Communications Security Establishment Commissioner

The Honourable Jean - Pierre Plouffe, C.D.

Commissaire du Centre de la sécurité des télécommunications

L'honorable Jean - Pierre Plouffe, C.D.

TOP SECRET // SI // CEO

Our file # 2200-86

March 31, 2015

The Honourable Jason Kenney, P.C., M.P.
Minister of National Defence
101 Colonel By Drive
Ottawa, ON K1A 0K2

Dear Minister:

The purpose of this letter is to provide you with the results of my review of the Communications Security Establishment's (CSE) metadata activities in a signals intelligence (SIGINT) context. This review was conducted under my general authority as articulated in Part V.1, paragraph 273.63(2)(*a*) of the *National Defence Act* (*NDA*), and in accordance with paragraph 10 of the Ministerial Directive: Communications Security Establishment Collection and Use of Metadata, 21 November 2011 (Metadata MD).

The objectives of this review were originally to examine CSE's SIGINT and information technology (IT) security activities that use metadata. However, due to the broad scope and high volume of information involved, the review of metadata was separated into three projects. This report focused on CSE's use of metadata in a SIGINT context. A second report will examine issues identified in the Commissioner's 2014 report, entitled *A Review of CSE's Office of Counter-Terrorism*, and will also examine network analysis and prioritization activities which involve metadata, and contact chaining activities [redacted] A third report, expected in the coming year, will focus on CSE's use of metadata in an IT security context.

CSE collects, uses and discloses unselected[1] metadata[2] under the authority of paragraph 273.64(1)(*a*) of the *NDA*, as affirmed by paragraph 3 of the Metadata MD. Two broad categories of metadata that are of particular interest are: Dialled Number Recognition (DNR) metadata,

[1] "Unselected" metadata is also referred to as "bulk" metadata, collected or shared without having gone through a targeting-selection process which ensures that at least one end of the associated communication is foreign and is related to a foreign intelligence priority of the GC.

[2] "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." (*Ministerial Directive: Communications Security Establishment Collection and Use of Metadata*, 21 November 2011)

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

which generally pertains to telephone or fax communications; and Digital Network Intelligence (DNI) metadata, which generally pertains to email, [redacted]

Various metadata activities have been subject to reviews in recent years, subsequent to a comprehensive overview of CSE's use of metadata in a SIGINT context that was reported on in 2008. Given the rapid pace of technological change, I decided to pursue another broad review of CSE's use of metadata in a SIGINT context for several reasons: to maintain a general awareness of systems and activities; to examine particular areas or issues in detail; and to identify topics for future in-depth reviews.

The collection and use of metadata by CSE and its international partners have also been the subject of a great deal of media coverage and debate over the past two years. Questions have been raised about the scope of such activities and their impact on the privacy of Canadians. While this review was planned prior to media coverage of documents leaked by former National Security Agency (NSA) contractor Edward Snowden, which began in June 2013, the prevalence of metadata-related issues in public discourse further confirms the value of having undertaken a broad review of CSE's collection, use and sharing of metadata, particularly in a SIGINT context.

During this review, CSE was forthcoming with information and assistance, both proactively and in response to specific requests by my office. The high profile of metadata activities by intelligence agencies in the wake of the unauthorized Snowden disclosures placed unique demands on both CSE and the Commissioner's office throughout this review. CSE recognized the importance of responding to requests of the Commissioner's office in a timely fashion. In addition, CSE proactively informed the Commissioner's office of incidents that it discovered during the review, which led to further in-depth investigation.

I found that metadata collection and analysis have evolved considerably since the last in-depth review of metadata activities. Metadata remains critical to all aspects of CSE's SIGINT mission. Technological developments have resulted in more methods for exploiting metadata for foreign intelligence purposes, and have led to a diverse set of new tools and systems. I found that the Canadian legal landscape has also changed since my office last conducted an in-depth review of CSE's collection and use of metadata. My office will continue to monitor how CSE responds to technological developments and the privacy implications thereof, as well as developments in the legal landscape that could impact its collection, use and disclosure of metadata.

I found that the 2011 Metadata MD lacks clarity regarding the sharing of DNI metadata with Five Eyes partners, as well as other aspects of CSE's metadata activities. **I therefore recommend** that CSE seek an updated ministerial directive that provides clear guidance related to the collection, use and disclosure of metadata.

I conducted an in-depth examination of Internet protocol (IP) profiling activities that were the subject of an unauthorized disclosure and media reporting in January 2014, and I found that these activities were authorized under paragraph 273.64(1)(a) of the *ND4* and that CSE took measures to protect the privacy of Canadians in undertaking them.

While I was conducting my review, CSE discovered on its own that DNI and [redacted] DNR metadata being shared with Five Eyes partners was not being minimized properly. Minimization is the process by which Canadian Identity Information (CII)[3] contained in [redacted] metadata is altered in such a way that it is rendered unidentifiable prior to sharing with Five Eyes partners. The Metadata MD provides guidance to CSE concerning the privacy protection measures that the Minister expects CSE to implement for the handling of [redacted] metadata. Minimization of [redacted] metadata is one of these privacy protection measures. Therefore, I found the fact that CSE did not properly minimize CII contained in [redacted] metadata shared with Five Eyes partners to be contrary to the Ministerial Directive, and also contrary to CSE's operational policy.

I found that CSE proactively suspended the sharing of both DNR and DNI metadata with Five Eyes partners in order to protect the privacy of Canadians while developing a solution to the problems it encountered in this area. The automated sharing of both DNR and DNI metadata with Five Eyes partners remains suspended, and CSE has indicated that it will remain so until the Chief, CSE is satisfied that proper systems are in place to ensure that all shared CII is properly minimized, in accordance with the Ministerial Directive. CSE informed me, as well as your predecessor, about these matters.

I found that CSE lacked a proper means of verifying whether minimization scripts were functioning properly for [redacted] DNR metadata shared with Five Eyes partners, and that CSE's system for minimizing [redacted] DNR metadata was decentralized and lacked appropriate control and prioritization. Furthermore, I found that CSE's system for sharing DNI metadata with Five Eyes partners was poorly understood by the organization. For both DNI and DNR metadata, CSE lacked a proper record-keeping process. As a result of this finding, **I recommend** that CSE use its existing centralized records system to record decisions and actions taken regarding new and updated collection systems, as well as decisions and actions taken regarding minimization.

During the course of the review, CSE discovered that DNI being shared with Five Eyes partners was not subject to proper validation, in accordance with CSE policy. According to *OPS-1 Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities*, prior to targeting selectors in order to intercept communications, CSE is required to validate those selectors to ensure that they are directed at foreign entities outside of Canada, and that they are consistent with Government of Canada intelligence priorities. CSE informed the Commissioner's office that it also relied on this process to guide the sharing of DNI metadata with Five Eyes partners. However, CSE did not validate DNI identifiers prior to sending associated metadata to Five Eyes partners, and therefore breached its operational policy.

Finally, I found that CSE's failure to minimize DNR and DNI metadata, and its failure to validate identifiers prior to sharing DNI metadata with Five Eyes partners, raise legal questions that my office continues to investigate as a high priority. Following this investigation, as mandated by paragraph 273.63(2)(c) of the *NDA*, I will make a determination with respect to CSE's compliance with the law.

---

[3] Identity information means information about an identifiable individual, such as any number, symbol or other data uniquely assigned to an individual. In a SIGINT context, this usually includes phone numbers, email addresses, names, [redacted] and IP address, among others.

CSE's Five Eyes partners recognize each other's sovereignty and respect each other's laws by pledging not to target one another's communications. CSE trusts that its Five Eyes partners will follow the general statements found in agreements signed among partners not to direct activities at Canadians or persons in Canada. In the broader context of SIGINT information sharing with allies, reported in my previous public annual report, I met with the Inspector General of the NSA in the United States in January to personally seek assurances beyond those CSE can provide to me as regards NSA's policies and procedures on the treatment of information about Canadians. I am satisfied with the assurance I obtained.

I will keep you apprised of any further major developments related to this matter. I appreciate CSE's ongoing candidness and cooperation throughout this process.

CSE officials were provided an opportunity to review and comment on the results of the review, for factual accuracy, prior to finalizing the enclosed report.

If you have any questions or comments, I will be pleased to discuss them with you at your convenience.

Yours sincerely,

Jean-Pierre Plouffe

c.c. Associate Minister of National Defence
Chief, CSE

Office of the
Communications Security
Establishment Commissioner

CANADA

Bureau du
Commissaire du Centre de la
sécurité des télécommunications

TOP SECRET // SI // CEO

Our File # 2200-86

Review of CSE's use of Metadata in a Signals Intelligence Context

March 31, 2015

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

TABLE OF CONTENTS

I. AUTHORITIES

The review is conducted under the authority of the Commissioner as articulated in paragraph 273.63(2)(*a*) of the *National Defence Act* (*NDA*), and in accordance with paragraph 10 of the 2011 *Ministerial Directive: Communications Security Establishment's Collection and Use of Metadata*.

II. INTRODUCTION

The Communications Security Establishment (CSE) 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."[1]

CSE collects and uses signals intelligence (SIGINT) metadata under the authority of paragraph 273.64 (1)(*a*) of the *NDA*. Collection and use of SIGINT metadata are further guided and constrained by the 2011 *Ministerial Directive: Communications Security Establishment's Collection and Use of Metadata*, as well as by CSE's operational policies. Additionally, CSE acquires metadata under the authority of paragraph 273.64 (1)(*b*) of the *NDA*.

CSE collects, uses and shares metadata for specific purposes in support of its foreign intelligence acquisition program, and to help ensure the protection of electronic information and information infrastructures of importance to the Government of Canada. CSE also uses metadata to gain a better understanding of the global information infrastructure, including cyber threat information. CSE acquires metadata from a variety of its own collection sources as well as those of its international partners, and may receive disclosures of metadata from domestic partners or from owners of systems of importance to the Government of Canada.

According to CSE policy, SIGINT may use metadata for the following purposes:[2]

- contact chaining;[3]

---

[1] *Ministerial Directive: Communications Security Establishment Collection and Use of Metadata*, November 21, 2011. A copy is attached at Annex C.

[2] CSE policy OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities*, December 1, 2012, section 3.6.

[3] "Contact chaining refers to the method developed to enable the analysis, from information derived from the 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." (CSE policy OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities*, December 1, 2012, section 8.4).

- network analysis and prioritization;[4]
- identifying new targets and selectors; and
- monitoring or identifying patterns of foreign malicious cyber activities.

CSE also uses metadata for information technology (IT) security purposes, to conduct the statistical analysis required for situational awareness and to detect new cyber threats against the Government of Canada.[5]

On November 21, 2011, the Minister of National Defence signed a Ministerial Directive (MD)[6] to the Chief CSE describing how the Minister expects CSE to collect, use and share metadata in the conduct of foreign intelligence activities. Included in the MD is a statement that activities undertaken pursuant to the MD are subject to review by the CSE Commissioner.

Rationale for conducting this review

The collection, use and sharing of metadata are important activities for both SIGINT and IT Security. While specific controls are placed on these activities to ensure compliance with legal, ministerial and policy requirements, including the 2011 MD, the potential impact on the privacy of Canadians of non-compliance while conducting these activities could be significant.

Over the past several years, the Commissioner's office has undertaken a number of reviews that deal in large part with CSE's collection, use and sharing of metadata in relation to its foreign intelligence activities, namely:

- *Report to the CSE Commissioner on CSE Support to Law Enforcement: Royal Canadian Mounted Police (RCMP) Phase II: CSE Mandate (a)* (2006);
- *OCSEC Review of the Ministerial Directive, Communications Security Establishment, Collection and Use of Metadata, March 9, 2005* (2008);

---

[4] "Network analysis and prioritization refers to the method developed to understand the GII, from information derived from metadata, in order to identify and determine telecommunication links of interest to achieve the GC foreign intelligence priorities. This method involves the acquisition of metadata, the identification of [redacted] the determination of the [redacted] the determination of the [redacted] (CSE policy OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities*, December 1, 2012, section 8.16).

[5] OPS-1-14, section 3.3

[6] *Ministerial Directive: Communications Security Establishment Collection and Use of Metadata*, November 21, 2011. This document replaced the 2005 MD of the same title.

- *Report to the CSE Commissioner on CSE Support to CSIS Phase I: CSE Mandate (a)* (2008);
- *A Review of Recommendation No. 1 from the January 2008 Review Report respecting CSE's Ministerial Directive on the Collection and Use of Metadata - CSE's [redacted] Network Analysis and Prioritization [redacted] Activities* (2009);
- *A Review of CSE's Contact Chaining Activities [redacted]* (2010); and
- *A Review of CSE's Office of Counter-Terrorism* (2014).

While particular metadata activities have been subject to reviews in recent years, a comprehensive overview of CSE's use of metadata in a SIGINT context has not occurred since 2008. Given the rapid pace of technological change, and the need for intelligence collection and analytic tradecraft to constantly adapt, CSE's use of metadata for SIGINT purposes is likely to have evolved considerably in that time. As such, the Commissioner's office decided to pursue a broad review of CSE's use of metadata in a SIGINT context, in order to maintain a general awareness of systems and activities, examine particular areas or issues in detail, and identify topics for future in-depth reviews.

This review provides an opportunity to once again examine CSE's use of metadata, to assess changes to its activities for compliance with the law, and to examine the measures in place to protect the privacy of Canadians. Due to the broad scope and high volume of information, the review of metadata will be separated into three reports. This report focuses on CSE's use of metadata in a SIGINT context. A second report will examine issues identified in the Commissioner's 2014 report, entitled *A Review of CSE's Office of Counter-Terrorism*, and will also examine network analysis and prioritization activities that involve metadata, and contact chaining activities [redacted] A third report, expected in the coming year, will focus on CSE's use of metadata in an IT security context. It will be the first comprehensive examination of CSE's use of metadata for IT security purposes.

The collection and use of metadata by CSE and its international partners have also been the subject of a great deal of media coverage and debate over the past two years. Questions have been raised about the scope of such activities and their impact on the privacy of Canadians. While this review was planned prior to media coverage of documents leaked by former National Security Agency (NSA) contractor Edward Snowden, which began in June 2013, the prevalence of metadata-related issues in public discourse further underscores the value of having undertaken a broad review of CSE's collection, use and sharing of metadata, particularly in a SIGINT context.

III. OBJECTIVES

The objectives of the review were: to examine CSE's use of metadata in a SIGINT context to assess whether CSE has complied with the law and acted consistent with ministerial direction, whether measures are in place to protect the privacy of Canadians, and whether the activities conform with CSE's own operational policies and procedures. This review also aimed to provide the Commissioner's office with updated knowledge and to identify any areas or issues that could form the basis for future, in-depth reviews of specific metadata activities in a SIGINT context.

Another objective of this review was to get a "bird's-eye view" of metadata collection, storage, use and sharing at CSE, and to learn how it has evolved since the last in-depth, comprehensive review of metadata occurred in 2008.

IV. SCOPE

The Commissioner's office examined CSE's use of metadata in a SIGINT context. This includes:

- The legal authorities and guidance governing the use of metadata in a SIGINT context, including changes between the 2005 and 2011 MDs;
- The collection, use, and sharing of metadata, including access, retention, and reporting;
- How CSE protects the privacy of Canadians while using metadata in a SIGINT context, including:
    - the volume of information about Canadians that CSE collects, uses, accesses, retains, reports and shares while using metadata in a SIGINT context, and how this information is treated; and,
    - the technologies, databases, and systems used for metadata activities in a SIGINT context, and how these tools and other measures may be used by CSE to protect the privacy of Canadians.

While an examination of CSE's contact chaining activities [redacted] was originally planned to form part of this review, it was decided that this would be better suited to a separate report.[7] Much work was done during the research phase of this review to follow up on recommendations from past reports related to contact chaining, which will help to inform a future report. However, as certain issues arose

Solicitor-Client Privilege

during this review that implicated the privacy of Canadians in a significant way, the Commissioner's office decided to pursue enquiry into these issues as a priority.

V. CRITERIA

The Commissioner's office assessed whether CSE's use of metadata in a SIGINT context complied with the law and protected the privacy of Canadians in the context of the Commissioner's standard review criteria.

A) Legal Requirements

The Commissioner expects that CSE conducts its activities in accordance with the *NDA*, *Privacy Act*, *Criminal Code*, *Canadian Charter of Rights and Freedoms*, and any other relevant legislation, and in accordance with Justice Canada advice.

B) Ministerial Requirements

The Commissioner expects that CSE conducts its activities in accordance with ministerial direction, following all requirements and limitations set out in a ministerial authorization or directive.

C) Policies and Procedures

The Commissioner expects that CSE:

i) has appropriate policies and procedures that guide the activities and provide sufficient direction respecting legal and ministerial requirements, including the protection of the privacy of Canadians;

ii) has personnel who are knowledgeable about and comply with the policies and procedures; and

iii) in accordance with its policies, has an effective policy compliance monitoring framework and activities to ensure the integrity of the operational activities is maintained on a routine basis, including appropriately accounting for important decisions and information relating to compliance and the protection of the privacy of Canadians.

VI. METHODOLOGY

The Commissioner's office reviewed relevant CSE records, conducted interviews with CSE employees, and observed demonstrations of various technologies, systems and tools from analysts in order to assess compliance with legal and ministerial requirements, as well as associated policies and procedures. The Commissioner's office also reviewed written responses provided by CSE to questions raised during the course of the review. This included the examination of documents such as CSE policies and procedures,

administrative records, briefing notes to the Chief, and applicable legal opinions or advice from the Department of Justice Canada.

The Commissioner's office examined other issues that arose during the course of the review which were directly relevant to CSE's use of metadata in a SIGINT context. These issues are outlined in this report.

As part of this review, the Commissioner's office received a great deal of information about CSE's SIGINT architecture, and participated in numerous briefings and demonstrations from various groups within SIGINT. As metadata is critical to virtually all of CSE's SIGINT activities in some form or another, conducting an in-depth review of all aspects of SIGINT metadata activities would have required an inordinate amount of time and resources, and it would have been impractical to comprehensively discuss them in a single report.

The approach taken for this review, then, was to acquire a general understanding of the architecture and the interaction between its various components, while focusing in on those areas of greatest importance from a privacy perspective. These areas are discussed in-depth below, and include certain metadata techniques, programs, tools and repositories, as well as certain groups within CSE that use metadata in a SIGINT context. Where appropriate, the Commissioner's office has identified aspects of CSE's work that will likely be of interest to future reviews. A comprehensive chart of SIGINT collection systems, repositories, analysis tools, data sharing platforms, and shared Five Eyes systems is available in Annex D.

VII. BACKGROUND

What is metadata?

In a SIGINT context, '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 which could reveal the purport of a telecommunication, or the whole or any part of its content."[8]

A telecommunication refers to a discrete event between two or more persons, a person and a machine, or between two machines. Telecommunications are transmitted on the Global Information Infrastructure (GII) in accordance with internationally agreed upon network protocols. Metadata is present in every layer of network protocols, can relate to the communicants, the features of a specific communication, or to the network itself.[9]

[8] *Ministerial Directive: Communications Security Establishment Collection and Use of Metadata*, November 21, 2011.
[9] *SIGINT Programs Instruction: Metadata in a SIGINT Context (SPI-2-13)*, effective July 24, 2013.

The following constitute examples of metadata, when associated with a telecommunications event:[10]

- Internet Protocol (IP) address (from and to)
- Time up, time down
- Application identification

[redacted]

Taken in isolation [redacted] an identifier, such as a telephone number or an email address, does not constitute metadata. Similarly, address books or "buddy lists"[11] acquired in the process of conducting FI activities, or acquired through other methods, are not metadata, [redacted]

Any data that describes the [redacted]

Finally, data that relates to the SIGINT source information such as collection program, [redacted] or the [redacted][2], is not metadata in the sense of the MD.

Two broad categories of metadata that are of particular interest are:

- Dialled Number Recognition (DNR) metadata, which generally pertains to telephone or fax communications; and

- Digital Network Intelligence (DNI) metadata, which generally pertains to email, [redacted]

While in the past there may have been a sharp distinction between these two categories, this distinction is continually eroding due to the increasingly complex manner in which communications travel on the GII, as well as the integrated nature of telecommunications devices available to end users. Nevertheless, they remain generally useful, if simplistic, categories.

While metadata does not reveal the content of communications, it nevertheless has the potential to reveal a great deal of information about individuals, including details about

[10] *Ibid.*
[11] According to CSE, buddy lists and/or address books can appear in various contexts on the GII, and may in certain context be considered metadata. Source: CSE Response to RFI 13.3, March 18, 2015

[redacted]

[redacted] As such, it can be of foreign intelligence value in many scenarios, and can correspond to significant privacy considerations in many others.

What is metadata used for?

CSE conducts its metadata activities according to the *MD on the Collection and Use of Metadata*, which specifies that metadata 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 (i.e., where one end of the communication is in Canada) strictly where a duly issued Ministerial Authorization is in effect, and in strict compliance with that Ministerial Authorization; and

c) Monitoring or identifying patterns of foreign malicious cyber activities to provide indications and warnings of actual or potential cyber intrusion directed against infrastructures of importance to the Government of Canada (GC).

Network Analysis and Prioritization

Network Analysis and Prioritization activities seek to identify and characterize telecommunication links of most value to meet GC foreign intelligence priorities, and include the following, in accordance with the MD:

- the identification of [redacted]
- the determination of the [redacted]
- the determination of the [redacted]

[redacted]

While some of the information that CSE acquires regarding telecommunications networks is derived from metadata, some of it is also acquired from other sources, including [redacted] human intelligence (HUMINT), and open source information.

Network Analysis and Prioritization activities are not covered in this report, but will be examined as part of the follow-up review of issues identified in the Commissioner's 2014 report entitled *A Review of CSE's Office of Counter-Terrorism*.

Contact Chaining

Contact chaining, which will be described in greater detail below, refers to the analysis of communications activities or patterns, using metadata, in order to build a profile of communications contacts of entities of foreign intelligence interest. Samples of contact chains [redacted] will be examined as part of the follow-up review of issues identified in the Commissioner's 2014 report entitled *A Review of CSE's Office of Counter-Terrorism.*[13]

Identifying New Targets

New targets may be identified through a variety of analytical techniques beyond contact chaining, including [redacted]

Monitoring or Identifying Patterns of Foreign Malicious Cyber Activities

Using metadata collected by the SIGINT system, CSE's [redacted] team is responsible for discovering, [redacted] cyber actors that pose a threat to Canada and its allies. While this is one of the usages of metadata provided for in the MD, it is beyond the scope of this report. However, the Commissioner's office will examine it in a subsequent study of Information Sharing between SIGINT and IT Security, and a review of CSE's use of metadata in an IT Security context.

How does CSE collect metadata?

Metadata is collected by the SIGINT program under the authority of paragraph 273.64(1)(a) of the *NDA*. In accordance with the MD, CSE may acquire what is known as "bulk" or "unselected" metadata at all SIGINT collection apertures for all telecommunications events.[14] Because this metadata is acquired without having gone through a targeting-selection process, it may include information that pertains to telecommunications events of which both ends are located in Canada. According to CSE, collection occurs only on telecommunications links known to have one end physically located outside of Canada. This approach greatly reduces the risk of incidental collection of two-end Canadian metadata events; however, the complexities of global routing and telecommunications infrastructure make it impossible to guarantee that only foreign

Solicitor-Client Privilege

[14] CSE uses the terms "unselected metadata" and "bulk metadata" interchangeably. These terms refer to metadata that is collected or shared without having gone through a targeting-selection process which ensures that at least one end of the associated communication is foreign and is related to a foreign intelligence priority of the Government of Canada.

ended traffic will be encountered.[18] Unselected metadata is held in a consolidated metadata repository called [redacted]

CSE also acquires metadata associated with selected traffic as a result of targeting activities. This metadata is stored with the content in the consolidated traffic repository (CTR) and a copy of this metadata is also held in [redacted] According to CSE, the volume of metadata [redacted]

While the SIGINT collection system does parse metadata for distinct telecommunications events, it may not always automatically extract all metadata contained in a given event. Some metadata may be [redacted]

[redacted]

Where is metadata stored?

Metadata used by CSE is stored in a variety of databases and repositories, [redacted] directly accessible by CSE analysts. The most commonly accessed repositories include [redacted] and [redacted] which are described in greater detail below, but many others exist in addition to these. A number of tools also exist to access, organize and manipulate data stored in these repositories, in order to enable a number of analytic techniques and tradecrafts.

According to the MD, the maximum retention period for SIGINT metadata collected by CSE is [redacted] unless CSE requests and the Minister of National Defence decides on reasonable grounds that a longer retention period is warranted to fulfill operational

[18] CSE Response to RFI 11.1 (March 4, 2015). CSE's response also notes that "metadata events may be observed to carry [redacted]

[redacted]

requirements.[17]

How is metadata accessed?

Metadata may be accessed only by individuals working within the SIGINT Production Chain, who have an operational requirement to do so. The main tool available to analysts for leveraging metadata is which is the user interface for accessing data held in the repository. acts as the gateway for SIGINT metadata,

Data in some of which include:

- Contact Chaining

The

How is metadata shared?

metadata may be shared with allied agencies, in accordance with international arrangements, provided any Canadian Identifying Information (CII)[18] is minimized (anonymized), in accordance with the MD. CSE shares minimized DNR metadata acquired at its SIGINT collection programs with Second Parties

CSE does not share DNI metadata Further to queries submitted DNI metadata DNI metadata

[17] *Ministerial Directive: Communications Security Establishment Collection and Use of Metadata*, November 21, 2011.

[18] According to *OPS-1 Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities* (December 1, 2012), CII refers to "information that may be used to identify a Canadian person, organization, or corporation, including, but not limited to, names, phone numbers, email addresses, IP addresses and passport numbers."

[redacted]

What measures are in place to protect the privacy of Canadians in CSE's use of metadata?

Access to metadata is subject to controls and permissions depending on the repositories and tools involved. For certain tools, [redacted]

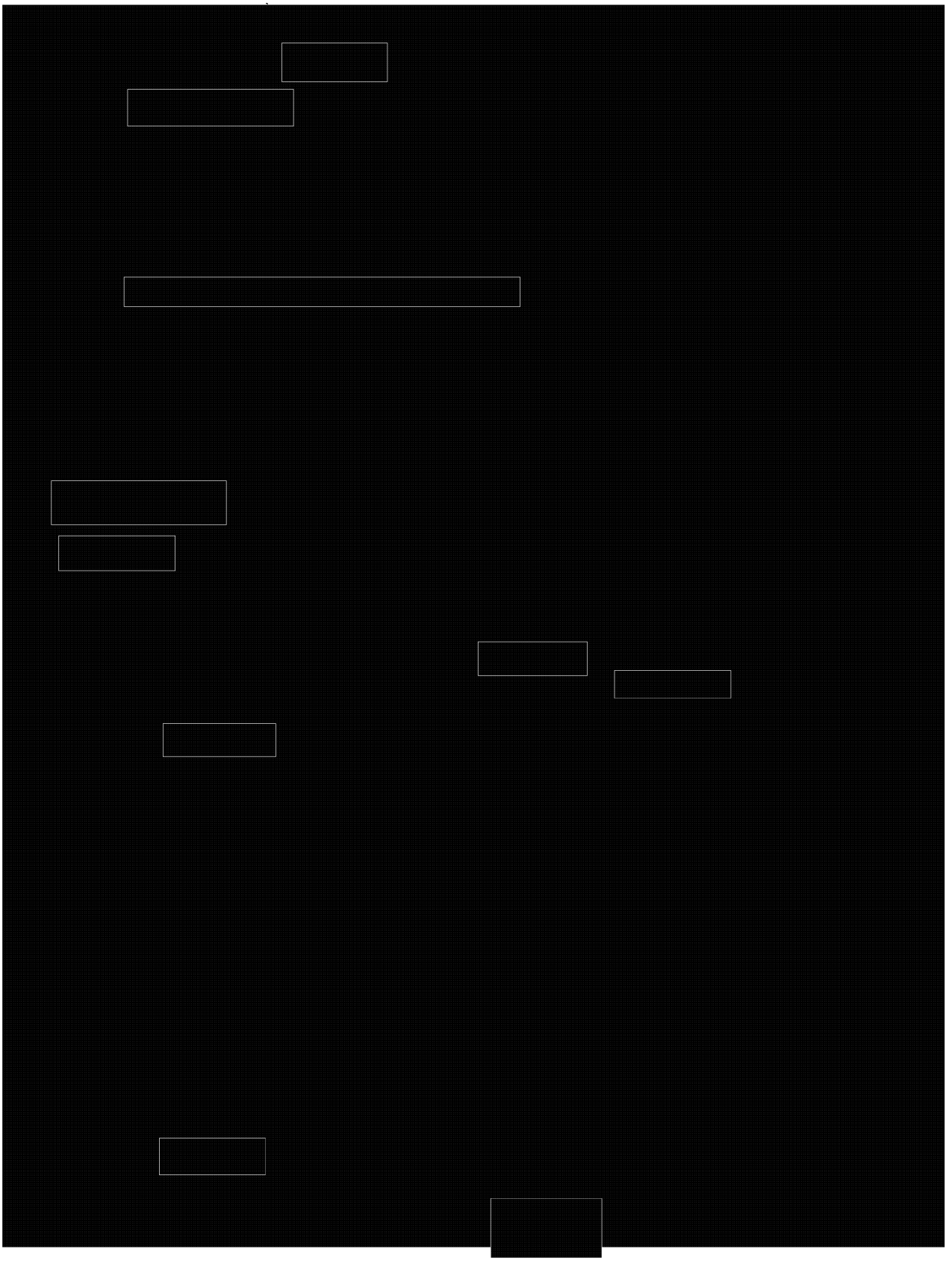
Furthermore, the MD prohibits the granting of access to Canada's allies to metadata known to be associated with Canadians or persons located in Canada, unless it is altered in such a way as to render the identification of those persons impossible. The MD also stipulates that metadata known to be associated with Canadians anywhere or any person in Canada must be suppressed when contained in CSE reports. Finally, the MD also imposes an obligation on CSE to destroy metadata acquired in a SIGINT context no later than [redacted] after its acquisition, unless the Minister of National Defence decides on reasonable grounds that a longer retention period is warranted to fulfill operational requirements.

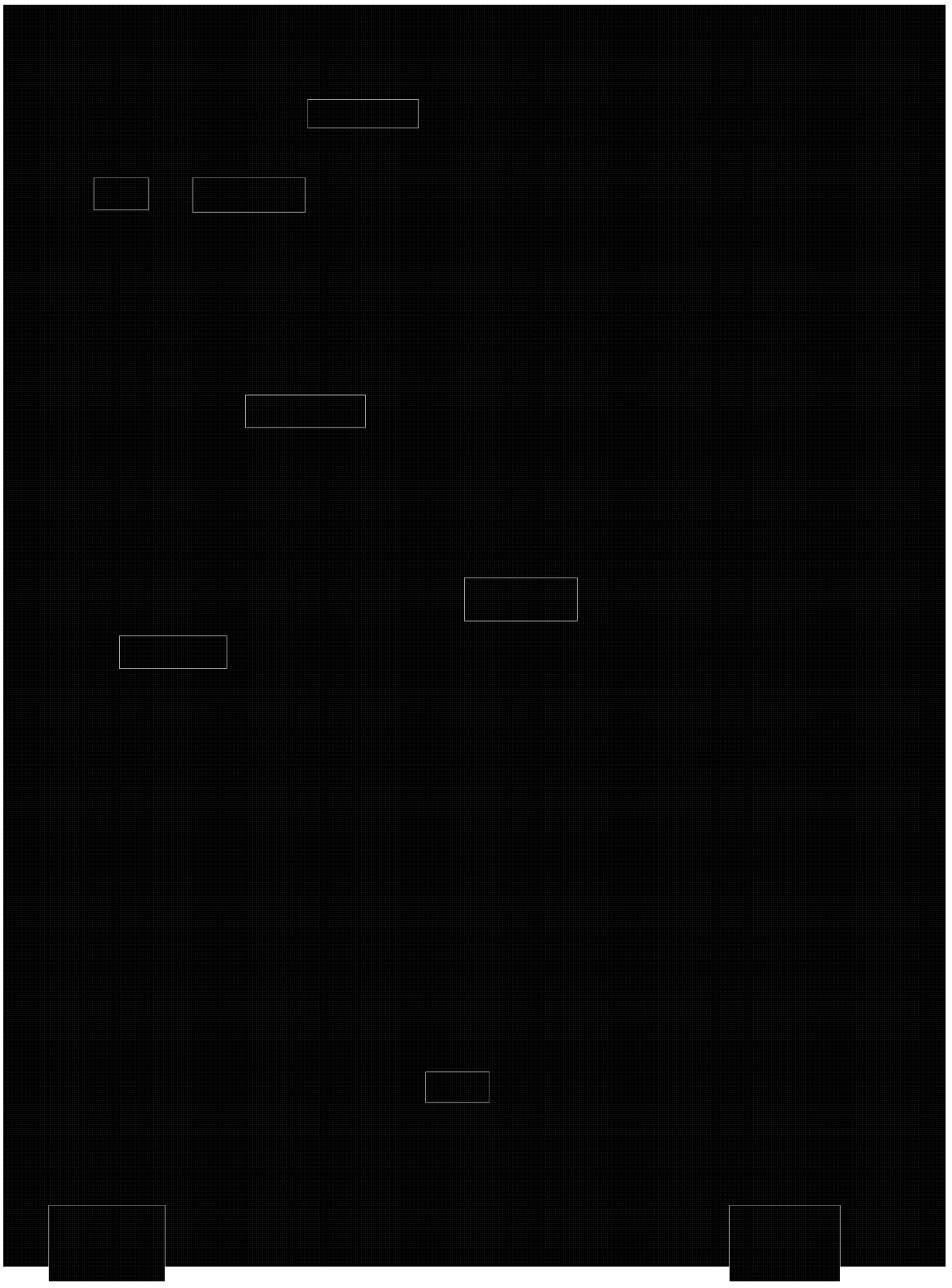
[redacted]

The [redacted] resides within CSE's [redacted]

- [redacted]

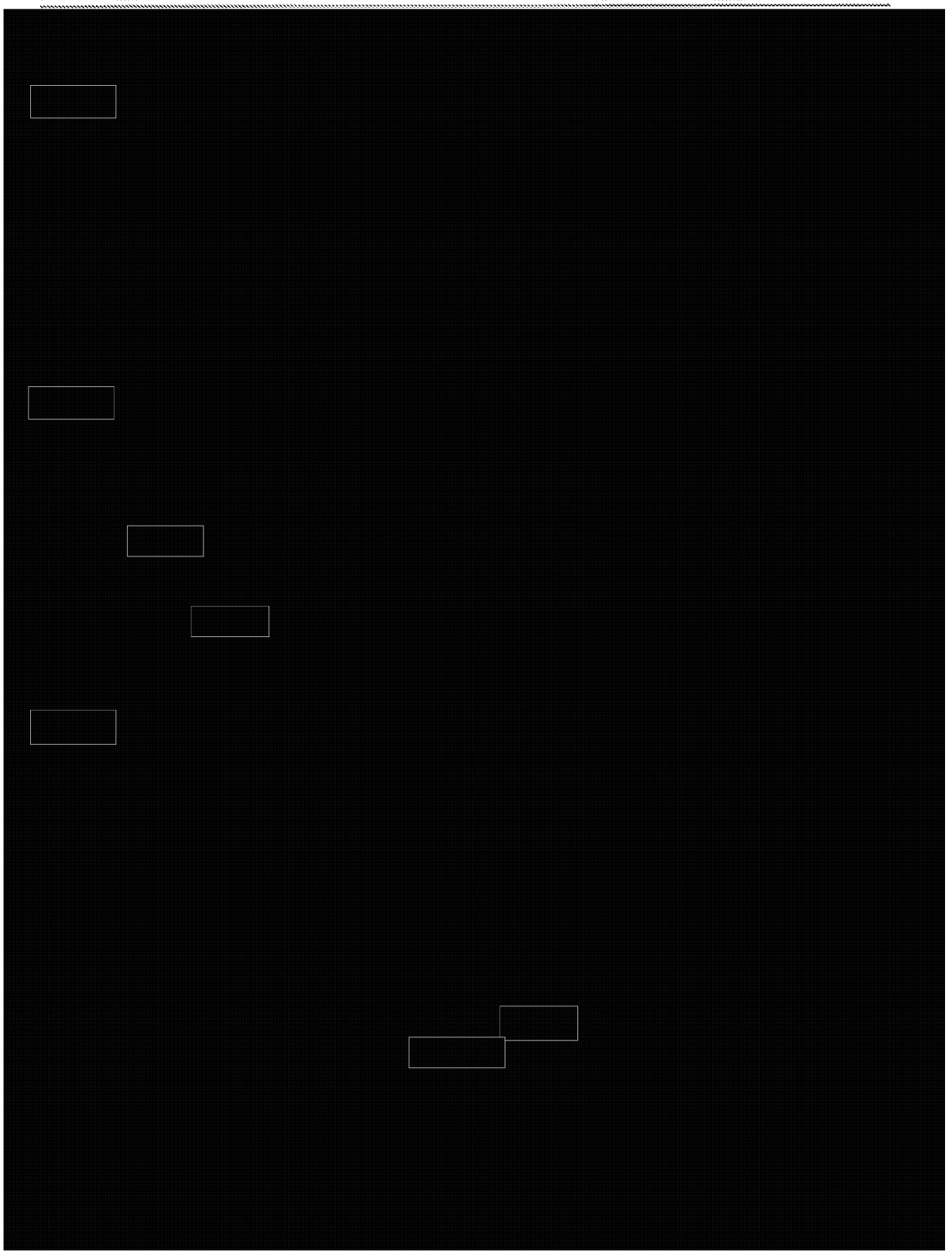
[redacted]





[redacted]

IRRELEVANT



Contact Chaining

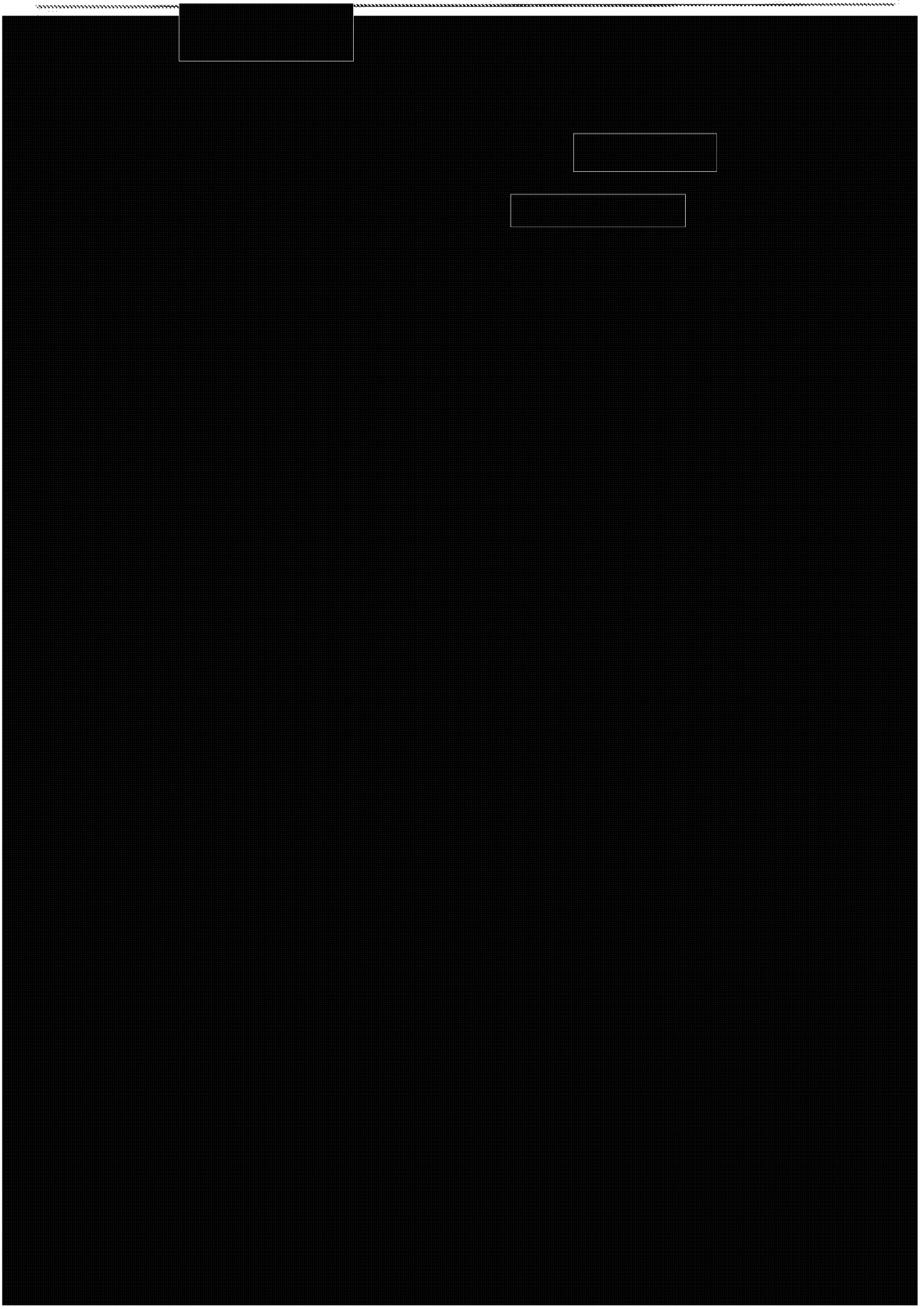
The 2011 Metadata MD defines contact chaining as:

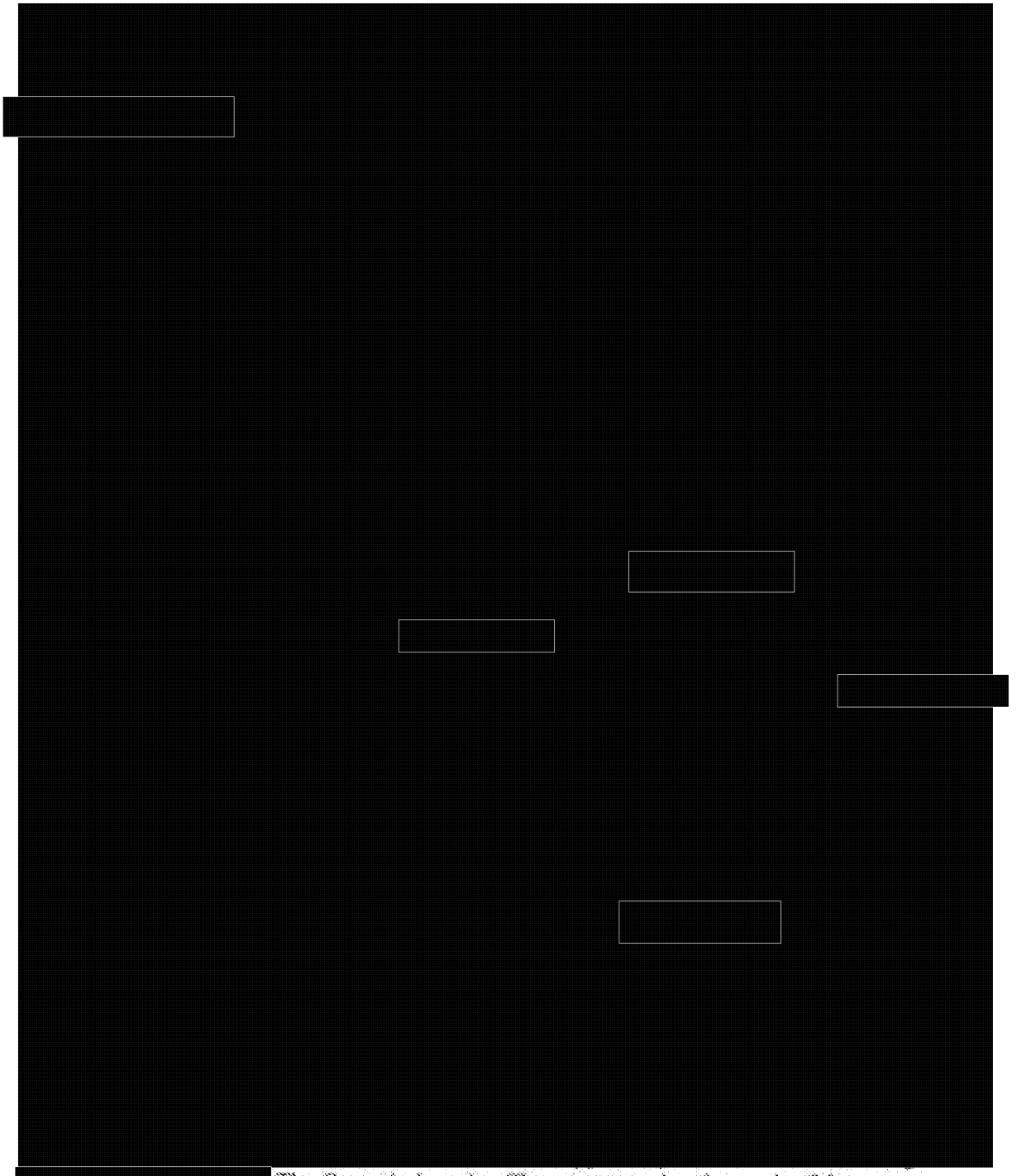
"The method developed to enable the analysis, from information derived from metadata, of communications activities or patterns to build a profile of communications contacts of various foreign entities of interest in relation to the foreign intelligence priorities of the Government of Canada, including 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 foreign entities and their networks."

OPS-1, Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities, provides that, in accordance with the *MD on Collection and Use of Metadata*, CSE may search metadata 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 entity as they relate to international affairs, defence or security. Contact chaining is one technique that SIGINT analysts use to identify and document the communications activities or patterns of entities of potential foreign intelligence interest.

As part of the research phase of this review, the Commissioner's office received an in-depth briefing on contact chaining, as well as a demonstration of how it takes place using various CSE [redacted]

[23] For a detailed description of [redacted] see *OCSEC Review of the Ministerial Directive, Communications Security Establishment, Collection and Use of Metadata, March 9, 2005* (2008).



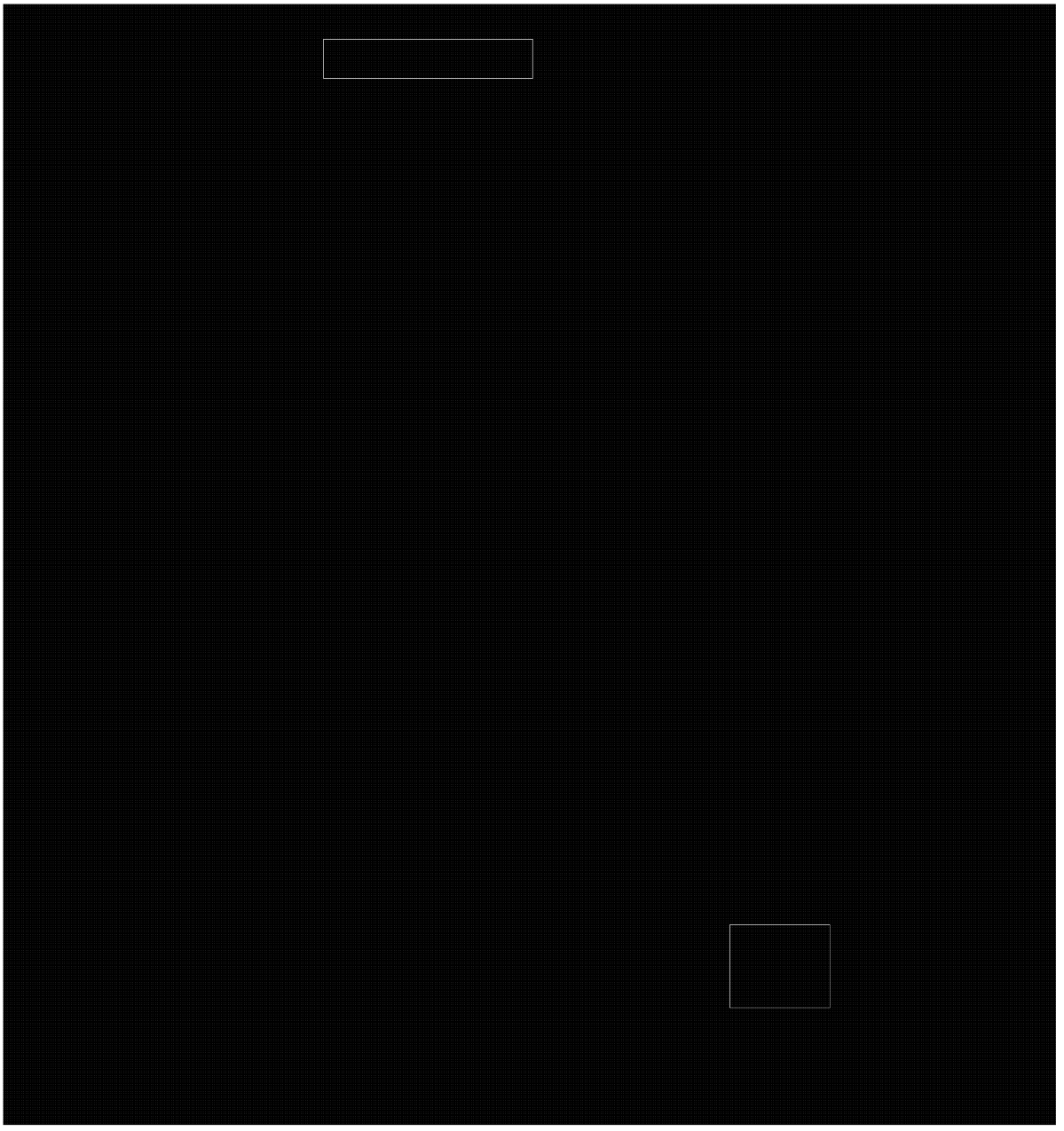


The Commissioner's office may examine the work of the team in greater detail as part of future reviews.

[redacted]

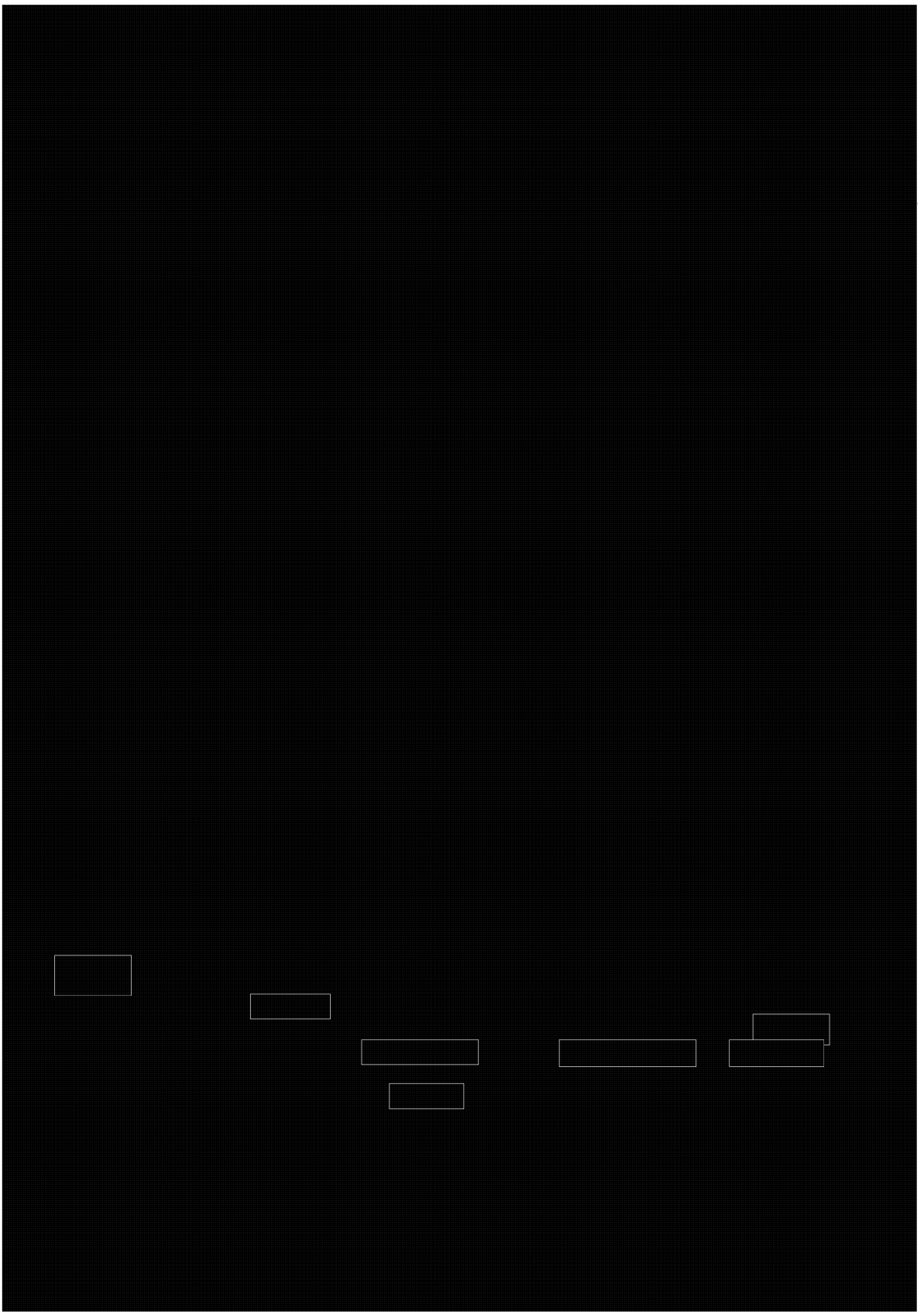
CSE provided the Commissioner's office with a briefing on [redacted] during the research phase of this review. [redacted] This was done in order to update the Commissioner's office's general knowledge and inform future reviews.

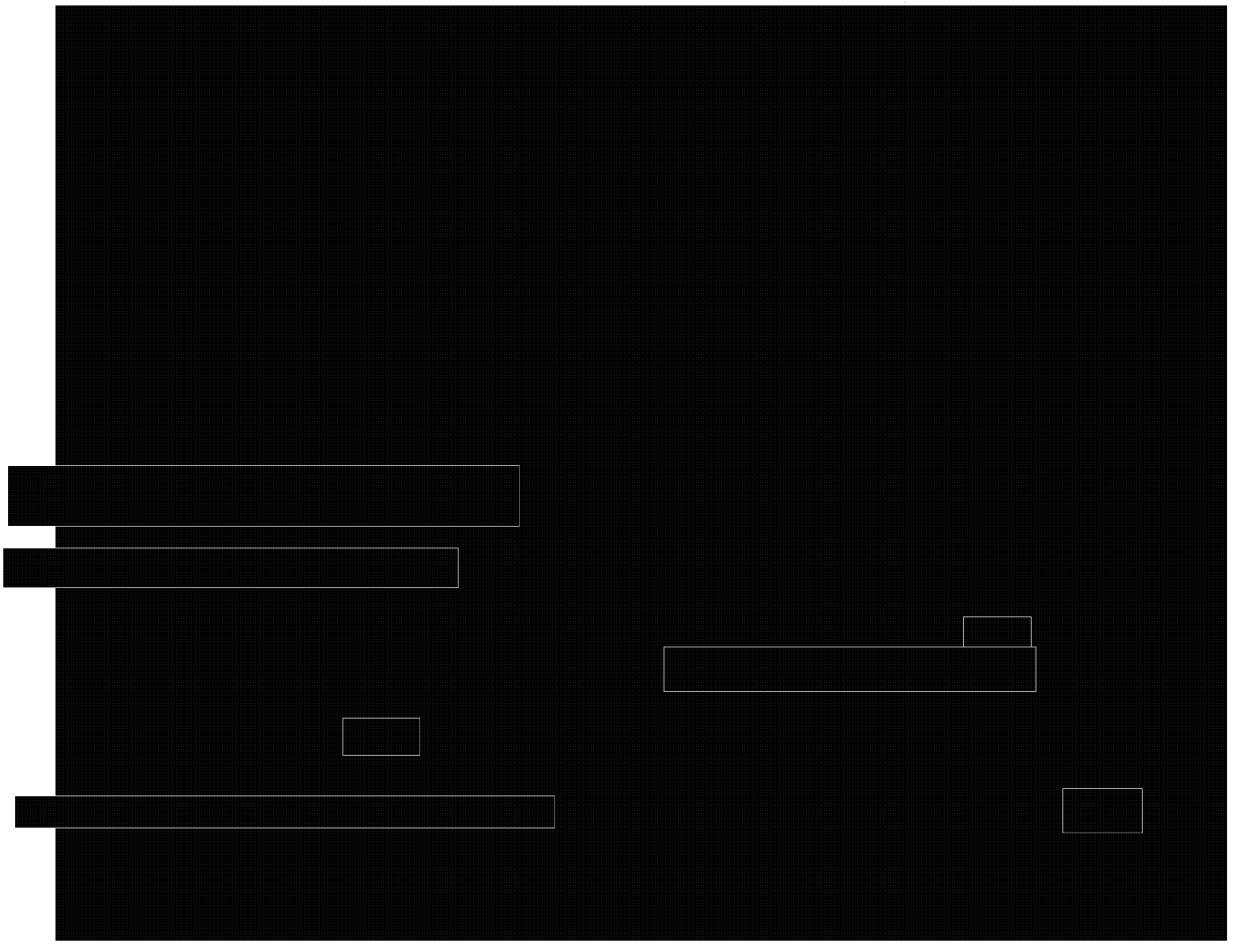
[redacted]



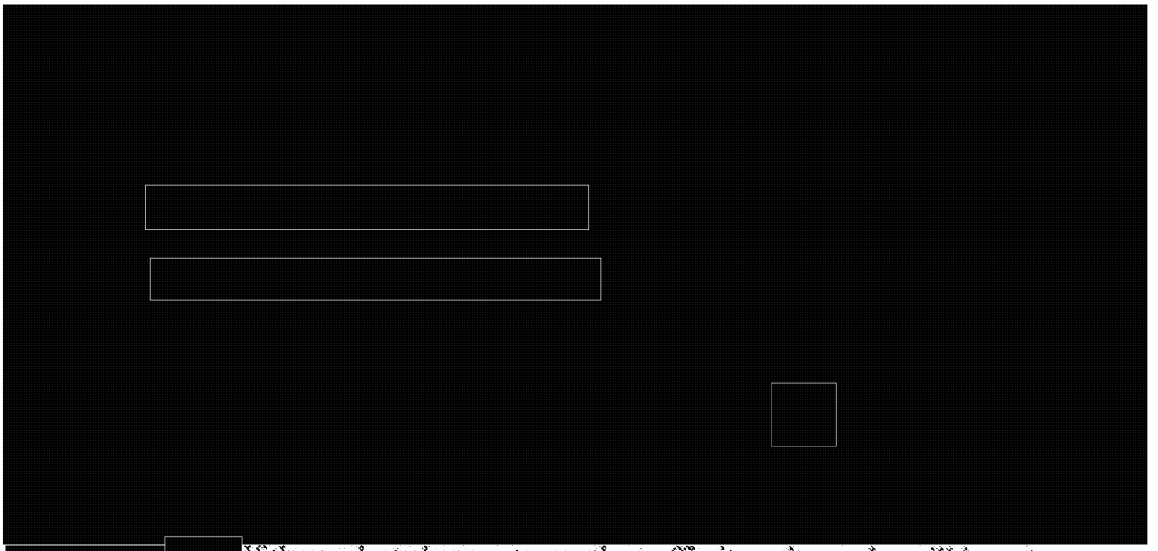
[22] The OPS-1 quiz is designed to test analysts' knowledge of policies and procedures that are in place to protect the privacy of Canadians and to ensure that CSE is legally compliant in its activities. Passing the quiz is meant to demonstrate that analysts understand and are able to apply these policies and procedures in the course of their day-to-day activities. For more information on the OPS-1 quiz, see the Commissioner's *Study of Communications Security Establishment Canada's Policy Compliance Monitoring Framework and Activities* (2014).

[23] According to long-standing conventions, the Five Eyes do not target one another's nationals, and therefore CSE's activities must not be directed at Second Party nationals located anywhere, or against anyone located in a Second Party's territory. However, in certain cases, information that would seem to be associated with a Canadian, such as an email address of the form ABC@Canada.ca, can in fact be associated with a foreign national located outside Canada. For reasons such as this, CSE analysts may choose to include Canadian or Five Eyes results in their queries.





Examples of analytics that [redacted] can run were demonstrated to the Commissioner's office, and include:



[redacted] If the analyst chooses to use the traffic item, he or she will have to

annotate it as a private communication having foreign intelligence value, if it has not already been annotated as such.

A deliberate effort was made to build privacy protections into the system from the beginning, rather than simply integrating them in as the system evolved. As a result, [redacted] was developed from an early stage in consultation with SPOC. Among the safeguards built into [redacted] is the fact that the program keeps a record of where result sets are saved when analysts receive them. While each individual analyst has a responsibility to annotate, store and eventually purge the data, this central record allows for auditing of such activity. It also tracks when and where an analyst accesses files, as well as when results have expired. Using this record, SPOC has the ability to send purge requests to analysts when information has been stored for longer than is operationally necessary. According to CSE, purge requests affecting [redacted] results have occurred approximately [redacted]

The Commissioner's office considers it a positive development that SPOC was involved in shaping [redacted] from its nascent stages, and encourages this practice as future systems emerge. It is also positive that SPOC provides direct oversight of the data result sets, to ensure that they are only kept for as long as operationally necessary. As [redacted] is primarily content-oriented and has the potential to implicate Canadian privacy, the Commissioner's office may examine it in more detail in the future.

[redacted]

Like [redacted] has been developed in consultation with SPOC from the beginning, as well as other interested counterparts (i.e. system owners) within CSE. [redacted] The Commissioner's office may examine these developments in more detail in the future.

VIII. FINDINGS

Finding no. 1: CSE was forthcoming with information and assistance, both proactively and in response to specific requests of the Commissioner's office.

The high profile of metadata activities by intelligence agencies in the wake of a series of unauthorized disclosures by Edward Snowden placed unique demands on both CSE and the Commissioner's office throughout this review. While the review was planned prior to the Snowden disclosures, after the disclosures, certain aspects of CSE's metadata activities became the subject of national and international media stories. CSE had to respond to increased media attention and Access to Information requests, as well as requests from the Commissioner's office regarding several facets of its SIGINT metadata activities. CSE recognized the importance of responding to requests of the Commissioner's office in a timely fashion. In addition, CSE proactively informed the Commissioner's office of incidents that it discovered during the review, which led to further in-depth investigation. These incidents will be discussed in further detail below.

Finding no. 2: Metadata collection and analysis has evolved considerably since the Commissioner's last in-depth review of metadata activities, and metadata remains critical to all aspects of CSE's SIGINT mission.

As CSE's collection posture has strengthened, particularly through the expansion of [redacted] activities, the volume of metadata collected by CSE has increased considerably.[26] Furthermore, technological developments have resulted in more methods for exploiting metadata for foreign intelligence purposes, and have led to a diverse set of new tools and systems, several of which were highlighted in the background section.[27]

Because CSE collects more metadata than it did during the time period covered by the previous in-depth review, it also shares more metadata, and in more ways. For example, since 2009, in addition to [redacted] DNR metadata, CSE has shared DNI metadata with Second Parties on a daily basis through an automatic, query-based mechanism, which will be described in more detail below. Additionally, as described in the background section, [redacted] to effectively [redacted] the metadata that is shared.

As the collection and analysis of metadata by CSE and its partners continues to evolve, it will be important for the Commissioner's office to remain engaged so as to understand changes to CSE's processes and their potential corresponding impact on the privacy of Canadians and compliance with the law.

---

[26] For more information about SIGINT collection volumes and the expansion of [redacted] see the *Annual Combined Review of Foreign Signals Intelligence Ministerial Authorizations and Intercepted Private Communications, 2012-2013* (March 31, 2014).

[27] See Annex D for a graphic outlining CSE's metadata repositories that are used in the SIGINT context.

Finding no. 3: The Canadian legal landscape has changed since the Commissioner's office last conducted an in-depth review of CSE's collection and use of metadata.

In an overview briefing provided to the Commissioner's office, CSE cited three foundational legal opinions that it relied on for guidance and advice Solicitor-Client Privilege

Solicitor-Client Privilege

The Commissioner's office asked CSE officials whether any of the foundational legal opinions had been updated since their original issuance, whether CSE had sought or received any legal opinions related to Solicitor-Client Privilege

Solicitor-Client Privilege

CSE continues to rely on the foundational legal advice that it received from Justice Canada in its original form. While CSE has not received further advice pertaining to

Solicitor-Client Privilege

In recent months, there have been further legal developments in Canada that could have implications for CSE's metadata activities. Two recent decisions of the Supreme Court of Canada are particularly notable in this regard: decisions in *Wakeling*[31] and *Spencer*[32]:

- In *Wakeling v. USA*, the main issue raised by this appeal was whether federal legislation authorizing the sharing of lawfully obtained wiretap information between Canadian and foreign law enforcement agencies is constitutional. Section 8 of the *Canadian Charter of Rights and Freedoms* (*Charter*) protects wiretap targets at both the interception and disclosure stages. A disclosure will be reasonable under section 8 of the *Charter* if it passes a three-part test. First, the disclosure has to be authorized by law, hence carried out in accordance with the procedural and substantive requirements the law provides. Second, the law authorizing the disclosure must be a reasonable law, which is not overbroad, vague or unconstitutional because of a lack of accountability mechanism. The disclosure must also be carried out in a reasonable manner, and therefore must have accountability and transparency mechanisms. At the third step, although not constitutionally mandated in each case, adherence to international protocols and the use of caveats or information-sharing agreements may be relevant to assess whether the disclosure was carried out in a reasonable manner.

- In *R. v. Spencer*, the Supreme Court ruled on a person's reasonable expectation of privacy within the context of the use of the Internet. The specific case dealt with the police obtaining subscriber information associated with an IP address from the internet service provider (ISP), without prior judicial authorization. The Court analyzed, among other things, whether the police obtaining the accused's subscriber information matching the IP address constituted a search, and whether this search was authorized by law. The Court stated what was particularly important in the context of Internet usage is the understanding of privacy as anonymity. The identity of a person linked to their use of the Internet must be recognized as giving rise to a privacy interest beyond that inherent to the person's subscriber information. Some degree of anonymity is a feature of much Internet activity and, depending on the totality of the circumstances, anonymity may be the foundation of a privacy interest that engages constitutional protection against section 8 of the *Charter*. In the case of *Spencer*, the police request to link a given IP address to subscriber information was in effect a request to link a specific person to specific online activities. This sort of request engages the anonymity aspect of the informational privacy interest by attempting to link the suspect with anonymously undertaken online activities, activities which have been recognized in other circumstances as engaging significant privacy interests.

The Commissioner's office will continue to monitor how CSE responds to technological developments and the privacy implications thereof, as well as developments in the legal landscape that could impact its collection, use and disclosure of metadata.[33]

---

[31] *Wakeling v. United States of America*, 2014 SCC 72.
[32] *R. v. Spencer*, 2014 SCC 43.

Ministerial Directive

Finding no. 4: The 2011 Ministerial Directive on Collection and Use of Metadata lacks clarity regarding the sharing of certain types of metadata with Second Parties, as well as other aspects of CSE's metadata activities.

The 2011 *Ministerial Directive on the Collection and Use of Metadata* updates the original MD of the same name, which was issued in 2005. The main difference in the 2011 document is that paragraphs 7(3) and 7(4) stipulate that IT Security cyber defence personnel may access unaltered metadata in CSE's bulk metadata repositories, for the purpose of helping to protect information infrastructures of importance to the Government of Canada.[34]

Beyond this, the MD includes several minor linguistic changes that add clarity to the text. Despite these changes, however, the 2011 MD lacks clarity regarding key aspects of CSE's collection, use and disclosure of metadata in a SIGINT context. The following are ambiguities and apparent discrepancies that the Commissioner's office identified in reviewing the MD. While CSE may disagree with some of the issues raised below, they may nevertheless be considered should CSE seek an updated MD.

First, the MD does not define what is meant by "bulk metadata"[35] and does not differentiate between the concept of "collecting" metadata and the concept of "acquiring" metadata. It is unclear whether these concepts are synonymous or whether they refer to distinct processes.

Furthermore, the MD does not reflect the fact that CSE shares DNI metadata with Second Parties through a query-based system, [redacted]. The original 2005 Metadata MD included paragraph 7(5) on the minimization of [redacted] metadata. CSE only started sharing DNI metadata in 2009 because it was incapable of minimizing the CII contained within it prior to that time.[36] The Metadata MD was revised in 2011 and still contains the same paragraph 7(5). This condition on minimization, which clearly applies

Solicitor-Client Privilege

[34] Paragraph 7(3) extends access to unaltered metadata to IT Security cyber defence personnel, as set out in paragraph 7(4), which states "To the extent that metadata containing Canadian identifying information is relevant to the protection of electronic information or information infrastructures of importance to the Government of Canada, this unaltered metadata may be disclosed to IT Security cyber defence personnel for the purpose of helping to protect information infrastructures of importance to the Government of Canada. Any use or retention of this metadata by IT Security cyber defence personnel for the purposes set out in paragraph 273.64(1)(b) will continue to be handled in accordance with existing policy and procedures related to the protection of the privacy of Canadians." The 2011 Ministerial Directive is attached at Annex C.

[35] Paragraph 7(3), *Ministerial Directive: Communications Security Establishment Collection and Use of Metadata*, December 16, 2011.

[36] Further information regarding the sharing and minimization of DNI metadata can be found on page 39.

to the sharing of DNR metadata, does not accurately reflect CSE's current practice of sharing DNI based on queries from Second Party partners.

CSE relies on policy relating to the targeting of communications for guidance on the sharing of DNI metadata with Second Parties. For example, according to OPS-1, prior to targeting selectors in order to intercept communications, CSE is required to validate those selectors to ensure that they are directed at foreign entities outside of Canada, and that they are consistent with GC intelligence priorities.[37] CSE informed the Commissioner's office that it also relied on this process to guide the sharing of DNI metadata with Second Parties. While these conditions are outlined in CSE policy for targeting purposes, there is no analogous policy instrument for the sharing of DNI metadata based on queries from partners. These conditions are also not reflected in the MD.

In addition, paragraph 8 of the MD provides that metadata acquired as part of CSE's foreign intelligence acquisition programs shall be used strictly for:

- network analysis and prioritization;
- contact chaining;
- identifying new targets and selectors; and,
- monitoring or identifying patterns of foreign malicious cyber activities.

The MD does not mention or provide any specific guidance related to [redacted] activities, which rely on metadata collected by CSE and its allies. [redacted] does not explicitly or entirely fit into any of the categories listed above. For example, unlike network analysis and prioritization [redacted]

Finally, paragraph 5 of the MD states: "In the fulfilment of its mandate as set out in paragraph 273.64(1)(a) of the *National Defence Act*, CSE may *search any metadata* acquired in the execution of its foreign intelligence acquisition programs[40] 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,

[37] This is outlined in section 2.6 of *OPS-1 Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities* (Effective 1 December 2012). For more information on how CSE validates selectors submitted by Second Parties, see *A Review of CSEC SIGINT's Targeting and Selector Management Activities* (March 15, 2011), pp. 41-43).

[38] See the definition of "Network Analysis and Prioritization" in the *Ministerial Directive: Communications Security Establishment Collection and Use of Metadata*, November 21, 2011.

[39] CSE Briefing on Target [redacted] June 20, 2014.

[40] While CSE notes that there is a distinction between the pool of metadata that may be searched and the manner in which it is to be searched, the Ministerial Directive is unclear in this regard.

as they relate to international affairs, defence or security, including any information relevant to the protection of electronic information or information infrastructures of importance to the Government of Canada" (emphasis added).[41]

As discussed above, in light of the Solicitor-Client Privilege

Solicitor-Client Privilege

Recommendation no. 1: CSE should seek an updated Ministerial Directive that provides clear guidance related to the collection, use and disclosure of metadata.

IP Profiling Analytics

Finding no. 5: CSE's IP Profiling Analytics tradecraft, which was the subject of an unauthorized disclosure, was authorized under 273.64(1)(a) of the NDA, and CSE took measures to protect the privacy of Canadians in undertaking this activity.

In January 2014, while this review was being undertaken, the Canadian Broadcasting Corporation ran a news story on its website relating to a classified CSE slide presentation to Five Eyes partners entitled *IP Profiling Analytics and Mission Impacts*. The presentation, one of several unauthorized disclosures emanating from material taken from NSA systems by Edward Snowden, was originally created in May 2012. Since the article discussed an activity undertaken by CSE that involved Canadian metadata, the Commissioner's office decided that it would be in the public interest to investigate this matter further as part of the ongoing review of CSE's use of metadata in a SIGINT context.

CSE briefed the Commissioner's office on the presentation shortly after the story was published, and the Commissioner released a public statement indicating that he was aware of the activities referred to in the story. The Commissioner's office then held several follow-up meetings with senior CSE officials, including the analyst who created the presentation and the tradecraft discussed within it. CSE explained the activity, showed results of the activity described in the presentation in great detail, and responded to numerous specific questions asked by the Commissioner's office.

[41] *Ministerial Directive: Communications Security Establishment Collection and Use of Metadata*, December 16, 2011.

The *IP Profiling Analytics and Mission Impacts* presentation was prepared for a SIGINT Development (SIGDEV) Conference, [redacted] The CSE analyst presented a tradecraft/technique that was developed through work in CSE's [redacted] The analyst did not present on the specific information discovered by applying the technique, or the data used for the technique, but on the technique itself.

IP profiling analytics falls under the broad category of Network Analysis and Prioritization (NAP). NAP is conducted under CSE authorities granted by paragraph 273.64(1)(a) of the *NDA* (part (a) of CSE's mandate) and guided by the 2011 Metadata MD. The aim of NAP is to identify and characterize telecommunications links of most value to meet Government of Canada foreign intelligence priorities. Prioritization activities include: [redacted] CSE shared with the Commissioner's office the guidance that had been provided to CSE personnel concerning this activity. This guidance has also been incorporated into a SIGINT Programs Instruction (SPI-2-14) document entitled *SIGINT* [redacted] *Data*, dated March 20, 2014.

IP profiling relies on metadata pertaining to telecommunications events. Metadata collected by CSE that is associated with telecommunications events is forwarded to a repository called [redacted]

The *IP Profiling Analytics and Mission Impacts* presentation describes tradecraft developed by a [redacted] analyst in order to supplement IP look-up information found in commercial databases that CSE purchases from private companies. While generally reliable, these commercial databases nevertheless contain some outdated, vague or inaccurate information. In addition to supplementing commercial look-up information using metadata and infrastructure data, the analyst wanted to use IP profiling to support real-time SIGINT alerting objectives.

The analyst used a metadata sample of all online events [redacted] for the period of March 16-29, 2011. This data is no longer accessible, but CSE estimates that it amounted to data for [redacted] of online events. This includes both [redacted]

[92] *SIGINT Programs Instruction, SIGINT* [redacted] *Data (SPI-2-14)*, Effective March 20, 2014.

[redacted] By observing the number of identifiers that show a presence at an IP address, and the length of time of that presence, the analyst could determine the function of that IP address. For example, hotels would have many identifiers present for a number of days, while airports would have many identifiers present for a brief period of time. Identifiers used at these addresses could also be followed forward in time to discover the IP addresses of other airports, for example. In this way, CSE could supplement IP address information available in commercial look-up databases with information from SIGINT.

The analytic on IP profiles is now generally available to CSE analysts. In order to use the analytic in a query, analysts enter a network IP address or range of addresses in the [redacted]tool. The search results return profiles, which are visually represented as different types of graphs, providing information about the function of the IP address, as well as volume of user activity over a period of time. In addition, it is envisioned that IP profiling could also be used to provide automatic alerts when CSE targets connect to IP addresses of interest, such as major airports or hotels. The operationalized analytics do not reveal any identifying information. When an analyst inputs an IP address or range, the graphs which are returned display aggregate traffic patterns without attaching any identifying information. Safeguards are also in place to ensure that data cannot be "reverse engineered" and users do not receive the background data that goes into making the graph. Finally, analysts can only enter specific characters (e.g. digits and periods representing the IP address) into the search field in order to query the tool.
According to CSE, very large traffic volumes are required to develop reliable pattern recognition analytics. CSE's collection of online event metadata is dependent upon the telecommunications networks that are available for metadata extraction. Prior to the expansion of CSE's [redacted] collection program, the online event metadata set had some gaps that hindered the reliability of IP profiling activities. Expansion of this collection program has helped to enlarge CSE's data set in this regard. Because of this, and because of the difficulty of obtaining such volumes of data abroad, foreign locations have not been used as the "seed" or point of origin for SIGINT development activities in the area of IP profiling.

Minimization of DNR and DNI Metadata

During the course of this review, CSE informed the Commissioner's office of problems it discovered in the application of minimization scripts to both DNR and DNI metadata shared with Five Eyes partners. These problems affected a number of collection systems and led CSE to suspend, in March/April 2014, the sharing of both DNR and DNI metadata with Second Parties. Such sharing remains suspended. CSE is designing new minimization software and reorganizing business practices in response to these issues. CSE has kept the Commissioner's office informed of developments in this regard and continues to be cooperative on all facets of this review. Findings related to these minimization issues are outlined in further detail below.

Dialled Number Recognition Metadata

Finding no. 6: During the course of the review, CSE discovered that [redacted] DNR metadata being shared with Five Eyes partners was not being minimized properly, contrary to the Ministerial Directive and to operational policy.

[redacted]

DNR metadata collection involves [redacted] However, prior to sending [redacted] DNR metadata [redacted] CSE is required to take measures to protect the privacy of Canadians, as specified in paragraph 273.64(2)(b) of the *NDA*, and as further outlined in the Metadata MD. The

[43] See Annex F for a copy of the [redacted]

[44] *Deficiencies in the Minimization of DNR Metadata Shared with Second Parties – Statement of Facts* (CSE, 4 February 2015).

minimization of Canadian Identity Information (CII) [45] in [redacted] metadata is one of these measures, and arguably the most important one in the context of sharing metadata with partners. The MD specifically states that CSE is required to minimize CII prior to sharing [redacted] metadata with allies. Minimization is the process by which CII contained in [redacted] metadata is altered in such a way that it is rendered unidentifiable prior to sharing with Second Party partners. Any metadata fields that could be analyzed and correlated with other information to identify a Canadian (e.g. phone numbers) are considered to be CII.[46]

CSE provided the Commissioner's office with a copy of the 2008 *Review of Minimization Procedures for* [redacted] [47] which sets out requirements for DNR metadata minimization, and includes a list of [redacted] fields as potentially containing CII. [redacted]

CSE applies minimization scripts to all DNR metadata from all SIGINT collection programs. Since each program is directed at distinct telecommunications [redacted] Furthermore, according to CSE, the [redacted] fields identified as requiring minimization do not all occur [redacted] in all DNR metadata records; some fields are nearly always populated, while others may not be.

Problems with DNR Minimization

In late 2013, CSE discovered anomalies in the minimization of DNR metadata shared with Second Parties. Investigation of these anomalies led to the identification of

[45] Identity information means information about an identifiable individual, such as any number, symbol or other data uniquely assigned to an individual. In a SIGINT context, this usually includes phone numbers, email addresses, names, nicknames, etc.
[46] *Deficiencies in the Minimization of DNR Metadata Shared with Second Parties – Statement of Facts* (CSE, 4 February 2015).
[47] According to CSE, the *Review of Minimization Procedures for* [redacted]

minimization deficiencies for various [redacted],[48] CSE provided the Commissioner's office with the following table, which summarizes the chronology of events[49]:

November 2013	[redacted]
December 2013	
January 2014	
February 2014	
March 2014	

Analysis of some of the minimization scripts for DNR metadata determined that only two (2) of the [redacted] fields identified for minimization were consistently addressed by the scripts: [redacted]

According to CSE, all minimization scripts for DNR metadata that were examined were found to have contained deficiencies. All of the scripts were successfully minimizing a subset of metadata fields, usually the equivalent to [redacted] but not all fields

[48] *Deficiencies in the Minimization of DNR Metadata Shared with Second Parties – Statement of Facts* (CSE, 4 February 2015).

[49] A list describing the technical acronyms used within this table was provided to OCSEC on 16 December 2014, and appears in Annex E.

that are required for full/effective minimization. CSE acknowledged that it is possible that other fields in the shared metadata could have contained [redacted] Therefore, it is possible that although these two fields were minimized, the information could have been available nonetheless. Due to the pervasiveness of the deficiencies, CSE suspended all DNR metadata sharing and decided to rebuild all DNR minimization scripts.

CSE compiled a sample of daily DNR communications event metadata for 11 randomly selected days between 2 July 2013 and 2 December 2013.[50]

a) This sample indicates that, for those 11 days, at least [redacted] DNR metadata records containing some unminimized CII were sent to [redacted] and made accessible to Second Parties.

b) These [redacted] metadata records amounted to approximately [redacted]% of the 11-day random sample.

c) CSE stakeholders are not in a position to state that this sample is representative of all DNR metadata formats shared with the Second Parties.

Since the sample was compiled from metadata collected [redacted]

CSE maintains, based on the sample, that the amount of unminimized CII shared with Second Parties is low relative to the total volume of metadata shared. While the problems with minimization may have been longstanding, CSE is unable to determine how many systems were impacted and for how long. The Commissioner's office asked if CSE could conduct a damage assessment to determine the extent of the DNR minimization deficiencies. While CSE acknowledged that the deficiencies were significant and complex, it was also noted that attempting to examine every single record that could have been affected by these deficiencies would be unmanageable, would take months of full-time effort by a team of developers, and would still result in significant information gaps. As such, CSE opted to conduct sampling of data to assess the scope of the deficiencies.

This incident was reported to CSE's Director General, Policy and Communications (DGPC) for inclusion in the Privacy Incident File (PIF), due to the possibility that Second Party employees may have been inadvertently exposed to metadata containing unminimized CII.

[50] The sample was taken from [redacted]

Finding no. 7: CSE lacked a proper means of verifying whether minimization scripts were functioning properly for [redacted] DNR metadata shared with Five Eyes partners, and lacked a proper record-keeping process.

According to CSE, updates to [redacted] tended to be communicated informally during meetings, or over telephone calls or emails.[51] The principal forum within CSE for discussing these updates was the [redacted]. Housed within [redacted] the [redacted] met on a bi-weekly basis to discuss and manage the technical aspects of system configuration and upgrades, as well as the deployment of new systems. Meetings of the [redacted] would feature roughly [redacted] supervisors from [redacted] including individuals involved in the updating of collection systems, as well as those responsible for updating minimization scripts (from the SIGINT Systems Development group). However, while the [redacted] made it possible for supervisors responsible for updating minimization scripts to learn about [redacted] updates, there was no subsequent process for CSE management to verify whether minimization scripts that were applied to updated [redacted] were functioning properly. CSE also lacked a proper record-keeping process, such that details of updates to minimization scripts were not made available beyond the SIGINT Systems Development group.

According to CSE, the changes to the corresponding minimization scripts are likely to have been sporadic and were probably not comprehensive or synchronized with [redacted] updates.[52] Furthermore, CSE noted that the [redacted] documentation detailing where to apply minimization to the CII-relevant fields in [redacted] DNR metadata may date back to 2008. As there is no record of past versions of minimization scripts, it is not possible to determine with certainty whether or how the scripts have changed over time. CSE's analysis of the issue determined that the minimization deficiencies were a result of the change management process being ineffective and a poor understanding of the implications of changes applied to data as it passes through the SIGINT enterprise.[53] Based on the information reviewed by the Commissioner's office, the office agrees with CSE's assessment that there was a poor change management process in place to ensure that minimization would continue to function properly as collection systems were updated.

SIGINT monitored the flow of DNR metadata to Second Parties, to ensure that minimization scripts were running, but this process did not include examination of the output of the scripts. This effectively resulted in the return of a "false positive", suggesting that scripts were working as intended, when in fact they were not.

---

[51] *Deficiencies in the Minimization of DNR Metadata Shared with Second Parties – Statement of Facts* (CSE, 4 February 2015), paragraph 21.
[52] *Deficiencies in the Minimization of DNR Metadata Shared with Second Parties – Statement of Facts* (CSE, 4 February 2015), paragraph 21.
[53] *Deficiencies in the Minimization of DNR Metadata Shared with Second Parties – Statement of Facts* (CSE, 4 February 2015), paragraph 22.

Records relating to the minimization of DNR metadata for the period preceding the discovery of the minimization anomalies are inadequate. According to CSE:[54]

- There is no capability to provide processing history on DNR metadata records;
- There was no systematic documentation of the fields for all of the DNR metadata formats being ingested by the minimization scripts;
- Some [redacted] documentation regarding minimization requirements had not been updated since 2008; and
- While some script updates were referenced informally in a source code tracking system beginning in 2009, it is unclear whether these updates correspond to changes in collection systems. Furthermore, changes to minimization scripts were not documented in formal release notes.

This represents a failure by CSE to ensure that CII shared with Second Parties was being afforded the privacy protections set out in the Ministerial Directive and in operational policy.

Finding no. 8: CSE's system for minimizing [redacted] DNR metadata was decentralized and lacked appropriate control and prioritization.

Problems and inconsistencies with minimization occurred as collection systems were gradually updated by CSE [redacted] to include additional fields of metadata, without the corresponding CSE processing systems being updated. Processing systems were not updated to account for new fields; therefore fields that were now displaced may have contained CII that was not properly minimized.

Responsibility for updating [redacted] and verifying that minimization scripts were working properly was dispersed across the organization, and CSE lacked a central authority responsible for testing, updating and verifying that minimization scripts were working appropriately.

CSE is now focused on corrective measures: a more effective change management process for new collection systems; central oversight of all DNR minimization and sharing; improved compliance validation measures; and, creating a common process for updating all scripts. The responsibility for conducting and overseeing minimization will now rest in the [redacted] CSE is continuing work to build new minimization scripts. The Commissioner's office will continue to monitor developments in order to ensure that minimization processes function properly once sharing with Second Parties has resumed.

[54] *Deficiencies in the Minimization of DNR Metadata Shared with Second Parties – Statement of Facts* (CSE, 4 February 2015), paragraph 24.

Digital Network Intelligence Metadata

Finding no. 9: CSE's system for sharing DNI metadata with Second Parties was poorly understood by the organization and lacked a proper record-keeping process.

Digital Network Intelligence (DNI) metadata is information that pertains to [redacted] (Internet-based) communication events. DNI collection is complex, and involves the processing of [redacted] telecommunications [redacted]

As with DNR metadata, [redacted] is responsible for keeping current on the various [redacted] When sharing [redacted] metadata with Second Parties, the MD stipulates that metadata is to undergo a minimization process to remove CII.[57]

[redacted]

[55] *Policy Compliance Issue Relating to Sharing of DNI Metadata with Second Parties – Statement of Facts* (CSE, 4 February 2015), paragraph 5.
[56] *Policy Compliance Issue Relating to Sharing of DNI Metadata with Second Parties – Statement of Facts* (CSE, 4 February 2015), paragraph 8.
[57] *Ministerial Directive: Communications Security Establishment Collection and Use of Metadata*, December 16, 2011.

[redacted]

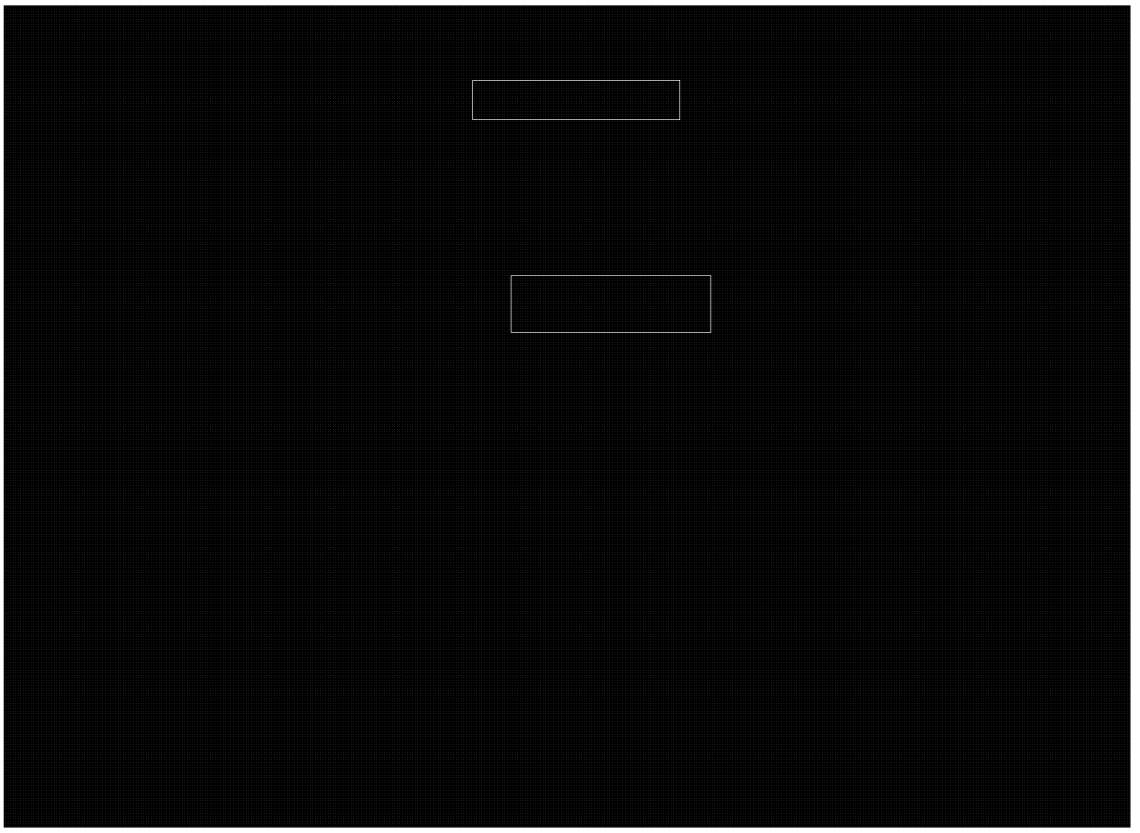
Of the DNI metadata fields that are regularly shared amongst the Five Eyes, CSE determined that [redacted] fields may contain CII in accordance with Canadian legal and policy requirements, and therefore would be subject to minimization if shared [redacted]

Since 2009, CSE has provided Second Parties with access to its DNI metadata [redacted]

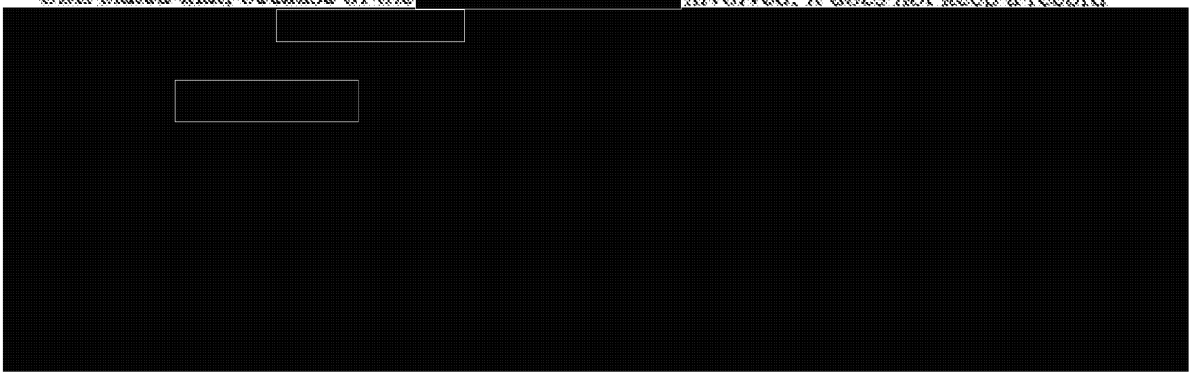
Because CSE is required to protect the privacy of Canadians in the conduct of its activities, and to minimize identifying information prior to sharing metadata [redacted] a minimization service was applied to [redacted]

According to CSE, Second Party access to CSE-acquired DNI metadata [redacted]

[38] *Policy Compliance Issue Relating to Sharing of DNI Metadata with Second Parties – Statement of Facts* (CSE, 4 February 2015), paragraph 15.
[39] *Policy Compliance Issue Relating to Sharing of DNI Metadata with Second Parties – Statement of Facts* (CSE, 4 February 2015), paragraph 16.
[40] *Briefing Note for Chief CSE – Summary of a Recent Compliance Issue – Metadata Minimization by* [redacted] (April 30, 2014).
[41] *Policy Compliance Issue Relating to Sharing of DNI Metadata with Second Parties – Statement of Facts* (CSE, 4 February 2015), paragraph 20.
[42] *Policy Compliance Issue Relating to Sharing of DNI Metadata with Second Parties – Statement of Facts* (CSE, 4 February 2015), paragraph 21.



CSE stated that, because of the [redacted] involved, it does not keep a record



As stated above, with respect to both DNI and DNR, decisions regarding the updating of [redacted] were taken informally, and were not systematically communicated to areas responsible for minimization. Furthermore, while some records existed regarding the application of minimization scripts to certain collection systems in the DNI context, no such records appear to have existed for DNR metadata. Moreover, the records that did exist resided within SIGINT Systems Development, rather than being centrally located. The Commissioner's office also noted

[69] *Policy Compliance Issue Relating to Sharing of DNI Metadata with Second Parties – Statement of Facts* (CSE, 4 February 2015), paragraph 25.

that CSE's guiding documentation as regards minimization is not up-to-date, and therefore may not reflect current minimization requirements.[64]

The use of CSE's existing centralized record-keeping system for minimization script updates and related documentation would promote compliance with policies and ministerial direction related to minimization. It could also allow CSE to periodically take stock of guidance documentation to ensure that it is kept up-to-date.

Recommendation no. 2: CSE should use its existing centralized records system to record decisions and actions taken regarding new and updated collection systems, as well as decisions and actions taken regarding minimization.

Finding no. 10: During the course of the review, CSE discovered that DNI being shared with Five Eyes was not subject to proper validation or minimization, in accordance with CSE policy and the Ministerial Directive.

If CSE shares [redacted] DNI metadata with Second Parties, the Metadata MD and operational policy require that the data be subjected to a minimization process to obfuscate CII. If CSE shares DNI metadata with Second Parties [redacted]

As noted above, CSE's DNI minimization service was supposed to include a process for email address minimization and IP address minimization. This minimization service is separate from [redacted] CSE to share DNI metadata with Second Parties.

According to CSE, the email address minimization process operates as follows:[65]

[redacted]

[64] CSE has recognized that its records relating to the minimization of metadata are inadequate. See *Deficiencies in the Minimization of DNR Metadata Shared with Second Parties – Statement of Facts* (CSE, 4 February 2015), paragraph 24.

[65] *Policy Compliance Issue Relating to Sharing of DNI Metadata with Second Parties – Statement of Facts* (CSE, 4 February 2015), paragraph 13.

[redacted]

On 21 March 2014, in the context of a meeting to discuss sharing [redacted] metadata, SIGINT Systems Development (SSD) informed SIGINT Programs Oversight & Compliance (SPOC) that DNI metadata was being shared with Second Parties [redacted] with minimization applied to Canadian email address fields, but with no minimization applied to Canadian IP address fields.

CSE had a compliance validation process in place to confirm that the minimization service was processing the results of [redacted] however, this process did not include the examination of minimization service outputs. Therefore, CSE was under the impression that minimization was taking place, when in fact it was not.

CSE believes that, since [redacted] the minimization processes have only been applied to email address fields. In the view of the Commissioner's office, this represents a failure on CSE's part to put in place an effective compliance validation system for ensuring that DNI was being shared in accordance with policy and ministerial direction.

[redacted]

While CSE initially suspended DNI metadata sharing [redacted] due to the discovery of minimization discrepancies, further examination led CSE to re-define the issue as a problem associated with selector validation.[66] According to CSE: "In its initial form, [redacted] to share [redacted] minimized DNI metadata. However,

[66] *Policy Compliance Issue Relating to Sharing of DNI Metadata with Second Parties – Statement of Facts* (CSE, 4 February 2015), paragraph 32.

[redacted]

A validation mechanism for selection criteria [redacted] would provide a means to ensure that the resulting automated searches are not directed at Canadians or persons in Canada, and to ensure that they align with Government of Canada (GC) intelligence requirements. Because the selection criteria would have been validated, the retrieved data could be provided without being subjected to a minimization process.

Complete records of all DNI metadata shared with Second Parties are not available for retrieval. Therefore, it is not possible to retroactively ascertain whether [redacted] had forwarded any selection criteria that were directed at Canadians or persons in Canada, and if CSE has forwarded any data in response.

CSE is unable to request deletion of non-compliant metadata records, as it is not technically possible to identify which of the shared records were non-compliant.

Notwithstanding the above, CSE assesses that there is a low probability that CII was unduly exposed to Second Parties [redacted] for the following reasons:[68]

a) The DNI metadata [redacted] was the result of queries based on [redacted]

[redacted]

[87] CSE response to RFI 9.21, Email from Senior Review Advisor, External Review, January 26, 2015.
[88] *Policy Compliance Issue Relating to Sharing of DNI Metadata with Second Parties – Statement of Facts* (CSE, 4 February 2015), paragraph 40.

[redacted]

d) As with any selection-based collection, there is a risk of incidental collection of CII when Canadians are in contact with foreign entities of intelligence interest to the Five Eyes, however there are policies and procedures for the handling of such information to mitigate the impact on the privacy of those individuals.

CSE recognized the DNI metadata sharing issue as a privacy incident and recorded it in the PIF.

> ***Finding no. 11: CSE proactively suspended the sharing of both DNR and DNI metadata with Second Parties in order to protect the privacy of Canadians while developing a solution to the problems it encountered in this area.***

At the time of writing this report, the sharing of [redacted] DNR metadata with Second Parties remains suspended, as does the sharing of DNI metadata [redacted] The [redacted] sharing service will remain disabled until corrective measures are in place. Prior to affected data flows being reactivated, SIGINT senior management will review and approve proposed improvements to the standardization of data formats, clarification of roles and responsibilities among CSE stakeholders, and enhancement of compliance requirements and validation activities. Internal consultations with SIGINT senior management, DGPC, Chief CSE, and with CSE's legal services are ongoing.

CSE notified the Office of the CSE Commissioner and the office of the Minister of National Defence of the issue in early June 2014. The Chief, CSE updated the Minister of National Defence on the issue during a meeting on 18 November 2014. CSE has notified Second Party partners that metadata flows have halted due to compliance problems. The Commissioner's office has been meeting with CSE regarding this issue as part of its ongoing review of metadata.

CSE is considering actions required to rectify this problem, which may include:

a) New policies and procedures concerning the sharing of DNI metadata, validation of selection-based queries [redacted] and validation of minimization scripts; and

b) Improvements to compliance validation activities, particularly regarding systems that are fully automated.

To address the recognized need for better compliance scrutiny of collecting and sharing information outside CSE, a decision was taken to appoint some of CSE's SIGINT executives as compliance officials. These officials will ensure that proper compliance rules and considerations are applied to SIGINT information that enters, leaves and is

stored in CSE systems. Over the medium to longer term, this will be complemented by other improvements, such as development of systems with built-in compliance features.

On 5 November 2014 a SIGINT Programs Instruction (SPI-7-14: Process for SIGINT Metadata Minimization) was issued by Director General, Programs to formalize the end-to-end DNR metadata minimization process within SIGINT. Furthermore, SIGINT continues to develop and implement procedures and guidelines to define data format standards, clarify roles and responsibilities, and enhance compliance requirements and validation activities.

The Commissioner's office will continue to monitor developments in CSE's ongoing response to this issue.

> ***Finding no. 12: CSE's failure to minimize DNR and DNI metadata, and its failure to validate identifiers prior to sharing DNI metadata with international partners, raise legal questions that need to be explored in further detail.***

CSE could not precisely define the scope of the privacy impact of the failure to minimize [redacted] DNR, nor could it undertake a comprehensive damage assessment, due to the complexity involved in such a task. However, based on figures provided by CSE following the sampling of one of its collection systems, the DNR incident may involve a significant amount of CII, even if CSE is unable to determine the precise extent.

The inadvertent sharing of DNR and DNI metadata containing unminimized CII constitutes a breach of CSE operational policy and of the minimization condition in the Metadata MD. Furthermore, CSE's failure to validate identifiers prior to sharing DNI metadata with its international partners also constitutes a breach of CSE operational policy. Both of these had an impact on the privacy of Canadians. This impact may have been mitigated in part through safeguards provided by the remaining privacy protection measures applied by CSE and its partners. CSE acknowledges that it failed to comply with ministerial direction and operational policy.

In light of these two incidents, questions have arisen with respect to CSE's compliance with the law, which need to be examined in further detail. The Commissioner's office has met with senior CSE managers, as well as with legal counsel from CSE's Directorate of Legal Services Unit (Justice Canada), in order to understand CSE's legal interpretation of these incidents. Discussions in this regard are ongoing. The Commissioner's office will continue its investigation of this issue and the Commissioner, as mandated by the *NDA*, will subsequently make a determination with respect to CSE's compliance with the law.

IX. CONCLUSION

The purpose of this review was to examine CSE's use of metadata in a SIGINT context to assess whether CSE complied with the law and acted consistent with ministerial direction, whether measures were in place to protect the privacy of Canadians, and

whether the activities conformed with CSE's own operational policies and procedures. This review also aimed to provide the Commissioner's office with updated knowledge and to identify areas or issues that could form the basis for future, in-depth reviews of specific metadata activities in a SIGINT context. CSE was forthcoming with information and assistance, both proactively and in response to specific requests of the Commissioner's office.

Metadata collection and analysis have evolved considerably since the Commissioner's last in-depth review of metadata activities, and metadata remains critical to all aspects of CSE's SIGINT mission. Not surprisingly, the Canadian legal landscape has changed since the Commissioner's office last conducted an in-depth review of CSE's collection and use of metadata. Also, the 2011 metadata Ministerial Directive lacks clarity regarding the sharing of certain types of metadata with Second Parties, as well as other aspects of CSE's metadata activities. It is recommended that CSE seek an updated Ministerial Directive that provides clear guidance related to the collection, use and disclosure of metadata.

While this review was being conducted, CSE's IP Profiling Analytics tradecraft was the subject of an unauthorized public disclosure. CSE's activities in this regard were authorized under 273.64(1)(a) of the *NDA*, and that CSE took measures to protect the privacy of Canadians in undertaking them.

As the review was being undertaken, CSE discovered on its own that [redacted] Dialled Number Recognition (DNR) metadata being shared with Five Eyes partners was not being minimized properly, contrary to the Ministerial Directive and to operational policy. CSE lacked a proper means of verifying whether minimization scripts were functioning properly for [redacted] DNR metadata shared with Five Eyes partners. In addition, CSE's system for minimizing [redacted] DNR metadata was decentralized and lacked appropriate control and prioritization. Furthermore, CSE's system for sharing Digital Network Intelligence (DNI) metadata with Second Parties was poorly understood by the organization. For both DNI and DNR metadata, CSE lacked a proper record-keeping process. As a result, it is recommended that CSE use its existing centralized records system to record decisions and actions taken regarding new and updated collection systems, as well as decisions and actions taken regarding minimization.

During the course of the review, CSE also discovered that DNI being shared with the Five Eyes was not subject to proper validation or minimization, in accordance with CSE policy and the metadata Ministerial Directive. In response to issues that it discovered, CSE took corrective actions and proactively suspended the sharing of both DNR and DNI metadata with Second Parties in order to protect the privacy of Canadians while developing a solution to the problems it encountered in this area.

CSE's failure to minimize DNR and DNI metadata, and its failure to validate identifiers prior to sharing DNI metadata with international partners, raise legal questions that need to be explored in further detail. The Commissioner, as mandated by the *NDA*, will subsequently make a determination with respect to CSE's compliance with the law.

The Commissioner's office will also continue work on two other reports that deal with CSE's use of metadata: the second report will examine issues identified in a 2014 report, entitled *A Review of CSE's Office of Counter-Terrorism*, and will also examine network analysis and prioritization activities which involve metadata, and contact chaining activities [redacted] A third report, expected in the coming year, will focus on CSE's use of metadata in an IT security context.

Jean-Pierre Plouffe, Commissioner

ANNEX A —Findings and Recommendations

Finding no. 1: *CSE was forthcoming with information and assistance, both proactively and in response to specific requests of the Commissioner's office.*

Finding no. 2: *Metadata collection and analysis has evolved considerably since the Commissioner's last in-depth review of metadata activities, and metadata remains critical to all aspects of CSE's SIGINT mission.*

Finding no. 3: *The Canadian legal landscape has changed since the Commissioner's office last conducted an in-depth review of CSE's collection and use of metadata.*

Finding no. 4: *The 2011 Ministerial Directive on Collection and Use of Metadata lacks clarity regarding the sharing of certain types of metadata with Second Parties, as well as other aspects of CSE's metadata activities.*

Recommendation no. 1: CSE should seek an updated Ministerial Directive that provides clear guidance related to the collection, use and disclosure of metadata.

Finding no. 5: *CSE's IP Profiling Analytics tradecraft, which was the subject of an unauthorized disclosure, was authorized under 273.64(1)(a) of the* NDA, *and CSE took measures to protect the privacy of Canadians in undertaking this activity.*

Finding no. 6: *During the course of the review, CSE discovered that* [redacted] *DNR metadata being shared with Five Eyes partners was not being minimized properly, contrary to the Ministerial Directive and to operational policy.*

Finding no. 7: *CSE lacked a proper means of verifying whether minimization scripts were functioning properly for* [redacted] *DNR metadata shared with Five Eyes partners, and lacked a proper record-keeping process.*

Finding no. 8: *CSE's system for minimizing* [redacted] *DNR metadata was decentralized and lacked appropriate control and prioritization.*

Finding no. 9: *CSE's system for sharing DNI metadata with Second Parties was poorly understood by the organization and lacked a proper record-keeping process.*

Recommendation no. 2: CSE should use its existing centralized records system to record decisions and actions taken regarding new and updated collection systems, as well as decisions and actions taken regarding minimization.

Finding no. 10: *During the course of the review, CSE discovered that DNI being shared with Five Eyes was not subject to proper validation or minimization, in accordance with CSE policy and the Ministerial Directive.*

Finding no. 11: *CSE proactively suspended the sharing of both DNR and DNI metadata with Second Parties in order to protect the privacy of Canadians while developing a solution to the problems it encountered in this area.*

Finding no. 12: *CSE's failure to minimize DNR and DNI metadata, and its failure to validate identifiers prior to sharing DNI metadata with international partners, raise legal questions that need to be explored in further detail.*

ANNEX B — Interviewees

The following CSE employees provided information or facilitated the review:

Director General, SIGINT Programs
Director General, Access
Director, SIGINT Program Requirements
Director, [redacted]
Team Leader, [redacted] Strategic Initiatives, [redacted]
Senior Research Analyst, [redacted]

Manager, SIGINT Programs Oversight and Compliance
Analyst, SIGINT Programs Oversight and Compliance
Analyst, SIGINT Programs Oversight and Compliance

Director General, Policy and Communications
Director, Disclosure, Policy and Review
Deputy Director, Disclosure, Policy and Review
Manager, External Review
Senior Review Advisor, External Review
Senior Review Advisor, External Review
Review Advisor, External Review

Linguist/Analyst, [redacted]
Manager [redacted]

Manager, [redacted]
Analyst [redacted]

[redacted] Analyst, Office of Counter-Terrorism [redacted]

[redacted] Project Manager, [redacted]
SIGDEV Analyst, [redacted]
Team Leader, [redacted]

Analyst, [redacted]
Team Leader, [redacted]

Acting Director, SIGINT Systems Development
Manager, Protocol Analysis, [redacted]

Executive Director and General Counsel, CSE DLSU

ANNEX C

National Defence / Défense nationale

National Defence Headquarters
Ottawa, Ontario
K1A 0K2

Quartier général de la Défense nationale
Ottawa (Ontario)
K1A 0K2

TOP SECRET//SI

Office of the Communications Security Establishment Commissioner

DEC 1 8 2011

Bureau du Commissaire du Centre de la sécurité des télécommunications

To: Chief, Communications Security Establishment

MINISTERIAL DIRECTIVE COMMUNICATIONS SECURITY ESTABLISHMENT COLLECTION AND USE OF METADATA

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's foreign intelligence acquisition programs pursuant to paragraph 273.64 (1) (a) of the *National Defence Act*:

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]

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. This Ministerial Directive relates to the activities carried out pursuant to paragraph 273.64 (1) (a) of the *National Defence Act* (CSE's foreign intelligence acquisition programs). 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.

Canada

TOP SECRET//SI

TOP SECRET//SI

4. Metadata acquired pursuant to its foreign intelligence acquisition programs will be subject to CSE's existing procedures to protect the privacy of Canadians.

5. In the fulfillment of its mandate as set out in paragraph 273.64 (1) (a) 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 relevant 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 programs 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, system administration staff of CSE and ITS cyber defence personnel as set out in paragraph (4) below.

(4) To the extent that metadata containing Canadian identifying information is relevant to the protection of electronic information or information infrastructures of importance to the Government of Canada, this unaltered metadata may be disclosed to ITS cyber defence personnel for the purpose of helping to protect information infrastructures of importance to the Government of Canada. Any use or retention of this metadata by ITS cyber defence personnel for the purposes set out in paragraph 273.64 (1) (b) will continue to be handled in accordance with existing policy and procedures related to the protection of the privacy of Canadians.

(5) 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 foreign malicious cyber activities to provide indications and warnings of actual or potential cyber intrusions directed against infrastructures of importance to the Government of Canada.

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 are subject to review by the CSE Commissioner to ensure they are in compliance with the law.

11. This Ministerial Directive replaces the Ministerial Directive Communications Security Establishment Collection and Use of Metadata, signed by the Minister of National Defence on March 9, 2005.

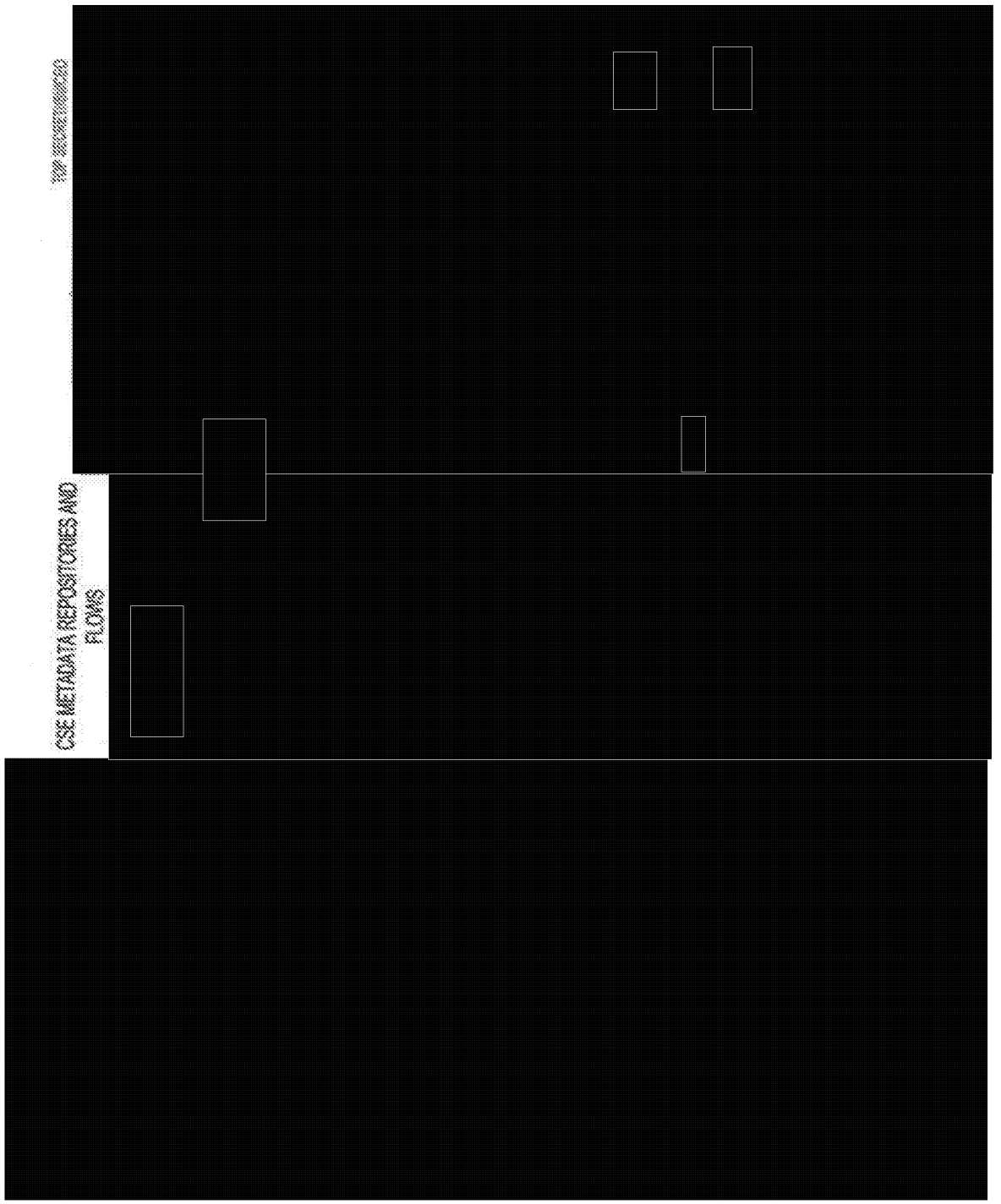
12. This Ministerial Directive comes into force on the date it is signed.

Dated at Ottawa, Ont. this 21st day of November, 2011.

The Honourable Peter MacKay, P.C., M.P.
Minister of National Defence

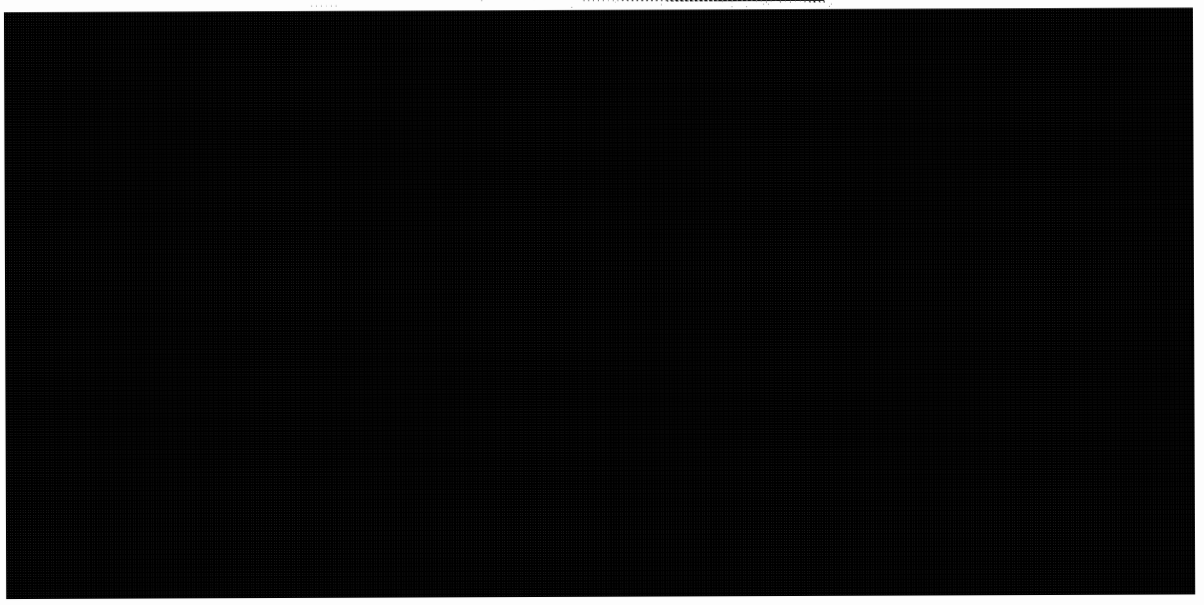
cc. National Security Advisor, Privy Council Office
Deputy Minister of National Defence

ANNEX D



ANNEX E

List of Technical Acronyms Used In DNR Table on Page 35



ANNEX F

[redacted]