty, Canada's allies shall not be granted access to metadata known to be associated with Canadians located anywhere or persons located in Canada (bulk metadata) unless it is altered prior to granting access in such a way as to render impossible the identification of the persons to whom the metadata relates.

8. The metadata acquired in the execution of the CSE's foreign intelligence acquisition programs shall be used strictly for:
  - a) Network Analysis and Prioritization, and for Contact Chaining purposes;
  - b) identifying new targets and target associated selectors, which can be used:
    - i) at any time to intercept foreign telecommunications (both-end foreign); or
    - ii) to intercept private communications strictly where a duly issued Ministerial Authorization is in effect, and in strict compliance with that Ministerial Authorization.
  - c) monitoring or identifying patterns of malicious cyber activities to provide indications and warnings of potential cyber attacks.
9. The metadata acquired in the execution of CSE foreign intelligence acquisition programs shall be destroyed after [REDACTED] unless CSE requests, and the Minister of National Defence decides on reasonable grounds, that a longer retention period is warranted to fulfill operational requirements.
10. Activities undertaken pursuant to this Ministerial Directive will be subject to review by the CSE Commissioner as part of his mandate.
11. This Ministerial Directive replaces the Annex to the Ministerial Directive, [REDACTED] Program, signed by the Minister of National Defence on March 15, 2004.
12. This Ministerial Directives comes into force on the date it is signed.

Dated at Ottawa this 9<sup>th</sup> day of March 2005.



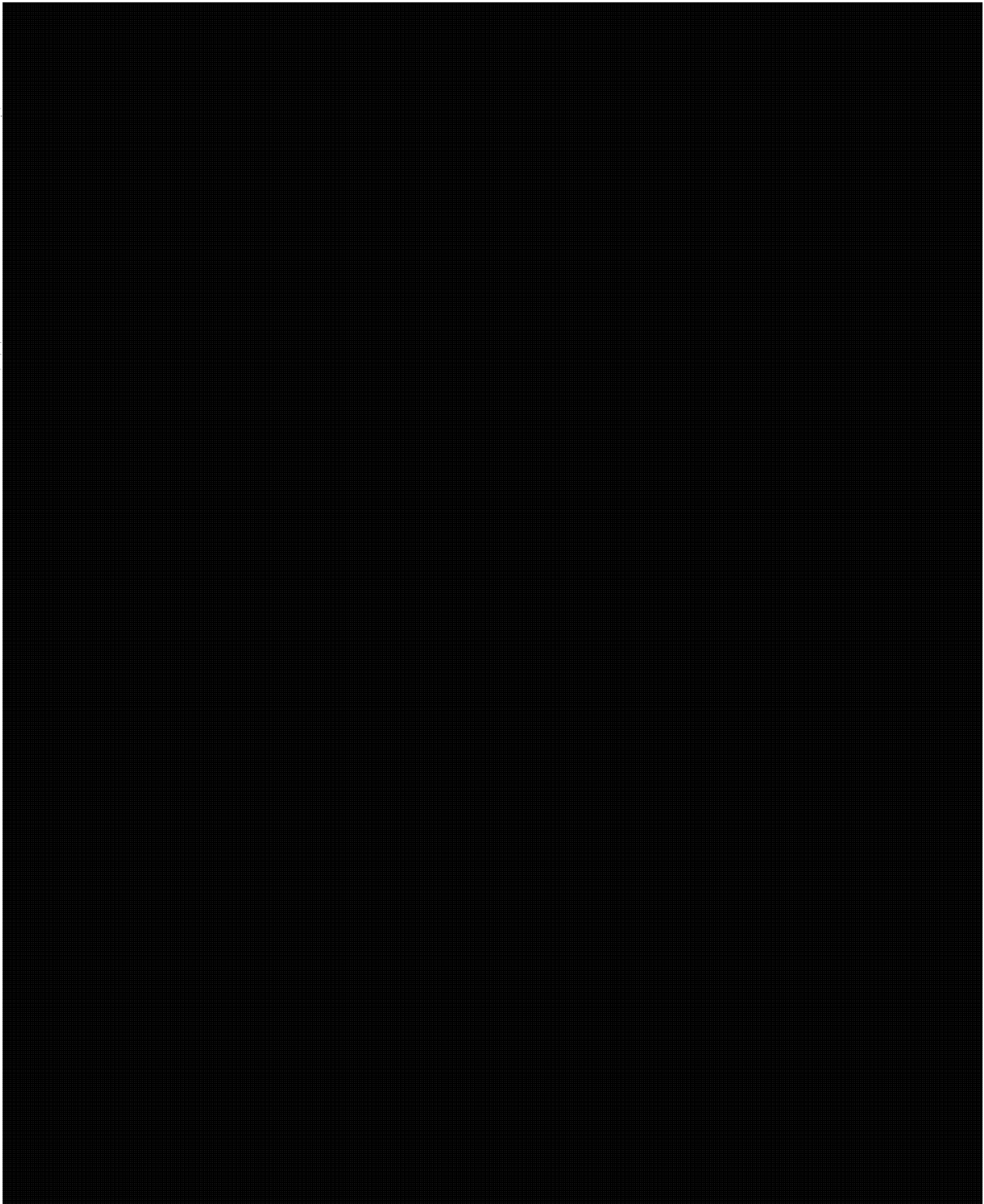
The Honourable William Graham  
Minister of National Defence



# Annex B

NOT REVIEWED

A0000384\_38-00979



NOT REVIEWED

A0000384\_39-00980

# Annex C

NOT REVIEWED

A0000384\_40-00981

## Review of Contact Chains

### Background

The *Ministerial Directive* [MD], *Communications Security Establishment, Collection and Use of Metadata*, dated March 9, 2005, identifies two distinct categories of activities, one being contact chaining.

Contact chaining involves the use and analysis of metadata [REDACTED] to identify and document the communications activities or patterns of entities of (potential) foreign intelligence interest.

The MD defines contact chaining as:

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 foreign 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.

Through chaining, CSE can [REDACTED]

Typically, contact chains [REDACTED] involve receipt (and approval) by CSE of a written request from a Government of Canada (GoC) client such as the Canadian Security Intelligence Service (CSIS) or the Royal Canadian Mounted Police (RCMP). Such requests are initiated by the client, who has obtained, most often, a phone number or an e-mail address as part of an ongoing security or law enforcement investigation in Canada. The client provides the identifier to CSE and requests that it provide them with any information it may have or receive that relates to the identifier.

NOT REVIEWED

A0000384\_41-00982

Details:

During the period April 1, 2005 to March 31, 2006, CSE received [REDACTED] client requests to contact chain [REDACTED]. We can confirm that these requests were subject to a process of internal review and managerial approval. The process was not, however, formally documented until June 2006, in the form of the draft OPS-1-10 procedures (discussed below). Also, not all documentation was provided or available for our review.

We were provided with documentation that related to [REDACTED] of the [REDACTED] client requests to [REDACTED] contact chains [REDACTED] supplied by the client. In every instance, the documentation consisted of a "Selector identification and tracking approval form". All but [REDACTED] of these were accompanied by a CSE addendum that presented the following:

- an assessment of whether a chain [REDACTED] could be expected to produce foreign intelligence;
- identified the foreign intelligence priority and objectives; and
- identified what measures CSE would take to protect privacy.

Some of the tracking approval forms [REDACTED] included copies of the original client request. One included both the client request and the resulting CSE reporting.

CSE encountered some difficulty in providing the chaining documentation we had requested in order to conduct our review. We had anticipated that CSE would have been able to provide us with the following:

- copies of client requests for a contact chain or information related to a [REDACTED] furnished by the client;
- copies of completed Selector identification and tracking approval forms;
- the resulting contact chain, if undertaken; and finally,
- copies of any resulting CSE reporting that contained derivative suppressed Canadian metadata identifiers.

In the event that clients subsequently requested disclosure of the suppressed information, we anticipated that CSE would have been able to produce documentation that would have:

- identified the client requestor;
- the client's authority to request the information and justification of his need to know it;
- evidence that CSE had assessed and approved/rejected the request; and
- confirmation of any requests for disclosure that were approved, complete with the relevant *Privacy Act* citation of the authority under which CSE disclosed the information.

NOT REVIEWED

A0000384\_42-00983

This was not the case, however, as it was not possible to draw a line between a metadata activity such as contact chaining, a derivative report containing a suppressed Canadian (metadata) identifier and the disclosure of that metadata to a client.

CSE did ask that we meet to allow them the opportunity to provide some of the missing details and documentation. We chose not to delay the review at this time with the expectation that we would return to review this one metadata activity in a separate, more encompassing study.

As has been documented in the full metadata MD classified report, there are a number of legal and policy issues that require re-examination. We believe, for example, that contact chaining will have to be studied and assessed, along with and in the context of the October 2003 Department of Justice legal opinion that deals with IRRELEVANT

In the meantime, we took the opportunity to briefly examine CSE's draft OPS-1-10 procedures, which has governed the activity since June 2006, some two to three months after our review period ended.

#### OPS-1-10

For the period under review, CSE did not have any formal procedures in place to guide CSE personnel who undertook contact chains [REDACTED] CSE did, however, provide us with a copy of a draft procedure dated June 2006 known as OPS-1-10, *Procedures for Metadata Analysis* [REDACTED] Copy found at Annex F.

A [REDACTED] is defined at paragraph 7.2 of these procedures as:

A [REDACTED] includes, but is not limited to:

- [REDACTED] (see 6.4)
- [REDACTED]
- [REDACTED]

[REDACTED]  
The above reference to para. 6.4 should, in fact, read 7.4, which defines [REDACTED] as:

NOT REVIEWED

A0000384\_43-00984

[REDACTED]

From this same document, we identified the following list of requirements that CSE personnel would have to satisfy as part of this type of chaining activity. The relevant OPS-1-10 paragraph is noted in brackets after each requirement.

- Identify whether the chain is to be completed under the authority of mandate (a) or (c) (para. 1.1).
- Identify any exceptional circumstances as to why the chain should be undertaken and if so, whether the authorization of the DGI was received (para. 1.3).
- Document the “reasonable belief” that the chain will lead to FI immediately or eventually (para. 1.3).
- Document from where/from whom the [REDACTED] was received (para. 2.1).
- Perform a test to establish: reasonable belief (as above); and whether the FI will satisfy a Government of Canada intelligence requirement (GCR) (para. 2.4).
- Provide a documented rationale for the above (para. 2.5).
- Document if any urgent situations existed and led to the chaining during the period under review (para. 2.7).
- Determine and record the validity of the chaining activity (i.e. is it to be a one-time activity or carried out for up to three months?) (para. 3.1).
- Document whether there is/was any revalidation of the form specified at para. 3.1 and the chaining authority (para. 3.2).
- Document how the nationality of the identifier was identified (para. 3.4).
- Document whether any identifiers were suppressed in subsequent contact chaining reporting (para. 3.5).
- Document whether any legal advice was sought for the chaining (para. 5.1).

Observations:

From our examination of the documentation presented to us by CSE for the [REDACTED] chaining requests made prior to the release of OPS-1-10, we can make the following observations:

- We cannot determine the mandated authority used to complete the chain.
- In most instances, we cannot determine the validity of the chaining activity.
- In those instances where a validity period was written in, there is no means to confirm whether the activity was ceased after, for example, the [REDACTED] period of authorization.
- There is no evidence that a chain was produced.
- We cannot determine if a chain resulted in a report and whether a report included a suppressed identifier(s).
- We do not know if legal advice was sought.

We would encourage CSE to continue to develop these procedures and to institute measures to record and track these contact chains.

NOT REVIEWED

A0000384\_44-00985

# Annex D

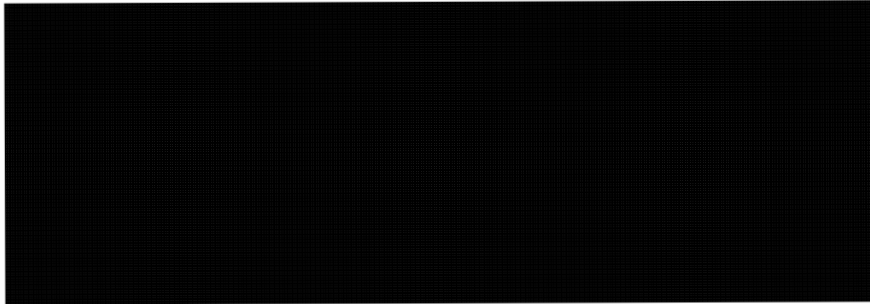
NOT REVIEWED

A0000384\_45-00986



Metadata: [REDACTED] Process: [REDACTED]

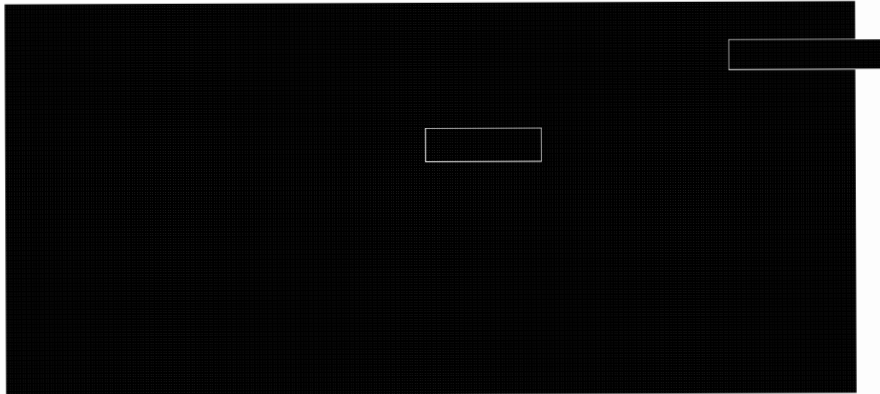
The terminology applied to metadata activities is not yet definitive within CSE's own written documentation. The following definitions, which apply generally to SIGINT acquisition, were provided to us by CSE and were important to our understanding of the collection and use of metadata as authorized by the metadata MD.



**Acquire/Collect:** *Used synonymously to indicate interception.*<sup>46</sup>

As indicated in these definitions, all data is [REDACTED]  
[REDACTED]

For CSE's purposes, each communication is seen as having two distinct parts: that known as the metadata and that known as the content. The metadata portion is the focus of [REDACTED]  
[REDACTED] by CSE and which result in [REDACTED]  
[REDACTED] database (see below). We understand these [REDACTED] processes to be as follows:



<sup>46</sup> Briefing entitled *Metadata Review Questions* given to OCSEC by CSE on February 26, 2007.

[REDACTED]

[REDACTED]

[REDACTED] is a CSE database that stores only metadata. The metadata has been [REDACTED] from both DNR (dialled number recognition) and DNI (digital network intelligence) communications traffic. Generally, DNR traffic is that commonly known as phone or fax, while DNI refers generally to e-mails. CSE will often refer to DNI [REDACTED] traffic.

The source of [REDACTED] metadata is CSE's own collection [REDACTED] and includes that acquired via [REDACTED] programme.

All CSE-collected DNR metadata is [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

<sup>47</sup>Typically, foreign intelligence traffic is obtained using *selectors* that represent foreign entities of intelligence interest. Selectors are alphanumeric data such as e-mail addresses or telephone numbers that are [REDACTED] into a [REDACTED] dictionary.

<sup>48</sup>The communications stored in these principal information databases are accessed mainly for foreign intelligence analysis purposes.

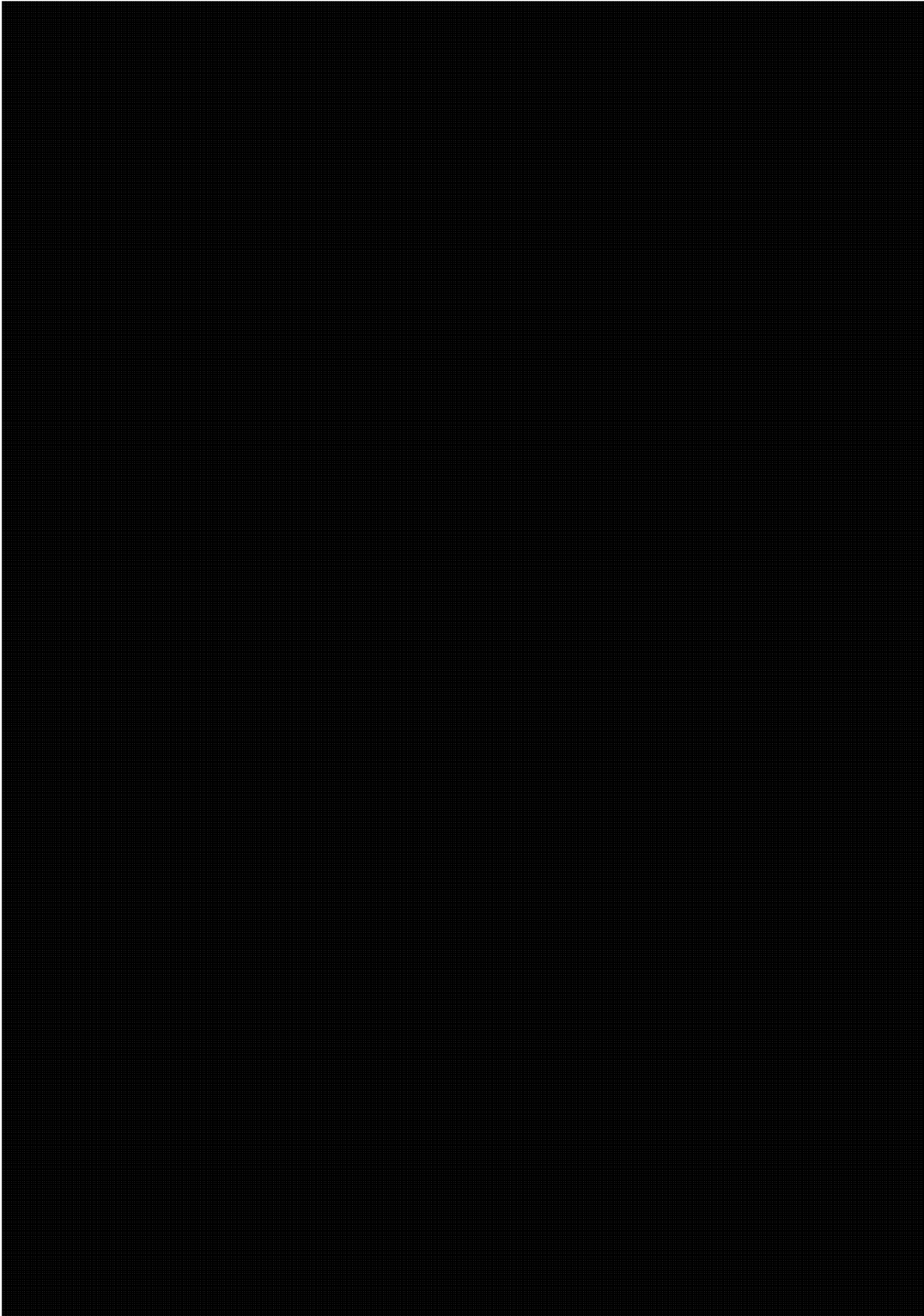
# Annex E

NOT REVIEWED

A0000384\_48-00989



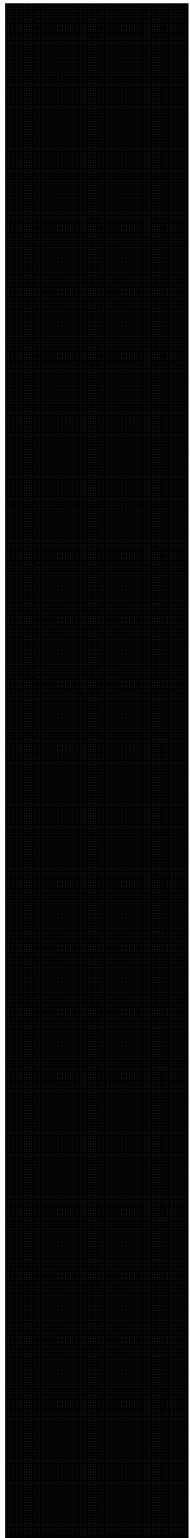
TOP SECRET//COMINT  
DNI Metadata Sample



NOT REVIEWED

A0000384\_50-00991

TOP SECRET//COMINT  
DNI Metadata Sample



NOT REVIEWED

A0000384\_51-00992

# Annex F

NOT REVIEWED

A0000384\_52-00993

**TOP SECRET//COMINT//Canadian Eyes Only**  
**June 2006**  
**DRAFT**



**OPS-1-10**

**Procedures for Metadata Analysis**

**NOT REVIEWED**

**A0000384\_53-00994**



57 of 74  
A-2017-00017--00733

---

## 1. Introduction

---

### 1.1 Objective

These procedures describe 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]

[REDACTED] a contact chain [REDACTED]  
[REDACTED]

Metadata analysis conducted in support of Federal Law Enforcement or Security Agencies (LESAs) to obtain Security or Criminal Intelligence (mandated under paragraph 273.64(1)(c) of the *NDA*, known as "Mandate C") is handled only in accordance with OPS-4-1, *Procedures for CSE Assistance to Canadian Federal Law Enforcement and Security Agencies*, and OPS-4-2, *Procedures for CSE Assistance under Section 12 of the CSIS Act*.

---

### 1.2 Authority

In accordance with these procedures, metadata analysis [REDACTED]  
[REDACTED] may be searched and analyzed for the purpose of providing FI, pursuant to paragraph 273.64(1)(a) of the *NDA*.

---

**1.3 Context and  
Limitations**

Metadata analysis [REDACTED]  
may only be conducted under exceptional  
circumstances with the authorization of DGI, in  
accordance with these procedures, and only in  
cases where there is a reasonable belief that the  
activity will lead to Foreign Intelligence  
(immediately or eventually; see 2.4).

---

**1.4 Application**

CSE staff, Canadian Forces Information  
Operations Group (CFIOG) staff, and any other  
parties conducting metadata analysis [REDACTED]  
[REDACTED]  
identifier) under CSE authorities are bound by  
these procedures.

---

NOT REVIEWED

50  
A0000384\_56-00997

---

## 2. Process

---

### 2.1 Receiving

[REDACTED] which may lead to foreign intelligence are obtained by CSE from:

- Departments or agencies of the Government of Canada
  - Allies, or
  - CSE/CFIOG SIGINT activities, including metadata analysis.
- 

### 2.2 Summary

The following is a summary of the process for conducting metadata analysis [REDACTED]

- 1) Determine whether [REDACTED] passes the FI test (see 2.4)
  - 2) Complete the Intelligence Branch Tracking Form (at Annex 1)
  - 3) Obtain appropriate approvals (as per 2.6, or 2.7 for [REDACTED] in emergencies)
  - 4) DGI Branch retains all forms and stores in a secure manner.
- 

### 2.3

In most cases, metadata analysis [REDACTED] [REDACTED] However, in some cases, when pursuing FI, metadata analysis may need to [REDACTED] (including those encountered during the analysis of the [REDACTED] These [REDACTED] may not be [REDACTED] or for further analysis, without following the formal documentation and approval process (detailed in 2.5 and 2.6).

---

#### 2.4 FI Test

The following questions must be addressed by analysts prior to [REDACTED] in metadata analysis.

Step	Considerations	If the answer is...	Then...
1	Is there a reasonable belief that chaining [REDACTED] will lead to FI (either immediately or eventually)?	YES	Analysts provide detailed rationale, using the form at Annex 1, as to why the identifier will likely lead to FI; go to step 2.
		NO	Do not [REDACTED] chain [REDACTED] unless it can be done under "Mandate C" (see 1.1).
2	Will the expected FI satisfy a formal GCR (Government of Canada Requirement)?	YES	Include GCR number on form (Annex 1); submit for approval (see 2.6 below)
		NO	Do not proceed with metadata analysis.

#### 2.5 Documenting Rationale

CSE Intelligence Branch and CFIOG analysts must document their rationale for believing a [REDACTED] will lead to FI, using the Intelligence Branch tracking form (Annex 1).

NOT REVIEWED

52  
A0000384\_58-00999

---

## 2.6 Approvals

[REDACTED]

The rationale for using [REDACTED] is presented by analysts using the form at Annex 1, reviewed by Intelligence Branch Team Leaders, Production Managers, or the [REDACTED] Mission Management Officer, and forwarded to the relevant Director, or Operations Officer. If satisfied with the rationale, the Director or Operations Officer will seek DGI's (or anyone officially acting as DGI) signed authorization.

The process may be terminated at any stage by anyone in the approval process, if they believe the answer to one of the considerations noted in 2.4 is "no". Intelligence Branch Directors and/or DGI may consult DLS for advice as necessary. DGI approval is required before metadata analysis using a [REDACTED] is conducted.

[REDACTED]

The rationale for using [REDACTED] is presented by analysts using the form at Annex 1, reviewed by Intelligence Branch Team Leaders, and is forwarded to an Intelligence Branch Level IV Manager for approval.

---

NOT REVIEWED

53  
A0000384\_59-01000

TOP SECRET//COMINT//Canadian Eyes Only  
OPS-1-10  
June 2006  
**DRAFT**

**2.7 Emergency  
Approval for**

[REDACTED]

In urgent situations (e.g. there is an imminent threat to life), if [REDACTED] (or anyone officially acting as [REDACTED] is unavailable, the relevant Director may authorize metadata analysis [REDACTED] [REDACTED] must be informed of the authorization, and confirm it in writing as soon as possible after the fact.

Should [REDACTED] not be satisfied with the FI rationale, activity [REDACTED] [REDACTED] must cease immediately; any SIGINT reports that may have resulted must be cancelled.

---

### **3. Tracking Requirements**

---

NOT REVIEWED

54  
A0000384\_60-01001

### 3.1 Records

[REDACTED] that are [REDACTED]  
contact chaining must be accompanied by a  
written FI rationale and appropriate signed  
approvals (using the form at Annex 1). [REDACTED]  
Branch will retain all forms; they will be securely  
stored with access limited to the relevant team,  
and subject to review (see 3.2).

Note that:

- [REDACTED]
- [REDACTED]
- [REDACTED]

### 3.2 Review of Requirement for Exceptional Activities

To ensure continued FI relevance, the rationale  
for each [REDACTED] that is  
being [REDACTED] for a period of  
up to [REDACTED] must be reviewed and  
[REDACTED] by  
the relevant [REDACTED] Branch Level IV Manager. If no  
longer of FI relevance, the [REDACTED]  
[REDACTED] must not be [REDACTED] against without a  
renewed justification in place. The form will be  
placed in an inactive file for audit and review  
purposes, and held indefinitely.

Contact chaining [REDACTED] is  
subject to management monitoring, and to review  
by various government review bodies, including  
the CSE Commissioner.

NOT REVIEWED

55  
A0000384\_61-01002

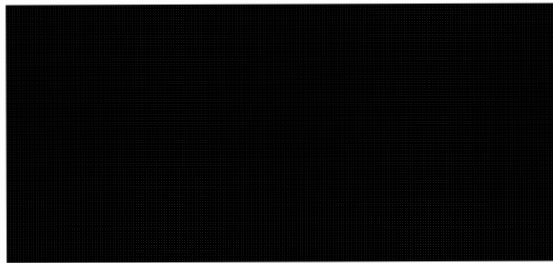


### 3.3 Reporting

SIGINT reports based on metadata analysis must adhere to existing policies and 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*
  - OPS-4-1, *Procedures for CSE Assistance to Canadian Federal Law Enforcement and Security Agencies*
  - OPS-4-2, *Procedures for CSE Assistance under Section 12 of the CSIS Act*
  - OPS-5-2, *CSE SIGINT Reporting Procedures*
- 

### 3.4



### 3.5 Dissemination

Unless a client who has provided a [REDACTED] requests otherwise, SIGINT reporting derived from metadata analysis [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.

[REDACTED] must be suppressed in reporting, in accordance with OPS-1-7 *SIGINT Naming Procedures*, and allied naming policies.

NOT REVIEWED

56  
A0000384\_62-01003

---

## 4. Metadata Analysis Involving [REDACTED]

---

### 4.1 CSE Metadata Repositories

Metadata analysis [REDACTED]  
[REDACTED]

**metadata repositories** requires the prior approval of a SIGINT Level IV Manager. (see Annex )

---

NOT REVIEWED

57  
A0000384\_63-01004

4 Metadata analysis [REDACTED]  
.  
2 [REDACTED] metadata  
repositories may only be conducted in  
accordance with [REDACTED] policies. For example,  
[REDACTED]

M  
e  
t  
a  
d  
a  
t  
a  
  
R  
e  
p  
o  
s  
i  
t  
o  
r  
i  
e  
s

---

## 5. Roles and Responsibilities

---

5.1

This table summarizes roles and responsibilities  
under these procedures.

Who	Roles
-----	-------

NOT REVIEWED

58

A0000384\_64-01005

**TOP SECRET//COMINT//Canadian Eyes Only**  
**OPS-1-10**  
**June 2006**  
**DRAFT**

<ul style="list-style-type: none"> <li>• Director General [REDACTED] (or anyone officially acting as [REDACTED])</li> </ul>	<ul style="list-style-type: none"> <li>• Approving metadata analysis [REDACTED]</li> <li>• Seeking legal advice when required</li> </ul>
<ul style="list-style-type: none"> <li>• Director, Legal Services</li> </ul>	<ul style="list-style-type: none"> <li>• Providing legal advice, when requested</li> </ul>
<ul style="list-style-type: none"> <li>• DG [REDACTED] Branch Level IV Managers</li> </ul>	<ul style="list-style-type: none"> <li>• Approving metadata analysis [REDACTED]</li> <li>• Reviewing rationales for metadata analysis [REDACTED]</li> </ul>
<ul style="list-style-type: none"> <li>• [REDACTED] Branch Directors, or</li> <li>• [REDACTED] Operations Officer* (for activity)</li> </ul>	<ul style="list-style-type: none"> <li>• Reviewing rationale and, if acceptable, recommending approval to [REDACTED] of metadata analysis [REDACTED]</li> <li>• Emergency approval authority (see 2.8)</li> <li>• Seeking legal advice from DLS when required</li> </ul>
<ul style="list-style-type: none"> <li>• DG [REDACTED] Branch Team Leaders or</li> <li>• [REDACTED] Mission Management Officer (for CFIOG activity)</li> </ul>	<ul style="list-style-type: none"> <li>• Reviewing and recommending proposals to [REDACTED] in metadata analysis</li> <li>• Reviewing forms quarterly, to ensure continued FI relevance</li> </ul>

\* Note: CFIOG personnel will consult DLS only in coordination with CSE [REDACTED] Branch Directors.

NOT REVIEWED

59  
A0000384\_65-01006

---

## 6. Additional Information

---

### 6.1 Accountability

The following table outlines the accountability structure with respect to these procedures.

Who	Responsibilities
Deputy Chief SIGINT	<ul style="list-style-type: none"><li>• Approving these procedures</li></ul>
DG Intelligence	<ul style="list-style-type: none"><li>• Applying these procedures</li><li>• Recommending changes to these procedures</li></ul>
DG Policy and Communications	<ul style="list-style-type: none"><li>• Approving these procedures</li></ul>
Director, Legal Services	<ul style="list-style-type: none"><li>• Reviewing these procedures to ensure they comply with the law</li></ul>

NOT REVIEWED

60  
A0000384\_66-01007

All CSE and CFIO G Mana gers invol ved in conta ct chain ing	<ul style="list-style-type: none"> <li>Ensuring their staff have read and understood these procedures and any amendments to these procedures</li> </ul>
<ul style="list-style-type: none"> <li>DG Intelligence staff</li> <li>CFIOG staff</li> <li>Operational Policy staff</li> </ul>	<ul style="list-style-type: none"> <li>Reading, understanding and complying with these procedures and any amendments to these procedures</li> </ul>
Mana ger Oper ation al Polic y	<ul style="list-style-type: none"> <li>Revising these procedures when required</li> <li>Responding to questions concerning these procedures</li> </ul>

## 6.2 References

- National Defence Act*
- Ministerial Directive "Privacy of Canadians", 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-5-2, *CSE SIGINT Reporting Procedures*

## 6.3 Amendments

Situations may arise where amendments to these procedures may be required because of changing or unforeseen circumstances. All approved amendments will be announced to staff and will be posted on the Operational Policy website at: [REDACTED]

NOT REVIEWED

61

A0000384\_67-01008

---

#### 6.4 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.

---

### 7. Definitions

---

#### 7.1 Canadian

'Canadian' refers to

- a) A Canadian citizen, or
  - b) A person who has acquired the status of permanent resident under the *Immigration and Refugee Protection Act*, S.C. 2001, c. 27, and who has not subsequently lost that status under that *Act*, or
  - c) A corporation incorporated under an Act of Parliament or of the legislature of a province. (NDA)
- 

#### 7.2 [REDACTED]

A [REDACTED] includes, but is not limited to:

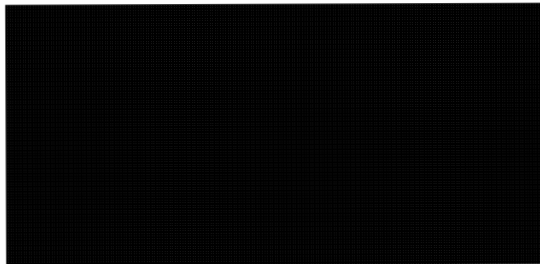
- [REDACTED]
  - [REDACTED]
  - [REDACTED]
- 

NOT REVIEWED

**7.3 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.

7.4



**7.5 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.

**7.6 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.

NOT REVIEWED

63

A0000384\_69-01010



7.7 Metadata  
Analysis

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

---

NOT REVIEWED

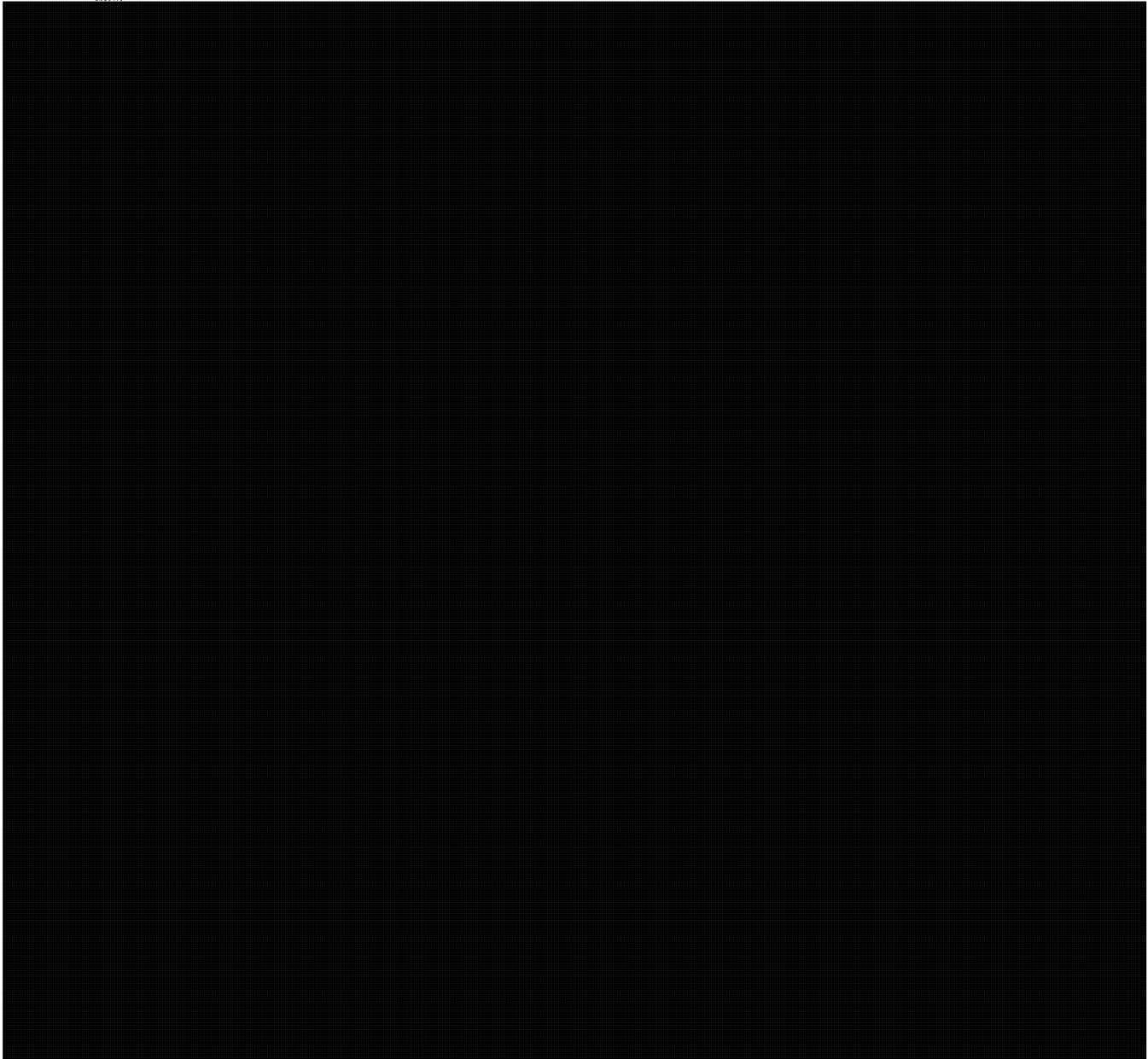
64  
A0000384\_70-01011

TOP SECRET//COMINT//Canadian Eyes Only



COMMUNICATIONS SECURITY ESTABLISHMENT  
INTELLIGENCE BRANCH

Tracking Approval Form to [REDACTED] Contact Chain [REDACTED]  
[REDACTED]



NOT REVIEWED

65  
A0000384\_71-01012