

Communications Security
Establishment Commissioner

The Honourable Jean - Pierre Plouffe, C.D.



Commissaire du Centre de la
sécurité des télécommunications

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

TOP SECRET // SI // CEO

Our file # 2200-73

February 24, 2014

The Honourable Robert Nicholson, P.C., Q.C., M.P.
Minister of National Defence
101 Colonel By Drive
Ottawa, On K1A 0K2

Dear Mr. Nicholson:

The purpose of this letter is to provide you with the results of my review of the activities of the Communications Security Establishment Canada (CSEC) Office of Counter Terrorism (OCT). The review was started by my predecessor, Commissioner Décary, and completed under my authority as articulated in Part V.1, paragraph 273.63(2)(a) of the *National Defence Act (NDA)*.

The purpose of this review was to acquire detailed knowledge of the OCT and the extent of any changes to its activities since the last in-depth review in 2007, to determine whether OCT activities complied with the law, and the extent to which CSEC protected the privacy of Canadians in carrying out the activities. Another specific objective was to assess how certain CSEC practices respecting the sharing of Canadian identity information with domestic and second party partners, particularly as regards the use of precise and consistent language in information exchanges, [REDACTED]

[REDACTED] The review encompassed a sample of OCT activities conducted by CSEC in 2011-2012.

I found that CSEC OCT activities were conducted in compliance with the law and ministerial direction. OCT activities are subject to the same legal requirements to protect the privacy of Canadians that apply to all CSEC activities. CSEC has sufficient policies and processes to satisfy the legal requirement not to direct its SIGINT activities at a Canadian wherever he or she may be or at any person in Canada. OCT employees demonstrated knowledge of policy and practices aimed at ensuring compliance with the law and privacy protection, and managers routinely monitor the activities for compliance.

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

A0000569_1-003418

TOP SECRET // SI // CEO

CSEC has promulgated new guidance and introduced a new process for recording information exchanges between CSEC and federal law enforcement and security agencies. This is significant and will promote clarity of language in such information exchanges. [REDACTED]

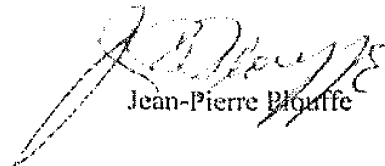
I did, however, identify some deficiencies respecting CSEC policy. I found that a sample of contact chaining activities conducted by the OCT [REDACTED] was generally conducted in compliance with operational policy. However, I found that parts of CSEC policy respecting this metadata activity did not reflect standard practices. I recommend that CSEC modify its policy for these activities to reflect its current practices, specifically for record keeping. I will pursue examination of this issue as part of my ongoing review of CSEC foreign signals intelligence and information technology security activities that may use metadata.

I also recommend that CSEC promulgate guidance to codify its practices for cases when an analyst observes that a second party partner — the United States' National Security Agency, the United Kingdom's Government Communications Headquarters, the Australian Signals Directorate or New Zealand's Government Communications Security Bureau — is targeting a Canadian, including notification to the Second Party to desist from such targeting and record keeping of such cases.

The enclosed report contains detailed information on the findings and recommendations. CSEC officials were provided an opportunity to review and comment on the results of the review, for factual accuracy.

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

Yours sincerely,


Jean-Pierre Blouffe

c.c. Mr. John Forster, Chief, CSEC

A0000569_2-003419

Office of the
Communications Security
Establishment Commissioner



Bureau du
Commissaire du Centre de la
sécurité des télécommunications

TOP SECRET // SI // CEO

Review of the Activities of the Office of Counter Terrorism

February 24, 2014

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

A0000569_3-003420

TABLE OF CONTENTS

I. AUTHORITIES.....	1
II. INTRODUCTION	1
<i>Rationale for Conducting This Review</i>	2
III. OBJECTIVES.....	3
IV. SCOPE.....	3
V. CRITERIA.....	4
VI. METHODOLOGY.....	4
VII. BACKGROUND	5
VIII. FINDINGS	13
A) Legal Requirements.....	13
B) Ministerial Requirements.....	16
C) Policies and Procedures.....	17
IX. CONCLUSION.....	24
ANNEX A — Findings.....	26
ANNEX B — Interviewees	28
ANNEX C — Tasking Workflow	29
ANNEX D — Targeting Workflow	31
ANNEX E — Contact Chaining [REDACTED]	34
ANNEX F — Report Production.....	35
ANNEX G — Annexes A & B to the Information Needs Process	39

I. AUTHORITIES

This review was conducted under the authority of the Communications Security Establishment Commissioner as articulated in Part V.1, paragraph 273.63(2)(a) and subsection 273.65(8) of the *National Defence Act (NDA)*.

The obligation for Communications Security Establishment Canada (CSEC) to take measures to protect the privacy of Canadians, as set out in paragraph 273.64(2)(b) of the *NDA*, applies to Office of Counter-Terrorism (OCT) activities. CSEC is required to have appropriate measures in place to protect the private communications of Canadians, as well as communications of Canadians located outside Canada and information about Canadians acquired through its mandated activities.

This review further derives authority from the ministerial directives (MDs) on *Privacy of Canadians* (November 20, 2012) and *Collection and Use of Metadata* (November 21, 2011) and the ministerial authorizations (MAs) authorizing the interception of private communications — as defined in section 183 of the *Criminal Code*¹ — under the foreign signals intelligence (SIGINT) collection programs known as [REDACTED]

[REDACTED] and Interception Activities Conducted in Support of Canadian Forces Operations in Afghanistan (Afghan MA activities). MAs current to the review period were in effect from December 1, 2010, to November 30, 2011, and from December 1, 2011, to November 30, 2012. MAs require CSEC to support and assist the Commissioner in his review of CSEC activities.

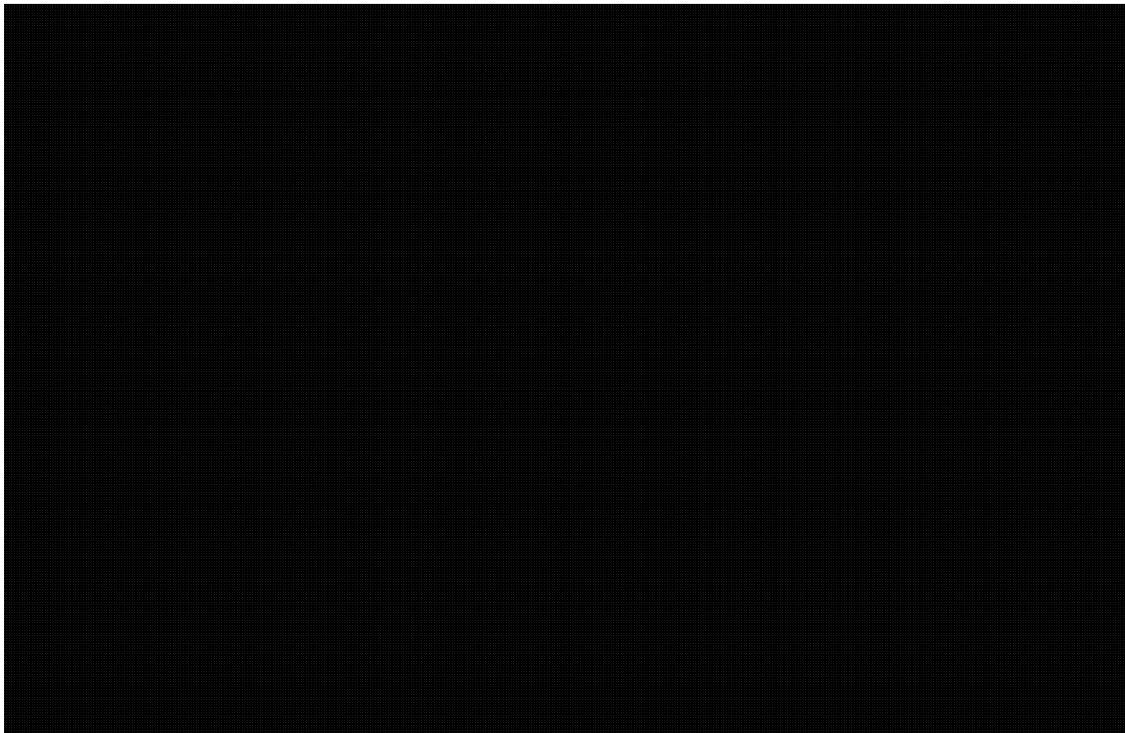
II. INTRODUCTION

The main purpose of the OCT is to provide actionable SIGINT for detecting and preventing terrorist threats against North America, as well as against Canadian and allied interests abroad.

¹ Section 183 of the *Criminal Code* defines a private communication as: “any oral telecommunication that is made by any originator who is in Canada or is intended by an originator to be received by a person who is in Canada, and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it, and includes any radio-based telephone communication that is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it.”

Rationale for Conducting This Review

OCT operations are subject to controls to ensure compliance with legal, ministerial and policy requirements. It is not uncommon for the OCT to acquire and use information relating to a Canadian as it is the main conduit for CSEC to share information relating to counter-terrorism with the Canadian Security Intelligence Service (CSIS). One of the main objectives of this review was to ensure that these exchanges were lawful and complied with CSEC policy. If OCT activities and information-sharing practices were found to be non-compliant with the law, the impact on the privacy of Canadians could be significant. CSEC's overview briefing indicated that there had been major procedural and technological changes to the OCT since the Commissioner's review of OCT in October 2007.



At the Commissioner's direction, the office started a review of recent activities of OCT that includes a follow-up on matters raised in that review, particularly respecting the first recommendation [REDACTED]

It is for these reasons that the Commissioner selected OCT activities for review at this time.

² The CSEC second-party partners, also known with CSEC collectively as the Five Eyes alliance include: the U.S. National Security Agency, the U.K. Government Communications Headquarters, Australia's Signals Directorate, and New Zealand's Government Communications Security Bureau.

III. OBJECTIVES

The objectives of this review were:

- to acquire detailed knowledge of and to document OCT activities;
- to assess whether the activities conducted by the OCT complied with the law;
- to assess the extent to which CSEC protected the privacy of Canadians in carrying out OCT activities; and
- to follow-up on recommendations in a previous report.

IV. SCOPE

The review focused on a sample of OCT activities conducted under paragraph 273.64(1)(a) of the *NDA* (otherwise known as part (a) of the CSEC mandate).

It encompassed processes and practices of the OCT in effect for the period of May 1, 2011, to May 1, 2012.

In addition to acquiring detailed knowledge about OCT activities, the Commissioner's office examined:

- the legislative and policy framework for OCT activities;
- the amount and treatment of private communications and information about Canadians acquired and used by OCT activities;
- OCT technologies, databases and systems;
- OCT methodologies, procedures, operational instructions and other guidance;
- the extent to which technology was used and other efforts were applied to protect the privacy of Canadians in OCT activities; and
- a sample of intercepted communications shared by the OCT and associated reporting.

The review was further informed by previous reviews from the Commissioner's office, namely the 2007 *Review of the Activities of CSE's Office of Counter Terrorism (OCT)*, [REDACTED] as well as CSEC activities in response to previous associated findings and recommendations made by the Commissioner.

V. CRITERIA

A) Legal Requirements

The Commissioner expected that CSEC conducted its OCT 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 conducted its OCT activities in accordance with ministerial direction, following all requirements and limitations set out in applicable MAs and MDs.

C) Policies and Procedures

The Commissioner expected that CSEC:

- i) had appropriate policies and procedures to guide OCT activities and provide sufficient direction respecting legal and ministerial requirements, including the protection of the privacy of Canadians;
- ii) had personnel who are knowledgeable about and complied with the policies and procedures; and
- iii) had an effective policy monitoring framework for maintaining the integrity and lawful compliance of OCT activities, including appropriately accounting for decisions taken and for information relating to compliance and the protection of the privacy of Canadians.

VI. METHODOLOGY

As a first step, the Commissioner's office researched, examined and documented OCT activities to develop an understanding of concepts and terminology. The office examined written and electronic records, files, correspondence and other documentation relevant to OCT activities, including policies, procedures and legal advice.³

To decide on a sample of operations, the Commissioner's office was provided with a wide sample of OCT [REDACTED] documents. A [REDACTED] document includes an operational file number, file reference, National SIGINT Priorities List (NSPL)⁴ reference, relevant GC [intelligence] requirements (GCRs), entities of interest,

³ 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.

⁴ See CSOI (Canadian SIGINT Operational Instruction)-1-1, *The National SIGINT Priorities List Process*, July 17, 2008.

as well as a status report, an operational summary and links to the operation's most significant reports, including the first and the most recent. The [REDACTED] also records current hypotheses driving the operation as well as a gaps analysis that documents inherent difficulties. This makes the [REDACTED] a useful tracking and documentation tool.

The contents of some of the relevant databases and systems were tested, with the assistance of CSEC officials acting under direction of the Commissioner's office, to ensure conformity with legal and ministerial requirements and associated policies and procedures.

The office also interviewed managers and other personnel involved in OCT activities. A list of interviewees is enclosed at Annex B.

VII. BACKGROUND

Prior to the attacks of September 11, 2001, the CSEC Directorate General Intelligence (DGI) focused primarily on [REDACTED] reporting. However, these events pushed public safety considerations to the forefront of foreign intelligence collection operations.

In response to this new imperative, CSEC established the OCT in early October 2001 to centralize SIGINT efforts relating to threats from international terrorism. The *Anti-Terrorism Act* was passed on December 24, 2001, and the emphasis on security was further reinforced in April 2004 with the introduction of Canada's National Security Policy.⁵

Generally, OCT activities involve acquiring and using information relating to terrorism and providing technical and operational assistance to federal law enforcement and security agencies relating to terrorism investigations. More specifically, the OCT conducts research and analysis of SIGINT data in order to identify terrorist targets and their operational and support networks.

In the conduct of its activities, the OCT collaborates closely with and regularly shares terrorism-related information with Canadian government departments and agencies involved in intelligence and security-related matters. These organizations include CSIS, the Royal Canadian Mounted Police (RCMP), the Canada Border Services Agency (CBSA), the Department of National Defence (DND) and the Department of Foreign Affairs, Trade and Development (DFATD). The OCT also works with CSEC's second party partners.

OCT work is characterized by the fact that foreign intelligence priorities and targets tend to change quickly as they are often crisis-based. The OCT, together with the CSEC Operational and Production Coordination Centre (COPCC), serves as the CSEC entry

⁵ *Securing an Open Society: Canada's National Security Policy*, April 2004, is a national strategy aimed at protecting the nation and its citizens ensuring Canada is not a base for threats to our allies and contributing to international security.

point for receiving notifications of critical incidents from domestic and international partners involving terrorism. The OCT may also assume the operational lead for the CSEC response to emergencies such as the hostage-taking of a Canadian citizen abroad.

1. Organizational Structure

Directorate General Intelligence

The DGI, also known as the Intelligence Branch, located within the SIGINT business line, is responsible for gathering foreign intelligence and producing reports in support of GC intelligence priorities. One of the main parts of the production process is the analysis of the intercepted and acquired communications and related data that results in end-product reports (EPRs).

DGI is divided into [REDACTED] groups. [REDACTED] of them are operational and analytical. [REDACTED] includes the OCT, which is made up of the [REDACTED] and [REDACTED] subgroups. Other DGI operational and analytical groups include the [REDACTED]. The remaining [REDACTED] groups provide horizontal support to operations: [REDACTED]

Group [REDACTED]

[REDACTED] Group is the largest group in DGI. It is mandated with producing SIGINT analysis, reporting and services in support of the GCRs⁶ on [REDACTED] as well as [REDACTED]

[REDACTED] (OCT)

[REDACTED] Group is divided in [REDACTED] subgroups of which the [REDACTED] subgroups are informally known as the OCT. [REDACTED] has a team that focuses on strategic issues and [REDACTED] and a second team responsible for SIGINT development [REDACTED] is more operations-oriented with [REDACTED] teams covering [REDACTED] and [REDACTED]

The [REDACTED] teams work in close contact with CSIS, with most of the interaction taking place at the team leader and analyst level. [REDACTED] currently has an analyst integree working with multiple CSIS teams.

The remaining [REDACTED] subgroups are [REDACTED] which covers [REDACTED] and [REDACTED] which covers [REDACTED] (also known as [REDACTED])

⁶ GCRs are an index that 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. See CSOI-1-1, *supra* note 4.

2. Staffing

OCT Analysts

DGI analysts are assigned [REDACTED]. Some [REDACTED] equate to specific [REDACTED] while others can be a specific [REDACTED]. A specific entity within a [REDACTED] such as [REDACTED] is identified as an entity of interest.

The main responsibility of the DGI analyst working in the OCT is to report on foreign intelligence on terrorism-related targets of interest to the Canadian government. Their various linguistic, technical and analytical skills [REDACTED]

OCT analysts follow the standard DGI path in the production of an EPR with the exception that it focuses on terrorism-related issues.

Team Leaders

OCT teams are managed by a team leader and usually number [REDACTED] analysts, which include foreign language experts, [REDACTED] analysts and intelligence analysts. [REDACTED] and [REDACTED] are each led by a level 4 manager who reports to the Director of [REDACTED] Group, who in turn reports to the Director General of Intelligence.

3. Foreign Intelligence Priorities

Government of Canada Requirements

GCRs are an index that permits the tracking of the SIGINT process against client requests. GCRs are applied to, for example, requests, reports, targets, and feedback. GCRs are also mapped to the NSPL as appropriate to be able to track activities against national priorities.

⁷ All selectors and methods used in the collection and acquisition of information from the global information infrastructure are to be directed at foreign entities located outside of Canada and associated with GC intelligence priorities. They are subject to annual review to ensure they are consistent with those priorities as per CSOI-4-4, *Targeting and Selector Management Using [REDACTED] National SIGINT Systems for Intelligence Reporting Purposes*, March 5, 2009. See also *A Review of CSEC SIGINT's Targeting and Selector Management Activities*, March 15, 2011.

⁸ To target in this context means: "To single out for collection or interception purposes. One 'targets' a selector to a collection system dictionary or directory (filtering and selection tool) to collect only wanted data." (Source: CSOI-4-4, section 6.22).

National SIGINT Priorities List

The NSPL was originally developed in 2004 to help CSEC focus its work on those areas of highest overall concern to the GC in order to best leverage resources and optimize the SIGINT system. The NSPL consists of two lists, the Standing Issues⁹ and the Watching Briefs,¹⁰ which define the priorities for the national SIGINT system. These two lists operate on different time scales, with different sources of information and processes.

4. Management Control Framework

[REDACTED]

[REDACTED] performs key mission management control functions, including the tasking of [REDACTED] the targeting of selection criteria, and the establishment of associated data flows. [REDACTED] ensures those functions are in compliance with CSEC policy for all of the DGI including the OCT. [REDACTED] is authorized to halt all tasking or targeting when it deems they are non-compliant. [REDACTED] is also responsible for tracking the capabilities, tasking, status and performance of Canadian [REDACTED] SIGINT collection and data-forwarding systems.¹¹

SIGINT Programs Oversight and Compliance (SPOC) personnel are also responsible for conducting compliance policy monitoring of OCT activities.

5. Storage Databases and Systems

The list of storage systems and databases presented in this section provides an overview of the more important and frequently used data repositories in the course of OCT activities.

[REDACTED]

[REDACTED] is the primary SIGINT traffic search and display tool. It allows OCT analysts and other DGI users to [REDACTED] content or metadata and it has [REDACTED] capability. The [REDACTED] aims to provide analysts with the ability to better manage their knowledge, giving them access to data from multiple repositories using a single tool. It also allows analysts to share their work with others, and helps them track their work from beginning to end.

⁹ A standing issue is an issue [REDACTED]

¹⁰ A watching brief list represents issues [REDACTED]

Consolidated Traffic Repository

The Consolidated Traffic Repository is the overall storage database for most SIGINT intercepts with the [REDACTED] serving as the interface.

[REDACTED] is the CSEC corporate SIGINT target knowledge database that contains information produced by analysts from a variety of sources about foreign entities of foreign intelligence interest to the GC and serves as a repository for their relevant selectors. [REDACTED] is used to manage selectors and targeting information [REDACTED] digital network intelligence¹² and dialed-number recognition¹³ selectors [REDACTED]

[REDACTED] is a [REDACTED]
[REDACTED]
[REDACTED] It is exclusively accessible by [REDACTED] and SIGINT Systems Development.

[REDACTED] is a compartment in [REDACTED] used for storing sensitive information [REDACTED] --- as well as for IRRELEVANT
IRRELEVANT

[REDACTED] is the CSEC EPR database and report-creating tool. Its major purpose is to disseminate reporting to GC clients and the five-eyes community. It has a multi-tiered setup for classification and controls access to information based on user roles and clearance levels.

6. Collection Processes

The tasking process and the targeting and selector management process are at the core of the SIGINT collection process. Both processes along with the relevant [REDACTED] responsibilities are detailed at annexes C and D of this review.

¹² Digital network intelligence is also referred to as [REDACTED] (Internet) communications and may contain many different types of information (e.g., e-mail, [REDACTED])

¹³ Dialed-number recognition metadata generally refers to telephone and facsimile communications, and [REDACTED]

It should be noted that the process for submitting designated selectors to [REDACTED] was recently automated. While responsibility ultimately lies with [REDACTED], most requests are now handled by an automated approval system, which either approves, rejects, pools¹⁴ or refers requests for manual inspection, as appropriate. Some requests directed at certain collection [REDACTED] are not handled by the automated tool. They are sent to [REDACTED] in the form of an e-mailed template, which [REDACTED] validates manually and forwards to the collection system, as it does for referred requests.

7. SIGINT Development

SIGINT Development, or SIGDEV, can be defined as preparatory work for successful foreign intelligence-yielding target exploitations. It encompasses signals analysis and development, research, network analysis and target development.

SIGDEV work involves sifting through large volumes of information using a variety of tools. [REDACTED] The aim is to

[REDACTED] in order to determine their [REDACTED]

[REDACTED]

Contact Chaining

Contact chaining is a common SIGDEV activity that enables the analysis of metadata information to build a profile of communications activities, patterns and contacts of

¹⁴ A pooled request is one that passes all the rules but is put on hold because the system cannot process it. It is expected to be processed at a later date.

¹⁵ CSEC [REDACTED] November 28, 2012.

various foreign entities of interest in relation to GC foreign intelligence priorities, including the number of contacts to or from these entities, the frequency of these contacts, the number of times contacts were attempted or made, the time period over which these contacts were attempted or made, as well as other activities aimed at mapping the communications of foreign entities and their networks.¹⁶

OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities*, provides that, in accordance with the MD on *Collection and Use of Metadata*, CSEC may search metadata for the purpose of providing any information or intelligence about the capabilities, intentions or activities of a foreign individual, state, organization, terrorist group or other such entity as they relate to international affairs, defence or security. OCT contact chaining usually concentrates on [REDACTED] relating to terrorism investigations.

Currently, CSEC chains [REDACTED]

Contact Chaining

OPS-1-10, *Procedures for Metadata Analysis* [REDACTED]¹⁷ provides direction on the process that CSEC analysts must follow when conducting metadata analysis pursuant to part (a) of the CSEC mandate in pursuit of foreign intelligence, [REDACTED]

The process for conducting metadata analysis from [REDACTED] metadata repositories [REDACTED] is listed at section 2.3 of OPS-1-10.¹⁸

8. Incoming Lead Information from Domestic Law Enforcement and Security Agencies

Information Needs Disclosure to CSEC

The Information Needs process¹⁹ assists CSEC in tracking sensitive disclosures by federal law enforcement and security agencies — typically CSIS, the RCMP and CBSA — that wish to share with CSEC information legally collected under their authorities.²⁰ The process was implemented in 2006–2007 as a means for these federal agencies to communicate disclosures as foreign lead information (such as targeting and/or

¹⁶ See OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities*, section 8.3, March 11, 2010.

¹⁷ September 26, 2008.

¹⁸ See Annex E at p. 34.

¹⁹ See Annex G at p. 39.

²⁰ See standard operating procedures for SIGINT information needs via [REDACTED] (MANDRAKE), April 20, 2011.

background information) to facilitate CSEC operations under part (a) of the CSEC mandate.

The information provided through this process is typically of a sensitive operational nature — it often contains Canadian identity information — that should not be included in a [REDACTED] message. It is for this reason that such messages are sent directly to DGI management via a CSEC e-mail address specifically created for this purpose on the MANDRAKE²¹ network. Clients are instructed to not send messages directly to individuals within CSEC. Any messages sent directly to individuals at CSEC are required to be redirected to the proper address via MANDRAKE.

In preparing the disclosure message, the client is responsible for including a caveat stating that the information provided was lawfully obtained by the originating department under its authorities and is being provided to CSEC in relation to its foreign intelligence mandate. The message has to include all relevant contextual information and all possible identifiers relevant to the case, regardless of users' nationalities. Any identifiers that belong to persons in Canada — including foreigners in Canada or Canadians abroad — must be flagged as such. The originating message must also refer to any previous or related messages sent to CSEC. The client must include contact information so CSEC can acknowledge receipt of the message and follow up.

Incoming Information Needs requests are routed to DGI management, which is responsible for receiving and assigning the incoming information to a point of contact. When the Information Needs information is particularly sensitive, it may be sent directly to the operational teams. A semi-automated process captures all disclosures via a template that prompts and autocorrects the user. Both the request and response template require the writer to log in before they can be sent out, thereby tagging the client and responder to the request and response respectively.

The point of contact is responsible for responding to the client using one of the four standard information needs formal responses:²²

- i. information justifies action on the part of CSEC — send acknowledgement type A;
- ii. information falls below the threshold for action — send acknowledgement type B;
- iii. no active GCR that meets the requirement — send acknowledgement type C; or
- iv. if the message cannot be accommodated under mandate (a) and requires mandate (c) assistance, the Information Needs request must be returned to the originator immediately using acknowledgement type D, which directs the client to submit a mandate (c) request for assistance.

²¹ MANDRAKE is the GoC Security and Intelligence community Top Secret/Security Intelligence level network. It incorporates two systems: MANDRAKE I, which provides e-mail connectivity, and MANDRAKE II, which provides an electronic intelligence dissemination network using web technology.

²² See Annex G at p. 39 for the four standard formal responses.

Responsibility for tracking the responses rests with SPOC.

IRRELEVANT

10. Report Production

OCT analysts follow the standard DGI path in the production of an EPR with the exception that it focuses on terrorism-related issues. Please refer to Annex F for a breakdown of the report production process.

VIII. FINDINGS

A) Legal Requirements

Finding no. 1: Compliance with the Law

Based on the information reviewed and the interviews conducted, CSEC Office of Counter Terrorism activities complied with the law.

An initial sample of five OCT operations was selected by the Commissioner's office for this review. More were added as the review progressed as not all operations selected had materialized and not all operations involved the specific kinds of activities that the office wanted to review.

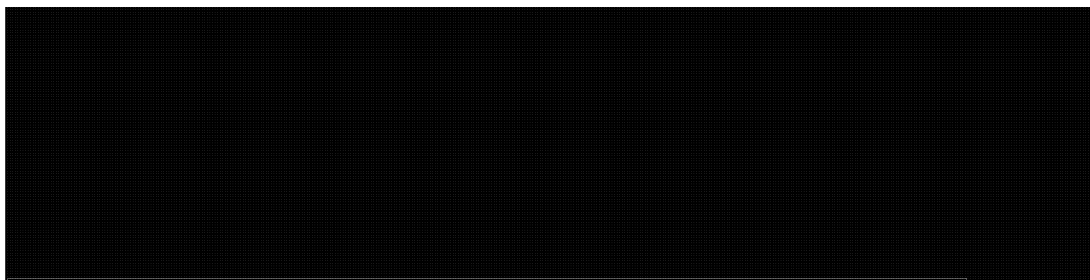
CSEC advised that there are no foundational legal opinions specific to OCT activities as they are the same type of activities as those regularly conducted as part of the general CSEC SIGINT mandate. OCT activities are subject to the same legal framework that applies to all CSEC SIGINT activities.

IRRELEVANT

A0000569_17-003434

Finding no. 2: Demonstration of Legal Compliance — Recording Information Exchanges with Federal Law Enforcement and Security Agencies

The introduction of the Information Needs process is significant and will promote clarity of language in CSEC information exchanges with federal law enforcement and security agencies.



CSEC

has made important changes to its sharing and related documentation policies and practices aimed at strengthening compliance with the law and the protection of the privacy of Canadians. The processing of Canadian identity information disclosure requests, which was done by operational sections of CSEC at that time, is now performed by the CSEC Operational Policy section. Furthermore, the process now requires CSEC employees to put their names on all records using a signature block, identifying their role and function at the time the record was created in order to ensure accountability and enhance the ability of CSEC to demonstrate compliance.

The Information Needs process has systematized and partly automated the approach to follow when receiving Canadian identity information from a client or second-party partner. More specifically, it has clarified and standardized the language to be used in such information exchanges.

The Information Needs Process

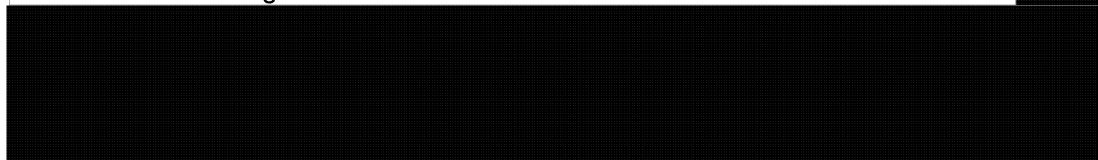
Section 273.64(2)(a) of the *NDA* states that CSEC activities carried out under parts (a) and (b) of its mandate “shall not be directed at Canadians or any person in Canada.”



Solicitor-Client Privilege

Solicitor-Client Privilege

Solicitor-Client Privilege



²⁴ The OCT operates under existing agreements that CSEC has with partners and departments such as CSIS and the RCMP. The OCT has no specific signed agreements with its clients.

[REDACTED]

Of importance, any identifiers belonging to persons in Canada — including foreigners in Canada — or Canadians abroad must be flagged as such. This process also makes the client responsible for confirming that the information provided was lawfully obtained by the originating department under its authorities and is being provided to CSEC in relation to CSEC's foreign intelligence mandate.

To assess the Information Needs process, we reviewed the initial information exchanges between CSEC and the various clients that related to each of our five sample operations and we found that the exchanges had respected established policy and the Information Needs standard operating procedures.

[REDACTED]

Interviewees demonstrated awareness that selectors and methods used in the collection and acquisition of information are to be directed at foreign entities located outside of Canada, associated with GC intelligence priorities and subject to annual review to ensure they are consistent with those priorities.²⁵

Finding no. 3: Protection of the Privacy of Canadians

CSEC's Office of Counter Terrorism activities are subject to the same legal requirements to protect the privacy of Canadians that apply to all CSEC SIGINT activities; CSEC has sufficient policies and processes to satisfy the legal requirement not to direct its SIGINT activities at a Canadian wherever he or she may be or at any person in Canada.

OCT practices and activities observed in this review were found to be consistent with the general requirements found in the MDs on *Accountability Framework* and *Privacy of Canadians*, namely with the requirements to comply with the law and to take measures to protect privacy.

Private Communications, Canadian Identity Information and Disclosures

²⁵ See CSOI-4-4, *supra* note 7.

The Commissioner's office reviewed SIGINT EPRs relating to five selected OCT operations that contained suppressed Canadian identity information or information derived from a private communication.

The operations selected for the review resulted in the production of [REDACTED] EPRs, which were reviewed via [REDACTED]. [REDACTED] of the [REDACTED] reports reviewed contained minimized Canadian identity information. [REDACTED] requests for the S. 37 CEA [REDACTED] S. 37 [REDACTED] reports were received by CSEC from the S. 37 C [REDACTED] CSIS, CBSA and the NSA. S. 37 CEA [REDACTED] in all cases. We examined the requests for release of suppressed information, including the approval and release forms²⁶ and we had no questions.

Privacy Incidents

During the period under review, CSEC recorded [REDACTED] incidents in its Privacy Incidents File relating to OCT operations. Each incident was previously examined as part of the Commissioner's annual *Reviews of CSEC's Privacy Incidents File* for 2011 and 2012. In both reviews, the Commissioner concluded that he was satisfied that CSEC took appropriate corrective actions in response to the recorded privacy incidents, including the [REDACTED] OCT incidents. These [REDACTED] incidents were examined in detail in the course of the two previous reviews and no adverse impact on the Canadian subjects was found.

B) Ministerial Requirements

Finding no. 4: Ministerial Direction

Based upon the information reviewed and the interviews conducted, CSEC carried out its Office of Counter Terrorism activities in accordance with ministerial direction.

The OCT is not subject to any specific reporting or other requirements under MAs or MDs. OCT activities, except for their focus on counter-terrorism, are the same as those conducted regularly as part of CSEC's mandate.

The Commissioner's office did not identify any issues that would suggest a requirement for specific ministerial direction to the OCT.

OCT team leaders and analysts demonstrated an awareness of ministerial direction.

²⁶ The Commissioner's office was provided with sample copies of product release forms for the purpose of demonstrating the auto-generated text by selecting specific OPS-1 categories.

C) Policies and Procedures

Finding no. 5: Appropriateness of Policies and Procedures

Operational policies and procedures for the Office of Counter Terrorism activities are in place and provide sufficient direction to CSEC employees respecting the protection of the privacy of Canadians.

The activities reviewed are not unique to the OCT but rather common to most SIGINT collection programs.

The Commissioner's office did not identify a requirement for OCT-specific operational policies or procedures.

OCT activities observed in the course of this review were generally consistent with policy (see finding no. 6).

The main policies applicable to OCT activities are:

- OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities*;
- OPS-1-1, *Procedures for the Release of Suppressed Information from SIGINT Reports*;
- OPS-1-7, *Operational Procedures for Naming in SIGINT Reports*;
- OPS-1-8, *Active Monitoring of Operations to Ensure Legal Compliance and the Protection of Privacy of Canadians*;
- OPS-1-10, *Procedures for Metadata Analysis* [REDACTED]
- OPS-1-11, *Retention Schedules for SIGINT Data*;
- OPS-1-13, *Procedures for Canadian* [REDACTED] *and Joint CSEC-[Canadian Armed Forces] Activities*;
- CSOI-1-1, *National SIGINT Priorities List (NSPL) Process*;
- CSOI-3-7, [REDACTED] *Authorities*;
- CSOI-4-1, *SIGINT Reporting*;

A0000569_21-003438

- CSOI-4-3, *Protecting the Privacy of Canadians in the Use and Retention of SIGINT*;
- CSOI-4-4, *Targeting and Selector Management*; and
- CSOI-5-8, *Active Monitoring Procedures for* [REDACTED]

Contact Chaining [REDACTED]

Finding no. 6: Contact Chaining [REDACTED]

A sample of contact chaining conducted by the Office of Counter Terrorism [REDACTED] was found to be generally conducted in compliance with operational policy.

The Commissioner's office reviewed a sample of eight contact chaining activities [REDACTED] pertaining to two separate operations, conducted by the OCT. The eight contact chains were found to be conducted in compliance with the operational policy in place, mainly OPS-1-10, *Operational Procedures for Metadata Analysis* [REDACTED]. There were, however, a few notable shortcomings in some processes and the application of policy, which are discussed below.

For this part of the review, the Commissioner's office relied partly on the CSEC Directorate of Audit, Evaluation and Ethics (DAEE) *Audit of Contact Chaining* [REDACTED] dated July 7, 2011, which assessed to what extent contact chaining activities [REDACTED] during a 16-month sample period were conducted in compliance with OPS-1-10. We used the audit's recommendations respecting policies,²⁷ records management, training, controls and the monitoring regime to guide our compliance verifications.

Section 3.6 of OPS-1 allows the use of metadata for contact chaining in accordance with the MD on *Collection and Use of Metadata*, and OPS-1-10 provides direction on the process that analysts must follow when conducting metadata analysis [REDACTED] in pursuit of foreign intelligence under part (a) of the CSEC mandate.

OPS-1-10 requires an approvals log documenting management approval up to the DGI for the conduct of contact chaining [REDACTED]. The policy directs that approval is granted for a [REDACTED] period, and that the pool of data that may be searched is limited to that collected up to and including the date of the DGI approval.

Since the initial five sample operations selected by the Commissioner's office for this review did not result in any contact chaining [REDACTED], CSEC provided us with a list of OCT OPS-1-10 activities from the review period from which we picked a

²⁷ In spite of the fact that – according to the DAEE *Audit of Contact Chaining* [REDACTED] – CSEC management had indicated its intention to complete a revision of OPS-1-10 by November 2011, the policy in effect remains the one dated June 26, 2010.

sample of eight contact chains [REDACTED] drawn from two different OCT operations.

Each file reviewed contained a properly completed DGI approval form. However, aside from the completed approval forms, much of the information retained was inconsistent from one file to the next: files contained printouts of query results but there was no analysis or foreign intelligence results such as new selectors or EPRs in the files reviewed. There was also no way of accounting for all contact chaining activities undertaken following approval. The information provided did not paint a comprehensive picture that would have allowed the Commissioner's office to draw conclusions with regard to the reviewed metadata activities.

The absence of tracking for denied or cancelled requests in the documents we reviewed made it difficult to provide a meaningful and consistent accounting of the chaining activities for OCT during the period under review. CSEC explained that we had been provided with a heavily edited version of the OPS-1-10 log to allow us to pick a sample of activities to be reviewed and that denials or cancellations could be found in the complete logs. Upon follow-up we were told that no activities were denied or cancelled during the period under review.

Recommendation no. 1: Revision of the Procedures for Metadata Analysis [REDACTED]

CSEC should modify its policy OPS-1-10, Procedures for Metadata Analysis [REDACTED] to reflect current practices for these activities, specifically for record keeping.

While the files reviewed demonstrated compliance with existing policies, it appears that, based on this review of a small sample of activities, many of the findings of the DAEE OPS-1-10 audit may remain to be corrected.²⁸

The OPS-1-10 process summary contained in section 2.3 of the policy clearly states that following the metadata analysis activity, the analyst must:

²⁸ In its *Audit of Contact Chaining* [REDACTED] DAEE indicated that the OPS-1-10 record management system provides neither an accurate nor a consistent accounting of contact chaining activities and that an analysis of approval logs maintained by DGPC and the OCT did not allow its Audit Team to definitely establish how many such activities had been approved, denied or cancelled during the audit timeframe. DAEE concluded that while the OPS-1-10 contact chaining approval process was robust, it may provide CSEC management with a false sense of complete compliance. According to DAEE, the lack of other controls and monitoring poses a non-compliance risk. DAEE also found that while all OPS-1-10 files contained request forms that were duly signed by appropriate authorities, the majority of files provided neither a full, consistent, nor meaningful accounting of the activity, nor an indication of what the results of the activity were. DAEE was expecting to find foreign intelligence results such as [REDACTED] EPRs and indications of analysis results.

5. Attach the results of the metadata analysis activities to the Approval Form, including, but not limited to the following:

- a. "nil" to indicate no results have been obtained, or
- b. a full contact chain, or
- c. a description or copy of the data obtained, and
- d. the [REDACTED] chosen for further analysis and/or targeting

The material provided did not reflect the policy.

In response to our query for more information, CSEC stated that it is neither feasible nor desirable to keep all the other operational material with the approval form. In addition to storage issues, it would unnecessarily [REDACTED] to an ongoing operation. This separation of documentation helps ensure that the focus remains on the foreign intelligence when the analyst is going about their daily business.

CSEC further explained that the OPS-1-10 approval files are not intended to provide information relating to the operations themselves. They are only meant to provide evidence that the correct approvals were sought and that the immediate policy requirements of OPS-1-10 are met.

The explanations provided by CSEC are contrary to its OPS-1-10 policy. CSEC should reconcile its policy to reflect its practices.

All records provided showed that the contact chaining activities reviewed had been conducted within the [REDACTED] period granted by approval. However, one query generated results that fell outside of the approved date-range. CSEC explained that this was an issue relating to the [REDACTED] database and that this incident was not an instance of a compliance-related automated function failing but a problem created within the system itself. CSEC had no information on whether this was a single incident or a systemic issue. CSEC indicated that even if it were the latter, their ability to fix such a problem is limited by the fact that [REDACTED]. Also, according to CSEC, [REDACTED] along with six other analyst tools, is scheduled to be decommissioned and replaced in 2014. This issue will be followed up in the Commissioner's ongoing *Review of CSEC SIGINT and IT Security Metadata Activities*.

While no new information was identified from the query results that fell outside the prescribed timeframe prescribed by OPS-1-10, this issue illustrates the potential for such violations to occur. It also illustrates the fact that full compliance cannot be assured by automation alone and reinforces the importance of compliance monitoring by managers.

Incident relating to the Targeting of a Canadian by a Second Party

Recommendation no. 2: Policy on Targeting of Canadian by a Second Party

CSEC should promulgate guidance to codify its practices to address cases when an analyst identifies that a Second Party is targeting a Canadian, including notification to the Second Party to desist from such targeting and record keeping of such cases.

Another problematic issue identified in the course of our assessment of documentation of this metadata activity was a screenshot from the [REDACTED] showing a clear indication of that a specific Canadian telephone number was targeted.

In response to our request for an explanation, CSEC provided a screenshot from [REDACTED] demonstrating that there was no CSEC targeting relating to this selector. In fact, the record had been annotated DO NOT TARGET to ensure that no CSEC analyst targeted it. Further information was provided in the annotation indicating that this selector was connected to a specific [REDACTED] operation.

Whilst a friendly agreement is in place between members of the five-eyes community²⁹ to not routinely target each other's citizens, it is acknowledged that each is a sovereign nation with their own priorities and requirements. When asked, CSEC confirmed that there is no specific policy currently in place that details a process to follow when it becomes clear that a Second Party has targeted a specific Canadian selector.

The Commissioner's recent *Review of CSEC SIGINT Information Sharing with the Second Parties* included a finding that:

Beyond certain general statements and assurances among the Second Parties, the Commissioner's office was unable to assess the extent to which CSEC's Second Party partners in the United States, United Kingdom, Australia and New Zealand follow the agreements with CSEC and protect private communications and information about Canadians in what CSEC shares with the partners

Currently, there are no policies or procedures that a CSEC employee can refer to when confronted with evidence of a Second Party targeting a Canadian's communications. CSEC indicated that there is an informal process in place which consists of having the analyst who discovers a case of a Second Party targeting a Canadian (selector) inform D2, who in turn will inform the Second Party in question and request that they desist. This process is not documented anywhere in the existing CSEC policy framework. The privacy of Canadians may be directly affected by this targeting. In the case identified in this review, CSEC had no record that such a request was made.

²⁹ The five-eyes SIGINT alliance evolved from collaboration during the Second World War. Long standing agreements and present-day resolutions provide the foundation for CSEC information sharing with the Second Parties.

In discussions, CSEC recognized that such policy guidance would be helpful and indicated that there are ongoing discussions to establish where this process would best fit in the existing CSEC policy framework. The Commissioner will monitor developments.

Following his recent *Review of CSEC SIGINT Information Sharing with the Second Parties*, Commissioner Décary advised his office to follow developments relating to second party practices involving private communications or information about Canadians closely. Accordingly, the observations in the current review with regard to second party targeting of Canadians as identified in [REDACTED] remain of interest and, as noted in the conclusion to the *Information Sharing* review, future reviews, including the ongoing review on metadata, will follow up on these questions.

Finding no. 7: Awareness of Personnel

Interviews with and observations of the Office of Counter Terrorism team leaders and analysts demonstrated that they are knowledgeable about policies and practices aimed at compliance with the law and the protection of the privacy of Canadians.

All interviewees were well aware that selectors and methods used in the collection and acquisition of information are to be directed at foreign entities located outside of Canada, associated with GC intelligence priorities and subject to annual review to ensure they are consistent with those priorities.³⁰

The interviews we conducted with team leaders revealed that they were well versed in the application of the Information Needs process and the underlying policies informing its intent. All were aware of their responsibilities for determining and documenting the assessment of the foreign status of a targeted entity and the justifications for targeting that entity. Some team leaders noted instances where disclosures came through the wrong channel or went directly to an analyst. We were told that in such cases, the sender was directed to resend his request through the proper channels.

Previous reviews by this office have established that CSEC is diligent in training all staff on the subjects of understanding the CSEC mandate and the responsibility to protect the privacy of Canadians. CSEC has core competency courses on the requirements for the protection of privacy of Canadians; knowledge of compliance requirements is one of the competencies required for all analysts following the analyst career track for promotions.

Finding no. 8: Policy Compliance Monitoring

CSEC managers routinely and closely monitor Office of Counter Terrorism activities.

The Commissioner expected that CSEC had an effective management control framework to ensure that the integrity of OCT activities is routinely maintained, including

³⁰ See CSOI-4-4, *supra* note 7.

appropriately accounting for important decisions and information relating to compliance and the protection of the privacy of Canadians.

To help verify that managers were effectively monitoring OCT activities, we were provided with the following internal compliance review documents:

- *SPOC Annual Compliance Validation Review*

SPOC staff briefed us on the results of its Compliance Management Team (CMT) review of the OCT and provided us with copies of SPOC's Annual Compliance Validation Review and Biannual Review of Annotated Traffic. This review, which concluded on October 25, 2011, was based on a sampling of █% of EPRs produced and the same percentage of metadata analyses conducted.

- *EPR Review*

In his summary of results, observations and recommendations, the OCT Level IV manager recommended that analysts ensure that a hard copy of all draft, advanced and final EPRs, as well as all relevant traffic be included in the file for permanent retention as per section 2.4 of CSOI-4-1, *CSE SIGINT Operations Instruction*.³¹

- *OPS-1-10 Review*

The manager also recommended that results of the metadata analysis must be attached or noted on the approval form, including a "nil" marking for a lack of results. EPR serial numbers must also be indicated on the approval form if a report was produced from the results of the metadata analysis as per section 2.3 of OPS-1-10.

- *Biannual review of annotated traffic*

CSOI-4-3, *Protecting the Privacy of Canadians in the Use and Retention of SIGINT*,³² provides guidelines to be followed to protect Canadian privacy-related information (CPRI)³³ that is encountered in the conduct of day-to-day SIGINT activities. CSOI-4-3 also requires designated managers to complete a review of all holdings of operational areas on a biannual basis. This review is documented in an Operational Area Biannual Confirmation of Review Activity Form.

The Commissioner's office was provided with a copy of the form for the OCT review completed in November 2011, which falls within the scope of this review. The form confirmed that an OCT manager had completed a review of all holdings and filled out the form confirming that CPRI retained by the OCT met the retention criteria outlined in section 1.3 of CSOI-4-3 and that any items no longer

³¹ November 13, 2008.

³² April 11, 2011.

³³ CPRI refers to private communications, communications of a Canadian abroad, information about Canadians or Canadian identity information.

meeting this criteria had been deleted or destroyed. The form also confirmed that access to CPRI was limited to a need-to-know basis. Shortcomings – which did not affect compliance – that were identified by the manager were the same issues identified in the EPR review and the OPS-1-10 review:

- *EPRs:* Working from a sample of 14 EPRs produced by the OCT during a six-month period (approximately █% of EPRs in that period), the OCT manager noted some files did not have a copy of all iterations and versions of released reports in the folder for permanent retention in accordance with CSOI-4-1.
- *Metadata analysis:* Working from a sample of 34 metadata analysis reports during a six-month period (approximately █% of reports in that period) conducted █ the manager noted that the analysis must be attached or noted on the approval form, including “nil” if no results were obtained and that the EPR serial number must be indicated on the approval form if a report was produced using the metadata analysis results.

The Commissioner’s office was satisfied with the conclusions from these internal reviews.

IX. CONCLUSION

The primary objectives of this review were to acquire a detailed knowledge of the OCT and the extent of any changes of its activities since the last review in 2007, to determine if CSEC activities relating to the OCT were conducted in accordance with the law, the extent to which CSEC protected the privacy of Canadians in carrying out its OCT activities, and to follow-up on a previous report’s recommendation.

Based on the information reviewed and the interviews conducted, the Commissioner’s office concluded that OCT activities were conducted in accordance with the law and ministerial direction.

CSEC OCT activities are subject to the same legal requirement to protect the privacy of Canadians that apply to all CSEC SIGINT activities; CSEC has sufficient policies and processes to satisfy the legal requirement not to direct its SIGINT activities at a Canadian wherever he or she may be or at any person in Canada.

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

Interviews with and observations of OCT team leaders and analysts demonstrated that they are knowledgeable about policies and practices aimed at compliance with the law and the protection of the privacy of Canadians and CSEC managers routinely and closely monitor OCT activities.

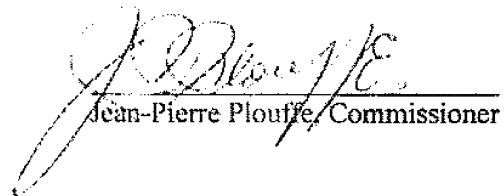
A sample of contact chaining conducted by the OCT █ was found to be generally conducted in compliance with operational policy. While some

issues were identified in the contact chaining section of the present review, these will be pursued in depth in the review of CSEC SIGINT and IT security metadata activities. The review of the sample contact chaining did result in two recommendations as a measure to protect the privacy of Canadians by CSEC:

1. CSEC should modify its policy OPS-1-10, *Procedures for Metadata Analysis* [REDACTED] to reflect current practices for these activities, specifically for record keeping; and
2. CSEC should promulgate guidance to codify its practices to address cases when an analyst identifies that a Second Party is targeting a Canadian, including notification to the Second Party to desist from such targeting and record keeping of such cases.

Another, more specific objective was to assess how CSEC practices in sharing Canadian identity information with domestic and second-party partners, especially regarding precise and consistent language, [REDACTED]

A list of findings and recommendations is enclosed at Annex A.


Jean-Pierre Plouffe, Commissioner

A0000569_29-003446

ANNEX A — Findings and Recommendations

Recommendation no. 1: Revision of the Procedures for Metadata Analysis

CSEC should modify its policy OPS-1-10, Procedures for Metadata Analysis to reflect current practices for these activities, specifically for record keeping.

Recommendation no. 2: Policy on Targeting of Canadian by a Second Party

CSEC should promulgate guidance to codify its practices to address cases when an analyst identifies that a Second Party is targeting a Canadian, including notification to the Second Party to desist from such targeting and record keeping of such cases.

Finding no. 1: Compliance with the Law

Based on the information reviewed and the interviews conducted, CSEC Office of Counter Terrorism activities complied with the law.

Finding no. 2: Demonstrating Legal Compliance – Recording Information Exchanges with Federal Law Enforcement and Security Agencies

The introduction of the Information Needs process is significant and will promote clarity of language in CSEC information exchanges with federal law enforcement and security agencies.

Finding no. 3: Protection of the Privacy of Canadians

CSEC's Office of Counter Terrorism activities are subject to the same legal requirements to protect the privacy of Canadians that apply to all CSEC SIGINT activities; CSEC has sufficient policies and processes to satisfy the legal requirement not to direct its SIGINT activities at a Canadian wherever he or she may be or at any person in Canada.

Finding no. 4: Ministerial Direction

Based upon the information reviewed and the interviews conducted, CSEC carried out its Office of Counter Terrorism activities in accordance with ministerial direction.

Finding no. 5: Appropriateness of policies and procedures

Operational policies and procedures for the Office of Counter Terrorism activities are in place and provide sufficient direction to CSEC employees respecting the protection of the privacy of Canadians.

Finding no. 6: Contact chaining [REDACTED]

A sample of contact chaining conducted by the Office of Counter Terrorism [REDACTED] were found to be generally conducted in compliance with operational policy.

Finding no. 7: Awareness of Personnel

Interviews with and observations of the Office of Counter Terrorism team leaders and analysts demonstrated that they are knowledgeable about policies and practices aimed at compliance with the law and the protection of the privacy of Canadians.

Finding no. 8: Policy Compliance Monitoring

CSEC managers routinely and closely monitor Office of Counter Terrorism activities.

ANNEX B — Interviewees

Director, Corporate and Operational Policy

Manager, SIGINT Operations

Head, IT Security Systems Development

Intelligence Analyst, Office of Counter-Terrorism

Intelligence Analyst, Office of Counter-Terrorism

Team Leader, [REDACTED]

Team Leader, [REDACTED]

Team Leader, [REDACTED]

Team Leader, [REDACTED]

Acting Team Leader [REDACTED]

A0000569_32-003449

ANNEX C — Tasking Workflow

The responsibility for all tasking for CSEC [REDACTED] collection assets resides with the [REDACTED] team.

The Activity Authorization Request

The first step in the tasking process is the submission of an Activity Authorization Request (AAR) that must be submitted prior to undertaking [REDACTED] operations and SIGINT Development (SIGDEV) or collection activities connected to the [REDACTED] collection programs.

In submitting the AAR, the analyst must relate the request to an intelligence requirement of foreign intelligence interest such as defined in a GCR. The AAR must include at a minimum:

- An intelligence requirement/GCR;
- NSPL tier level;
- Collection source and [REDACTED] – as applicable – against the activity to take place;
- Target details, if available;
- Targeting and collection handling procedures;
- [REDACTED] collection options;
- Sponsoring elements; and
- Tracking number.

Upon the receipt of a new tasking request, the [REDACTED] team shall complete the AAR and obtain approval from the Director SPOR, and the Director for [REDACTED] Group.

Upon signed approval, [REDACTED] SIGINT development or collection connected to the [REDACTED] collection programs may proceed. Tasking may also be registered with [REDACTED] by [REDACTED]

An automated record of all tasking requests is maintained in the [REDACTED] allowing [REDACTED] to originate, retrieve and track collection [REDACTED] and link the intelligence requirement to the collection.

[REDACTED] Tasking Check

The [REDACTED] team is required to confirm that CSEC collection activity is conducted in accordance with an existing AAR on a [REDACTED] basis. Any unauthorized tasking must be immediately removed until such time as a valid AAR is written and approved and the unauthorized tasking reported to the [REDACTED] manager and SPOC staff and documented in CERRID.

Tasking Revalidation

Following an initial tasking request, the [REDACTED] team is required to revalidate at [REDACTED] intervals. Revalidation includes an assessment on all tasking associated with the AAR and the maintenance of automated record in [REDACTED] for all revalidation requests. During these assessments, the analyst can revalidate or terminate the tasking. Once completed, the information is either destroyed or archived.

A0000569_34-003451

ANNEX D — Targeting Workflow

CSEC targets communications using selectors. In a SIGINT context, targeting means to single out for collection or interception purposes and a selector is a piece of identifying information used by an entity for communications, such as a telephone number or an e-mail address.

The targeting process allows SIGINT to direct its collection activities at foreign entities associated with foreign intelligence requirements located outside Canada while selector management consists of the identification of selectors that can be used to target and retrieve data that can be specifically assigned and attributable to a target.

The 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, thereby ensuring that the entity is neither Canadian, nor from one of the five-eyes countries.

Targeting Request

A targeting request is an official request for the targeting of specific selectors to acquire associated communications data.

i) Targeting requirements

Analysts are responsible for the development of selectors, namely to conduct research and document that all conditions for targeting have been met and submitting targeting requests for validation via the automated targeting tool.

Selectors are developed following targeting requirements. This ensures that collection systems will only collect data that contains the selector. Once successfully validated they are inserted into a dictionary [REDACTED] for the purpose of identifying traffic (communications data) that relates to national foreign intelligence requirements. Selectors enable CSEC to filter out extraneous data.

The rules-based targeting process begins with the analyst submitting a fully documented targeting request for validation, including the following elements of information:

- a target identification number generated by [REDACTED]
- an identifier [REDACTED]
- an entity name,
- an entity nationality,
- an entity location,
- an associated intelligence priority,
- a pre-approved targeting justification,
- a targeting priority, with justification,
- a security classification,
- [REDACTED]

A0000569_35-003452

- [REDACTED]

Other elements can be included, as appropriate, such as a Canadian Eyes-Only (CEO) comment or justification.

ii) Analysts Search Selected Traffic via [REDACTED]

The [REDACTED] links the selectors to the Consolidated Traffic Repository (CTR) which contains selected traffic. The traffic is identifiable and searchable through its [REDACTED] [REDACTED] which comprises information including:

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

Protected entities, such as Canadian citizens or potential targets located within Canada have to be identified and annotated as such so that they are not targeted.

iv) [REDACTED] Validates Selectors

[REDACTED] is responsible for the validation and action, if appropriate, targeting requests and to inform the analyst of the status of a targeting request (approved or denied) and the selector (targeted or de-targeted).

The process through which OCT analysts submit designated selectors to [REDACTED] is fully automated. While responsibilities ultimately lies with [REDACTED] most requests are now handled by the automated approval system, which either approves, rejects, pools or refers requests for manual inspection, as appropriate. The analysts are still required to input the selectors into [REDACTED]. No selectors will be forwarded to collection [REDACTED] without validation from [REDACTED].

All referred targeting requests are manually validated by [REDACTED], in accordance with CSOI-3-7, [REDACTED] *Authorities*.

Specifically, the validation process ensures that:

- the selection string is in the proper format,
- the targeting is directed at a foreign entity located outside Canada,
- the targeting is related to an active GCR, and
- the targeting justification is adequate.

Targeting requests that pass all the rules in the targeting tool are automatically approved — or manually approved by [REDACTED] — and forwarded to collection systems. Some requests are not handled by the automated tool. Requests directed at certain collection [REDACTED] are received by [REDACTED] in the form of an e-mailed template, which [REDACTED] validates manually and forwards to the collection system, as it does for referred requests.

If all elements of a targeting request are valid, the analyst receives a notification that the targeting request has been approved and [REDACTED] forwards the selector to a collection system or systems. [REDACTED] may also input valid selectors in other tools [REDACTED] as required.

On an annual basis — or more frequently, if required — the analyst must confirm that the selector is valid, meaning that the targeted entity is of a foreign nationality and located outside Canada and productive, meaning that the intercepted communication contains foreign intelligence associated with a GCR and aligned with the NSPL. The analyst is required to de-target selectors which are no longer valid or which are resulting in intercepted communications of no foreign intelligence value, or for which there is no longer an associated GCR. De-targeting also frees up space in the targeting dictionaries.

Targeting requests which fail one or more rules are rejected and do not proceed to collection systems. [REDACTED] provides the requesters with a notification of the rejection with the reason, so that they may — if appropriate — modify and resubmit the request. The new request for targeting becomes a new record in [REDACTED] targeting history and the original request that was refused remains a record.

v) Perform Capacity Management

The [REDACTED] team does a daily manual scan of incoming collection metrics. This is supplemented by automated alerts that are set up throughout the SIGINT end-to-end system to flag any issue requiring immediate action.

In cases where a selector may cause or threaten to cause issues due to [REDACTED] collection, an e-mail is sent to the [REDACTED] to de-target the selector. The team removes the selector from the system and informs the appropriate analyst that their selector was removed due to [REDACTED] collection providing the opportunity to [REDACTED] of the selectors and retarget the problematic selector.

vi) Analysts Annually Revalidate Selectors

OPS-1 requires, at a minimum, that selectors be subjected to annual review to ensure they remain consistent with the GC intelligence priorities. Analysts monitor selectors to ascertain their value regarding the production of usable intelligence. Analysts must update their targeting regularly. In other cases, they must de-target selectors by deleting the ones that are unproductive or that bring in irrelevant traffic.

ANNEX E — Contact Chaining

The process for conducting metadata analysis from [REDACTED] metadata repositories [REDACTED] is listed at section 2.3 of OPS-1-10. The analyst is responsible for:

- a. determining whether the metadata analysis is within the OPS-1-10 requirements;
- b. completing the Intelligence Branch Approval Form;
- c. obtaining the appropriate approvals;
- d. conducting the metadata analysis activities; and,
- e. attaching the results of the activities to the Approval Form, including, but not limited to the following:
 - i. “nil” to indicate no results have been obtained, or
 - ii. a full contact chain, or
 - iii. a description or copy of the data obtained, and
 - iv. the [REDACTED] chosen for further analysis and/or targeting.

An analyst who becomes aware of a [REDACTED] that could be a candidate for [REDACTED] metadata analysis must first apply the “foreign intelligence test” prior to initiating the approval process as per section 2.4 of OPS-1-10. Before proceeding to the contact chaining activity, the analyst must ensure that other avenues of foreign intelligence target development have been considered. In that case, the analyst must provide a detailed rationale, using the Approval Form, as to why the [REDACTED] will likely lead to foreign intelligence. The pertinent GCR number must be included on the Approval Form. The analyst can then submit the completed Approval Form. Any negative response to any of these steps means that the analyst should not proceed with the contact chaining.

Once a request to conduct a contact chain [REDACTED] is approved by the DGI, in accordance with OPS-1-10, an analyst may, for a period of [REDACTED] from the date of the approval, conduct an [REDACTED] using the approved [REDACTED] and using data acquired up to the date of approval.

The goal is to create a chain of foreign contacts that can help identify foreign intelligence entities of interest and to obtain foreign intelligence that meets the government’s intelligence priorities.

ANNEX F — Report Production

The main responsibility of the DGI analyst affected to the Office of Counter-Terrorism is to produce foreign intelligence reporting on terrorism-related targets of interest to the Canadian government on the basis of intercepted communications. This reporting is documented in a security-based EPR.

OCT analysts follow the standard DGI path in the production of an EPR. However their various linguistic, technical and analytical skills are related to specific terrorism issues,

[REDACTED]

The report production process is outlined below:

1. Scanning

Scanning plays a major role in the activities of the analyst. In order to determine if a piece of traffic is reportable, the analyst needs to ensure the topic falls within the parameters of foreign intelligence, meets the clients' needs and would not be available through open sources.

Traffic

Once a selector is targeted, the analyst uses the [REDACTED] traffic-scanning tool to examine the data amalgamated in the CTR for reportable intelligence. It also allows the analyst to directly access several other applications such as the [REDACTED] and [REDACTED] databases for data that includes [REDACTED] fax, [REDACTED] traffic to cross reference what targeted information [REDACTED] has been reported. The [REDACTED] allows the analyst to write and store transcripts of scanned traffic and perform other functions related to traffic analysis.

To facilitate traffic scanning, analysts may create saved queries that may include keywords or selectors relevant to their targets. Such queries ensure that only traffic pertaining to specific targets will be retrieved.

Analysts regularly monitor and update their saved queries to ensure that the most productive results are produced.

End-Product Reports

The analyst scans EPRs in [REDACTED] on a daily basis in order to be informed of recent developments in current issues and matters relating specifically to the targets. Scanning also allows the analyst to be informed of what five-eyes partners are reporting, especially on the target [REDACTED] and may show up in an analyst's channel if relevant to the topics he or she researches. The analyst can also scan EPRs for client feedback on the reporting line, which can provide valuable information that may influence future reporting as it often

reveals the areas of heightened interest or concerns about timeliness, relevance, or other factors.

Open-Source Material

Open-source publications can be scanned for content that may provide background information and augment the collated intelligence.

2. Annotating Traffic for Privacy

Private Communications

The CTR default position automatically deletes unmarked data at the end of its retention period unless an analyst specifically marks it for retention. In order to protect the identity of Canadians and their communications while scanning traffic, analysts must annotate any traffic³⁴ where:

- one communicant is physically located in Canada,
- one communicant is Canadian and physically located outside Canada, or
- both communicants are foreign and located outside Canada and the communication contains information about a Canadian, but that information does not constitute foreign intelligence.

Guidelines on annotating traffic can be found in OPS-1, Annex 2. More information on annotations can be found in the [REDACTED] under "Privacy Annotations".

Canadian Identity Information

In case where such information is to be shared with GC clients and Second Parties, the analyst is required to suppress Canadian identity information, substituting a nondescript term for sensitive information.³⁵

3. Translating Traffic

If the traffic is in a foreign language, a linguist analyst will produce a polished translation that will be checked by a co-worker. The analyst has access to [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED] an expert linguist for full translation.

³⁴ There is a statutory requirement to destroy records with privacy annotations that have been viewed and deemed irrelevant. Records with privacy annotations may only be retained if they are relevant and essential as per OPS-1, section 3.3. Such records receive a retention date of [REDACTED] years from the time the marking is applied.

³⁵ See OPS-1-7 *Operational Procedures for naming in SIGINT Reports*, July 8, 2011.

4. Determining Reportability

In order to determine if a piece of traffic is worth reporting, the analyst needs to ensure it constitutes foreign intelligence, meets the clients' needs and would not be available through open sources. The analyst must take into consideration such things as:

- Government of Canada [intelligence] Requirements;
- the NSPL;
- previous reporting on the topic;
- Second Party reporting related to the topic;
- whether the information would be available through open sources;
- the current reporting threshold – in relation to time and risk management.

5. Research and Analysis

IRRELEVANT

6. Drafting

IRRELEVANT

7. Entering the Report Metadata

IRRELEVANT

8. Editing

IRRELEVANT

IRRELEVANT If the report contains privacy information it is recommended to a senior executive.

9. Obtain the Necessary Sign-Offs

Once the report is written and properly edited, the analyst submits the entire report package to the releasing officer for final review and approval. It is released following the approval of the unit head who confirms that the EPR conforms to all legal and policy guidelines. If a report contains sensitive information it may require different or additional signoffs.

10. Releasing the Report

Once authorized for release, the analyst releases the report through [REDACTED]. Reports may be limited to Canadian clients or may be disseminated to all of, or a subset of the five-eyes community.

ANNEX G —Annexes A & B to the Information Needs Process

ANNEX A: How to send information to CSEC (Instructions for Government of Canada clients)

1. Prepare

Include in the message:

- The caveat: "The following information was lawfully obtained by [Your Department] under its authorities and is being provided to CSEC in relation to CSEC's foreign intelligence mandate to provide information about the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group, as they relate to international affairs, defence or security in accordance with Government of Canada foreign intelligence and national SIGINT priorities."
- all relevant contextual information regardless of nationalities
- all possible "identifiers" (see list below) relevant to the case, regardless of users' nationalities
- any identifiers that belong to persons in Canada – including foreigners in Canada – or Canadians abroad must be flagged as such
- possible identifiers include (but are not limited to):
 - ☐ telephone numbers [REDACTED]
 - ☐ e-mail addresses [REDACTED]
 - ☐ IP addresses [REDACTED]

- references to any previous or related messages sent to CSEC
- your contact information so CSEC can acknowledge receipt of the message, and follow up

Do not include...

- any request to target a Canadian
- requests for information about Canadians

2. Send

- you can state in your message to whom you would like it to go (e.g.) "ATTN: "Name", Team Leader, [REDACTED] but always send the message to the above e-mail address
- feel free to CC: the relevant CSE integree to ensure we are aware of your message

Sending messages directly to individuals causes confusion and messages get lost. Please do not send messages to INDIVIDUALS at CSE.

A0000569_43-003460

ANNEX B: How CSEC will acknowledge GoC messages (Instructions for DGI)

Upon receipt of your message, the relevant area at CSEC will acknowledge your message in one of four possible ways:

A) "Thank you for the information you have provided which we have determined corresponds to Government of Canada SIGINT Requirement _____. This issue is ranked as Tier ____ on the National SIGINT Priorities List. CSEC will use your information for foreign target development and/or to generate foreign intelligence in relation to CSEC's Mandate to provide information or intelligence about the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group, as they relate to international affairs, defence or security. The point of contact will be _____, who can be reached by telephone at (613) 9 _____ or by Mandrake e-mail at _____."

B) "Thank you for the information you have provided corresponding to Government of Canada SIGINT Requirement _____. Given current resources and priorities, CSE may not be able to undertake target development or intelligence generating activities related to this information. However, it will be retained in the event resources and/or priorities related to this subject change. Should you have any questions, please contact _____, who can be reached by telephone at (613) 9 _____ or by Mandrake e-mail at _____."

C) "Thank you for the information you have provided. The information does not conform to any current Government of Canada SIGINT Requirement. As such, CSEC will not undertake target development or intelligence generating activities related to this information. However, it will be retained in the event this situation changes. Should you have any questions, please contact _____, who can be reached by telephone at (613) 9 _____ or by Mandrake e-mail at _____."

D) "Thank you for your message. CSEC is not able to undertake any activities related to this information under our Foreign Intelligence mandate to provide information or intelligence about the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group, as they relate to international affairs, defence or security. However, we may be able to assist you under our mandate to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties. Should you wish to pursue this as a request for technical assistance, please contact CSEC or the CSEC Liaison office within your organization, which will be able to provide the requisite request template for signature from an executive or equivalent and forwarding to CSEC."