Communications Security Establishment Commissioner

The Honourable Robert Décary, Q.C.

Canada

Commissaire du Centre de la sécurité des télécommunications

L'honorable Robert Décary, c.r.

TOP SECRET/COMINT/CEO

March 15, 2011

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

Dear Mr. MacKay:

The purpose of this letter is to provide you with the results of a review of Communications Security Establishment Canada (CSEC) signals intelligence (SIGINT) targeting and selector management activities. This review was undertaken under my general authority as articulated in Part V.1, paragraph 273.63(2)(*a*) of the *National Defence Act* (*NDA*). I examined CSEC's processes and practices in place while the review was being conducted – September 2009 to December 2010 – and tested specific activities for the period September 2008 to August 2009, that is, the period immediately preceding the start of the review, given that review is of past activities.

Paragraph 273.64(1)(*a*) of the *NDA* mandates CSEC "to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence priorities". To comply with the *NDA*, CSEC must distinguish those communications which involve foreign entities located outside Canada and those that are not. In the course of its foreign intelligence collection activities, CSEC must target only foreign entities located outside Canada. It cannot intercept any one-end Canadian communications, unintentionally in the course of its foreign intelligence collection, unless it is authorized to do so by the Minister. Finally, CSEC's targeting and selector management activities must contain measures to protect the privacy of Canadians.

In a SIGINT context, targeting means to single out for collection or interception purposes. CSEC targets communications using selectors. A selector is an identity used by an entity for communications, such as a phone number, Internet Protocol or e-mail address. Targeting and selector management are at the foundation of CSEC's foreign intelligence collection programs. Specific and important controls are placed on these activities to ensure compliance with legal, ministerial and policy requirements. The potential impact to the privacy of Canadians would be

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

significant, should there be an instance of non-compliance with the law while conducting these activities. Past Commissioners made findings and recommendations respecting these activities and which required follow-up. Major changes to certain technology and procedures relating to these activities have recently occurred and others are in progress. It is for these reasons that CSEC SIGINT's targeting and selector management activities were selected as the subject of this review.

The objectives of the review were to: document CSEC SIGINT's targeting and selector management activities and associated processes and practices; assess whether the activities comply with the law; and assess the extent to which CSEC protected the privacy of Canadians in carrying out the activities.

Based upon the information reviewed and the interviews conducted, CSEC conducts its SIGINT targeting and selector management activities in accordance with the law. CSEC has sufficient policies and processes to satisfy the legal requirement not to direct its SIGINT interception activities at a Canadian (anywhere) or any person in Canada.

During the period under review, CSEC identified and recorded [redacted] privacy incidents involving the unintentional targeting of a Canadian. I am satisfied that CSEC responded appropriately to these [redacted] privacy incidents.

CSEC takes measures in the design of its targeting and selector management systems and databases to promote compliance with the law and the protection of the privacy of Canadians. As identified in my report, recent enhancements made or planned to these systems and databases assist in ensuring and demonstrating compliance with the law, ministerial requirements and policy.

I did find, however, certain deficiencies in some of the targeting and selector management systems and databases, and I will monitor ongoing CSEC efforts to address these weaknesses. Specifically, I will monitor CSEC's efforts to implement in one system known as [redacted] as well as a capability to record the Government of Canada intelligence requirement(s) associated with a second party targeting request. I will also monitor CSEC efforts to modify its systems to permit a monthly comparison of targeted selectors in [redacted] with those in the "dictionaries" (holding the selectors) [redacted] Finally, I will monitor CSEC efforts to modify the selector database known as [redacted] to accommodate targeting for [redacted] and for [redacted] targeting capability.

Based upon the information reviewed and the interviews conducted, CSEC conducts its SIGINT targeting and selector management activities in accordance with ministerial direction.

Operational policies and procedures for SIGINT targeting and selector management activities are in place and provide sufficient direction to CSEC employees respecting the protection of the privacy of Canadians. CSEC employees interviewed and observed were aware of relevant policies and procedures and their application to SIGINT targeting and selector management activities. CSEC managers routinely and closely monitor SIGINT targeting and selector management activities to make certain the activities comply with governing authorities.

However, operational policies and procedures applicable to [redacted] provide only limited direction respecting targeting for such activities. I am recommending that CSEC provide specific guidance for [redacted] targeting.

Based on the interviews conducted by my officials, for the period under review, while most targeting documentation requirements were met, CSEC's intelligence analysts did not always document in [redacted] the source of a selector. Recording such information is important for accountability purposes and to assist CSEC in demonstrating that it met statutory requirements. When the source of a selector was documented, it was done in different ways, and with different levels of detail. It is, however, a positive development – that assists in demonstrating compliance with the law, ministerial requirements and policy – that in March 2009, analysts were required – by policy and by technical means – to record in [redacted] the source of a selector. CSEC indicated that it is considering changes to policy and procedures to provide additional guidance respecting how to document in [redacted] the source of a selector and I will monitor CSEC's efforts respecting this subject.

In addition to the above-noted objectives, I examined CSEC's activities in response to associated findings and recommendations made by former Commissioner Gonthier in his reports to you of June 2008 respecting [redacted] and March 2008 respecting [redacted] I am satisfied that improvements to CSEC's policies and procedures as well as significant development efforts made and other planned enhancements to associated systems and databases address the recommendation and negative findings in these reports.

Finally, I examined CSEC's activities in response to previous associated recommendations of CSEC's internal Audit, Evaluation and Ethics Directorate. I am satisfied that CSEC has addressed the negative findings in CSEC's 2006 SIGINT Legal Compliance Final (audit) Report respecting second party targeting requests.

The enclosed report contains detailed information on these and other findings as well as related issues. CSEC officials were provided an opportunity to review and comment on the report, for factual accuracy, prior to finalizing it.

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

Yours sincerely,

Robert Décary

Enclosure: (1)

c.c. Mr. John Adams, Chief, CSEC
Mr. Stephen Rigby, National Security Advisor to the Prime Minister, Privy Council Office
Mr. Robert Fonberg, Deputy Minister, National Defence

Office of the
Communications Security
Establishment Commissioner

CANADA

Bureau du
Commissaire du Centre de la
sécurité des télécommunications

TOP SECRET//COMINT//CEO

A Review of CSEC SIGINT's Targeting and Selector Management Activities

March 15, 2011

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

This review was conducted under the authority of the CSE Commissioner as articulated in Part V.1, paragraph 273.63(2)(*a*) of the *National Defence Act* (*NDA*).

The review is in conformance with signals intelligence (SIGINT) ministerial authorizations (MAs) permitting the unintentional interception of private communications (PCs) - as defined in section 183 of the *Criminal Code* - under collection programs known as [redacted] and Interception Activities Conducted in Support of Canadian Forces Operations in Afghanistan (Afghan MA activities).[1] Section 273.63 and subsection 273.65(8) of the *NDA* mandate the CSE Commissioner to review activities carried out under MAs.

The review is also in accordance with ministerial directives (MDs) on "Accountability Framework"[2], "Privacy of Canadians"[3], and "Collection and Use of Metadata"[4] that indicate that associated activities will be subject to review by the CSE Commissioner or that require CSEC to cooperate fully with the Commissioner in the exercise of reviews.

II. INTRODUCTION

Paragraph 273.64(1)(*a*) of the *NDA* mandates CSEC "to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence [FI], in accordance with Government of Canada [GC] intelligence priorities" [part (a) of CSEC's mandate].

To comply with the *NDA*:

- CSEC must distinguish those communications which involve foreign entities located outside Canada and those that are not; and
- CSEC's targeting and selector management activities must contain measures to protect the privacy of Canadians.

In a SIGINT context, *targeting* means "to single out for collection or interception purposes".[5] CSEC collects operationally meaningful data using *selectors*. CSEC policy OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the*

[1] Activities conducted under MA must be undertaken in accordance with conditions set out by the Minister of National Defence in the MAs, e.g., respecting measures to protect intercepted PCs. This review encompassed [redacted] and Afghan MA activities under the MAs in effect from December 23, 2007 to December 22, 2008 and from December 23, 2008 to December 22, 2009.
[2] Issued June 19, 2001.
[3] Issued June 19, 2001.
[4] Issued March 9, 2005.
[5] OPS-1, p. 51 (CERRID# 142875-v6E).

Conduct of CSE[C] Activities, effective December 23, 2009, indicates *selectors* "are terms that may include a name, [redacted] [Internet Protocol] IP or e-mail address, facsimile or telephone number, or other alphanumeric character stream [redacted] for the purpose of identifying traffic that relates to national foreign intelligence requirements and isolating it for further processing." (p. 49) The Canadian SIGINT Operations Instruction (CSOI) CSOI-4-4, *Targeting and Selector Management Using* [redacted] *National SIGINT Systems For Intelligence Reporting Purposes*, effective March 5, 2009, defines a *selector* as: "an identity used by an entity for communications, such as an e-mail address, [redacted] or phone number [redacted]

In CSEC, there are two approaches to targeting using [redacted] collection (CSOI-4-4 refers):

1. *Targeting using "Strong Selectors"*, which allows SIGINT to direct its targeting activities at foreign entities[7] located outside Canada and which are associated with foreign intelligence requirements. "Strong selectors" allow SIGINT to select information from the GII on the basis of unique communications addresses which can be reliably correlated with entities in the physical world.[8]

2. [redacted] *Targeting*, which selects information from the GII on the basis of [redacted]

Another approach to targeting involves [redacted] (OPS-3-1, Procedures for [redacted] activities.)

Selector management refers simply to the process of managing selectors, including the research and development of selectors, the analysis of associated intercepted communications to confirm targeting is valid and productive, and the de-targeting of selectors that are no longer valid or productive.

[redacted] Afghan MA activities are CSEC's [redacted] interception collection. [redacted] is considered an [redacted] interception activity.

[7] An *entity* means: "a person, group, trust, partnership, or fund or an unincorporated association or organization and includes a state or political subdivision or agency of a state." (*NDA*, section 273.61).

[8] "Strong selectors" are metadata, such as a telephone number, e-mail address or Internet address that are [redacted] into a [redacted] dictionary. *Metadata* is: "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." (MD on the Collection and Use of Metadata)

[9] Targeting for [redacted] is described at pp. 28-30.

The *NDA* requires that activities under part (a) of CSEC's mandate "shall not be directed at Canadians or any person in Canada" [paragraph 273.64(2)(*a*)].[10]

One of the conditions to issue an MA under the *NDA* is that the Minister of National Defence (Minister) must be "satisfied that the interception will be directed at foreign entities located outside Canada" [paragraph 273.65(2)(*a*) of the *NDA*].

All MAs include the following requirement:

> To facilitate the review by the Commissioner of the Communications Security Establishment of the statutory requirement that interceptions of private communications must be directed at foreign entities located outside Canada, the Communications Security Establishment [Canada] shall establish and maintain an automated directory of selectors which it has grounds to believe relate to foreign entities located outside Canada.

Targeting and selector management activities are also conducted pursuant to ministerial direction. Specifically, the MD on "Privacy of Canadians" indicates:

> ...it is incumbent upon you, as Chief of CSE[C], to ensure that CSE[C] does not target the communications of Canadians and will continue to adopt procedures to minimize the inadvertent [unintentional] collection of such communications... (p. 1)

CSEC's OPS-1 policy requires, at a minimum, selectors to be subject to annual review to ensure they remain consistent with the GC intelligence priorities.

Rationale for conducting this review

CSEC's FI collection activities conducted under MA involve a number of distinct methods of acquiring information from the GII. Nevertheless, there are a number of common business processes and associated tools, as well as common systems and databases, which support these collection methods and which CSEC uses to deal with the information obtained. For example, common to all of the collection methods are the processes by which CSEC: selects foreign entities located outside Canada that are of FI interest (the subject of this report); uses, shares and reports information to clients and international partners; and retains or disposes of intercepted communications. Rather than examine thoroughly individual MAs, it was assessed as more effective to examine thoroughly each process common to CSEC's FI collection activities under MA. This new approach, which cuts across the collection methods, is referred to as *horizontal review* and is designed to provide the Commissioner with an even more comprehensive understanding of how CSEC conducts its activities. Ultimately, its objective is to increase the degree of assurance the

[10] In a crisis situation where the life and safety of Canadian individuals are threatened, such as during a kidnapping, and [redacted] CSEC is required to closely monitor any resultant intercepted communications and to de-target the selectors when the situation is resolved or when the selectors no longer result in communications related to GC intelligence priorities.

Commissioner can provide to the Minister that CSEC is complying with the law and protecting the privacy of Canadians.

Targeting and selector management are at the foundation of CSEC's SIGINT collection programs. SIGINT collection relies on targeting. Specific and important controls are placed on SIGINT targeting and selector management activities to ensure compliance with legal, ministerial and policy requirements. The potential impact on the privacy of Canadians would be significant, should there be an instance of non-compliance with the law while conducting these activities. Past Commissioners made findings and recommendations respecting these activities and which require follow-up. Major changes to certain technology and procedures relating to these activities have recently occurred and others are in progress. It is for these reasons that the Commissioner selected CSEC SIGINT's targeting and selector management activities as the subject of one of the first in-depth horizontal reviews of a SIGINT common business process.

III. OBJECTIVES

The objectives of the review were to:

- document CSEC SIGINT's targeting and selector management activities and associated processes and practices;
- assess whether the activities comply with the law; and
- assess the extent to which CSEC protected the privacy of Canadians in carrying out the activities.

IV. SCOPE

The Commissioner's office examined CSEC's processes and practices in place while the review was being conducted – September 2009 to December 2010 – and tested specific activities for the period September 2008 to August 2009, that is, the period immediately preceding the start of the review, given that review is of past activities.

In addition to acquiring detailed knowledge of CSEC SIGINT's targeting and selector management activities, the Commissioner's office examined:

1. the legislative and policy framework;
2. how CSEC develops selectors, e.g., from its collection, contact chaining activities, lead information, other sources;
3. whether selectors relate only to foreign entities located outside Canada;
4. whether selectors are in accordance with GC intelligence requirements (GCRs)[11] and consistent with CSEC's National SIGINT Priorities List (NSPL)[12];
5. the extent to which technology is used and other efforts are applied to protect the privacy of Canadians;
6. the content of dictionaries and databases of selectors, how they work, how they interact with other tools, collection equipment and databases;
7. how selectors are validated (e.g., to ensure they remain in accordance with GC intelligence priorities) or de-targeted (e.g., in the event that a Canadian or person in Canada is unintentionally targeted);
8. what occurs when an intelligence analyst recognizes that a PC (including solicitor-client communications) or information about Canadians is associated with a particular selector;
9. how CSEC approves selectors proposed by the Second Parties[13];

---

[11] CSOI-1-1, *The National SIGINT Priorities List (NSPL)* Process, effective July 17, 2008, defines the GCRs as: "an index which permits the tracking of the SIGINT Process against client requests. GCRs are applied to requests, reports, targets, feedback, etc. GCRs are also mapped to the NSPL as appropriate to be able to track effort against national priorities." (p. 14)

[12] According to CSOI-1-1, the NSPL is: "A tiered list which officially defines issues of national interest from a SIGINT perspective and the level of interest and effort afforded to each one. The list is divided into Standing Issues and Watching Briefs...". (p. 14)

[13] The Second Parties are CSEC's four SIGINT partners: the U.S. National Security Agency (NSA), the U.K. Government Communications Headquarters (GCHQ), the Australian Defence Signals Directorate (DSD), and the New Zealand Government Communications Security Bureau (GCSB). Collectively, the Second Parties and CSEC are known as the Five-Eyes alliance. According to long-standing conventions, the Five-Eyes do not target one another's communications. Accordingly, CSEC's interception activities are

10. CSEC's activities in response to previous associated findings and recommendations of the Commissioner, namely: a number of findings in the March 2008 review report respecting [redacted] (see pp. 48-49 and p. 56) as well as finding no. 6 and recommendation no. 1 in the June 2008 [redacted] review report and the September 2008 response from the Minister of National Defence (see pp. 49-50 and p. 56). (The March 2006 report on [redacted] and the February 2005 [redacted] report also provide background information respecting targeting and selector management); and

11. CSEC's activities in response to previous associated recommendations of CSEC's Audit, Evaluation and Ethics Directorate, namely: recommendations 2.8.2 of the Directorate's April 2006 *SIGINT Legal Compliance* final report respecting selectors. (See p. 51)

The review did not include an examination of:

- information technology security activities under part (b) of CSEC's mandate[14];
- tasking requests respecting Activity Authorization Requests for [redacted] SIGINT development activities[15];
- targeting and selector management activities in support of federal law enforcement or security agencies under part (c) of its mandate[16]

IRRELEVANT

IRRELEVANT and

- [redacted] by CSEC and the Second Parties.[19]

---

not to be directed at second party nationals located anywhere, or against anyone located in second party territory.

[14] Paragraph 273.64(1)(*b*) of the *NDA* mandates CSEC "to provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada."

[15] The Commissioner's March 2009 report respecting CSEC's [redacted] Network Analysis and Prioritization and [redacted] Activities discussed [redacted] and SIGINT development activities, including the use of "soft selectors". "Soft selectors" relate to [redacted]

[16] Paragraph 273.64(1)(*c*) of the *NDA* mandates CSEC "to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties."

[17] This will be addressed in a separate review.

[18] [redacted]

[19] This will be addressed in a separate review.

V. CRITERIA

A) Legal Requirements

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

B) Ministerial Requirements

The Commissioner expected that CSEC conducts its targeting and selector management activities in accordance with ministerial direction, namely the requirements and approval frameworks outlined in relevant MAs and MDs.

C) Policies and Procedures

The Commissioner expected that CSEC:

i) had appropriate policies and procedures that guide its targeting and selector management activities;
ii) had personnel who are aware of and comply with the policies and procedures; and
iii) had an effective management control framework to ensure that the integrity of the activities is maintained on a routine basis, including appropriately accounting for important decisions and information.

VI. METHODOLOGY

The Commissioner's office examined relevant written and electronic records, files, correspondence and other documentation, including policies and procedures and legal advice.[20] Throughout the course of the review, CSEC provided answers to a number of written questions.

The Commissioner's office conducted interviews with 21 CSEC managers and other employees involved in the activities (Annex B). With the assistance of CSEC employees acting under our direction, we tested the contents of relevant databases and systems to ensure conformity with legal and ministerial requirements and associated policies and procedures.

As a first step, the Commissioner's office documented and described CSEC's targeting and selector management activities, processes and systems, the legislative and policy framework, and ensured a common understanding of concepts and terminology.

[20] If legal advice given to CSEC is shared with the Commissioner's office, this is done on the understanding that the sharing by CSEC of information which is subject to solicitor-client privilege does not constitute a waiver by CSEC of its privilege.

Subsequently, we assessed CSEC's activities against the established criteria and developed conclusions respecting the objectives. This is a report of the outcomes of the review.

Prior to forwarding a draft report to CSEC for comment as to factual accuracy, the Commissioner's office presented a summary of our findings to CSEC.

VII. BACKGROUND

In CSEC, there are two approaches to targeting using [redacted] collection (CSOI-4-4 refers):

> 1. *Targeting using "Strong Selectors"*, which allows SIGINT to direct its targeting activities at foreign entities located outside Canada and which are associated with foreign intelligence requirements. "Strong selectors" allow SIGINT to select information from the GII on the basis of unique communications addresses which can be reliably correlated with entities in the physical world.
>
> 2. [redacted] *Targeting*, which selects information from the GII on the basis of [redacted]

Another approach to targeting involves [redacted] (OPS-3-1, Procedures for [redacted] activities.)

1. [redacted] authorities

CSEC's [redacted] and its analysts[21] are responsible to develop selectors, namely:

- to conduct research and document that all conditions for targeting have been met;
- submit targeting requests to CSEC's [redacted] group[22]; and
- on an annual basis, or more frequently as required, validate targeted selectors (i.e., being used in a collection system(s) to filter and intercept only wanted

[21] In this report, references to a [redacted] analyst may include a Canadian Forces Information Operations Group (CFIOG) analyst performing the same targeting activities.

[22] CSEC's [redacted] group in its Advanced Network Tradecraft Directorate performs mission management control functions, including approving and monitoring for compliance [redacted] authorities and responsibilities are discussed at pp. 18-19.

communications), and de-target selectors which are no longer valid, or which are resulting in intercepted communications of no FI value, or for which there is no longer an associated GCR.[23]

A [redacted] analyst is responsible to monitor intercepted communications and confirm that the targeting is valid (i.e., the entity is of a foreign nationality and located outside Canada) and productive (i.e., the communications contain FI associated with a GCR and aligned with the NSPL).

A [redacted] analyst must regularly update a selector with any elements of information that may have changed (e.g., different location digraph[24]), and de-target a selector that is no longer valid or productive.[25]

[23] Section 2.8, CSOI-4-4, p. 10.
[24] Targeting digraphs and trigraphs are discussed at p. 26 and at Annex D. The digraph is a two-letter code representing the assessed location of the targeted entity. The trigraph is a three-letter code representing the assessed nationality (two letter digraph of the country of nationality) as well as a single letter code representing the targeted entity's function. [redacted]
[25] Section 3.4, CSOI-4-4, p. 16.

2. Targeting and selector management tools

On October 15, 2009, the Commissioner's office received a technical brief respecting targeting and selector management systems and tools.

TOP SECRET//COMINT//CANADIAN EYES ONLY

Communications Security Establishment Canada / Centre de la sécurité des télécommunications Canada

Canada

CERRID# 368869, October 15, 2009, slide 6, e-mail from Policy and Review Advisor, External Review and Policy Management, November 27, 2009. Note: The above representation of a targeting system is a simplified version for presentation purposes [redacted]' is a template used by a [redacted] analyst to seek [redacted] approval for targeting selectors [redacted] and for targeting [redacted] See p. 29.)

[redacted] – ***Target Knowledge Base***

The target knowledge [data] base (or TKB, commonly and hereinafter referred to by its cover name [redacted] contains information – from a variety of sources – populated by [redacted] analysts respecting foreign entities of FI interest to the GC and associated selectors. [redacted] links CSEC's target knowledge with selectors.

In addition to containing a target knowledge database, [redacted] provides a targeting tool, which [redacted] analysts use to submit selectors to [redacted] for validation and targeting. [redacted] permits a [redacted] analyst to monitor the status of any selector for which they are responsible (targeted or not).

[redacted] digital network intelligence (DNI)[26] selector – such as an e-mail address or Internet Protocol (IP) address [redacted] for a dialled number recognition (DNR)[27] selector – such as a telephone or fax number.

[redacted]

On October 5, 2009, a CSEC Specialist-Linguist provided a comprehensive "live" demonstration of [redacted] involving extant FI entities and associated selectors, including: [redacted] a foreign entity; [redacted] a DNR (wireless telephony) selector and [redacted] a DNI selector (e-mail address) [redacted]

[redacted]

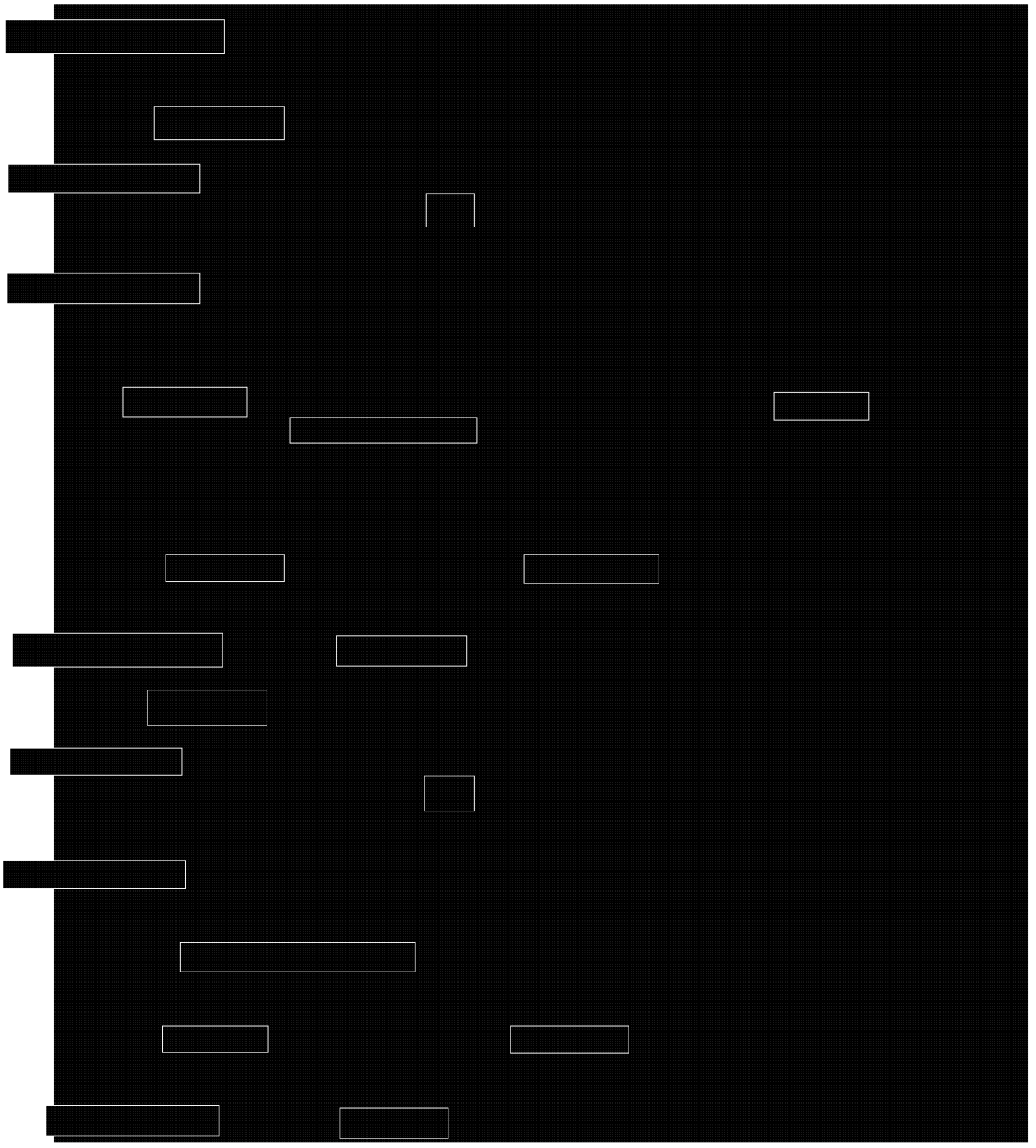
[redacted] is a CSEC-designed targeting and selector management database. It is accessed exclusively by [redacted] analysts do not have direct access to [redacted]

[redacted]

[26] DNI is also referred to as [redacted] (Internet) communications and may contain many different types of information (e.g., e-mail [redacted]

[27] DNR metadata generally refers to telephone and fax communications, and includes identifiers such as [redacted]

[28] CERRID# 338097-v1A, November 27, 2009, e-mail from Policy and Review Advisor, External Review and Policy Management, p. 7 and CERRID# 699823, February 8, 2011, e-mail from Director, Corporate and Operational Policy, p. 6.



3. How the tools process targeting and de-targeting requests

DNR selectors

CERRID# 368869, slide 14, October 15, 2009, e-mail from Policy and Review Advisor, External Review and Policy Management, November 27, 2009. Note: The above representation of a targeting system is a simplified version for presentation purposes.

To target or de-target a DNR selector, a [redacted] analyst enters certain information into [redacted] (a [redacted] analyst's responsibilities respecting targeting and documentation requirements are discussed at pp. 24-27). [redacted]

DNI selectors

TOP SECRET//COMINT//CANADIAN EYES ONLY

Communications Security Establishment Canada / Centre de la sécurité des télécommunications Canada

CSE analyst targeting/de-targeting
DNI Selector

[redacted]

Canada

CERRID# 368869, slide 13, October 15, 2009, e-mail from Policy and Review Advisor, External Review and Policy Management, November 27, 2009. Note: The above representation of a targeting system is a simplified version for presentation purposes.

There are three ways to target or de-target a DNI selector:

1. [redacted]
2.
3.

[29] [redacted] is the cover name for [redacted] activities and associated systems.

4. How the tools process targeting and de-targeting requests from the Second Parties

A Second Party sends a request to target a DNR selector [redacted]

A Second Party sends a request to target a DNI selector [redacted]

5. [redacted] authorities

[redacted] roles and responsibilities respecting targeting are namely:

- to validate and action, if appropriate, a targeting request of a [redacted] analyst; and
- to inform a [redacted] analyst of the status of a targeting request (approved or disapproved) and selector (targeted or de-targeted).

[redacted] authorities are detailed in CSOI-3-7, [redacted] *Authorities*[30]. For a targeting request, in accordance with CSOI-3-7, targeting is actioned by [redacted] provided that:

- the selector is in the right format;
- the targeting is directed at a foreign entity outside Canada;
- the targeting is related to an active GC intelligence requirement; and
- the targeting justification is adequate.

(pp. 24-27 and 34-36 contain detailed information respecting targeting research and documentation requirements.)

If all elements of a targeting request are valid, [redacted] forwards a selector to a collection system or systems, and the [redacted] analyst receives a notification that the targeting request has been approved.

If the request is deemed not valid, [redacted] rejects the request and provides a reason(s) for denial to the [redacted] analyst, who may adjust and re-submit the request. The new request for targeting is a new record in [redacted] and the original request that was refused remains a record.

[30] Effective September 2, 2008.

On November 25, 2009, the Commissioner's office received a demonstration and briefing from the [redacted] Team Leader, a [redacted] Analyst and a [redacted] Analyst respecting how [redacted] validates and denies a targeting request – for both CSEC-initiated and second party-initiated selectors – in [redacted] (with references to [redacted]

In addition, the Commissioner's office examined examples of special targeting circumstances, such as those involving the temporary use of [redacted]. We had also asked to examine a sample in [redacted] of [redacted] *selectors*[33] involving [redacted] IP addresses or other identifiers; however, as of the date of the demonstration (November 25, 2009), CSEC had not yet targeted any [redacted] selectors because no such selectors were identified to be of FI interest.

[redacted]

6. Volume of targeting requests

Respecting the quantity of selectors generally processed by [redacted] the Commissioner's office asked CSEC for information concerning the targeting requests [redacted] validated and forwarded to the collection systems in June to August 2009. CSEC responded:[34]

> Due to limitations inherent to targeting systems, CSEC can only provide a breakdown by agency for Digital Network Information (DNI) [Internet] selectors. For the months of June 2009, July 2009 and August 2009, [redacted] validated and forwarded to the collection systems the following number of targeting requests, by agency, as per [redacted] data:

[Requesting] Agency	Month	Total number of [DNI] targeting requests approved by [redacted] as [redacted]
DSD	June 2009	[redacted]
	July 2009	
	August 2009	
GCHQ	June 2009	
	July 2009	
	August 2009	
NSA	June 2009	
	July 2009	
	August 2009	
GCSB	June 2009	
	July 2009	
	August 2009	
CSEC	June 2009	
	July 2009	
	August 2009	

[redacted]

processed these [redacted] DNI selectors from June to August 2009. [redacted] teams were operational for 12 hours a day, five days a week, during that period of time.[35]

CSEC indicated that in June to August 2009, the U.S. NSA sent CSEC a series of updates to existing targeting requests [redacted] DNI selectors[36], and

[34] CERRID# 338097-v1C, e-mail from Policy and Review Advisor, External Review and Policy Management, January 8, 2010, p. 21.
[35] CERRID# 338097-v1H, e-mail from Policy and Review Advisor, External Review and Policy Management, September 1, 2010, p. 2.
[36] DNI selector [redacted] DNI selectors [redacted]

that these were automatically approved as they did not modify the four essential elements of information to validate a targeting request. This accounted for the increased volume of DNI selectors from the U.S. NSA during that period of time. The Commissioner's office has no questions respecting these updates.

CSEC targeting systems do not log the amount of time [redacted] employees dedicate to specific activities. CSEC indicated that the amount of time allocated to validate a targeting request may vary greatly depending on, e.g., whether the request contains one or several selectors, whether the selector(s) will be sent [redacted] and whether the selector(s) requires follow-up with the requestor to obtain clarification.

The Commissioner's office asked what action CSEC is taking to address the "limitations inherent to targeting systems" that permitted CSEC to only provide a breakdown by agency for DNI selectors. CSEC indicated that wher[redacted] [redacted] the ability to generate statistics regarding selectors across [redacted]

Given the absence of automated capabilities to generate statistics on DNR selectors for the period under review, the Commissioner's office asked CSEC to estimate and provide a general description based on experience of the approximate volume of DNR targeting requests in comparison to DNI requests. CSEC indicated:

> ...for the period of 1 September 2008 to 31 August 2009, based on manual extraction of available data, [redacted] counted [redacted] DNR selectors and [redacted] DNI selectors. From day to day, volumes vary considerably. Several factors may impact these numbers, such as [redacted] capabilities, shifting intelligence requirements, etc.[38]

Therefore, for the period under review, CSEC targeted approximately [redacted] times the amount of DNI selectors than DNR selectors. Based on the volume of selectors and number of [redacted] employees, it appears [redacted] employees process a significant number of selectors.[39] While these volumes appear significant, we assess them as manageable at this time because of the automation and safeguards built into CSEC's systems, the direction contained in CSEC's policies and procedures and the awareness of CSEC employees of the policies.

---

if the communications intercepted by CSEC's collection system is [redacted]

[37] *Supra*, note 35, at p. 3.
[38] *Supra*, note 35, at p. 3.
[39] Five [redacted] employees processed more than [redacted] selectors in one year. [redacted] processes targeting requests – not selectors – which may vary greatly in the number of selectors they contain, and the volume of targeting requests submitted on a daily basis may vary greatly.

The Commissioner's office also asked for information respecting the number of [redacted] analysts' targeting requests [redacted] initially rejected in June to August 2009. CSEC responded:[40]

> Due to limitations inherent to targeting systems, CSEC can only provide a monthly breakdown of rejected targeting requests for Digital Network Information (DNI) selectors, based on data stored in [redacted]
> The number of targeting requests generated by [redacted] analysts that were rejected by [redacted] for the months of June 2009, July 2009 and August 2009 are:

Agency	Month	Total number of targeting requests rejected by [redacted] as per [redacted]
CSEC	June 2009	[redacted]
	July 2009	
	August 2009	

Finally, respecting the quantity of selectors generally processed by [redacted] the Commissioner's office asked CSEC for information respecting the number of de-targeting requests received by [redacted] in November 2008 to January 2009. CSEC responded:[41]

> Based on [redacted] data (which holds targeting information about DNI selectors), [redacted] received the following de-targeting requests, by agency, for the months of November 2008, December 2008 and January 2009:

Agency	Month	Total number of de-targeting requests received by [redacted] based on [redacted] data
DSD	November 2008	[redacted]
	December 2008	
	January 2009	
GCHQ	November 2008	
	December 2008	
	January 2009	
NSA	November 2008	
	December 2008	
	January 2009	
GCSB	November 2008	
	December 2008	
	January 2009	
CSEC	November 2008	

[40] *Supra*, note 34, at p. 23.
[41] *Supra*, note 34, at pp. 23-24.

	December 2008 January 2009	[redacted]

7. Targeting using "strong selectors" – "Metadata-first rule"

Targeting using "strong selectors" allows SIGINT to pull information from the GII on the basis of unique communications addresses which can be reliably correlated with foreign entities in the physical world. [redacted]

CSOI-4-4, *Targeting and Selector Management Using* [redacted] *National SIGINT Systems for Intelligence Reporting Purposes*, March 5, 2009, (p. 33) describes a "strong selector" as follows:

> In the context of targeting activities, a strong selector is defined as an "identifier [redacted]

Section 2.5 of CSOI-3-7 indicates that [redacted] "ensure[s] that selectors targeted [redacted] metadata first." (emphasis added) Based on this statement,

[42] According to CSOI-4-4, [redacted]

the Commissioner's office asked CSEC if it intercepts communications, for itself or for the Second Parties, [redacted] using selectors [redacted] CSEC responded:

> In accordance with CSOI-3-7 and CSOI-4-4, CSEC intercepts communications using a metadata-first approach. An exception is made for [redacted] targeting [see pp. 30-37]; due to the [redacted] i.e. metadata and content. In addition, much of the intercept related to [redacted] involves [redacted] an associated expectation of privacy. At this time, [redacted]

"Strong selection" targeting research and documentation

[redacted] is CSEC's system of record for all selectors involving "strong selection".

In order to target a "strong selector", and in accordance with OPS-1 and OPS-1-13, CSOI-4-4[44] requires the following information to be researched by a [redacted] analyst and documented in [redacted] (each of which is described in detail below):

- the source *of the selector* and a *security classification*[45];
- associated GC intelligence requirement(s) (GCRs) and priority in line with the NSPL;
- foreign assessment (assessment to determine foreignness); and
- targeting justification.

Source of the selector

Examples of sources include: from SIGINT (e.g., an intercepted communication), metadata analysis, CSIS information or other human intelligence (HUMINT) and open sources (e.g., media).

---

[43] CERRID# 338097-v1E, February 19, 2010, e-mail from Policy and Review Advisor, External Review and Policy Management pp. 12-13 and CERRID# 699823, February 8, 2011, e-mail from Director, Corporate and Operational Policy, p. 8.

[44] Section 3.2, *Strong Selection Targeting Research and Documentation*, pp. 11-15.

[45] OPS-5-14, *The SIGINT Classification System*, June 2006, provides guidance respecting assigning security classification markings.

It has been a requirement to document the source of a selector since March 2009.[46] [redacted] also now includes a "technical block" that does not permit an analyst to continue with targeting until she/he completes a specific field in [redacted] with information respecting the source of a selector. The field is "free form"; analysts may choose what information and the level of detail to include in the field respecting the source of a selector.

Associated GCRs and priority in line with the NSPL

The [redacted] analyst must associate the selector with an entity (e.g., person, organization, network or communications equipment) of FI interest. According to CSEC, the GCRs are prioritized regularly and the NSPL is updated weekly.[47]

Foreign assessment

The [redacted] analyst must make an informed assessment of the foreign status of the entity associated with the selector by considering both the nationality as well as the location of the entity of interest (i.e., determine if the entity is not Canadian, and not from one of the 5-Eyes countries). Various pieces of information can assist in making this assessment, for example:

- [redacted]
- [redacted]
- [redacted]
- [redacted]

In isolation, some of these factors may be insufficient to make an assessment. It is the [redacted] analyst's responsibility to determine whether there is enough information to make an informed assessment of the foreign status of the entity. Second Party targeting requests are subject to the same validation process.

A [redacted] analyst may encounter information that indicates that an entity may be Canadian or a Canadian dual-national, e.g., intelligence suggests that the person studied or worked in Canada or has relatives in Canada. In such a case, an analyst may obtain passport or

[46] CSEC overview briefing respecting SIGINT Targeting and Selector Management, slide 7, September 2, 2009; CSOI-4-4 was effective March 11, 2009.

[47] The Commissioner receives a copy of the CSEC *Intelligence Priorities Ministerial Directive* that outlines the yearly GC intelligence priorities as approved by the Ad Hoc Committee of Ministers on Security and Intelligence. The MD directs CSEC to use these priorities to guide its FI activities in accordance with its legislative authority. CSEC derives the GCRs from this direction. CSOI-1-1, *The National SIGINT Priorities List (NSPL) Process*, effective July 17, 2008, outlines the process involved in the creation and maintenance of the NSPL. CSEC maps the GCRs to the NSPL to track efforts against national priorities.

citizenship information from Foreign Affairs and International Trade Canada, Citizenship and Immigration Canada, or the Canadian Border Services Agency in order to clarify the nationality of the entity.

A [redacted] analyst may also use open source information, e.g., information on [redacted] is often publicly available on the Internet.

Once the assessment to determine foreignness is made, the [redacted] analyst must document it by assigning the entity a *location digraph* [redacted] and an [redacted] *trigraph* indicating nationality (country digraph) and function (single letter code representing an entity's function, such as [redacted] The Five-Eyes community has adopted a common list of digraphs (Annex D). The nationality digraph in the [redacted] trigraph may not be the same as the target location digraph, [redacted]

As a matter of practice, [redacted] does not question the [redacted] foreign assessment (or second party) and relies on the analyst's informed assessment.[48]

Targeting justification

The [redacted] analyst must enter a justification respecting why the selector is being targeted:

- who is the entity of interest?
- why is it being proposed for targeting?
- what activities is it suspected or known to be involved in?

CSOI-4-4 provides examples of adequate and inadequate justifications.

In addition to the above core elements, the [redacted] analyst must assign a [redacted]

CSOI-4-4 contains detailed guidance respecting the actions, roles and responsibilities respecting the process for submitting a targeting request relating to a "strong selector".[49] For each entity of interest, [redacted] generates a *target identification number* (TID).

[48] [redacted] brief and interviews, November 25, 2009, and August 25, 2010.
[49] Section 3.4, *Submitting a Targeting Request*, pp. 15-16.

According to CSEC as indicated in CSOI-4-4[50], a valid location digraph, nationality and function trigraph, GCR number, and an adequate targeting justification demonstrate that a [redacted] analyst has reasonable grounds to believe that targeting activities are aimed at a foreign entity located outside Canada, in response to a GC intelligence priority.

When viewing a communication intercepted by CSEC, a [redacted] analyst can determine the [redacted] However, if an intercepted communication is [redacted]

[redacted] analysts perform ongoing maintenance of selectors as part of their day-to-day jobs. [redacted] will flag [redacted] for re-examination selectors that are resulting in unusually large volumes of intercepted communications. [redacted] does not flag selectors that do not result in any intercepted communications.[51] In deciding whether to action a [redacted] targeting request, [redacted] "often" examines the detailed information in [redacted] respecting the source of the selector and the justification for targeting.[52]

Once a [redacted] analyst sends a selector to [redacted] for approval, the [redacted] analyst may not re-open and make changes to the associated record in [redacted] If [redacted] rejects the request for targeting, the [redacted] analyst may change and re-submit the request. The new request for targeting is a new record in [redacted] and the original request that was refused remains a record.

As indicated above, in October and November 2009, the Commissioner's office received demonstrations from [redacted] and [redacted] employees respecting "strong selection" and the use of [redacted]

[redacted] and the incident reported as a privacy incident.[53] CSEC keeps all incidents in the central Privacy Incidents File that is reviewed by the Commissioner's office.

[50] Section 3.3, *Demonstrating Legal Compliance*, p. 15.
[51] Demonstration and interviews, October 5, 2009.
[52] Interview, November 25, 2009.
[53] CSOI-4-4, section 3.12, [redacted], p. 20.

The Commissioner's office asked CSEC to explain the rationale to not treat as a privacy incident the first occurrence [redacted] CSEC responded:

> CSEC does not treat instances of [redacted] as privacy incidents, as the initial targeting request is based on a valid foreign assessment made by the analyst on the basis of information available at that time, which included a valid foreign [redacted]
>
> [redacted] On a daily basis, a listing of [redacted] is forwarded to [redacted] who manually de-targets the associated selectors, and then notifies the analysts that the selectors were de-targeted [redacted]
>
> CSEC recognizes that there is the potential for delays between the time [redacted] and the time it is de-targeted. At this time, the DNR targeting system cannot support automated de-targeting.[54]

CSEC explained how the automated tool works as follows:

[redacted]

8. Targeting for [redacted]

On December 22, 2009, a [redacted] analyst provided an overview briefing on targeting for [redacted] including targeting processes, roles and responsibilities, associated documentation,

[54] *Supra*, note 35, at p. 3.
[55] E-mail from Policy and Review Advisor, External Review and Policy Management, October 6, 2010.

and information repositories. In addition, the Commissioner's office observed first-hand [redacted] in a shared electronic directory.

OPS-3-1, *Procedures for* [redacted] *Activities*, December 23, 2009, governs CSEC's [redacted] activities conducted under both parts (a) and (c) of its mandate. [redacted] used by foreign entities of interest [redacted] are the targets of [redacted] activities. [redacted] opportunities may be identified by the [redacted] Group or a [redacted] analyst may identify a gap in collection and request such access. Sources for [redacted] selectors include open source information (e.g., public directories such as an e-mail list [redacted] analysis of previously acquired SIGINT, HUMINT and information provided by GC and second party partners.

Selectors for [redacted] SIGINT collection methods that involve "strong selection". Commissioner Gonthier's February 26, 2009, review report respecting CSEC activities under the 2004 to 2007 [redacted] Ministerial Authorizations provides in-depth background information respecting [redacted] activities.

[redacted] is CSEC's system of record for all selectors [redacted] A [redacted] analyst sends to [redacted] a targeting request for [redacted] These [redacted] are stored in a shared electronic folder, while associated research and documentation, including the assessment of foreignness, is stored in [redacted] Therefore, like targeting involving "strong selection", all targeting requests for [redacted] receive a unique target identification number (in [redacted]

CSEC is modifying [redacted] to accommodate [redacted] capabilities and eliminate the need to use [redacted] CSEC indicated that it is planning to take a phased approach, enabling requests for [redacted] activities as a first step, beginning in the next fiscal year (2011-2012).[56]

While developing or [redacted] if there is any suggestion that a targeted entity is not foreign, [redacted] is located in Canada or that communications of a Canadian may be involved, the [redacted] employee is required to halt activities and immediately file a *Non-Standard Operations* report.[57]

The [redacted] analyst interviewed by the Commissioner's office indicated that he validated selectors on an ongoing basis [redacted] (in his case, approximately [redacted] Therefore if a selector

[56] E-mail from Policy and Review Advisor, External Review and Policy Management, November 25, 2010. The [redacted] activities are described in OPS-3-1, *Procedures for* [redacted] *Activities*.

[57] [redacted] *Standard Operating Procedure*, section 206, Reporting Non-Standard Operations.

did not after some time result in intercepted communications or if it produced irrelevant communications, the analyst would de-target the selector.

[redacted] *targeting research and documentation*

Like targeting involving "strong selection", and in accordance with OPS-1, all targeting requests for [redacted] requires the following information to be researched by a [redacted] analyst and documented in [redacted]

- the source *of the selector* and a *security classification*;
- associated GCRs and priority in line with the NSPL;
- assessment to determine foreignness; and
- targeting justification.

However, CSOI-4-4 does not apply to [redacted] Section 1.3 of CSOI-4-4 notes: [redacted]

Section 6.2 of OPS-3-1 indicates that:

> CSEC maintains a list of selection criteria for identifying targets [redacted] [i.e., intercepted] Before any [redacted] activities can be conducted, CSEC personnel must be satisfied, based on all the information that CSEC has available to it at the time, that the proposed selection criteria are associated with a foreign entity located outside Canada, and that they relate to a GC intelligence priority." (p. 17)

OPS-3-1 does not contain detailed guidance like the CSOI-4-4 instructions. (See finding no. 16, *Policies and Procedures for* [redacted] *Targeting*, p. 53)

9. Targeting for [redacted]

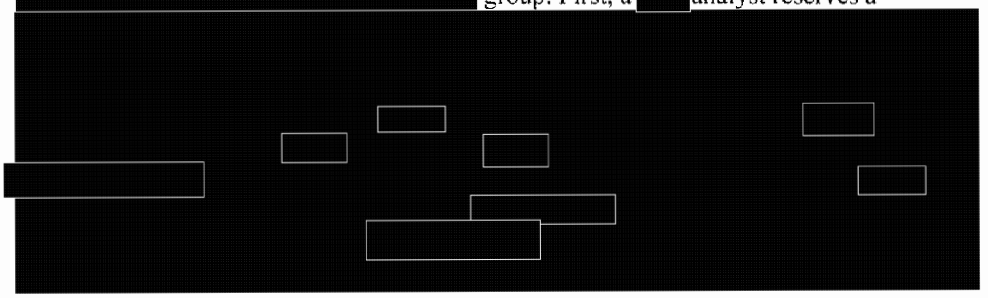
[redacted]

At the time of the preparation of this report, CSEC conducted [redacted] activities [redacted] selectors may be metadata [redacted] which will reduce the likelihood of inadvertently targeting Canadian persons or persons in Canada."[58]

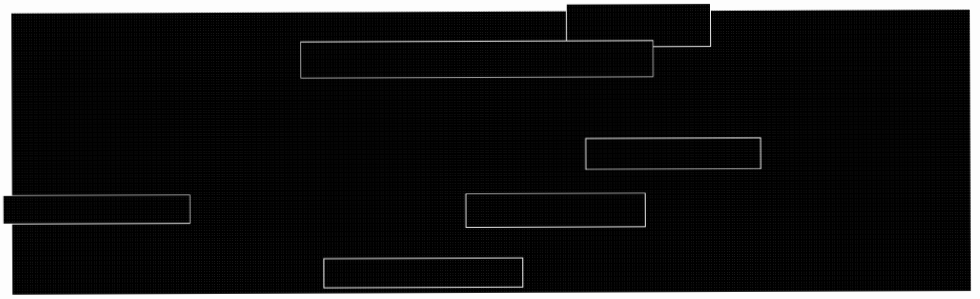
[redacted] *targeting process* [redacted]

[58] *Supra*, note 28, at p. 13.

The preceding diagram[59] illustrates the targeting process. In short, targeting is developed by approved by and actioned by group. First, a analyst reserves a



mostly involves the analysis of analysts in examine both the metadata and content of intercepted data, to provide FI



On November 2, 2009, CSEC provided an overview briefing on and On November 25, 2009, the Commissioner's office received a second brief from an Analyst, respecting targeting processes, roles and responsibilities, associated documentation, and information repositories. In addition, the Commissioner's office observed first-hand the use of targeting and for targeting.

targeting requests are stored in targeting – like those used for - in a shared electronic folder, while associated research and documentation, including the assessment to determine foreignness, is stored in

[59] CERRID# 368869-v1, e-mail from Policy and Review Advisor, External Review and Policy Management, November 27, 2009, at slide 4 (with amendments).

November 2, 2009.

[62] *Supra*, note 59.

CSEC indicated that: "[r]equirements for [redacted] to accommodate [redacted] selectors for targeting have been submitted to [redacted] Due to current priorities and limited resources, CSEC has not yet set timelines for implementing [redacted] targeting capability in [redacted]"[63] Following approvals from [redacted] targeting information in [redacted] Prior to conducting [redacted] to identify [redacted] A number of tools such as [redacted] inform [redacted] targeting by [redacted] CSEC SIGINT [redacted]

When intercepted communications related to [redacted] are deemed essential for FI purposes and become the subject of a SIGINT end-product report, the communications are stored in a special directory in [redacted] and the [redacted] analyst can link the communications to the associated report in [redacted] When the intercepted communications are not used in a report, the communications are automatically deleted from [redacted] Records in [redacted] whether on a [redacted] retention schedule [redacted] retained materials - are accessible only by [redacted] employees.

[redacted] analysts view intercepted communications using tools which offer a view of the information exchanged by [redacted] retained for analysis and reporting, the content of that communication is assessed, and if it is recognized to be a PC, it is marked and handled as such, in accordance with OPS-1.

The intercepted communication viewed by a [redacted] analyst may consist of [redacted] communication that is [redacted] or that suggests the possibility of [redacted] When the intercepted communication viewed by a [redacted] analyst consists of a [redacted] communication or is [redacted] but is not deemed essential for FI purposes and is not used in reporting, it is automatically deleted after [redacted] along with all unessential, un-reported communications.

[63] *Supra*, note 43, at p. 7.

In the [redacted] context, a large portion of intercepted communications is [redacted]

CSEC indicated that: "[h]istorically and for the period under review, CSEC did not have clarity on the status of [redacted] and erred on the side of caution by marking [redacted] as 'private communications'."[64] [redacted] as well as [redacted] collected for the purpose of [redacted] and used in reporting were stored in a special directory in [redacted] tracked in [redacted] and reported as PCs in the context of the annual accountability letter to the Minister on MAs for each of CSEC's collection programs. CSEC does not compile separate metrics for [redacted]

CSEC indicated that:

> CSEC recognizes that this reporting practice may have distorted results for the period under review, as we did not distinguish between [redacted] communications. Under the current version of OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities*, Solicitor-Client Privilege
> Solicitor-Client Privilege
> Solicitor-Client Pr in the annual accountability letter to the Minister on Ministerial Authorizations for each of our collection programs.[65]

Solicitor-Client Privilege

[redacted] targeting research and documentation

Similar to "strong selection", [redacted] targeting activities require the following to be documented in targeting [redacted] and in [redacted]

- justification;

The [redacted] analyst in [redacted] must describe the [redacted]

- assessment to determine foreignness (based on past observed activities);

The [redacted] analyst in [redacted] must make an informed assessment respecting the foreign status of the entity associated with the [redacted] activity by considering, [redacted]

[64] *Supra*, note 43, at pp. 7-8.
[65] *Supra*, note 43, at p. 8.

[redacted] further characteristics such as [redacted] may assist CSEC in making the foreign assessment.

- [redacted]
- extent of targeting; and

The [redacted] analyst in [redacted] is responsible to develop [redacted] are as specific as possible [redacted] and to refine them as FI becomes available.

- associated GCRs.

The following GCRs are related to [redacted] activities:

[redacted]

The associated NSPL priorities are:

- Tier 1 - [redacted]
- Tier 2 - [redacted]

CSOI-4-4 contains detailed guidance respecting the actions, roles and responsibilities respecting the process for [redacted] targeting.[69]

The Commissioner's office questioned the following statement in CSOI-4-4:

> The targeting documentation requirements for [redacted] selectors [redacted]

[redacted]

[67] *Supra*, note 35, at p. 5.
[68] *Ibid.*
[69] Section 4.4, *Submitting a* [redacted] *Targeting Request*, pp. 25-26.

of the potential for collecting private communications or traffic with Canadian content. (p. 23)

In some respects at first glance, this statement appears to be inconsistent with the foreign assessment requirements that appear to be less rigid than for targeting using "strong selection". It also appears inconsistent as a "strong selector" is generally linked to a specific GCR related to the targeted entity whereas a selector for [redacted] targeting is generally linked to broad GCRs. The Commissioner's office asked CSEC to clarify why it believes [redacted] targeting documentation is more extensive. CSEC responded:

> [redacted] SIGINT analysts who conduct [redacted] activities develop [redacted] Targeting [redacted] could therefore be perceived as being a more [redacted] activity than "metadata-first" [redacted] While the entity [redacted] Therefore, in theory, the likelihood of intercepting a communication (but not necessarily a private communication) originating or terminating in Canada may increase. In practice, what CSEC targets and acquires [redacted] are [redacted] The language in the CSOI was intended to reflect this *potential* for collecting private communications. As CSEC's familiarity with and experience in [redacted] targeting further develops, CSEC will consider revising the language in the CSOI.
>
> [redacted] analysts in [redacted] are expected to document their activities extensively, by describing the [redacted]
>
> Furthermore, analysts in [redacted] are expected to develop [redacted] that are as specific as possible, to reduce the volume of interception, which in turn reduces the risk of inadvertently collecting private communications or communications with information about Canadians.
>
> Finally, requirements for documentation assist with audit and review activities, by providing supporting evidence that the [redacted] selectors are associated with activities of foreign entities located outside Canada, in support of Government of Canada intelligence priorities.[70]

[70] *Supra*, note 28, at pp. 2-3.

The Commissioner's office accepts CSEC's explanation and has no remaining questions respecting the controls in place for [redacted] targeting. CSEC has indicated that it will consider revisions to its procedures and we will monitor any changes made.

SIGINT indicated that it may provide [redacted]

The Commissioner's office asked questions respecting how CSEC SIGINT's [redacted] interacts with CSEC IT Security's [redacted] Specifically, we asked questions respecting a statement made during interviews that sharing between SIGINT and IT Security is limited to reporting [redacted] CSEC responded:

[redacted]

The Commissioner's office has no outstanding questions respecting the sharing of selectors between CSEC SIGINT and IT Security.

[71] E-mail from Policy and Review Advisor, External Review and Policy Management, December 10, 2010.
[72] *Supra*, note 28, at p. 4.

10. Volume of/metrics respecting selectors

Number of "strong selectors" in [redacted]

The Commissioner's office asked CSEC: what is the total number of "strong selectors" in [redacted] and how many of the selectors are CSEC selectors and how many were originated by CSEC's second party partners? CSEC responded:[73]

> Current targeting systems are not designed to produce comprehensive metrics. [redacted] is the target knowledge base which contains the selectors targeted by CSEC analysts, not those targeted by other agencies.
>
> CSEC is able to extract information from [redacted] which holds targeting data on Digital Network Information (DNI) selectors only, by agency.
>
> As of 31 August 2009, the total number of strong DNI selectors with a targeted status in [redacted] by agency:

Agency	Total number of strong DNI selectors targeted via CSEC [redacted] in [redacted]
DSD	[redacted]
GCHQ	
NSA	
GCSB	
CSEC	

Number of "strong selectors" [redacted]

The Commissioner's office asked CSEC: how many CSEC "strong selectors" and how many second party selectors were [redacted] into the dictionaries [redacted] CSEC responded:

> Due to limitations inherent to targeting systems, CSEC can only provide a breakdown by agency and by collection program for [redacted] (Dialled Number Recognition (DNR)) [redacted]

[73] *Supra*, note 35, at p. 18.

As of 31 August 2009, the following numbers of DNR selectors were targeted under each collection program, by agency:

Collection Program	Agency	Total number of targeted DNR selectors by collection program
[redacted]	CSEC	[redacted]
	GCHQ	
	NSA	
	DSD	
	GCSB	
	TOTAL	
[redacted]	CSEC	
	GCHQ	
	NSA	
	DSD	
	GCSB	
	TOTAL	
[redacted]	CSEC	
	GCHQ	
	NSA	
	DSD	
	GCSB	
	TOTAL	
[redacted]	CSEC	
	GCHQ	
	NSA	
	DSD	
	GCSB	
	TOTAL	
[redacted]	CSEC	
	GCHQ	
	NSA	
	DSD	
	GCSB	
	TOTAL	

[redacted]

[74] *Supra*, note 34, at pp. 18-19.

Number of selectors

Respecting the Commissioner's office asked CSEC: what is the total number of targeted by CSEC in the collection systems? During the November 2, 2009, brief, the Manager, queried the system and indicated that as of the brief, were currently being targeted. In response to a written question, CSEC indicated that as of August 31, 2009, CSEC had

Number of selectors per analyst

The Commissioner's office asked CSEC: "Generally, how many selectors is a analyst responsible to manage?" CSEC responded:

> The number of selectors that a analyst is responsible to manage varies greatly, depending on the nature of the entities that are targeted. Some manage some some manage Some entities have many selectors associated with them, and therefore the task of managing is not as demanding as it seems. Other entities have few selectors, which produce considerable amount of traffic. There is not an "average" number of selectors.[76]

CSEC's written response is consistent with the answers provided by analysts in interviews.

Audit of selectors

The Commissioner's office asked CSEC a number of questions respecting whether it audits the selectors in its targeting databases . CSEC responded:

> CSEC does not have an automated means to regularly audit selectors in its targeting databases, Each targeting request that is
>
> In accordance with CSOI-5-8, responsible for conducting a monthly comparison of targeted selectors in

[75] *Supra*, note 28, at p. 12.
[76] *Supra*, note 28, at p. 6.
[77] *Supra*, note 28, at pp. 6-7.

[redacted] with those [redacted] dictionaries; however, current systems do not allow for this. A requirement has been submitted for [redacted] to develop the capability. In the meantime, [redacted] dictionaries are synchronized with [redacted] on a [redacted] basis. [redacted] maintains a copy of the synchronization. At this time, the synchronization is applied for DNI selectors [redacted] there is no capability to perform synchronization [redacted][78] For DNR selectors, a synchronization is performed for [redacted] on a [redacted] basis, and for other directories [redacted] it is done when needed, approximately every [redacted] For [redacted] receives an e-mail acknowledgement that [redacted] collection [redacted] did indeed receive a given targeting request (for both DNR and DNI selectors), which reduces the need for synchronization, as potential issues are flagged in almost real-time.[79]

(See finding no. 8, *Limitations in Targeting and Selector Management Systems*, p. 45, and finding no. 10, *Demonstrating Legal Compliance – Follow-up to the Commissioner's 2008 Review of* [redacted] *Activities*, p. 48.)

It is perplexing that CSEC would put in policy a requirement to do something that its current systems do not permit.

11. Targeting by CSEC for the Second Parties

CSEC subjects second party targeting requests to CSEC's requirements, e.g., selectors must be metadata associated with a foreign entity outside Canada and associated with a GC intelligence priority. According to CSEC, it will not enable a Second Party to target entities that CSEC is not permitted to target. CSEC rejects requests that do not match its criteria [redacted]

[redacted] validates and forwards targeting requests [redacted] when selectors submitted by a Second Party:

- relate to a foreign entity (expressed via the nationality trigraph);
- relate to an entity located outside Canada (expressed via the location digraph);
- are accompanied by a justification detailing why the entity is of interest; and

[redacted]

[79] *Supra*, note 43, at pp. 10-11.

- are consistent with an active Government of Canada intelligence requirement (GCR).

Assessment to determine foreignness

Second Parties provide CSEC with a foreign assessment consisting of a location digraph and a nationality and function trigraph. Like a CSEC targeting request, the foreign status of the entity is documented in the form of [redacted] (the trigraph) which is a three-letter combination that indicates the target's nationality and function[redacted] As a matter of practice, [redacted] does not question and relies on the Second Parties' foreign assessments associated with a proposed selector.

Also like a CSEC targeting request, a second party targeting request includes a location digraph that identifies the second party analyst's assessment of the[redacted] of the targeted entity. Provided the targeting request contains an acceptable target digraph, as a matter of practice, [redacted] accepts and does not question the Second Party's assessment of the foreign location of the entity.

As a result of limitations in certain [redacted] for the period of review, in some cases in relation to CSEC targeting of second party DNR selectors, the foreign location information submitted by the second party may not have accurately represented the second party analyst's assessment of the[redacted] of the targeted entity. This is because second party [redacted] digraph automatically based on the [redacted] associated with the targeted selector and could not therefore take into account targets[redacted] This limitation has been addressed in [redacted]

Targeting justification

Due to targeting tool design constraints associated with [redacted] to be addressed in [redacted] the five-eyes community has developed a list of agreed upon abbreviations (Annex G provides a sample of these abbreviations) to include justification information [redacted] When the information is unclear or incomplete, [redacted] contacts the requester for additional details. If the information provided still does not clearly answer the essential questions of *who, what, where* and *why*, [redacted] rejects the request. The Commissioner's office reviewed and has no questions respecting a sample of second party [redacted] targeting requests with abbreviated justifications.[80]

Associated GCR

A selector submitted by a Second Party for targeting [redacted]

[80] CERRID# 605885, September 1, 2010, e-mail from Policy and Review Advisor, External Review and Policy Management, pp. 2-14.

[redacted] analysts are trained to match the second party request to a GCR based on the information provided regarding the foreignness and the justification for targeting. For the period under review, this was a manual process and associated GCRs were not recorded in [redacted] At this time, a specific field does not exist in these tools to record such information. CSEC indicated that: "Targeting systems are currently undergoing a transformation; the new system is being designed to address this requirement. Based on the assumption that there are no changes in resources, priorities, or strategy, CSEC plans to implement a capability to associate Second Party targeting requests to GCRs during FY 2011/2012."[81]

[redacted] *interaction with the Second Parties*

[redacted] is in regular contact with the Second Parties to clarify operational, policy and technical requirements. [redacted] rejects incomplete second party targeting requests and may contact a Second Party to obtain more information regarding a specific request that is deficient and can not be actioned. For example, on November 25, 2009, [redacted] sent an e-mail to the [redacted] indicating that CSEC will not target a selector relating to an "unknown" or "unidentified" location or nationality. CSEC does not accept these values as they do not provide assurance that an entity of interest is foreign and/or located outside Canada.[82]

The Commissioner's office was interested in whether the Second Parties have work groups that perform similar functions to [redacted] and in the controls in place and the rigour of the second party targeting processes. In response to a request to review for factual accuracy draft notes based on an interview with CSEC, CSEC wrote: "With respect to other agencies' organizational design, CSEC does not have all the details. [redacted] has counterparts at all five-eyes partner agencies, however internal business processes vary."[83]

VIII. FINDINGS AND RECOMMENDATION

A) LEGAL REQUIREMENTS

Finding no. 1: Compliance with the Law

Based upon the information reviewed and the interviews conducted, CSEC conducts its SIGINT targeting and selector management activities in accordance with the law.

[81] *Supra*, note 43, at pp. 4-5.
[82] CERRID# 452880, February 19, 2010, e-mail from Policy and Review Advisor, External Review and Policy Management.
[83] *Supra*, note 43, at p. 5.

Finding no. 2: Protection of Canadians

CSEC has sufficient policies and processes to satisfy the legal requirement not to direct its SIGINT interception activities at a Canadian (anywhere) or any person in Canada.

The *NDA* requires that activities under part (a) of CSEC's mandate, including SIGINT targeting and selector management activities, shall be:

- consistent with the GC intelligence priorities (paragraph 273.64(1)(a))[84];
- not directed at Canadians or any person in Canada (paragraph 273.64(2)(a)); and
- subject to measures to protect the privacy of Canadians in the use and retention of intercepted information (paragraph 273.64(2)(b)).

The Commissioner's office's examination and sample results indicate that CSEC is only using approved selectors for collection, the selectors are directed at foreign entities outside Canada, and the selectors are consistent with the GC intelligence priorities.

The number of [redacted] analysts' DNI targeting requests initially rejected by [redacted] is an indication that [redacted] is performing its function to validate a targeting request for compliance with the law and CSEC policy. (See p. 22.)

The number of [redacted] analysts' DNI de-targeting requests processed by [redacted] is an indication that [redacted] analysts regularly de-target a selector that is no longer valid or productive. (See pp. 22-23.)

Finding no. 3: Targeting by CSEC for the Second Parties – Volume of Selectors

Approximately [redacted] per cent of the selectors CSEC targeted [redacted] were originated by CSEC; approximately [redacted] per cent of the selectors at CSEC [redacted] were targeted by CSEC for the Second Parties.

CSEC, with approximately 1,800 employees, is a member of a community that is approximately [redacted] strong (the US' NSA employs approximately [redacted] the UK's GCHQ approximately [redacted] Australia's DSD approximately [redacted] and New Zealand's GCSB approximately [redacted]. As such, personnel-wise, CSEC represents approximately [redacted] of the community. [redacted] The volume of selectors is discussed at pp. 38-40.

[84] According to OPS-1, selectors are subject to annual review to ensure they are consistent with GC intelligence priorities.
[85] CERRID# 699823, February 8, 2011, e-mail from Director, Corporate and Operational Policy, p. 10.

Finding no. 4: Targeting by CSEC for the Second Parties – Foreign Nationality and Location Assessments

As a matter of practice, CSEC relies on and does not question the Second Parties' foreign nationality and location assessments for targeting.

CSEC conducts its targeting for the Second Parties in accordance with the law and assesses second party selectors using the same criteria applied to CSEC-initiated selectors. CSEC ensures that the Second Party assessment of foreign location and nationality are congruent with the targeting justification. Second party targeting requests do not contain contextual information respecting how the nationality and location of a target was determined. CSEC's employees are trained to recognize, and targeting systems flag, identifiers likely relating to a Canadian or person in Canada (e.g., Canadian telephone area codes or Internet addresses) (See pp. 40-42.) The Commissioner's office is reviewing SIGINT information sharing with the Second Parties.

Finding no. 5: Targeting by CSEC for the Second Parties – Government of Canada Intelligence Requirements

CSEC's plan to implement in FY 2011-2012 a capability in [redacted] to record the Government of Canada intelligence requirement(s) associated with a second party targeting request is a positive development that will increase accountability with legal requirements.

Currently, however, CSEC does not record the GCR(s) associated with a second party targeting request. The Commissioner's office will monitor CSEC's efforts to implement in [redacted] a capability to record the GC intelligence requirement(s) associated with a second party targeting request.

Finding no. 6: Demonstrating Legal Compliance – Recording the Source of a Selector

It is a positive development – that assists in demonstrating compliance with the law, ministerial requirements and policy – that in March 2009, [redacted] analysts were required – by policy and by technical means – to record in [redacted] the source of a selector.

CSEC practices and sample results respecting documenting the source of a selector are discussed at pp. 24-25, 27, 30, 33, 54-55 and 57.

Finding no. 7: Targeting and Selector Management Systems that Promote Privacy Protection

CSEC takes measures in the design of its targeting and selector management systems and databases to promote compliance with the law and the protection of the privacy of Canadians.

CSEC has automated the targeting process to the extent possible and has in place extensive audit logging as well as active and compliance monitoring. To the extent current technology permits, CSEC regularly synchronizes dictionaries of selectors [redacted] with targeting systems and databases.

[redacted] automatically de-targets selectors with the [redacted] digraph that have not been reviewed and updated with a precise country digraph within [redacted] of the initial targeting request, as required by CSOI-4-4. (See footnote 32, p. 19.)

[redacted] contains controls to document compliance. For example, once a [redacted] analyst sends a targeting request to [redacted] for approval, the [redacted] analyst may not re-open and make changes to the associated record in [redacted] An amended request for targeting is treated as a new record in [redacted] and the original request that was refused remains a record. (See p. 27.)

CSEC uses technology to limit the unintentional targeting of DNR [redacted] however, CSEC does not have at this time an automated tool to identify if other DNR or DNI Internet devices [redacted] (See p. 28.)

[redacted]

Respecting CSEC targeting for the Second Parties, it is a positive development that [redacted] has addressed previous limitations in [redacted] respecting justification information and to address targets [redacted] (See p. 42.)

Finding no. 8: Limitations in Targeting and Selector Management Systems

The Commissioner's office will monitor ongoing CSEC efforts to address deficiencies in targeting and selector management systems and databases.

It is a positive development that [redacted] will, when fully deployed, address limitations in current targeting systems that permit CSEC to only provide a breakdown of targeted selectors by agency for DNI selectors and include the ability to generate statistics regarding selectors [redacted] (See p. 21.)

The Commissioner's office will monitor CSEC efforts to modify its systems to permit a monthly comparison of targeted selectors in [redacted] with those [redacted] in the dictionaries [redacted] (See p. 60.)

The Commissioner's office will also monitor CSEC efforts to modify [redacted] to accommodate targeting for [redacted] and [redacted] targeting capability and eliminate the need to use [redacted] (See pp. 29 and 33.)

1. Targeting of [redacted] selectors

During the period under review, [redacted] approved targeting requests for [redacted] selectors. All were for DNI selectors. Such e-mail or IP addresses, which may be [redacted] may be targeted provided [redacted] analysts have adequate justification to demonstrate the associated entity is foreign. The Commissioner's office examined a random sample of five such targeting requests generated by CSEC and by the Second Parties.[86] These selectors complied with CSEC policies and procedures, specifically the requirement to demonstrate that the associated entity is foreign.

2. Privacy incidents – unintentional targeting of a Canadian or person in Canada

Finding no. 9: Privacy Incidents – Unintentional Targeting of Canadians

During the period under review, CSEC responded appropriately to the [redacted] privacy incidents it identified and that involved the unintentional targeting of Canadians.

It is possible that a Canadian or a person in Canada is unintentionally targeted, e.g., as a result of unexpected travel or incomplete information received by CSEC from another GC entity.

Sections 2.6 and 2.7 of OPS-1 and section 3.15 of CSOI-4-4 require CSEC to take the following actions as soon as possible if a Canadian or person in Canada is unintentionally targeted:

- the [redacted] analyst informs her or his supervisor, immediately submits a de-targeting request, annotates in the CTR[87] any associated traffic for deletion, and cancels [redacted][88] any associated SIGINT reports;

[86] *Supra*, note 80, at pp. 3-14.
[87] CSEC's Common Traffic Repository (CTR) is the single data repository for CSEC SIGINT's intercepted information.
[88] [redacted] is CSEC's SIGINT production and dissemination system (including Second Party reporting). It is used for client requirements gathering; end-product report authoring, storage and searching; dissemination of reports; and as a reporting feedback tool. Access to documents in [redacted] is strictly controlled, e.g., based on security clearance and indoctrinations, caveats, and user access permissions.

- [redacted] de-targets the selector on a priority basis;
- the [redacted] section deletes any communications from CSEC databases;
- a [redacted] supervisor notifies SIGINT Programs, Oversight and Compliance (SPOC)[89] and Operational Policy Section of the incident and apprises them of actions taken; and
- the incident is recorded in CSEC's Privacy Incident File (PIF).

During the period under review, CSEC identified and recorded [redacted] privacy incidents involving the unintentional targeting of a Canadian (Annex E).[90] The PIF includes a description of the incidents, the groups involved, how the incident was observed, why the incident occurred, potential damages, actions taken and follow-on activities. The Commissioner's office assessed CSEC's responses to the incidents as appropriate.

3. CSEC's activities in response to the 2008 review of CSEC's activities conducted under the [redacted] MD and MA

Finding no. 10: Demonstrating Legal Compliance – Follow-up to Commissioner's 2008 Review of [redacted] Activities

The improvements to CSEC's policies and procedures – namely CSOI-3-7 and CSOI-4-4 – as well as the enhancements made or planned to associated systems and databases address the negative findings relating to targeting and selector management in the Commissioner's 2008 review of CSEC's [redacted] activities.

Specifically, the Commissioner's office considers findings 12, 13, 25, 27 and 28 of Commissioner Gonthier's 2008 [redacted] review as addressed.[91]

---

[89] Among its responsibilities, SPOC conducts compliance validation monitoring of [redacted] active monitoring procedures for SIGINT targeting and selector management activities. SPOC is authorized to halt targeting activities that are not compliant.

[90] CERRID# 345109, October 22, 2009, e-mail from Policy and Review Advisor, External Review and Policy Management.

[91] *Finding no. 12*: Based upon the information provided and the comments of the CSE[C] staff interviewed, policy was found stating the requirement of this imposed condition [that the interception will be directed at foreign entities located outside Canada] but little evidence could be found reflecting specific procedures. *Finding no. 13*: The absence of any requirement to document the reasonable grounds upon which an analyst has determined that a selector is directed at foreign entities located outside Canada and is consistent with the [GC] intelligence priorities leaves no means to audit and review approved selectors and thus renders [the Commissioner's office] incapable of verifying compliance with this condition. *Finding no. 25*: As a result of the identified limitations, [the Commissioner's office] cannot assess compliance with the statutory requirement that intercept of private communications must be directed at foreign entities located outside Canada. *Finding no. 27*: The provided information leads to the conclusion that [redacted] is an incomplete database of DNI and DNR selectors [redacted]

CSOI-4-4 requires [redacted] analysts to record all selectors in [redacted][92] CSEC has implemented processes to enforce the use of [redacted] as the single repository for targeted selectors. All targeting requests forwarded to [redacted] for approval [redacted] must have a [redacted]-generated target identity number, confirming the selectors are recorded in [redacted] CSEC indicated: [redacted]

The [redacted] selector dictionaries [redacted] and other collection [redacted] are updated on a [redacted] or more frequent basis to make certain that the content of the [redacted] dictionary (and that of other collection programs) matches the list of authorized selectors documented in [redacted] (the synchronization processes are described in detail at p. 41 and 60).

4. CSEC's activities in response to the 2008 review of CSEC's [redacted] activities

Finding no. 11: Second Party Targeting Requests – Follow-up to 2008 Review of CSEC's [redacted] Activities

Improvements to CSEC's policies and procedures – namely CSOI-4-4 – as well as significant systems development efforts by CSEC will address the negative finding relating to targeting and selector management in the Commissioner's 2008 review of CSEC's [redacted] activities.

Finding no. 6 in Commissioner Gonthier's 2008 [redacted] review report was:

> Pending the development of an automated system, we question how CSEC can confirm that selectors (proposed by CSEC or by a Second Party) remain valid, directed at a foreign entity located outside Canada, and consistent with a FI priority of the Government of Canada.

At the time of the [redacted] report, there was no standard process, annually or otherwise, when CSEC sought confirmation from its analysts and the Second Parties that a selector remained valid and should continue to be used. There was no set period of time after which CSEC and second party selectors automatically expired. CSEC asked its analysts and the Second Parties to confirm that selectors related to ongoing and important targets in cases where [redacted]

Finding no. 28: Analysis of the content of the required automated database of selectors does not provide the means to verify that CSE[C] has grounds to believe that all intercept of private communications is related to foreign entities located outside Canada.

[92] This is a requirement of all MAs except for the [redacted] MA.

[93] *Supra*, note 28, at p. 8.

The Minister responded to the [redacted] report in a September 10, 2008, letter:

> In your letter, you questioned how CSEC can confirm that SIGINT selectors remain valid, directed at a foreign entity located outside Canada, and consistent with a foreign intelligence priority of the Government of Canada. While it is clear that the present system does not facilitate annual reviews of selectors, CSEC is developing an automated system which will require that selectors are reviewed and validated annually. This system will be implemented by the end of May 2009.

CSOI-4-4, section 5, *Validation and De-Targeting* (pp. 27-29) now requires targeted selectors to be reviewed on a regular basis. It requires [redacted] analysts to validate, at a minimum annually, the four elements of a targeting request (i.e., assessment to determine foreignness, location, GCR(s), and justification). When any of the four elements are no longer valid, the analyst must send to [redacted] a de-targeting request. The targeting history of a selector is recorded in [redacted] including: the date range during which a selector was targeted, and, if appropriate, the reason for de-targeting.

CSEC has also invested significant development resources to address this previous finding of the Commissioner. [redacted] which will replace current targeting tools, will prompt analysts to review and validate selectors once a year after a selector is first submitted. CSEC described the status of this work as follows:

> Presently, CSEC is finalizing work on the annual selector validation tool to implement the automatic de-targeting of selectors when validation has not been performed in the last year (365 days). This automatic de-targeting mechanism will be an additional safeguard in ensuring that targeted selectors are directed at foreign entities located outside Canada, and that the associated intercept is in response to Government of Canada intelligence requirements. CSEC anticipates this work will be completed before the end of the current fiscal year [2009-2010]. This date is based on the assumption that there are no changes in resources, priorities, or strategy. The automated system will apply an expiry date to a selector upon targeting, such that a selector will "expire" 365 days after the initial targeting is approved, or 365 days after the last update or validation was performed. Also, a Validation Date will be generated, based on the initial approval date of the last update or validation date (whichever is later). Three months (90 days) prior to the expiry date of a targeted selector (365 days after its approval), an alert will be sent to the analyst responsible for this selector, reminding them to validate the selector by the expiry date. If the selector is not validated at the expiry date, it will be automatically de-targeted by the system.[94]

[94] *Ibid*, at p. 7.

5. CSEC's activities in response to 2006 CSEC audit of SIGINT Legal Compliance

Finding no. 12: Second Party Targeting Requests – Follow-up to 2006 CSEC Audit of SIGINT Legal Compliance

The Commissioner's office is satisfied that CSEC has addressed the negative finding in CSEC's 2006 SIGINT Legal Compliance Final (audit) Report respecting second party targeting requests.

An April 12, 2006, audit by CSEC's Directorate of Audit Evaluation and Ethics (DAEE) entitled "SIGINT Legal Compliance Final Report" found: "Some of these [Second Party] tasking requests do not have a corresponding Canadian requirement. Nevertheless, the resulting collection is forwarded to both the requesting second party and to the CSE DT/IR [the DT/IR is CSEC's former primary SIGINT information repository that has been replaced by the CTR]. As a result, there can be intercepts in the DT/IR that are not directly linked to an approved Canadian selector or a GCR." DAEE recommended: "DC SIGINT should assess the consequences of acquiring collection within the DT/IR that is not associated with an appropriate GCR". (pp. 8-9)

As a follow-up to the 2006 audit, the Commissioner's office asked CSEC how it has addressed this recommendation of DAEE; is it now possible to link all second party selectors to a GCR? CSEC responded:

> The data stored in the CTR (formerly DT/IR) is exclusively based on CSEC selected traffic, which is associated with a selector targeted in support of Government of Canada intelligence needs, expressed via [GCRs]. Collection managers responsible for the vetting of targeting requests, including those from [the] Second Parties, are expected to map all requests to GCRs, in accordance with on-the-job training guidelines. Collection managers refer to the weekly Watching Briefs and [the] National SIGINT Priorities List, as they assess the validity of Second Party targeting requests.[95]

6. Legal Advice

Finding no. 13: [redacted] ***Communications***

CSEC's decision to no longer count [redacted] as private communications will clarify accountability reporting to the Minister.

Solicitor-Client Privilege

[95] *Ibid*, at pp. 14-15.

Solicitor-Client Privilege

OPS-1; CSEC did not request and Justice Canada did not provide a separate legal opinion on this subject.

OPS-1, dated December 23, 2009, section 2.8, *SIGINT Privacy Annotations and Verification Requirements*, states that [redacted]

As explained in the section on [redacted] *targeting research and documentation* at pp. 34-37, data intercepted for the purpose of [redacted] is purged after [redacted] unless it is deemed essential for FI purposes.

The Commissioner's office has no questions respecting the advice Solicitor-Client Privilege Solicitor-Client Privilege

B) MINISTERIAL REQUIREMENTS

Finding no. 14: Ministerial Direction

Based upon the information reviewed and the interviews conducted, CSEC conducts its SIGINT targeting and selector management activities in accordance with ministerial direction.

CSEC met the requirement in the ministerial authorizations to facilitate the review by the CSE Commissioner of the statutory requirement that interceptions of private communications must be directed at foreign entities located outside Canada by

Solicitor-Client Privilege

[97] *Supra*, note 43, at p. 8.

establishing and maintaining an automated directory of selectors [redacted] which CSEC has grounds to believe relate to foreign entities located outside Canada.

CSEC met the requirement in the Ministerial Directive on Privacy to have procedures to minimize the unintentional collection of the communications of Canadians.

One of the conditions to issue an MA under the *NDA* is that the Minister of National Defence must be "...satisfied that... the interception will be directed at foreign entities located outside Canada" [paragraph 273.65(2)(*a*)]. CSEC has indicated that the threshold of "reasonable grounds to suspect" is appropriate for this condition because there may be technological challenges (e.g., [redacted] and because prior to targeting, CSEC may have only information about the [redacted] Unlike the RCMP or CSIS that have other methods to learn about their targets, CSEC may know little or nothing about the foreign entities to be targeted.

C) POLICIES AND PROCEDURES

Finding no. 15: Appropriateness of Policies and Procedures

Operational policies and procedures for SIGINT targeting and selector management activities are in place and provide sufficient direction to CSEC employees respecting the protection of the privacy of Canadians.

The Commissioner's office expected that CSEC would have appropriate policies and procedures that guide its SIGINT targeting and selector management activities. CSEC has a number of policy instruments – issued under the authority of the Chief, CSEC – and procedures – issued under the authority of the DC, SIGINT, CSEC – that contain guidance respecting targeting and selector management. Overall, the following policies and procedures provide comprehensive guidance for targeting and selector management activities:

a) OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities*, effective and last updated March 11, 2010 (CERRID# 142875-v6J);

   OPS-1 is CSEC's "cornerstone" policy and provides direction respecting the protection of the privacy of Canadians in the use and retention of intercepted information and compliance with the laws of Canada, including Part V.1 of the *NDA*, and with ministerial direction.

b) OPS-1-13, *Procedures for Canadian* [redacted] *Activities*, December 23, 2009 (CERRID# 319956-v5);

This policy documents the approval process for [redacted] collection programs conducted under part (a) of CSEC's mandate; prescribes an accountability trail for these activities; provides direction respecting the treatment of communications acquired pursuant to MDs and MAs relating to these activities; and outlines measures to protect the privacy of Canadians.

c) OPS-3-1, Procedures for [redacted] Activities, December 23, 2009 (CERRID# 317036-v3);

This policy documents the approval process for [redacted] activities; prescribes an accountability trail for these activities; provides direction respecting the treatment of communications acquired pursuant to MDs and MAs relating to these activities; and outlines measures to protect the privacy of Canadians.

IRRELEVANT

e) CSOI-1-1, *The National SIGINT Priorities List (NSPL) Process*, July 17, 2008;

These instructions outline the process for the creation and maintenance of the NSPL.

f) CSOI-3-7, [redacted] Authorities, September 2, 2008; and

These instructions describe the authorities and responsibilities of [redacted].

g) CSOI-4-4, *Targeting and Selector Management Using* [redacted] *National SIGINT Systems for Intelligence Reporting Purposes*, March 5, 2009;

These are the principal instructions providing detailed direction to CSEC and the Canadian Forces Information Operations Group (CFIOG) SIGINT analysts respecting the targeting of foreign selectors and the management of these selectors.

CSEC indicated that it is considering changes to CSOI-4-4 to provide additional guidance respecting how to document in [redacted] the source of a selector.[98] Increased specificity and consistency in such records could

[98] Interview, Manager, SIGINT Programs, Oversight and Compliance, August 25, 2010.

permit CSEC to better demonstrate compliance (as well as enhance operations). For example, it is unclear why, when appropriate, [redacted] analysts are not required to record in [redacted] the serial number of a report or an identifier of an intercepted communication that was the source of a selector. The Commissioner's office will monitor CSEC's efforts respecting this subject. (See finding no. 6, *Demonstrating Legal Compliance – Recording the Source of a Selector*, p. 44)

Finding no. 16: Policies and Procedures for [redacted] Targeting

Operational policies and procedures applicable to [redacted] provide limited direction respecting targeting for such activities.

CSOI-4-4 does not apply to targeting requests for [redacted] While the interviews and sample results demonstrated that CSEC used appropriate selectors for [redacted] collection, CSEC should document specific policy or operations instructions for [redacted] to clarify obligations and strengthen CSEC's ability to meet legal and ministerial requirements.

Recommendation no. 1: Policies and Procedures for [redacted] Targeting

CSEC should provide specific guidance for [redacted] targeting.

h) GPW-003-07 (GPWs are working aids), [redacted]

i) GPW-004-07, *Summary of Interim CSE*[C]*/CFIOG Targeting Procedures*, May 10, 2007.

These guidelines summarize targeting rules for Canadian collection activities conducted under part (a) of CSEC's mandate.

It should be noted that the GPW-003-07 and GPW-004-07 working aids were in effect in 2008 and were subsumed by the publication of CSOI-4-4 in March 2009 (Annex 2 and Annex 1 respectively).

CSEC's activities in response to the 2008 reviews of CSEC activities conducted under the [redacted] MAs

Finding no. 17: Guidance for Targeting and Selector Management – Follow-up to 2008 Reviews of CSEC's [redacted] Activities

Improvements to CSEC's policies and procedures – namely CSOI-3-7 and CSOI-4-4 – address the recommendation in the Commissioner's 2008 [redacted] review and the negative finding in the 2008 [redacted] review relating to guidance for targeting and selector management.

The 2008 [redacted] MA and 2008 [redacted] MA reviews identified as an issue the lack of documentation, to support the reasonable grounds upon which a [redacted] analyst has assessed that a selector is directed at a foreign entity located outside Canada and is consistent with a GC intelligence requirement, which diminishes the Commissioner's capability of review.

Recommendation no. 1 of the 2008 [redacted] MA report was that: "CSEC adopt and publish, as soon as practicable, written guidance respecting the process [redacted] analysts are to follow when deciding whether to approve or reject a selector."

On September 18, 2008, CSEC promulgated CSOI-3-7 which addresses the authorities and responsibilities of [redacted] analysts for validating selectors. CSOI-4-4 provides comprehensive guidance respecting targeting, including requirements for documenting and validating selectors.

Finding no. 18: Awareness of Personnel

CSEC employees interviewed and observed were aware of relevant policies and procedures and their application to SIGINT targeting and selector management activities.

Finding no. 19: Policies and Procedures

Based upon the information reviewed and the interviews conducted, CSEC met the policy requirement that selectors are subject at a minimum to annual review to ensure that the selectors remain consistent with the Government of Canada intelligence priorities.

The Commissioner's office expected that CSEC employees would be aware of and comply with the policies and procedures respecting SIGINT targeting and selector management activities.

All of the CSEC employees with whom the Commissioner's office spoke were forthcoming and demonstrated knowledge of and a professional approach to the activities under review. The managers and employees in [redacted] and in SPOC that we interviewed demonstrated a mastery of SIGINT targeting and selector management activities and associated policies and procedures.

The Commissioner's office conducted interviews with six [redacted] analysts to assess their awareness of and compliance with the policies and procedures. Annex F provides details respecting the approach and sample for the [redacted] interviews. The [redacted] employees interviewed and observed were aware of relevant policies and procedures and their application to SIGINT targeting and selector management activities. The information and documentation reviewed indicated that the actions of the [redacted] employees were in compliance with policies and procedures. The [redacted] analysts regularly reviewed selectors to ensure that the selectors remain consistent with the GC intelligence priorities.

Based on our sample, while most targeting documentation requirements were met, [redacted] analysts did not always document in [redacted] the source of a selector. When it was documented, it was done in different ways, and with different levels of detail. Some analysts included in [redacted] comprehensive information or a clear link to the source of a selector (e.g., link to a CSEC report or to intercepted communications). Other analysts included more limited information in notes fields. Some [redacted] analysts did not include in [redacted] information about the source of a selector. In such cases, however, the analysts readily identified in interviews the source of their selectors, despite the fact that the source was not documented in [redacted]

The uneven compliance by [redacted] analysts with the policy requirement to document the source of a selector observed during interviews, results in part because of the period of time of the interview sample (i.e., pre-policy) and the newness of this as a mandatory requirement. It is our expectation that the changes made by CSEC to policy and to [redacted] has increased compliance with this requirement. (See finding no. 6, Demonstrating Legal Compliance – Recording the Source of a Selector, p. 45.) The Commissioner's office will monitor CSEC's efforts respecting this subject.

Finding no. 20: Management Control Framework

CSEC managers routinely and closely monitor SIGINT targeting and selector management activities to make certain the activities comply with governing authorities.

The Commissioner's office expected that CSEC would have an effective management control framework to maintain the integrity of SIGINT targeting and selector management activities, including appropriately accounting for important decisions and

information. To assess CSEC's compliance with this criterion, the Commissioner's office asked CSEC a number of questions respecting its active and compliance monitoring activities.

The Commissioner's office asked CSEC: pursuant to section 2.8 of CSOI-4-4, does CSEC have evidence to demonstrate that analysts have successfully completed the OPS-1 on-line quiz and that [redacted] Team Leaders and CFIOG Supervisors "ensure analysts review and validate targeted selectors on a regular basis, at least annually, in accordance with OPS-1-8 [*Active Monitoring of Operations to Ensure Legal Compliance and the Protection of the Privacy of Canadians*, effective December 23, 2008]..."? Does CSEC record and maintain written records of the test results respecting such management monitoring? CSEC responded:

> The Office of SIGINT Studies (OSS) keeps records of the test results of the online OPS-1 quiz. Quiz results are automatically forwarded to the OSS and to the analyst who has taken the quiz. Monitoring of OPS-1 Quiz results is not done at the moment. Team leaders and managers also ensure analysts act in compliance with all OPS and instructions including OPS-1 and CSOI-4-4, as part of their ongoing supervisory duties and also in the context of the annual performance review exercise.[99]

It is perplexing that CSEC would require a quiz but not evaluate the results.

The Commissioner's office asked CSEC whether management monitoring occur annually or more frequently. CSEC responded: "Monitoring is ongoing, with a minimum requirement of once per year. CSEC team leaders send reminders to their team members to conduct validation. CSEC does not have a record that team leaders or managers have audited the validation process."[100] Interviews with [redacted] employees and mangers confirmed that validation occurs on an ongoing basis.

The Commissioner's office asked CSEC: consistent with section 2.1 of OPS-1-8, *Active Monitoring of Operations to Ensure Legal Compliance and the Protection of the Privacy of Canadians*, December 23, 2008, please describe in concrete terms what active monitoring activities [redacted] operational supervisors and managers do on a regular basis and what compliance monitoring activities SPOC does respecting CSEC SIGINT's targeting and selector management activities. CSEC responded:

> In accordance with OPS-1-8 and CSOI-4-4, [redacted] operational supervisors and managers ensure that:
>
> - staff is familiar and complies with all policies and instructions that impact targeting;
>
> - staff has successfully completed the OPS-1 online quiz; and

[99] *Supra*, note 28, at p. 14.
[100] *Ibid.*

- staff validates selectors at least once per year.

[redacted] supervisors and managers also inform Operational Policy and SPOC when Canadians or persons in Canada have been unintentionally targeted and report the corrective measures that have been applied.

While not in the period of review, CSOI-5-8, *Active Monitoring Procedures for* [redacted] came into effect on 5 January 2009. Since then, SPOC has been working with [redacted] to ensure compliance checks are implemented.

SPOC gathers information when an unintentional targeting incident has occurred, and reports the matter to Operational Policy. If SPOC identifies a problem in a given area, SPOC meets with the supervisor and staff of that area, and provides additional guidance to ensure compliance and prevent further incidents.[101]

The Commissioner's office asked CSEC: Consistent with section 1.5 of OPS-1-8, please provide copies of documentation maintained for audit and review purposes respecting active and compliance monitoring activities in relation to CSEC SIGINT's targeting and selector management activities for the period of June 1, 2009, to August 31, 2009. CSEC responded:

On a daily basis, the [redacted] team must ensure targeting and collection activities on each selector submitted by CSEC and Second Party analysts are compliant with and abide by Canadian and allied laws, statutes or policies.

In accordance with OPS-1-8 and CSOI-5-8, *Active Monitoring Procedures for* [redacted] collection managers in [redacted] receive a daily [redacted] report from the [redacted] On receipt of this report collection managers perform the following actions:

- use current operational policies and guidelines to identify which selector needs to be de-targeted;
- query selectors in targeting tool to identify the SIGINT analyst responsible for them;
- notify the responsible SIGINT analyst that selector de-targeting has occurred for their target;
- ensure [redacted] that have been de-targeted will only be retargeted upon the receipt of data confirming [redacted] and

[101] *Supra*, note 43, at p. 10.

- produce a monthly summary of [redacted] activity; the monthly summary will be documented in CERRID.

For the period under review, [redacted] has produced the following monthly [redacted] reports:

- CERRID #322588 (August 9 to August 31, 2009); and
- CERRID #317976 (July 9 to August 6, 2009).

[The Commissioner's office reviewed and has no questions respecting these reports (CERRID# 447609 and 447612).]

In accordance with CSOI-5-8, *Active Monitoring Procedures for* [redacted] is responsible for conducting a [redacted] comparison of targeted selectors in [redacted] with those on [redacted] collection at [redacted] however, current systems do not allow for this. A requirement has been submitted for [redacted] [SIGINT Systems Development] to develop the capability. In the meantime, [redacted] dictionaries are synchronized with [redacted] basis. [redacted] maintains a copy of the synchronization. At this time, the synchronization is applied for DNI selectors [redacted] there is no capability to perform synchronization [redacted] For DNR selectors, a synchronization is performed for [redacted] on a [redacted] basis, and for other directories [redacted] it is done when needed, approximately every [redacted] receives an e-mail acknowledgement that [redacted] collection [redacted] did indeed receive a given targeting request (for both DNR and DNI selectors), which reduces the need for synchronization, as potential issues are flagged in almost real-time.[102]

Finally, the Commissioner's office asked CSEC: please describe in brief the differences between [redacted] verification function and both types of monitoring. CSEC responded:

> In accordance with OPS-1-8, *Active Monitoring* is defined as the monitoring of operational activities to assess compliance with policy instruments in effect specifically related to legal compliance, and protection of the privacy of Canadians. This monitoring is done by operational supervisors and managers on a regular basis; first line Supervisors do this frequently (e.g., daily, weekly) while other levels of Management will do this on a less frequent basis (e.g., monthly), in accordance with operational instructions.
>
> *Compliance Validation Monitoring* is typically performed by SPOC (for SIGINT). As part of the second phase of Active Monitoring, SPOC will periodically and independently assess operational activities for compliance with policy instruments aimed at ensuring legal compliance, including the protection of the privacy of Canadians.

[102] *Ibid*, at pp. 10-11.

Active Monitoring

On a daily basis, collection managers in [redacted] conduct *active monitoring* of targeting requests, in accordance with CSOI-5-8, *Active Monitoring Procedures for* [redacted] Validation of targeting and collection activities constitutes Active Monitoring, as it ensures that targeting requests are compliant with and abide by Canadian laws and policies.

On a monthly basis, Collection managers conduct *active monitoring* of targeted selectors in targeting applications (e.g., [redacted]) with those on [redacted] collection in [redacted] dictionaries; any discrepancies are reported to the manager [redacted] also conducts active monitoring of [redacted] selectors and compiles a monthly report.

Compliance Validation Monitoring

On an annual basis, SPOC ensures that [redacted] staff have reviewed the necessary policies and procedures and completed the sign-off forms. SPOC documents any anomalies against this requirement and takes appropriate follow-up action.

On a monthly basis, SPOC conducts Compliance Validation Monitoring of [redacted] reports prepared by [redacted] and the synchronization of dictionaries and [redacted][103]

CSEC's answers to the above questions, as well as the results of the interviews with [redacted] and SPOC employees, permit the Commissioner's office to conclude that, despite ongoing CSEC efforts to clarify OPS-1-8 and improve SIGINT's active monitoring program in general, CSEC has a robust management control framework for SIGINT targeting and selector management activities. While not in the period of review, CSOI-5-8 appears to provide a solid foundation for active monitoring of SIGINT targeting and selector management activities.

IX. CONCLUSION

CSEC's FI collection activities conducted under MA involve a number of distinct methods of acquiring information from the GII. Nevertheless, there are a number of common business processes and associated tools, as well as common systems and databases, which support these collection methods and which CSEC uses to deal with the information obtained. For example, common to all of the collection methods are the processes by which CSEC selects foreign entities located outside Canada that are of FI interest (the subject of this report), uses, shares and reports information to clients and international partners, and retains or disposes of intercepted communications (the subjects of ongoing reviews). Rather than examine thoroughly individual MAs, it was assessed as more effective to examine

[103] *Ibid*, at pp. 11-12.

thoroughly each process common to CSEC's FI collection activities under MA. This new approach, which cuts across the collection methods, is referred to as *horizontal review* and is designed to provide the Commissioner with an even more comprehensive understanding of how CSEC conducts its activities. Ultimately, its objective is to increase the degree of assurance the Commissioner can provide to the Minister that CSEC is complying with the law and protecting the privacy of Canadians.

In a SIGINT context, targeting means to single out for collection or interception purposes. CSEC targets communications using selectors. Targeting and selector management are at the foundation of CSEC's SIGINT collection programs. SIGINT collection relies on targeting. Specific and important controls are placed on SIGINT targeting and selector management activities to ensure compliance with legal, ministerial and policy requirements. The potential impact to the privacy of Canadians would be significant, should there be an instance of non-compliance with the law while conducting these activities. Past Commissioners made findings and recommendations respecting these activities and which require follow-up. Major changes to certain technology and procedures relating to these activities have recently occurred and others are in progress. It is for these reasons that the Commissioner selected CSEC SIGINT's targeting and selector management activities as the subject of one of the first in-depth horizontal reviews of a SIGINT common business process.

To comply with the *NDA*, CSEC must distinguish those communications which involve foreign entities located outside Canada and those that are not. CSEC's targeting and selector management activities must also contain measures to protect the privacy of Canadians.

The objectives of the review were to: document CSEC SIGINT's targeting and selector management activities and associated processes and practices; assess whether the activities comply with the law; and assess the extent to which CSEC protected the privacy of Canadians in carrying out the activities.

Based upon the information reviewed and the interviews conducted, CSEC conducts its SIGINT targeting and selector management activities in accordance with the law. CSEC has sufficient policies and processes to satisfy the legal requirement not to direct its SIGINT interception activities at a Canadian (anywhere) or any person in Canada. During the period under review, CSEC responded appropriately to the [redacted] privacy incidents it identified and that involved the unintentional targeting of Canadians.

CSEC takes measures in the design of its targeting and selector management systems and databases to promote compliance with the law and the protection of the privacy of Canadians. As identified in this report, recent enhancements made or planned to these systems and databases assist in ensuring and demonstrating compliance with the law, ministerial requirements and policy.

However, the Commissioner's office will monitor ongoing CSEC efforts to address deficiencies identified in this report respecting targeting and selector management systems. The Commissioner's office will monitor CSEC's efforts to implement in [redacted] the ability to generate statistics regarding selectors across [redacted]

[redacted] as well as a capability to record the GC intelligence requirement(s) associated with a second party targeting request. The Commissioner's office will also monitor CSEC efforts to modify its systems to permit a monthly comparison of targeted selectors in [redacted] with those on [redacted] collection in the dictionaries [redacted] Finally, the Commissioner's office will monitor CSEC efforts to modify [redacted] to accommodate targeting for [redacted] and for [redacted] targeting capability (and thereby eliminate the need to use targeting [redacted]).

Based upon the information reviewed and the interviews conducted, CSEC conducts its SIGINT targeting and selector management activities in accordance with ministerial direction.

Operational policies and procedures for SIGINT targeting and selector management activities are in place and provide sufficient direction to CSEC employees respecting the protection of the privacy of Canadians. CSEC employees interviewed and observed were aware of relevant policies and procedures and their application to SIGINT targeting and selector management activities. CSEC managers routinely and closely monitor SIGINT targeting and selector management activities to make certain the activities comply with governing authorities.

However, operational policies and procedures applicable to [redacted] provide only limited direction respecting targeting for such activities. It is recommended that CSEC provide specific guidance for [redacted] targeting.

Based on our interviews, while most targeting documentation requirements were met, [redacted] analysts did not always document in [redacted] the source of a selector. This is important for accountability purposes and to assist CSEC in demonstrating that it met statutory requirements. When it was documented, it was done in different ways, and with different levels of detail. It is, however, a positive development – that assists in demonstrating compliance with the law, ministerial requirements and policy – that in March 2009, [redacted] analysts were required – by policy and by technical means – to record in [redacted] the source of a selector. CSEC indicated that it is considering changes to CSOI-4-4 to provide additional guidance respecting how to document in [redacted] the source of a selector. The Commissioner's office will monitor CSEC's efforts respecting this subject.

In addition to the above-noted objectives, the Commissioner's office examined CSEC's activities in response to previous associated findings and recommendations of the Commissioner in the June 2008 [redacted] review report and the March 2008 review report respecting [redacted] Improvements to CSEC's policies and procedures as well as significant development efforts made and other planned enhancements to associated systems and databases address the recommendation and negative findings in these reports.

Finally, the Commissioner's office examined CSEC's activities in response to previous associated recommendations of CSEC's Audit, Evaluation and Ethics Directorate. The Commissioner's office is satisfied that CSEC has addressed the negative findings in CSEC's 2006 SIGINT Legal Compliance Final (audit) Report respecting second party targeting requests.

A list of findings and the recommendation is enclosed at Annex A.

Robert Décary, Commissioner

ANNEX A – Findings and Recommendation

Finding no. 1: Compliance with the Law

Based upon the information reviewed and the interviews conducted, CSEC conducts its SIGINT targeting and selector management activities in accordance with the law.

Finding no. 2: Protection of Canadians

CSEC has sufficient policies and processes to satisfy the legal requirement not to direct its SIGINT interception activities at a Canadian (anywhere) or any person in Canada.

Finding no. 3: Targeting by CSEC for the Second Parties – Volume of Selectors

Approximately [redacted] per cent of the selectors CSEC targeted [redacted] were originated by CSEC; approximately [redacted] per cent of the selectors [redacted] were targeted by CSEC for the Second Parties.

Finding no. 4: Targeting by CSEC for the Second Parties – Foreign Nationality and Location Assessments

As a matter of practice, CSEC relies on and does not question the Second Parties' foreign nationality and location assessments for targeting.

Finding no. 5: Targeting by CSEC for the Second Parties – Government of Canada Intelligence Requirements

CSEC's plan to implement in FY 2011-2012 a capability in [redacted] to record the Government of Canada intelligence requirement(s) associated with a second party targeting request is a positive development that will increase accountability with legal requirements.

Finding no. 6: Demonstrating Legal Compliance – Recording the Source of a Selector

It is a positive development – that assists in demonstrating compliance with the law, ministerial requirements and policy – that in March 2009, [redacted] analysts were required – by policy and by technical means – to record in [redacted] the source of a selector.

Finding no. 7: Targeting and Selector Management Systems that Promote Privacy Protection

CSEC takes measures in the design of its targeting and selector management systems and databases to promote compliance with the law and the protection of the privacy of Canadians.

Finding no. 8: Limitations in Targeting and Selector Management Systems

The Commissioner's office will monitor ongoing CSEC efforts to address deficiencies in targeting and selector management systems and databases.

Finding no. 9: Privacy Incidents – Unintentional Targeting of Canadians

During the period under review, CSEC responded appropriately to the [redacted] privacy incidents it identified and that involved the unintentional targeting of Canadians.

Finding no. 10: Demonstrating Legal Compliance – Follow-up to Commissioner's 2008 Review of [redacted] Activities

The improvements to CSEC's policies and procedures – namely CSOI-3-7 and CSOI-4-4 – as well as the enhancements made or planned to associated systems and databases address the negative findings relating to targeting and selector management in the Commissioner's 2008 review of CSEC's [redacted] activities.

Finding no. 11: Second Party Targeting Requests – Follow-up to 2008 Review of CSEC's [redacted] Activities

Improvements to CSEC's policies and procedures – namely CSOI-4-4 – as well as significant systems development efforts by CSEC will address the negative finding relating to targeting and selector management in the Commissioner's 2008 review of CSEC's [redacted] activities.

Finding no. 12: Second Party Targeting Requests – Follow-up to 2006 CSEC Audit of SIGINT Legal Compliance

The Commissioner's office is satisfied that CSEC has addressed the negative finding in CSEC's 2006 SIGINT Legal Compliance Final (audit) Report respecting second party targeting requests.

Finding no. 13: [redacted] Communications

CSEC's decision to no longer count [redacted] as private communications will clarify accountability reporting to the Minister.

Finding no. 14: Ministerial Direction

Based upon the information reviewed and the interviews conducted, CSEC conducts its SIGINT targeting and selector management activities in accordance with ministerial direction.

Finding no. 15: Appropriateness of Policies and Procedures

Operational policies and procedures for SIGINT targeting and selector management activities are in place and provide sufficient direction to CSEC employees respecting the protection of the privacy of Canadians.

Finding no. 16: Policies and Procedures for [redacted] Targeting

Operational policies and procedures applicable to [redacted] provide limited direction respecting targeting for such activities.

Finding no. 17: Guidance for Targeting and Selector Management – Follow-up to 2008 Reviews of CSEC's [redacted] Activities

Improvements to CSEC's policies and procedures – namely CSOI-3-7 and CSOI-4-4 – address the recommendation in the Commissioner's 2008 [redacted] review and the negative finding in the 2008 [redacted] review relating to guidance for targeting and selector management.

Finding no. 18: Awareness of Personnel

CSEC employees interviewed and observed were aware of relevant policies and procedures and their application to SIGINT targeting and selector management activities.

Finding no. 19: Policies and Procedures

Based upon the information reviewed and the interviews conducted, CSEC met the policy requirement that selectors are subject at a minimum to annual review to ensure that the selectors remain consistent with the Government of Canada intelligence priorities.

Finding no. 20: Management Control Framework

CSEC managers routinely and closely monitor SIGINT targeting and selector management activities to make certain the activities comply with governing authorities.

Recommendation no. 1: Policies and Procedures for [redacted] Targeting

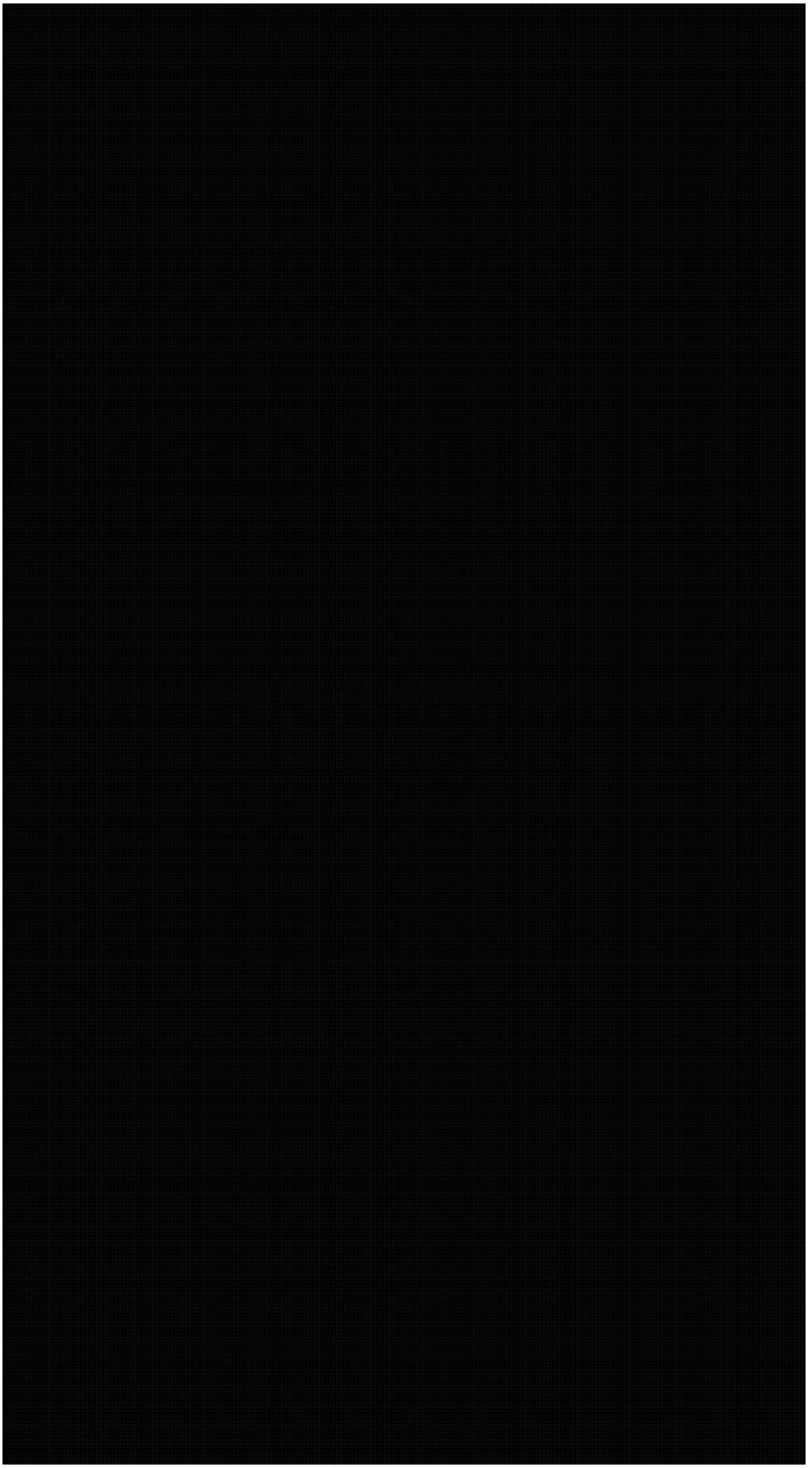
CSEC should provide specific guidance for [redacted] targeting.

ANNEX B – Interviewees

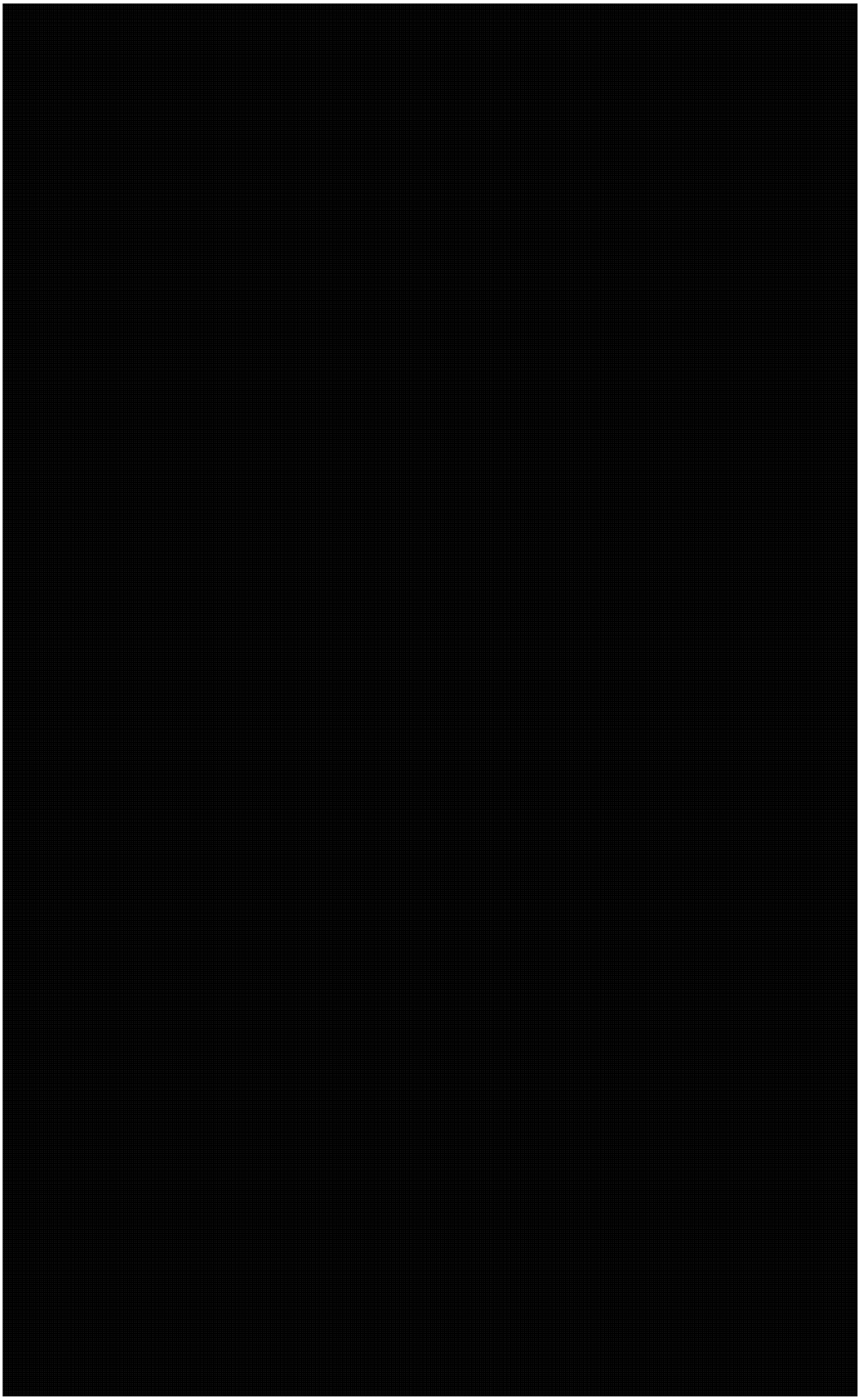
Director, SIGINT Requirements
Manager, [redacted]
Manager, [redacted]
Manager, SIGINT Programs, Oversight and Compliance (SPOC)
Manager, SIGINT Systems Development
Team Leader, [redacted]
Collection Analyst, [redacted]
Specialist - Linguist, [redacted]
Intelligence Analyst, [redacted]
Intelligence Analyst, [redacted]
Intelligence Analyst [redacted]
Intelligence Analyst, [redacted]
Intelligence Analyst, [redacted]
Intelligence Analyst, [redacted]
Intelligence Analyst [redacted]
Intelligence Analyst, Office of Counter Terrorism [redacted]
Senior Advisor, SPOC
Director, Corporate and Operational Policy
A/Director, Corporate and Operational Policy
Manager, External Review and Policy Management
Policy and Review Advisor, External Review and Policy Management

ANNEX C – Generic "Screenshots" of [redacted]

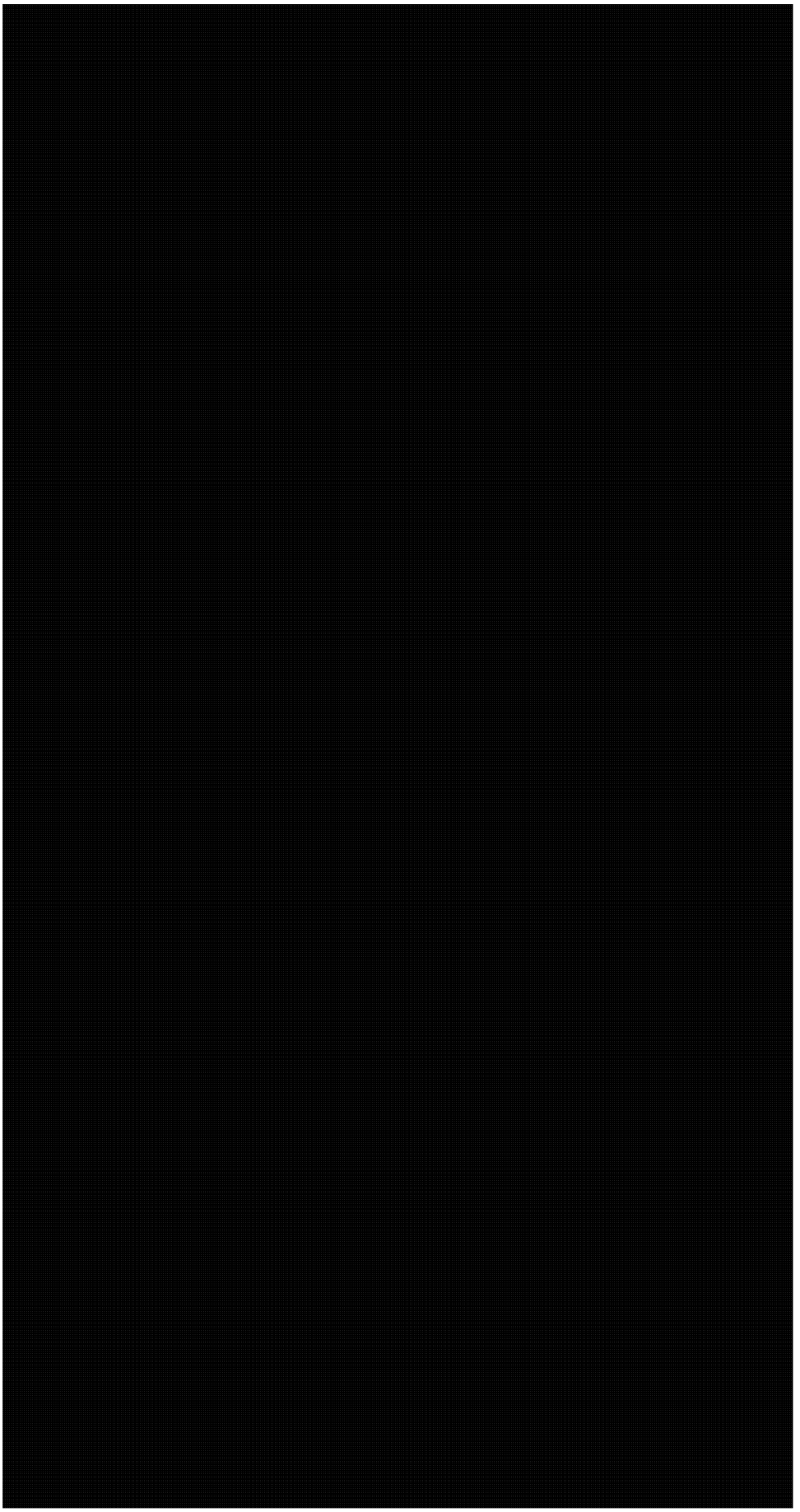
Source: CERRID# 364700, 10 pages, hand delivered by Policy and Review Advisor, External Review and Policy Management on November 2, 2009.

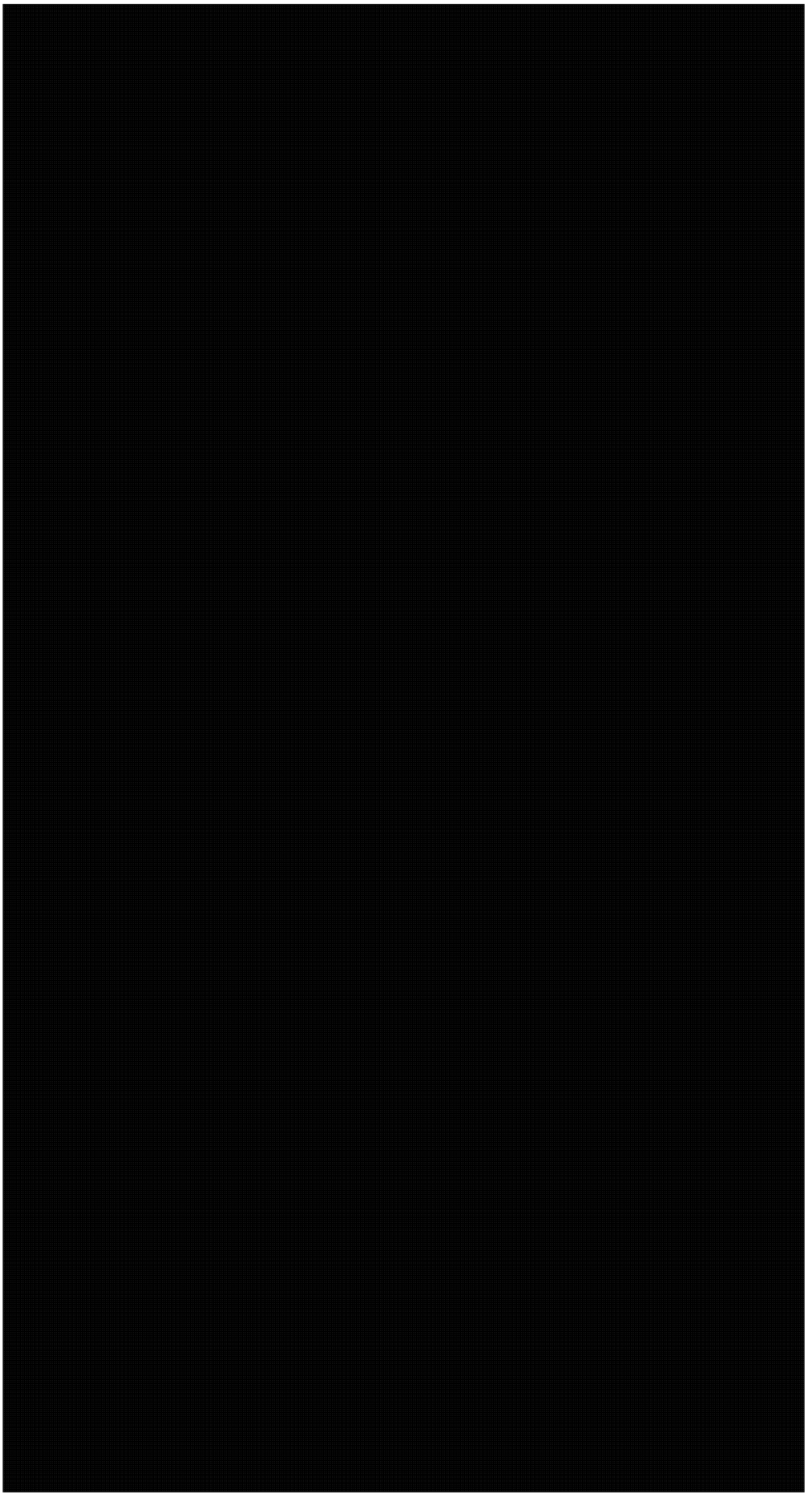


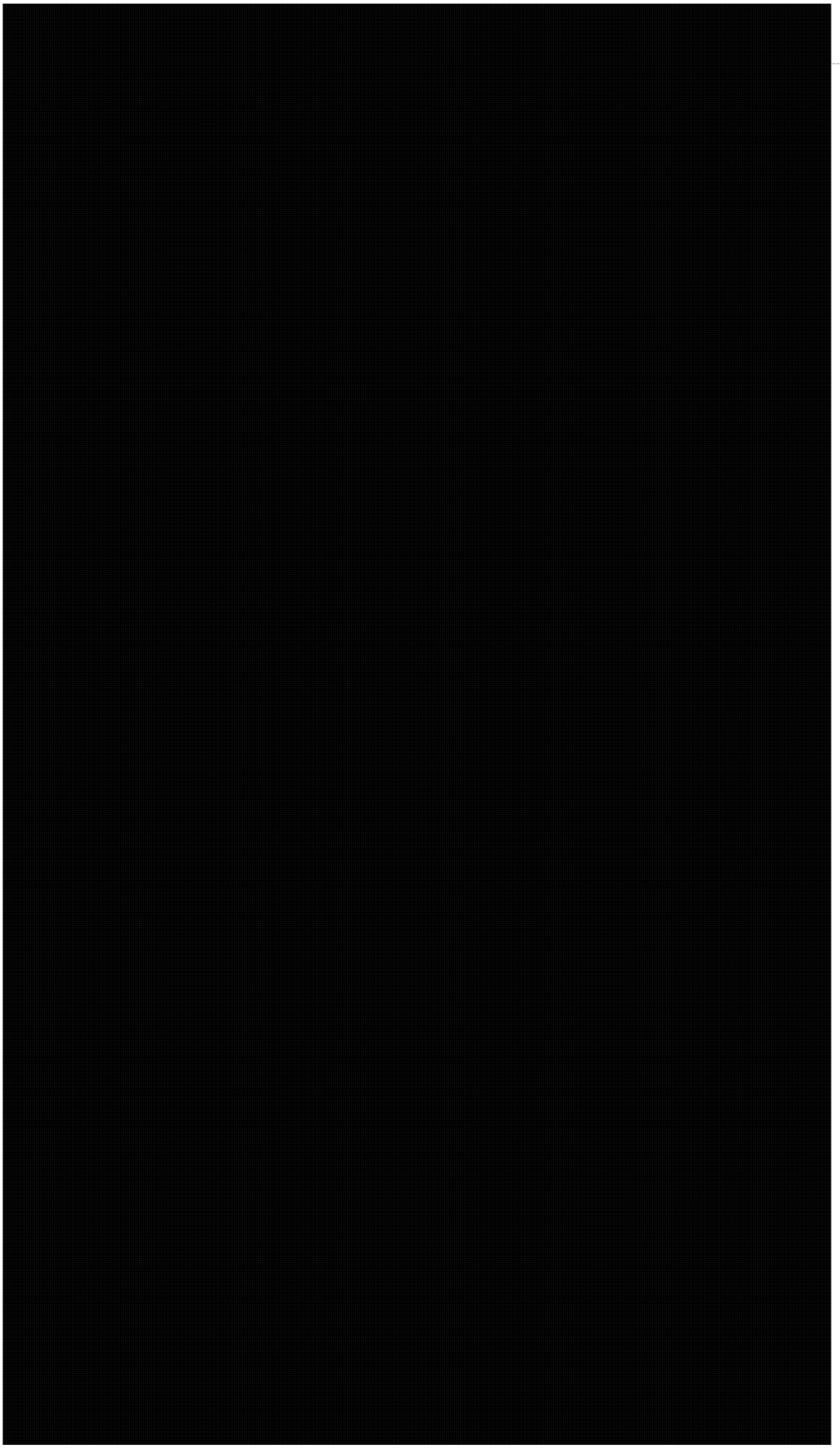
[redacted]



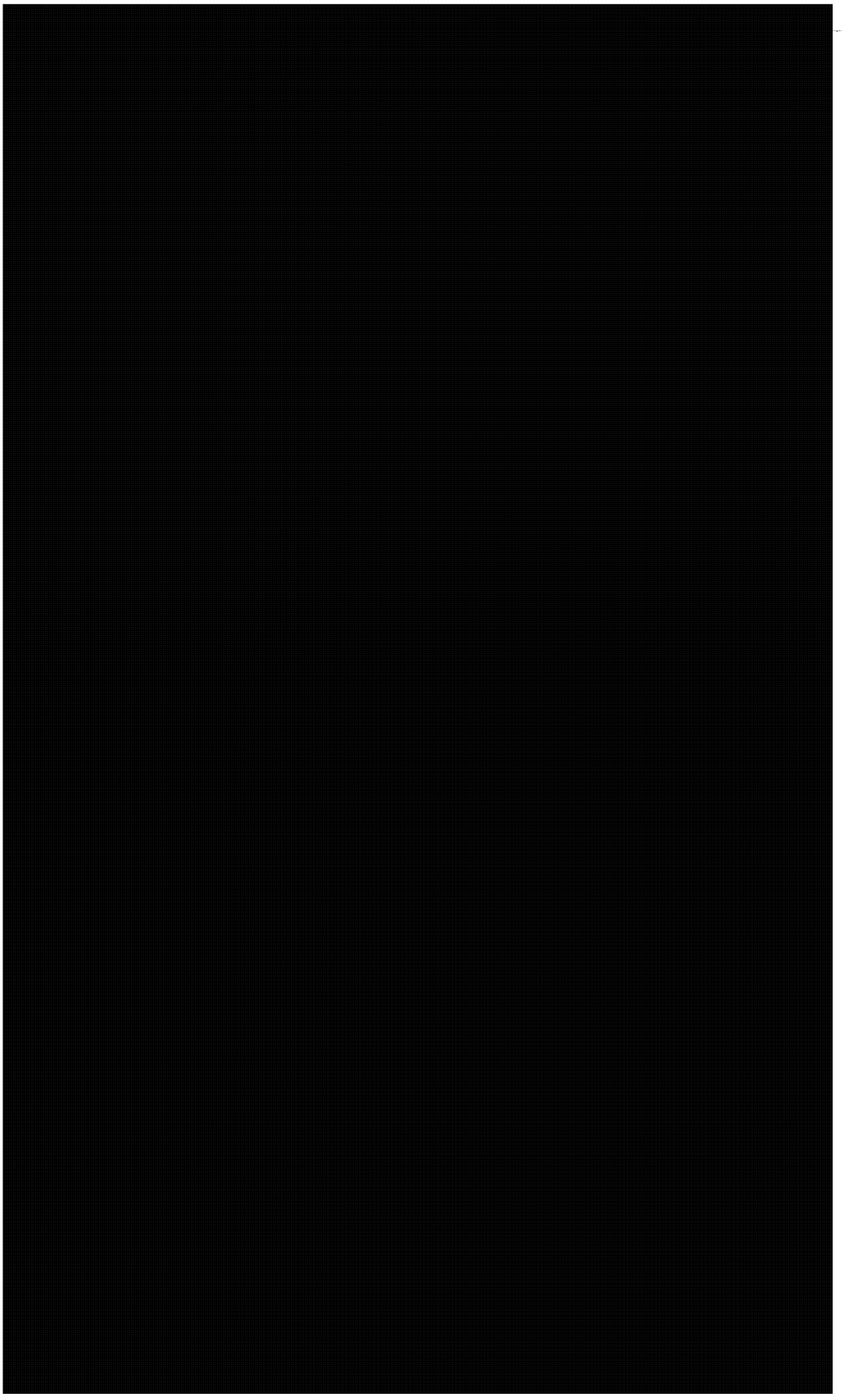
[redacted]

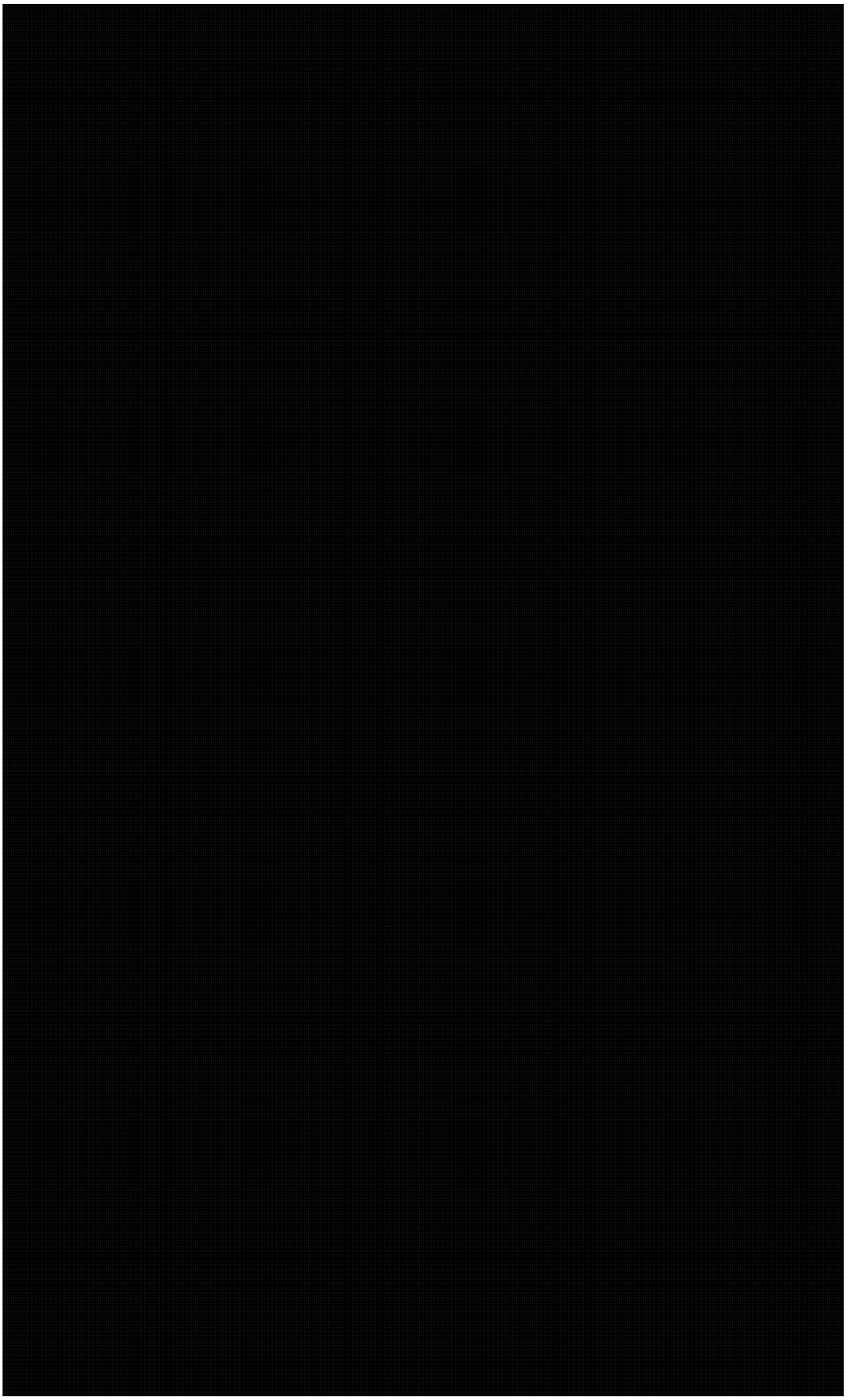






[redacted]





ANNEX D – Five-Eyes' Common List of Digraphs

The *location digraph* is a two-letter code representing the assessed location of a targeted entity. The [redacted] *trigraph* is a three-letter code representing the assessed nationality (two letter digraph of the country of nationality) as well as a single letter code representing the targeted entity's functior[redacted]

Source: CERRID# 358663, six pages, e-mail from Policy and Review Advisor, External Review and Policy Management, October 22, 2009 and one page "target designator" handout from [redacted] interview and demonstration, November 25, 2009.

Version 1.4 [redacted] Digraph	Country, Area, Organization, or Target Activity	Accepted in [redacted] by CSEC as nationality TRIGRAPH	Accepted in [redacted] by CSEC as location DIGRAPH
[redacted]			

Version 1.4 [redacted] Digraph	Country, Area, Organization, or Target Activity	Accepted in [redacted] by CSEC as nationality TRIGRAPH	Accepted in [redacted] by CSEC as location DIGRAPH
[redacted]			

Version 1.4 [redacted] Digraph	Country, Area, Organization, or Target Activity	Accepted in [redacted] by CSEC as nationality TRIGRAPH	Accepted in [redacted] by CSEC as location DIGRAPH
[redacted]			

Version 1.4 [redacted] Digraph	Country, Area, Organization, or Target Activity	Accepted in [redacted] by CSEC as nationality TRIGRAPH	Accepted in [redacted] by CSEC as location DIGRAPH
[redacted]			

Version 1.4	Country, Area, Organization, or Target Activity	Accepted in [redacted] by CSEC as nationality TRIGRAPH	Accepted in [redacted] by CSEC as location DIGRAPH
[redacted] Digraph			

[redacted]

Version 1.4 [redacted] Digraph	Country, Area, Organization, or Target Activity	Accepted in [redacted] by CSEC as nationality TRIGRAPH	Accepted in [redacted] by CSEC as location DIGRAPH
[redacted]			

Target Designator

[redacted]

Letter Description

[redacted]

ANNEX E – Summary of Privacy Incidents

Source: CERRID# 345109, one page, e-mail from Policy and Review Advisor, External Review and Policy Management, October 22, 2009.

CSE Privacy Incidents File							
Date	Description	Group(s) Involved	How Incident Observed	Why Incident Occurred	Potential Damages	Actions Taken for Non-Compliance	Follow-on Activities *(weaknesses in operational activities, monitoring measures or policy instruments)*
[redacted]							

ANNEX F – [redacted] Interviews

We conducted interviews with six [redacted] analysts to assess their awareness of and compliance with the policies and procedures respecting SIGINT targeting and selector management activities.

Initially, CSEC proposed a list of names of 13 analysts with varying lengths of experience in [redacted] and at CSEC. We randomly selected four analysts:

1. [redacted] Analyst with less than one year experience at CSEC;
2. [redacted] Analyst with less than three years of experience;
3. Office of Counter Terrorism [redacted] Analyst with between three and 10 years experience; and
4. [redacted] Analyst with over ten years of experience.

CSEC provided the number of EPRs produced by the four analysts (as primary author) by month for the period of review. We selected for review, again at random, the "nth" report from specific months:

1. for the first analyst [redacted], two reports produced in the period of review, one in July 2009 [redacted] and one in August 2009 [redacted];
2. for the second analyst, one report produced in May 2009 [redacted][104], one in June 2009 [redacted], and two in July 2009[105];
3. for the third analyst, the second report produced in each month of September [redacted], October [redacted], November [redacted] and December 2008 [redacted]; and
4. for the fourth analyst, the third report produced in each month of December 2008 [redacted] and January [redacted], February [redacted] and March 2009 [redacted].

We reviewed 11 EPRs with the above four analysts.

Following these interviews, we selected, at random using the directory of employees on CSEC's Intranet (i.e., not from a list proposed by CSEC), an additional two [redacted] analysts. As was done previously, CSEC provided the number of EPRs analysts produced as primary author by month for the period of review and we selected at random, specific reports for review:

[104] We did not question the analyst respecting this EPR as it was a re-issue of a [redacted] report.
[105] Not completed due to time constraints.

1. Intelligence Analyst [redacted] three to 10 years experience, the second report produced in February [redacted] March [redacted], April [redacted] and May 2009 [redacted].

2. Intelligence Analyst [redacted] one to three years experience, the two reports prepared in March 2009 [redacted] and [redacted] and the two reports prepared in August 2009 [redacted] and [redacted]

This next set of two analysts accounted for an additional eight EPRs reviewed.

Proceeding in this manner permitted us to prepare questions in advance respecting the EPRs we selected and provided the analysts with time to refresh their memories.

We asked each analyst general questions respecting their work designed to test their knowledge of the policies and procedures respecting SIGINT targeting and selector management activities. For each of the analysts' EPRs, we assessed whether the selectors and documentation in [redacted] associated with the EPRs complied with the policies and procedures. We used the following checklist to record our findings.

[redacted] record indicates selectors are metadata ☐
type (e.g., phone number, e-mail or IP address): _____
[redacted]

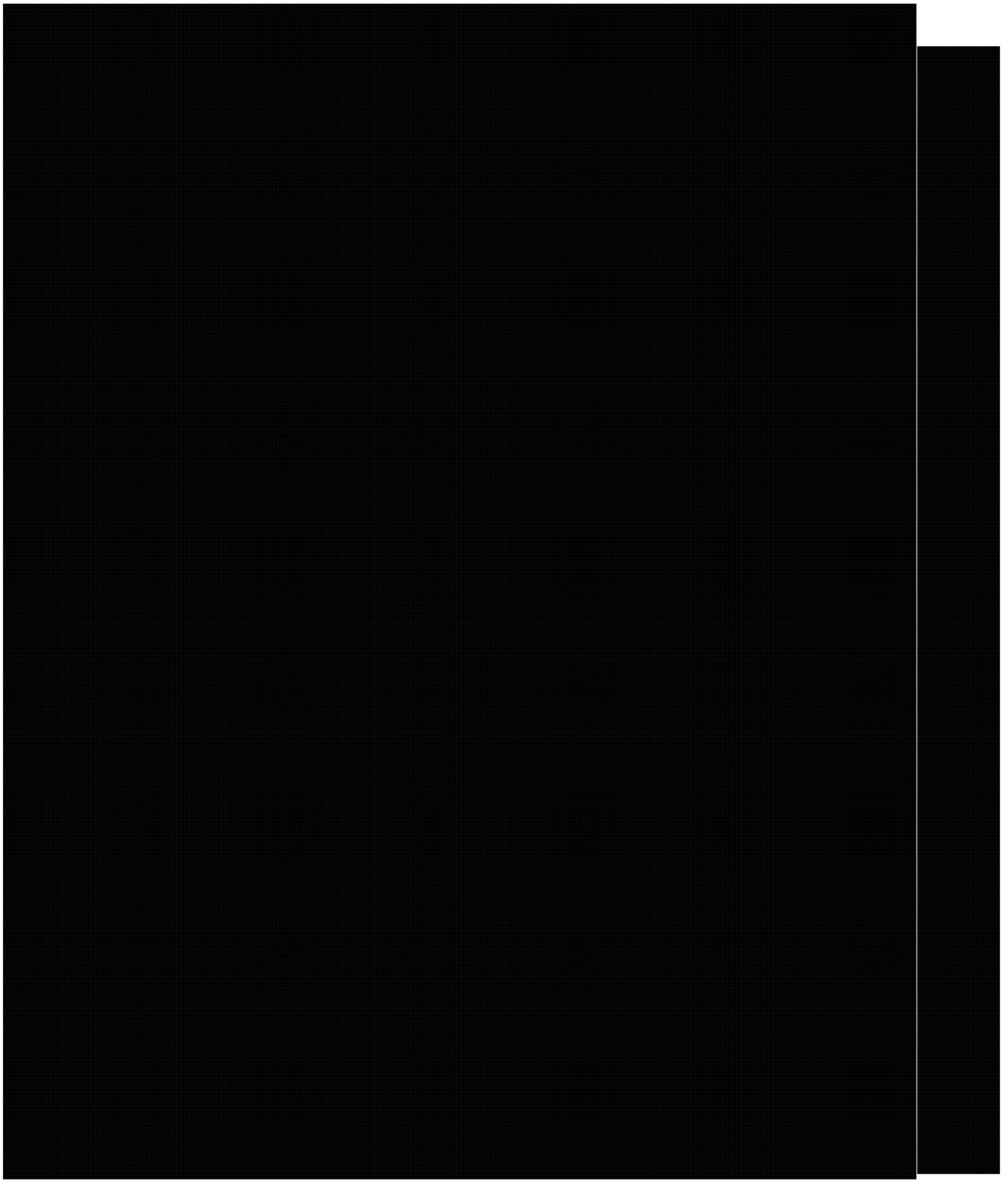
- source of selector documented ☐
- associated with a GCR ☐ and aligned with the NSPL ☐
- foreign assessment (location digraph, nationality and function trigraph [redacted]:
  - associated with foreign entity (nationality) ☐ outside Canada (location) ☐
  - sufficiently documented rationale respecting reasonable grounds (facts and analytical assumptions) ☐
  - evidence of enquiries to DFAIT, CBSA, others, as appropriate ☐
- clear targeting justification (what/who is entity, why is it targeted, what is it doing?) ☐
- at time of review, selector is active ☐ or de-targeted ☐
  - if > 12 months, evidence of annual review and validation ☐

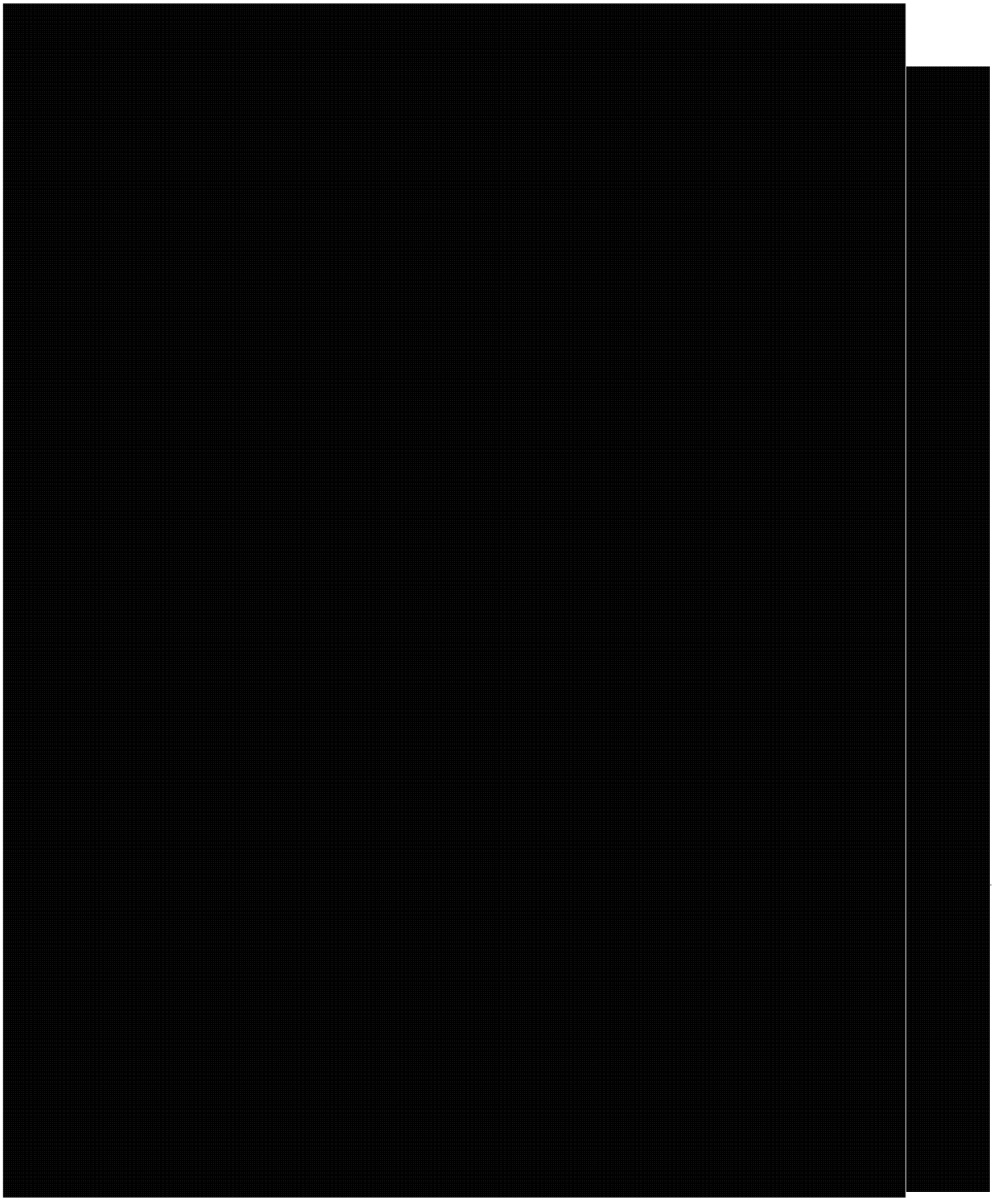
Reports:

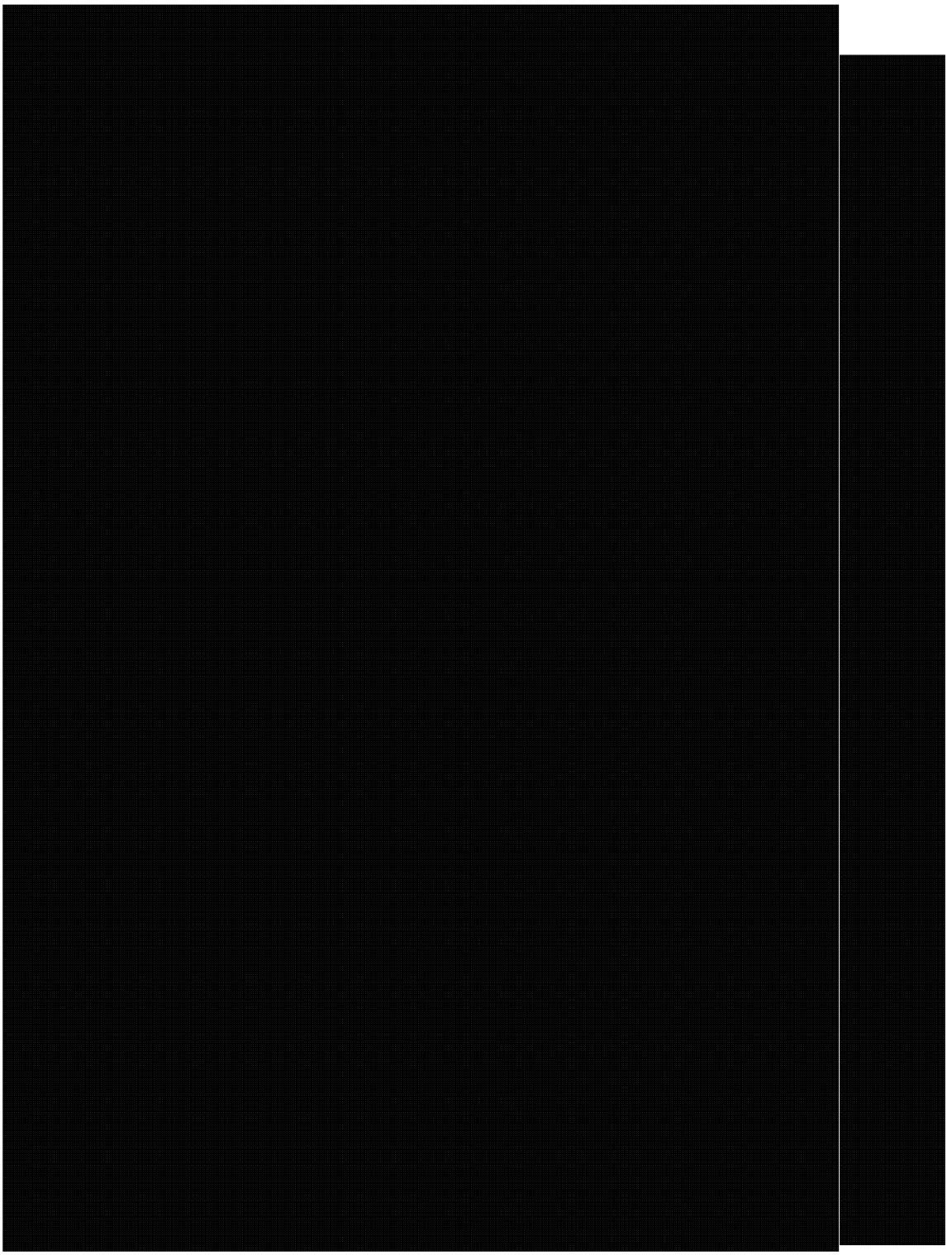
- source(s) of collection: Afghan MA [redacted]
- relates to same FI priority as selector record in [redacted]

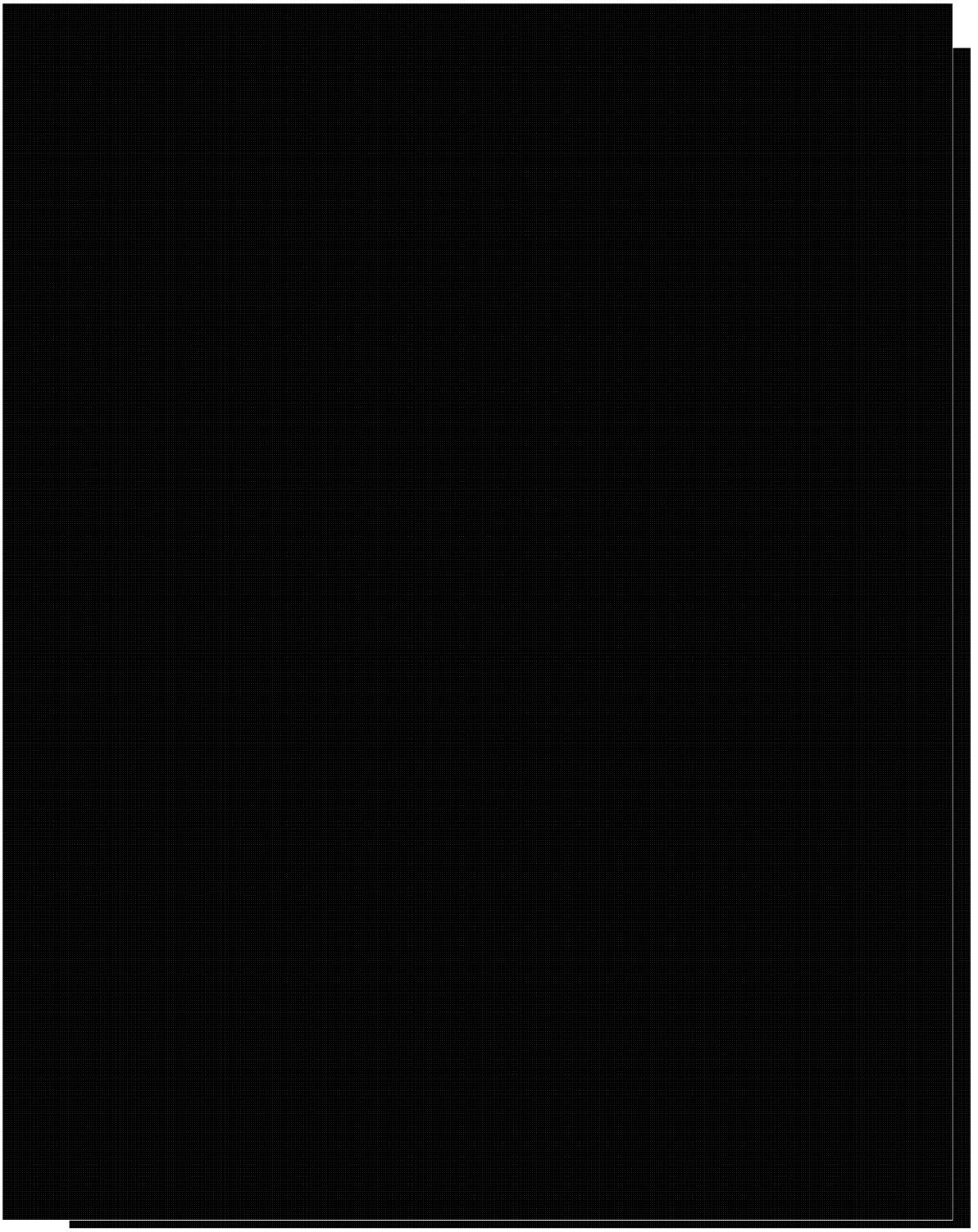
ANNEX G – Sample of abbreviations used to [redacted] amongst Five Eyes

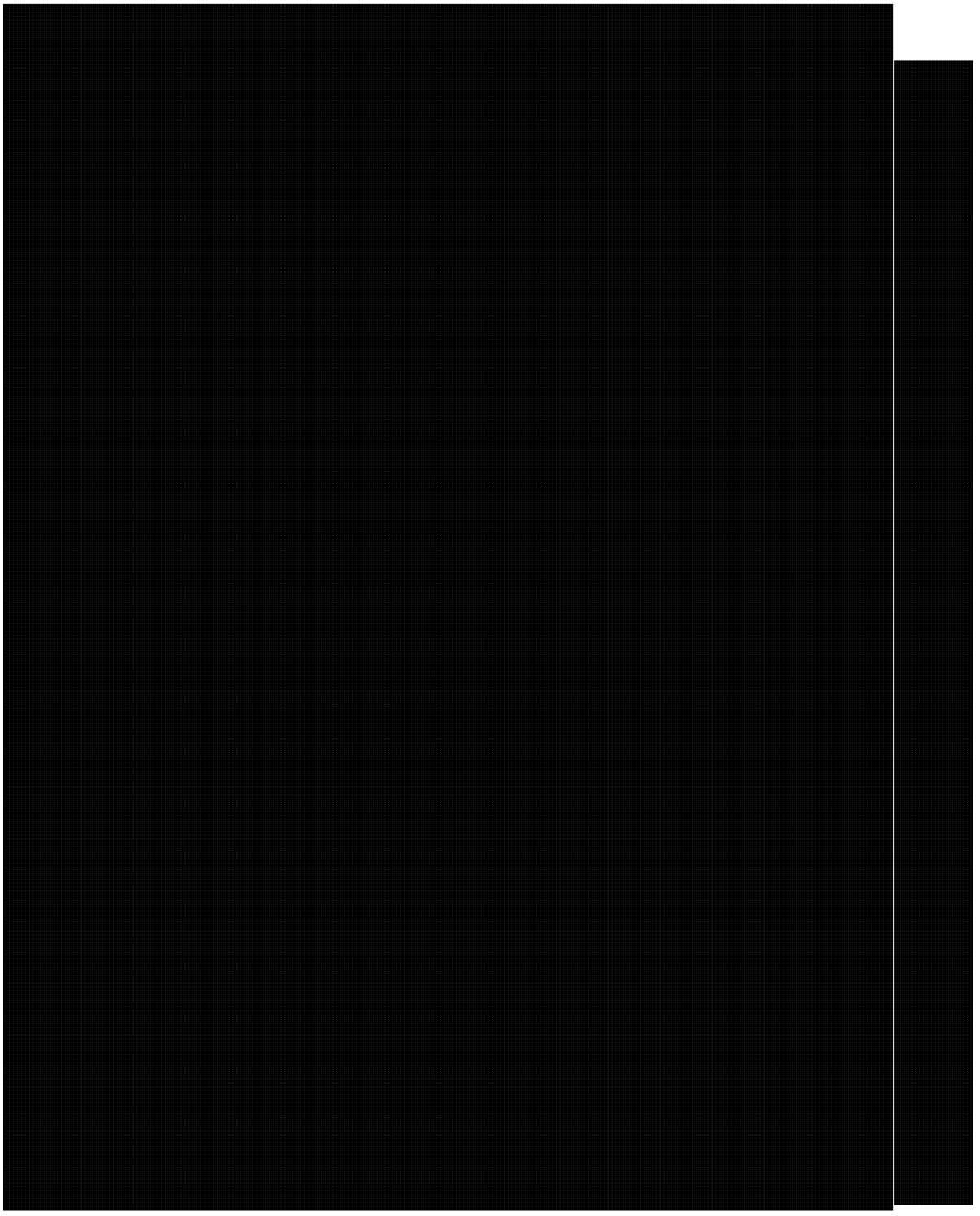
[redacted]



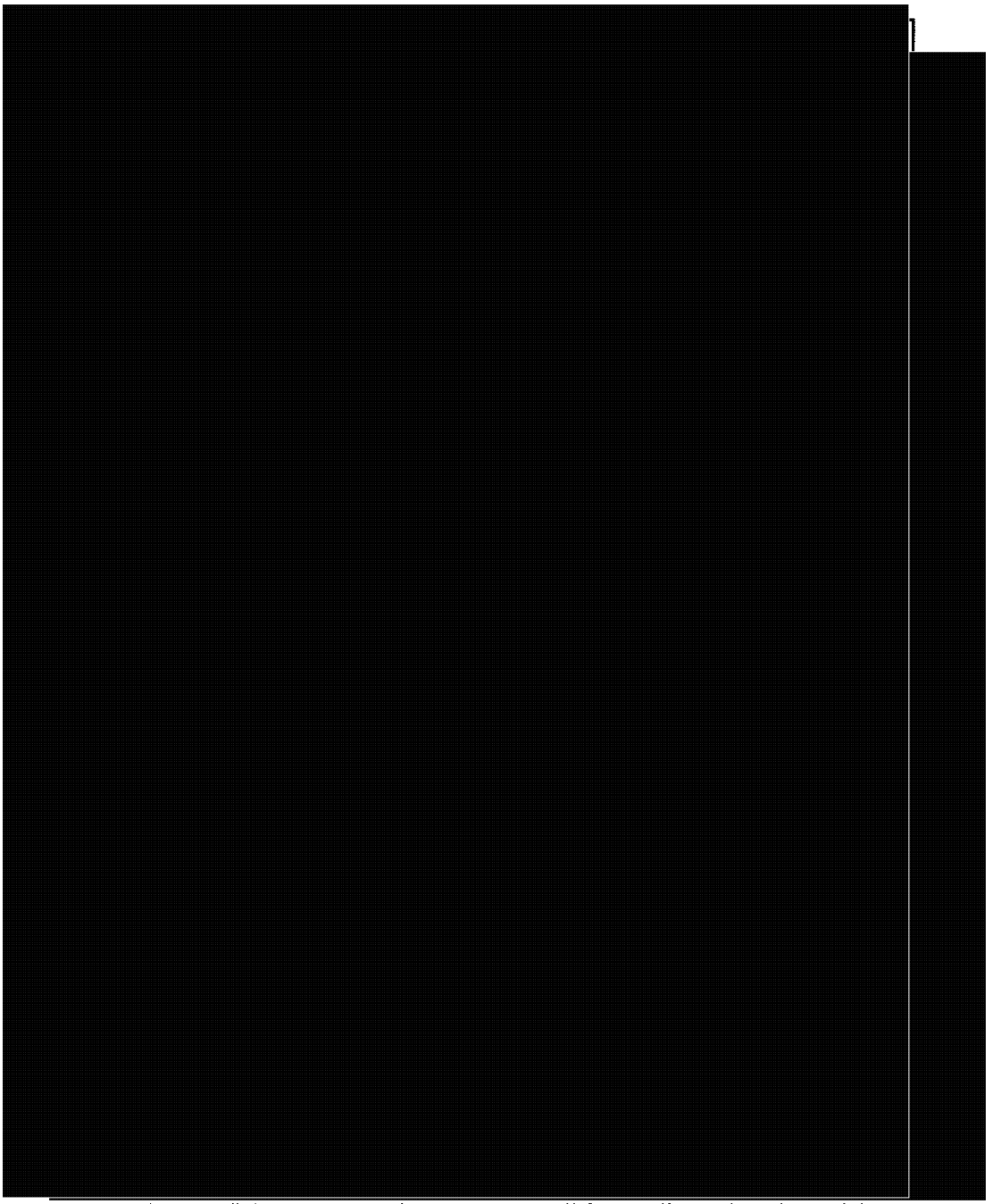








[redacted]



Source: CERRID# 605885, September 1, 2010, e-mail from Policy and Review Advisor, External Review and Policy Management, pp. 15-23.