

Communications Security
Establishment Commissioner

The Honourable Robert Décary, Q.C.



Commissaire du Centre de la
sécurité des télécommunications

L'honorable Robert Décary, c.r.

TOP SECRET/COMINT/CEO

December 16, 2010

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's (CSEC) contact chaining activities [REDACTED]. These activities involve the analysis of metadata – such as phone numbers and e-mail and Internet addresses – whereby CSEC determines and examines, for example, [REDACTED] which can be valuable to CSEC for identifying foreign intelligence entities of interest and obtaining foreign intelligence that meets Government of Canada intelligence priorities.

With respect to these activities, my predecessors recommended that CSEC re-examine its interpretation and application of its mandate under paragraphs 273.64 (1)(a) [foreign intelligence collection] and (c) [assistance to federal law enforcement and security agencies] of the *National Defence Act (NDA)*. Three reports over the past five years involved some degree of examination of CSEC's contact chaining activities: CSEC's support to the Royal Canadian Mounted Police (2006); CSEC's collection and use of metadata (2008); and CSEC's support to the Canadian Security Intelligence Service (2008).

In April 2007, the Chief of CSEC suspended contact chaining activities [REDACTED]. [REDACTED] CSEC resumed these activities in October 2008 after making significant changes to the conduct of the activities and to the associated policy and accountability framework.

This review was initiated under the authority of my predecessor, the late Honourable Charles D. Gonthier, as articulated in Part V.1, paragraph 273.63(2)(a) of the *NDA*. The objectives of the review were: to acquire detailed knowledge of and document CSEC's new approach to contact chaining activities [REDACTED] to assess whether the activities

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

NOT REVIEWED

A0000405_1-01089

complied with the law; and to assess the extent to which CSEC protected the privacy of Canadians in carrying out the activities.

This review examined the [REDACTED] contact chains [REDACTED] that CSEC conducted from the resumption of these activities in October 2008 to October 2009. This was the first review focused exclusively on CSEC's contact chaining activities [REDACTED]

Based upon the information reviewed and the interviews conducted by the Commissioner's office, CSEC conducted its contact chaining activities [REDACTED] during the period of review in accordance with the law Solicitor-Client Privilege. These contact chains were appropriately authorized under part (a) of CSEC's mandate. With the significant changes made to these activities as outlined in CSEC's new policy on this subject, I have no questions like those raised in previous reviews as to whether the activities would be more appropriately authorized under part (c) of CSEC's mandate. I assess the new processes put in place and followed by CSEC, for the activities conducted during the period of review, as consistent with part (a) of CSEC's mandate.

CSEC's contact chaining activities [REDACTED] conducted during the period of review were conducted in accordance with ministerial requirements set out in ministerial directives.

CSEC has appropriate policies and procedures that govern its contact chaining activities [REDACTED]. New policies, guides and forms address previous findings and recommendations relating to gaps in policies and procedures. CSEC managers and officials are aware of and comply with the policies and procedures. CSEC managers routinely and closely monitor contact chaining activities [REDACTED] to make certain the activities comply with the governing authorities.

During the period under review, which began immediately following the October 2008 resumption of activities after the changes CSEC made, the number of contact chains [REDACTED] conducted by CSEC was significantly smaller than the number of such contact chains conducted prior to the Chief of CSEC suspending these activities.

Given the significant changes made by CSEC and the positive results of this review, I consider the past recommendations of my predecessors as completed and the issues raised in statements made by my predecessors in past public Annual Reports as addressed.

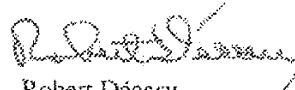
CSEC officials were provided an opportunity to review and comment on the enclosed report, for factual accuracy, prior to finalizing it. While the results of the review are positive, I have directed my officials to monitor these activities because they involve information about Canadians and may affect the privacy of Canadians.

NOT REVIEWED

A0000405_2-01090

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

Yours sincerely,



Robert Décaré

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

NOT REVIEWED

A0000405_3-01091

Office of the
Communications Security
Establishment Commissioner



Bureau du
Commissaire du Centre de la
sécurité des télécommunications

TOP SECRET/COMINT/CEO

A Review of CSEC's Contact Chaining Activities

December 16, 2010

NOT REVIEWED

P.O. Box 68, 1964, Station "B" / Succursale "B"
Ottawa, Canada
K1P 5B5
(613) 992-3044 Fax: (613) 992-4096
info@csec-hccst.gc.ca

A0000406_1-01092

TABLE OF CONTENTS

I. AUTHORITIES	1
II. INTRODUCTION	1
Rationale for conducting this review	2
III. OBJECTIVES	2
IV. SCOPE	3
V. CRITERIA	3
VI. METHODOLOGY	4
VII. BACKGROUND	4
What is contact chaining and why does CSEC contact chain?	4
How does CSEC contact chain? Approval Framework for contact chaining	6
Justice Canada legal advice	9
Reviews by the CSE Commissioner	10
VIII. FINDINGS	13
A) LEGAL REQUIREMENTS	14
Summary of CSEC changes to contact chaining activities [REDACTED]	15
[REDACTED] following resumption of the activities in October 2008 ...	15
B) MINISTERIAL REQUIREMENTS	16
Ministerial Directives	16
Ministerial Authorizations	17
C) POLICIES AND PROCEDURES	18
i. Appropriateness of policies and procedures	18
ii. Awareness of personnel	20
iii. Management control framework	20
IX. CONCLUSION	21
ANNEX A – Findings	23
ANNEX B – Interviewees	24
ANNEX C – Timeline of Events	25

I. AUTHORITIES

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

The review is also in accordance with ministerial directives (MDs) on "Accountability Framework"¹, "Privacy of Canadians"², "Collection and Use of Metadata"³, and "Support to Law Enforcement and National Security Agencies"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

This is the first review focussed exclusively on CSEC's contact chaining⁵ activities

Over the last five years, a number of reviews conducted by the Commissioner's office recommended that CSEC re-examine its interpretation and application of parts (a) and (c) of its mandate⁶, particularly in the context of contact chaining activities

At the time of the reviews, the first of which started in March 2005, CSEC would, under part (a) of its mandate: receive requests for information from the Canadian Security Intelligence Service (CSIS) and other client agencies; conduct contact chains using the information obtained; collect foreign intelligence on the basis of the results of the contact chains; and report on the foreign intelligence obtained, including reporting to the agency that originally requested information. Reviews by the Commissioner's office identified inconsistencies in interpretation between legal opinions provided to CSEC by Justice Canada and the application of that advice. In the reviews and in discussions with CSEC and Justice Canada, the Commissioner's office questioned whether part (c) of CSEC's mandate would be more appropriate for some of these activities, since the

¹ Issued June 19, 2001.

² Issued June 19, 2001.

³ Issued March 9, 2005.

⁴ Issued June 19, 2001.

⁵ *Contact chaining* refers to: "the method developed to enable the analysis, from information derived from the metadata, of communications activities or patterns to build a profile of communications contacts of various foreign entities of interest in relation to the foreign intelligence priorities of the GC [Government of Canada], including the number of contacts to or from these entities, the frequency of these contacts, the number of times contacts were attempted or made, the time period over which these contacts were attempted or made as well as other activities aimed at mapping the communications of foreign entities and their networks." (Source: section 8.3, CSEC policy OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities*, March 11, 2010)

⁶ Paragraph 273.64(1)(a) of the NDA [part (a)] mandates CSEC: "to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with the Government of Canada intelligence priorities. Paragraph 273.64(1)(c) of the NDA [part (c)] mandates CSEC: "to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties."

activities could be considered to be directed at a Canadian, which is prohibited under paragraph 273.64(2)(a) of the *NDA*. The Commissioner's office consulted its independent legal counsel, who, after reviewing certain cases independently, **Solicitor-Client Privilege**

Solicitor-Client Privilege

Solicitor-Client Privilege

In

April 2007, the Chief of CSEC suspended all contact chaining activities [REDACTED]. CSEC resumed contact chaining activities [REDACTED] in October 2008 after making significant changes to the conduct of the activities and associated policy and accountability framework. The background section of this report and Annex C provide a summary and timeline of events related to these matters.

Rationale for conducting this review

Contact chaining [REDACTED] involves CSEC use of information [REDACTED] for foreign intelligence purposes. Specific controls are placed on these activities to ensure compliance with legal, ministerial and policy requirements. Past Commissioners made findings and recommendations respecting these activities. Major changes to certain practices and procedures relating to these activities have recently occurred. It is for these reasons that we selected contact chaining [REDACTED] as a subject of review. This is the first review of these activities since the Chief's decision to suspend and resume the activities and includes follow-up to issues identified by past Commissioners.

III. OBJECTIVES

The objectives of the review were:

- to acquire detailed knowledge of and document CSEC's new approach to contact chaining activities [REDACTED]
- to assess whether the contact chaining activities [REDACTED] complied with the law; and
- to assess the extent to which CSEC protected the privacy of Canadians in carrying out the contact chaining activities [REDACTED]

NOT REVIEWED

A0000406_4-01095

IV. SCOPE

The Commissioner's office examined the [REDACTED] contact chaining activities [REDACTED] that CSEC conducted from the resumption of these activities in October 2008 to October 2009, as well as any associated reporting and disclosures of information about Canadians.

V. CRITERIA

A) Legal Requirements

The Commissioner expected that CSEC conducted its contact chaining activities [REDACTED] in a manner that is in accordance with the *National Defence Act (NDA)*, *Canadian Charter of Rights and Freedoms*, *Privacy Act*, *Criminal Code*, and any other relevant legislation and Justice Canada advice.

B) Ministerial Requirements

The Commissioner expected that CSEC conducted its contact chaining activities [REDACTED] in a manner that is in accordance with ministerial direction.

C) Policies and Procedures

The Commissioner expected that CSEC:

- i. has appropriate policies and procedures that guide its contact chaining activities [REDACTED] and provide sufficient direction respecting legislative and ministerial requirements;
- ii. has personnel who are aware of and comply with the policies and procedures; and
- iii. has an effective management control framework to ensure the integrity of the activities is maintained on a routine basis, including appropriately accounting for important decisions and information relating to compliance and the protection of the privacy of Canadians.

VI. METHODOLOGY

The Commissioner's office examined applicable written and electronic records, files, correspondence and other documentation, including policies and procedures, ministerial direction and legal advice.⁸ Respecting the [REDACTED] chains conducted by CSEC in the period under review, this documentation included the approvals to conduct the chaining activities, the results (the chains), associated reporting and disclosures.

CSEC provided answers to a number of written questions, and we interviewed managers and other personnel involved in contact chaining activities [REDACTED]. Annex B provides a list of interviewees, by position title.

On June 11, 2009, CSEC provided a demonstration of contact chaining activities.

As a first step, we documented and described CSEC's contact chaining activities [REDACTED] and associated processes and systems, the legislative and policy framework, and ensured a common understanding of concepts and terminology. Subsequently, we assessed CSEC's conformity with the criteria and developed conclusions respecting the objectives.

Prior to forwarding a draft report to CSEC for comment as to factual accuracy, a meeting was held with personnel at CSEC involved in the review, to present a summary of the findings.

VII. BACKGROUND

What is contact chaining and why does CSEC contact chain?

CSEC's OPS-1 policy, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities*⁹, establishes baseline measures to protect the privacy of Canadians in the use and retention of intercepted information and to ensure compliance of CSEC activities with relevant laws of Canada, including Part V.1 of the *NDA*. Detailed requirements for CSEC to protect privacy are found in activity specific CSEC policy instruments.

⁸ Legal advice given to CSEC is shared with the Commissioner's office 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.

⁹ Issued March 11, 2010.

OPS-1 provides that, in accordance with the MD on "Collection and Use of Metadata", CSEC may search metadata¹⁶ for the purpose of providing any information or intelligence about the capabilities, intentions or activities of a foreign individual, state, organization, terrorist group or other such entities as they relate to international affairs, defence or security, including any information related to the protection of electronic information or information infrastructures of importance to the Government of Canada. OPS-1 limits CSEC use of metadata to specific purposes, including contact chaining.¹⁷

Contact chaining involves the use and analysis of metadata. Metadata includes, but is not limited to phone numbers and e-mail and Internet addresses, that are also referred to as [REDACTED]. CSEC conducts metadata analysis, including contact chaining, to generate foreign leads and identify targets of foreign intelligence interest. The purpose of contact chaining is to identify and profile the communications contacts of foreign entities of intelligence interest. Contact chains may include the number of contacts to or from targeted entities, the frequency of these contacts, the number of times contacts were attempted or made, the time period during which the contacts were attempted or made, as well as other information used to map the entities' communications and their networks.¹⁸

Metadata is not the content or purport of a communication and therefore does not constitute a private communication as defined in the *Criminal Code*. Therefore, CSEC does not require a ministerial authorization to conduct metadata activities like contact chaining because these activities do not involve private communications.

In most cases, CSEC initiates metadata analysis and contact chains [REDACTED]. However, in some instances where other signals intelligence (SIGINT) development avenues have already been considered by CSEC, initiating metadata analysis with [REDACTED] may be the most suitable option for CSEC for conducting target discovery activities where there are reasonable grounds to believe that this activity may provide foreign intelligence that is in accordance with the Government of Canada's intelligence priorities.

When CSEC conducts a contact chain [REDACTED] CSEC employees are not required to obtain senior management approval for this activity. However, CSEC employees must adhere to applicable policy and procedures. For example, in the event any subsequent reporting resulting from the chaining [REDACTED] contains information about Canadians, CSEC analysts must ensure that the privacy of Canadians is safeguarded, e.g., by suppressing Canadian identity information and replacing it with a generic term in the reporting. In the case of contact chaining

¹⁶ *Metadata* means: information associated with a telecommunication to identify, describe, manage or route that telecommunication or any part of it as well as the means by which it was transmitted, but excludes any information or part of information which could reveal the purport of a telecommunication, or the whole or any part of its content. (Source: MD on "Collection and Use of Metadata", March 9, 2008)

¹⁷ Section 3.6, OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities*, March 11, 2010.

¹⁸ Section 6.3, OPS-1-10, *Procedures for Metadata Analysis* [REDACTED] September 26, 2008.

[REDACTED] the Director General [REDACTED] of
CSEC must approve the activity on the recommendation of the [REDACTED]
[REDACTED]

How does CSEC contact chain? Approval Framework for contact chaining

At the outset of the review, we received a demonstration of contact chaining from an intelligence analyst in CSEC's Office of Counter Terrorism (OCT). To initiate a contact chain [REDACTED] an intelligence analyst must complete an approval form - included as an Annex in CSEC policy, OPS-1-10, *Procedures for Metadata Analysis* [REDACTED].¹³ The form requires the analyst to record a justification including: the CSEC operational file number; Government of Canada intelligence requirement; and the source of the identifiers, i.e., a department or agency of the Government of Canada, SIGINT Development, CSEC IT Security, a Second Party partner,¹⁴ [REDACTED]. A rationale summary details how CSEC believes the listed identifiers will lead to the acquisition of foreign intelligence. The form includes the dates and signatures of the analyst and approving authorities.

CSEC advised that once a request to conduct a contact chain [REDACTED] is approved by the [REDACTED] in accordance with OPS-1-10, an analyst may, for a period of [REDACTED] from the date of the approval, conduct an unlimited number of chains using the approved identifier and using data collected up to the date of approval.

Once approved, contact chaining may be done through a number of tools, such as CSEC's Metadata Query Tool (MQT/[REDACTED]). In the specific cases examined by the Commissioner's office as part of this review, CSEC conducted the contact chains using a [REDACTED]

¹³ Issued September 26, 2008.

¹⁴ CSEC's *second party partners* are: the U.S. National Security Agency (NSA), the U.K. Government Communications Headquarters (GCHQ), Australia's Defence Signals Directorate (DSD), and New Zealand's Government Communications Security Bureau (GCSB).

[REDACTED], August 18, 2006)

"To *target* (verb) 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."

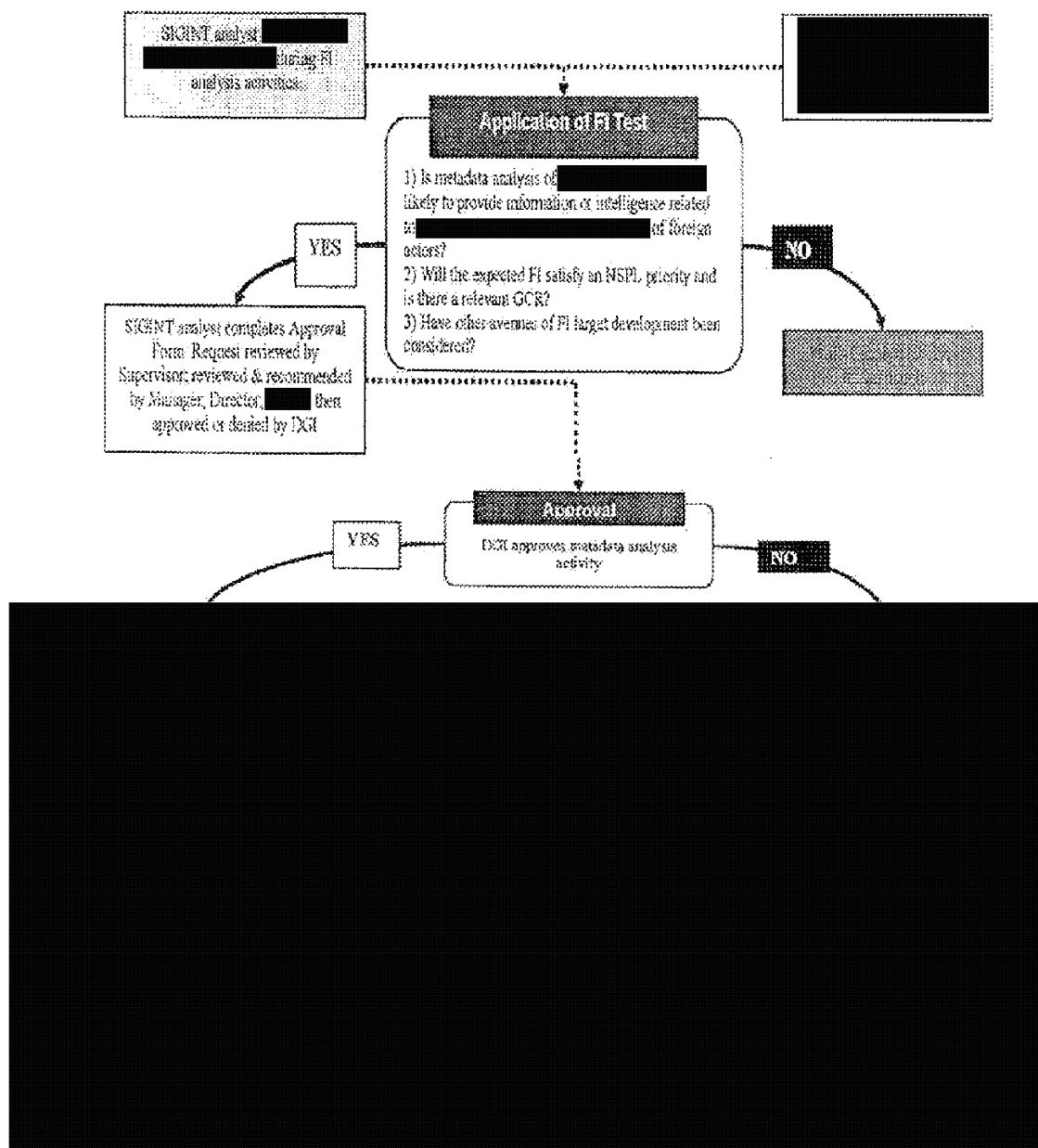
Contact chaining is [REDACTED] process; after an identifier is [REDACTED] [REDACTED] Sometimes, only partial identifiers, (e.g. part of a phone number) [REDACTED] The analyst then assesses the results for foreign intelligence value, that is to say, assesses whether the identifiers that are produced have the potential to produce foreign intelligence of interest and meet a Government of Canada intelligence requirement. Sometimes the chain will not produce any foreign leads or will produce identifiers which are not of interest. If a foreign identifier is of interest, it may be used as a selector and tasked to the various collection programs.

(Source: Section 6.22, Canadian SIGINT Operations Instruction CSOI-4-4, *Targeting and Selector Management Using [REDACTED] National SIGINT Systems For Intelligence Reporting Purposes*, March 5, 2009.

NOT REVIEWED

A0000406_9-01100

The following flowchart from CSEC's OPS-1-10 policy summarizes and illustrates CSEC's process for conducting metadata analysis (of which contact chaining is a part)



NOT REVIEWED

A0000406_10-01101

Contact chains may be linear, or be in the form of a diagram or a graphic representation. A diagram may help the analyst visualize connections between entities. Analysts have a choice of applications to do their diagrams and they may, or may not save their chains. Contact chaining is just one of several tools analysts can use when performing metadata analysis. OPS-1-10 requires that CSEC analysts must attach the results or notation of the results of any metadata analysis to the Approval Form, including, but not limited to:

- 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) any identifiers chosen for further analysis and/or targeting.

Because the policy requires that CSEC retains a proper description or record of the activity along with the approval form, we are not concerned that CSEC may not always save the chains themselves. In addition, CSEC retains in the [REDACTED] database any foreign identifiers resulting from a chain that CSEC targets for collection (i.e., selectors).

For the demonstration, CSEC used one of the contact chains that were the subject of this review. CSEC saved the chain in a shared folder on a computer system restricted to OCT personnel. A similar directory exists in the [REDACTED]. The segregation of and controlled access to operational databases helps CSEC to safeguard information about Canadians as per the MDs and CSEC policies and procedures relating to privacy.

Justice Canada legal advice

On October 1, 2003, Justice Canada issued a legal opinion entitled: Solicitor-Client Privilege. According to the opinion, Solicitor-Client Privilege.

¹⁸ [REDACTED] is CSEC's target knowledge database. It contains information from a variety of sources populated by CSEC's intelligence analysts respecting foreign entities of foreign intelligence interest to the Government of Canada and associated selectors. [REDACTED] links CSEC's target knowledge with its [REDACTED]

In May and September 2004, Justice Canada counsel provided CSEC with other legal advice related to Solicitor-Client Privilege

Solicitor-Client Privilege

Reviews by the CSE Commissioner

Commissioners have conducted three reviews involving some degree of examination of CSEC's contact chaining activities [REDACTED] *CSE's Support to Law Enforcement (RCMP) - Phase II* (2006); *Ministerial Directive, Communications Security Establishment, Collection and Use of Metadata, March 9, 2005, [Metadata MD Review]* (2008); and *CSE Support to CSIS - Phase I: CSE Mandate (a)* (2008).

The *Metadata MD Review* included the following recommendation, which was reiterated in the *CSE Support to CSIS* review:

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

Commissioner Gonthier made the above-noted recommendation because of questions respecting whether certain contact chaining activities conducted by CSEC were appropriately authorized under part (a) of its mandate. The *Metadata MD Review*, which covered the period of April 1, 2005 to March 31, 2006, encompassed [REDACTED] contact chains conducted by CSEC during that period. In each instance, the [REDACTED] used to [REDACTED] chain was provided to CSEC by a client. In all but one instance, the [REDACTED] that CSEC contact chained related to a national security or criminal investigation in Canada being conducted by CSIS or the Royal Canadian Mounted Police (RCMP). CSEC explained that the purpose of contact chaining those [REDACTED] was to discover *foreign* entities who may be operationally linked to the persons under investigation by CSIS or the RCMP. CSEC indicated that although the [REDACTED] were input into CSEC's information holdings, CSEC never targeted the

NOT REVIEWED

A0000406_12-01103

identifiers for collection. The metadata review confirmed this. Similarly, in the *Support to CSIS Review*, in most instances when forwarding what was then termed a "request for information", or RFI, CSIS provided the [REDACTED] used by CSEC to [REDACTED] the contact chain.

In both of these reviews, the Commissioner questioned whether certain of the contact chaining activities being undertaken would be more appropriately authorized under part (c) of CSEC's mandate. The Commissioner's independent legal counsel [REDACTED] Solicitor-Client Privilege

Solicitor-Client Privilege

In response to the questions from the Commissioner's office, as part of the *Metadata MD Review*, CSEC indicated that it believed that part (c) of its mandate may be insufficient authority and was not the appropriate authority under which to contact chain the [REDACTED] provided by law enforcement and security agencies. CSEC suggested that part (a) of its mandate was appropriate for contact chaining [REDACTED] because the resulting information consisted of foreign intelligence and was provided as such to the agencies as part of normal reporting processes. CSEC also advised that part (c) of its mandate may not apply as it requires the use of the authorities of the requesting agencies and the agencies do not have the appropriate mandate [to collect foreign intelligence themselves], as the agencies' warrants/authorizations may not apply extraterritorially.¹⁹

The *Metadata MD Review* included the following observation:

...In all instances, even though the interception activity was directed at a foreign target outside Canada, and thus outside the jurisdiction of the Canadian courts, there was a known link between the foreign target and criminal suspects in Canada. It was the person(s) in Canada, in fact, who was/were the source of the foreign information (phone number) and the ultimate target of RCMP interest. It could be reasonably assumed that targeting the foreign entity would produce communications traffic that would lead back into Canada and to the suspect(s) under investigation.

Commissioner Gonthier was not convinced that possible extraterritorial limitations provided a justification for CSEC's practices respecting contact chaining [REDACTED] in place at the time of the above noted reviews. Commissioner Gonthier continued to question whether these activities may be considered "directed at" the subject of the CSIS or RCMP investigations. The Commissioner's office and CSEC decided to pursue discussions on this subject outside the framework of any specific review.

¹⁹ CSEC "Comments on OCSEC 2nd Draft Review Report of the Ministerial Directive on the Collection and Use of Metadata" at p.6, e-mail to OCSEC's Director of Operations, December 6, 2007.

In January 2008, the Commissioner's office provided CSEC with a discussion paper approved by Commissioner Gonthier concerning CSEC's use of parts (a) and (c) of its mandate. The paper raised two principal questions: (1) are parts (a) and (c) of CSEC's mandate independent? and, (2) are CSIS/law enforcement agencies (LEAs) being put in a position of having to choose whether it is more important to attempt to obtain foreign intelligence in support of their investigations or to potentially jeopardize their sources?

CSEC advised the Commissioner's office during discussions that it uses part (c) of its mandate for three purposes:

1. to provide technical assistance to CSIS/LEAs;
2. to assist CSIS under s.16 of the *CSIS Act*; and
3. to assist CSIS/LEAs by intercepting the communications of a Canadian/person in Canada that is subject to a CSIS warrant (s.12 of the *CSIS Act*) or an LEA's authorization (under Part VI of the *Criminal Code*).

Commissioner Gonthier suggested that this may be a narrow interpretation of part (c) of CSEC's mandate, as part (c) could also permit CSIS and LEAs to request that CSEC use its (a) mandate for CSIS/LEAs' benefit, such as to provide foreign intelligence relating to a [REDACTED] which is in addition to the three purposes described above. Therefore, parts (a) and (c) of CSEC's mandate may not be considered independent of each other; the (c) mandate supplements but does not contradict the (a) mandate.

CSEC responded to the discussion paper and disagreed with the Commissioner's suggestions regarding the merged authorities of parts (a) and (c) of CSEC's mandate. CSEC also rejected the argument that its interpretation of parts (a) and (c) of its mandate may be hindering CSIS/LEAs investigations. [REDACTED]

Solicitor-Client Privilege
[REDACTED]

In his 2007-2008 public annual report, Commissioner Gonthier indicated:

In last year's Annual Report, I noted that one of the issues raised by my review of CSEC's foreign intelligence collection in support of the RCMP was "whether [the foreign intelligence part of CSEC's mandate] was the appropriate authority in all instances for CSE to provide intelligence support to the RCMP in the pursuit of its domestic criminal investigations." Pending a re-examination of the legal issues raised, I decided that no assessment would be made of the lawfulness of CSEC's activities in support of the RCMP under the foreign intelligence part of CSEC's mandate as it is currently interpreted and applied. This issue remained unresolved as of March 31, 2008. My review of CSEC's support to CSIS, which is reported on below, raised similar issues. As I note in this instance, and unlike the matter of

³⁰ Letter from the A/Director General, Policy and Communications, CSEC to the Executive Director, March 11, 2008.

ministerial authorizations, I am in agreement with the advice that the Department of Justice has provided to CSEC. However, in certain cases, I question which part of CSEC's mandate should be used as the proper authority for conducting these activities. Discussions on these matters are ongoing.

In September 2008, officials from the Commissioner's office and CSEC met to continue discussions respecting CSEC's application of parts (a) and (c) of its mandate using scenarios prepared by CSEC based on factual cases previously examined by the Commissioner's office during reviews. During this meeting, it became evident that CSEC's practices had changed significantly since the *Support to CSIS* and *Support to RCMP Reviews*. CSEC provided a document entitled *CSEC's Current Practices Related to Parts (a) and (c) of the Mandate*²¹, identifying new practices to be implemented on resumption of contact chaining activities, including: (1) a guide for CSIS on how to disclose information to CSEC in support of CSEC's FI mandate; (2) a form for how CSEC will acknowledge CSIS' messages; and (3) a CSEC form used to document how such information was used (if at all) and the context within which foreign intelligence value was expected. This meeting coincided with CSEC's issuing of a finalized and amended OPS-1-10 policy. Prior to suspension in April 2007, CSEC had been using a draft form of this policy to guide its metadata activities.

Since the resumption of these activities, the number of contact chains [REDACTED] conducted by CSEC was [REDACTED] a significantly smaller number of such contact chains than conducted prior to the Chief's suspension of these activities. As noted in the *Metadata Review*, CSEC had conducted [REDACTED] contact chains [REDACTED] at that time. [REDACTED] of the [REDACTED] RFIs examined as part of the *CSE Support to CSIS* review involved contact chains [REDACTED]

VIII. FINDINGS

The Commissioner's office examined the [REDACTED] contact chains [REDACTED] conducted by CSEC during the period of review. These contact chains were [REDACTED]

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

²¹ CSEC document CERRID #138049, September 26, 2008.

• [REDACTED]

A) Legal Requirements

Finding no. 1: Compliance with the law

Based upon the information reviewed and the interviews conducted, CSEC conducted its contact chaining activities [REDACTED] from October 2008 to October 2009 in accordance with the law and Justice Canada advice.

The contact chains [REDACTED] conducted by CSEC during the period under review were appropriately authorized under part (a) of CSEC's mandate.

With the significant changes made to these activities as described in the background section of the report and as summarized on the next page, the Commissioner has no questions like those raised in previous reviews as to whether such activities would be more appropriately authorized under part (c) of CSEC's mandate. The new processes put in place and followed by CSEC for the activities conducted during the period of review are assessed as consistent with part (a) of CSEC's mandate.

As metadata analysis does not involve the interception of private communications, the *Criminal Code* provisions relating to interception do not apply to these activities.

The Commissioner's office requested a copy of any legal opinions received by CSEC on this subject in addition to those described in the background section of this report. In particular, we requested any opinions or advice relating to the Chief of CSEC's decision to suspend contact chaining activities in April 2007. CSEC replied that while there was no written advice provided to the Chief, his decision resulted following discussions involving CSEC legal counsel.

CSEC explained the Chief's April 2007 decision to suspend all contact chaining activities [REDACTED] as follows:

... The Chief had initial concerns that the activities could be considered "directed at" a Canadian. Following a review of the "cornerstone" legal opinions related to the Solicitor-Client Privilege [REDACTED]

Solicitor-Client Privilege

However, the Chief directed that additional policy guidance related to the activities needed to be put in place to ensure that they would be conducted lawfully and that appropriate management accountabilities would be exercised. The activities were resumed following the approval of [a revised] *Procedures for Metadata Analysis* [REDACTED] (OPS-1-10), which

NOT REVIEWED

A0000406_16-01107

satisfied the Chief's requirements for additional policy guidance and management accountabilities.²²

The following is a summary of CSEC changes to contact chaining activities [REDACTED] following the resumption of these activities in October 2008

Prior to suspension of activities

October 2008 - present

- | | |
|--|--|
| <ul style="list-style-type: none"> • CSEC relied on interim guidance in draft policy form and had no formal policy or procedures for contact chaining activities [REDACTED] • CSEC would, under part (a) of its mandate, conduct contact chaining [REDACTED] in response to "requests for information" from Government of Canada client agencies. • CSEC did not formally respond to "requests for information" from clients. • Clients requested/provided information about Canadians to CSEC for [REDACTED] in different ways. • The clients' expectations in providing information about Canadians to CSEC for [REDACTED] were not always clear or documented. | <ul style="list-style-type: none"> • CSEC published OPS-1-10 in September 2008, which provides comprehensive guidance for contact chaining activities [REDACTED] including an approval process and documentation requirements. • OPS-1-10 prohibits contact chaining [REDACTED] in response to a client request for information about Canadians. CSEC conducts metadata analysis to obtain security or criminal intelligence in support of CSIS/LEA investigations under part (c) of CSEC's mandate. • To manage client expectations, CSEC acknowledges "messages" or "disclosures" of information about Canadians from client agencies using a standard form. <p>CSEC created a client guide for CSIS to clarify how to provide information to CSEC in support of CSEC's foreign intelligence mandate. CSEC follows the processes in this guide for other clients.</p> <ul style="list-style-type: none"> • CSEC requires clients to indicate to CSEC in messages or disclosures that the client obtained the information it is providing lawfully under its authorities and that the client is providing the information to CSEC in relation to CSEC's foreign intelligence mandate. |
|--|--|

²² E-mail from Senior Policy and Review Advisor, External Review and Policy Management, April 16, 2009, CERRID # 234834.

- CSEC did not record the expected foreign intelligence value of contact chaining activities [REDACTED]
- CSEC uses a standard template to document: the context within which the foreign intelligence value is expected; how [REDACTED] was used in operations (if at all); and any actions taken after the acknowledgement was sent to the client.

B) Ministerial Requirements

Finding no. 2: Compliance with Ministerial Directives

CSEC conducted its contact chaining activities [REDACTED] during the period under review in accordance with the Ministerial Directives on "Accountability Framework", "Privacy of Canadians", "Collection and Use of Metadata", and "Support to Law Enforcement and National Security Agencies".

Ministerial Directives

The MD on *Privacy of Canadians* includes the following requirements that are relevant to this review:

- CSEC must ensure that it does not target the communications of Canadians and continues to adopt procedures to minimize the inadvertent collection of such communications and that in using or retaining information CSEC takes all possible measures and implements appropriate policies to protect the privacy of Canadians; and
- CSEC is to fully cooperate with the CSE Commissioner...

The MD on *Accountability Framework* includes the following requirements:

- CSEC is to provide full support and cooperation to the CSE Commissioner... and
- CSE employees must have a clear understanding of the roles and responsibilities of the organization.

The MD on *Collection and Use of Metadata* includes the following requirements:

- CSEC will apply procedures for the use and retention of metadata acquired through its program consistent with CSEC's existing procedures to protect the privacy of Canadians; and

- The metadata acquired in the execution of the CSE's foreign intelligence acquisition programs shall be used strictly for:
 - a) Network Analysis and Prioritization, and for Contact Chaining purposes;
 - b) identifying new targets and target associated selectors, which can be used:
 - i) at any time to intercept foreign telecommunications (both-end foreign);...
- Activities undertaken pursuant to this Ministerial Directive will be subject to review by the CSE Commissioner as part of his mandate.

The MD on *Support to Law Enforcement and National Security Agencies* includes the following requirements:

- CSEC will assist RCMP, CSIS and other federal government departments and agencies with law and regulatory enforcement functions by providing intelligence through its signals intelligence program in response to Government of Canada and agency-specific intelligence priorities;
- In providing support CSEC will protect the privacy of Canadians, be accountable, and ensure requests for assistance are in accordance with lawful authority; and
- CSEC will be subject to review by the CSE Commissioner.

CSEC has developed a comprehensive series of policies and procedures, which address the requirements, as set out in the above noted MDs. Detail and discussion can be found in Section C) Policies and Procedures below.

In addition, CSEC management and personnel provided full support and cooperation to the Commissioner's office during the review.

Ministerial Authorizations

Contact chaining activities, including contact chaining [REDACTED] do not involve interception and therefore ministerial authorizations (MAs) authorizing the interception of private communications are not required for these activities.

However, the memoranda for the Minister of National Defence (Minister) requesting the MA under collection programs known as, [REDACTED]

[REDACTED] and Interception Activities Conducted in Support of Canadian Forces Operations in Afghanistan (Afghan MA activities) inform the Minister that:

For your information, CSE[C] also acquires telecommunications-related information used to identify, describe, manage or route all or part of the telecommunication, information referred to as "metadata", to gain a better understanding of the global information infrastructure and identify new targets. This activity, also authorized under paragraph 273.64(1)(a) of the *National Defence Act*, does not require a Ministerial Authorization and is conducted in accordance with the 2005 Ministerial Directive entitled "Collection and Use of Metadata".²³

C) Policies and Procedures

i. Appropriateness of policies and procedures

Finding no. 3: Appropriateness of policies and procedures

CSEC has appropriate policies and procedures that govern its contact chaining activities [REDACTED]

The promulgation of a complete and revised OPS-1-10 in September 2008 addressed concerns previously raised by the Commissioner in the *Metadata Review Report*, including the concern that CSEC should not rely on draft policy as guidance.

The revised OPS-1-10 includes increased and comprehensive detail with respect to the process of metadata analysis (of which contact chaining is a part) [REDACTED]. Such guidance did not form part of the draft policy in use prior to September 2008.

The following points summarize some of the improvements made to OPS-1-10:

- The authorities for conducting metadata analysis [REDACTED] are clearly referenced as part (a) of the CSEC mandate, (*NDA* paragraph 273.64(1)(a)) and the *Ministerial Directive on the Collection and Use of Metadata, March 2005*;
- Greater context is provided with respect to the rationale for conducting metadata analysis, the requirement that privacy measures be applied to metadata known to be associated with Canadians anywhere or any person in Canada and therefore the need for senior management level approval prior to conducting any analysis;

²³ Request for MAs in effect December 23, 2009 to December 22, 2010. The memoranda respecting [REDACTED] does not contain this statement.

- Clear and more comprehensive policy statements tying metadata analysis [REDACTED] to the relevant laws of Canada, Ministerial Directives, and the requirement to institute measures to protect the privacy of Canadians;
- Expanded detail related to the application of the foreign intelligence test including reference to items to be included on the Approval form;
- Approval granted for a period of [REDACTED] limited to metadata collected up to and including the date of the approval, as opposed to a period of up to [REDACTED] as previously permitted;
- Clearly stated limitations on metadata analysis activities [REDACTED] (e.g., OPS-1-10 prohibits the contact chaining of [REDACTED] obtained by CSEC from departments or agencies of the Government of Canada [REDACTED]²⁴); and
- Specific dissemination, tracking and retention requirements.

In addition to the above noted changes in OPS-1-10, and as the operational interaction between CSEC and CSIS is greater than with other Government of Canada clients, in early 2008, CSEC implemented a new guide informing CSIS how to provide [REDACTED] to CSEC in support of CSEC's FI mandate.

CSEC also introduced two new forms. The first is a form to acknowledge receipt of [REDACTED] from CSIS. This form provides four possible CSEC responses as follows:

- accepting the CSIS information for use under part (a) of CSEC's mandate;
- advising that the information is being accepted but due to other priorities is not able to immediately action;
- advising that the information does not meet any current Government of Canada foreign intelligence requirements; and
- advising that the information cannot be actioned under part (a) of the CSEC mandate but would be able to reconsider information if a request was submitted as a request under part (c) of CSEC's mandate.

CSEC indicated that it applies the same principles and processes to information about Canadians received from other law enforcement and security agencies for contact

²⁴ Section 2.8 of OPS-1-10, *Procedures for Metadata Analysis* [REDACTED] September 2008.

chaining purposes. OPS-1-10, the guide for CSIS and the new CSEC forms provide comprehensive guidance respecting CSEC's contact chaining activities [REDACTED]

[REDACTED] The new policy, guide and forms address findings and recommendations by past Commissioners relating to gaps in CSEC policy and procedures.

CSEC uses the second form to document the context within which the foreign intelligence value is expected. The CSEC intelligence analysts record how the information received from clients was integrated into current foreign intelligence operations, what actions were taken subsequent to receiving it from clients, the relevant Government of Canada intelligence requirements, the priority of the information, and a summary of the SIGINT context.

ii. *Awareness of personnel*

Finding no. 4: Awareness of personnel

Based on the interviews conducted, CSEC managers and personnel are aware of and comply with the policies and procedures that guide contact chaining activities [REDACTED]

CSEC personnel involved in the activities reviewed demonstrated a solid awareness of the policies and procedures related to contact chaining activities. The personnel interviewed were knowledgeable as to their respective responsibilities concerning compliance with the law and the protection of the privacy of Canadians. CSEC's Operational Policy Section and SIGINT Programs Oversight and Compliance Section briefed CSEC's DGI management team respecting the requirements of the new OPS-1-10 policy on October 1, 2008.

iii. *Management control framework*

Finding no. 5: Management control framework

Based on the information reviewed and the interviews conducted, CSEC has the means to determine if contact chaining activities [REDACTED] have been conducted in a manner consistent with policies and procedures and that the integrity of the activities is maintained on a routine basis, including appropriately accounting for important decisions and information.

Based on our direct observation of contact chaining activities [REDACTED] as well as the organization and practices of the teams in OCT, [REDACTED] and [REDACTED] conducting such activities, it is our assessment that CSEC managers routinely and closely monitor contact chaining activities [REDACTED] to make certain that the activities comply with the governing authorities. Managers were able to provide the Commissioner's office with copies of all requisite documentation related to each of the contact chains including the

metadata queries, end-product reporting and properly authorized contact chaining requests.

CSEC has initiated, in accordance with the provisions of its OPS-1-8 policy (*Active Monitoring of Operations to Ensure Legal Compliance and the Protection of the Privacy of Canadians*), periodic reviews of compliance with its OPS-1 policy, including for contact chaining activities [REDACTED] CSEC's Directorate of Audit, Evaluation and Ethics completed an audit of OPS-1-8 compliance in April 2009. CSEC management accepted the auditors' recommendations to clarify OPS-1-8 and improve SIGINT's active monitoring program. The Commissioner's office anticipates that these efforts will enhance CSEC's management control framework and contribute to the degree of understanding and consistency that CSEC officials apply to the direction provided in the OPS-1 policy. The Commissioner's office will monitor CSEC's efforts to address recommendations from its internal auditors to clarify OPS-1-8 and improve SIGINT's active monitoring program.

OPS-1-8, also addresses the direction provided in the MDs on *Accountability Framework* in addition to *Privacy of Canadians*, by setting out the requirements at CSEC necessary to reinforce compliance with legal and privacy-related operational policy.

IX. CONCLUSION

Over the last five years, a number of reviews conducted by the Commissioner's office recommended that CSEC re-examine its interpretation and application of parts (a) and (c) of its mandate, particularly in the context of contact chaining activities [REDACTED]

In April 2007, the Chief of CSEC suspended all contact chaining activities [REDACTED] CSEC resumed contact chaining activities [REDACTED] in October 2008 after making significant changes to the conduct of the activities and to the associated policy and accountability framework.

This review examined the [REDACTED] contact chaining activities [REDACTED] that CSEC conducted from the resumption of these activities in October 2008 to October 2009. The review was conducted under the authority of the CSE Commissioner as articulated in Part V.1, paragraph 273.63(2)(a) of the *NDA*. This is the first review focussed exclusively on CSEC's contact chaining activities [REDACTED]

The objectives of the review were: to acquire detailed knowledge of and document CSEC's new approach to contact chaining [REDACTED] to assess whether the contact chaining activities [REDACTED] conducted during the period under review complied with the law; and to assess the extent to which CSEC protected the privacy of Canadians in carrying out those activities.

NOT REVIEWED

A0000406_23-01114

Based upon the information reviewed, it is clear that contact chaining [REDACTED] can be a valuable tool for CSEC in identifying foreign intelligence entities of interest and obtaining foreign intelligence that meets Government of Canada intelligence priorities.

Based upon the information reviewed and the interviews conducted, CSEC conducted its contact chaining activities [REDACTED] during the period of review in accordance with the law and Justice Canada advice. The contact chains [REDACTED] conducted by CSEC during the period under review were appropriately authorized under part (a) of CSEC's mandate. With the significant changes made to these activities as outlined in OPS-1-10, the Commissioner's office has no questions like those raised in previous reviews as to whether such activities would be more appropriately authorized under part (c) of CSEC's mandate. The Commissioner's office assesses the new processes put in place and followed by CSEC, for the activities conducted during the period of review, as consistent with part (a) of CSEC's mandate.

Based upon the information reviewed and the interviews conducted, CSEC's contact chaining activities [REDACTED] during the period of review were also conducted in accordance with ministerial requirements set out in ministerial directives.

CSEC has appropriate policies and procedures that govern its contact chaining activities. [REDACTED] New policies, guides and forms address findings and recommendations by past Commissioners relating to gaps in policies and procedures. CSEC managers and officials are aware of and comply with the policies and procedures. CSEC managers routinely and closely monitor contact chaining activities [REDACTED] to make certain the activities comply with the governing authorities.

During the period under review, which began immediately following the October 2008 resumption of activities after the changes CSEC made, the number of contact chains [REDACTED] conducted by CSEC was significantly smaller than the number of such contact chains conducted prior to the Chief of CSEC suspending these activities.

Given the significant changes made by CSEC and the positive results of this review, the Commissioner considers past recommendations as completed and issues raised in statements made in past public Annual Reports as addressed.

However, given that these activities involve information about [REDACTED] and may affect the privacy of Canadians, the Commissioner has directed his officials to regularly monitor the number of contact chains [REDACTED] that CSEC conducts and to review them.

A list of all findings is enclosed at Annex A.


Robert Décarie, Commissioner

NOT REVIEWED

A0000406_24-01115

ANNEX A – Findings

Finding no. 1: Compliance with the law

Based upon the information reviewed and the interviews conducted, CSEC conducted its contact chaining activities [REDACTED] from October 2008 to October 2009 in accordance with the law and Justice Canada advice.

Finding no. 2: Compliance with Ministerial Directives

CSEC conducted its contact chaining activities [REDACTED] during the period under review in accordance with the Ministerial Directives on "Accountability Framework", "Privacy of Canadians", "Collection and Use of Metadata", and "Support to Law Enforcement and National Security Agencies".

Finding no. 3: Appropriateness of policies and procedures

CSEC has appropriate policies and procedures that govern its contact chaining activities [REDACTED]

Finding no. 4: Awareness of personnel

Based on the interviews conducted, CSEC managers and personnel are aware of and comply with the policies and procedures that guide contact chaining activities [REDACTED]

Finding no. 5: Management control framework

Based on the information reviewed and the interviews conducted, CSEC has the means to determine if contact chaining activities [REDACTED] have been conducted in a manner consistent with policies and procedures and that the integrity of the activities is maintained on a routine basis, including appropriately accounting for important decisions and information.

NOT REVIEWED

A0000406_25-01116

ANNEX B -- Interviewees

Production Manager, Office of Counter Terrorism

Production Manager, [REDACTED]

Team Leader, Office of Counter Terrorism

Team Leader, Office of Counter Terrorism (2)

Intelligence Analyst, Office of Counter Terrorism

Intelligence Analyst, [REDACTED]

Intelligence Analyst, [REDACTED]

NOT REVIEWED

A0000406_26-01117

ANNEX C – Timeline of Events

October 2003 – Justice Canada issued a legal opinion entitled Solicitor-Client Privilege
Solicitor-Client Privilege

The Commissioner's office had no questions respecting this advice.

May and September 2004 – Advice from Justice Canada counsel presented in PowerPoint presentations states that Solicitor-Client Privilege
Solicitor-Client Privilege
Solicitor-Client Privilege

Solicitor-Client Privilege The
Commissioner's office had no questions respecting this advice.

June 2006 – Commissioner's report on (*CSEC Support to Law Enforcement: Royal Canadian Mounted Police Phase II: CSEC Mandate (a)*) included the following recommendation:

Recommendation no. 2:

We believe that CSE must re-examine its interpretation and application of mandates (a) and (c) and ensure that all decisions and resulting activities are based upon criteria that have been consistently applied and are statutorily defensible.

Until such time as this occurs, we will not provide an assessment of the lawfulness of CSE's activities in support of law enforcement under mandate (a) as currently interpreted and applied.

CSEC accepted the recommendation.

NOT REVIEWED

A0000406_27-01118

June 2006 – CSEC provides a copy of draft policy OPS-1-10, *Procedures for Metadata Analysis* [REDACTED]

April 2007 – CSEC suspends contact chaining activities [REDACTED]
[REDACTED] The reasons for the suspension were never put in formal correspondence, although a response provided to queries in this regard is detailed in the Findings section of this report.

June 2007 – Commissioner's 2006-2007 public annual report indicated:

"During the second phase of the review, a detailed examination of CSE's response to RCMP requests for intelligence-related information identified two issues of concern that required further legal study by CSE. The first was whether mandate (a) was the appropriate authority in all instances for CSE to provide intelligence support to the RCMP in the pursuit of its domestic criminal investigations. Pending a re-examination of this issue by CSE, no assessment was made of the lawfulness of CSE's activities in support of this agency under mandate (a) as currently interpreted and applied by CSE. My staff is monitoring the issue."

January 2008 – Commissioner's report on *Ministerial Directive, Communications Security Establishment, Collection and Use of Metadata - March 9, 2005*, included the following recommendation:

Recommendation no. 2: Contact Chaining

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

January 2008 – The Commissioner's report on *CSEC Support to CSIS Phase I* included the following:

Observation no. 3

CSIS requests for information that may relate to a specific investigation or warranted activity under section 12 of the *CSIS Act*, such as any e-mails or telephone calls related to a Canadian's telephone numbers or e-mail addresses, may be more appropriately made and dealt with under CSE's (c) mandate, as they are in fact being used by CSIS to further an authorized investigation being conducted by CSIS.

As was indicated in the report on CSE support to the RCMP dated June 2006, and the review of the *Ministerial Directive, Communications Security Establishment, Collection and Use of Metadata, March 9, 2005*, submitted to the Minister in

NOT REVIEWED

A0000406_28-01119

January 2008. CSE should be able to assess its activities in response to any client department seeking intelligence support based on foreign information obtained from, and/or linked to, persons in Canada under lawful investigation. (p. 8)

CSIS requests for security intelligence concerning foreign entities in support of authorized section 12 investigations in Canada are therefore requests to provide operational support to a national security agency, thus requiring CSE to conduct its activities under its (c) mandate. This distinction is important because it determines how CSE handles the information it is collecting, which differs depending on whether it is acting as the principal, under mandate (a), or as the agent, under mandate (c). (p. 9)

Recommendation no. 2:

In accordance with the above-noted observation and Recommendation no. 1, as well as with Recommendation no. 2 from the *RCMP Phase II* review (submitted to the Minister of National Defence, June 16, 2006), CSE should re-examine its interpretation and application of mandates (a) and (c) and ensure that all decisions and resulting activities are based upon criteria that have been consistently applied and are statutorily defensible. (p. 9)

January 2008 – Commissioner's office provided CSEC with a discussion paper approved by Commissioner Gonthier concerning CSEC's use of parts (a) and (c) of the mandate. This paper raised two principal questions: (1) Are CSEC's (a) and (c) mandates truly independent as suggested by CSEC? (2) Are CSIS/LEAs being put in a position of having to choose whether it is more important to attempt to obtain foreign intelligence in support of their investigations or to potentially jeopardize their sources?

February 2008 – Commissioner's independent counsel [REDACTED] Solicitor-Client

Solicitor-Client Privilege

Solicitor-Client Privilege

March 11, 2008 – CSEC responded to the Commissioner's office's discussion paper and rejected suggestions relating to "merged authorities" and that CSEC's interpretation of parts (a) and (c) of its mandate may be hindering CSIS/LEAs investigations.

May 2008 – Commissioner's 2007-2008 public annual report indicated:

Interpretation of foreign intelligence mandate

In last year's Annual Report, I noted that one of the issues raised by my review of CSEC's foreign intelligence collection in support of the RCMP was "whether [the foreign intelligence part of CSEC's mandate] was the appropriate authority in all instances for CSE to provide intelligence support to the RCMP in the pursuit of its domestic criminal investigations." Pending a re-examination of the legal issues

NOT REVIEWED

A0000406_29-01120

raised. I decided that no assessment would be made of the lawfulness of CSEC's activities in support of the RCMP under the foreign intelligence part of CSEC's mandate as it is currently interpreted and applied. This issue remained unresolved as of March 31, 2008. My review of *CSEC's Support to CSIS*, which is reported on below, raised similar issues. As I note in this instance, and unlike the matter of ministerial authorizations, I am in agreement with the advice that the Department of Justice has provided to CSEC. However, in certain cases, I question which part of CSEC's mandate should be used as the proper authority for conducting these activities. Discussions on these matters are ongoing.

July 2008 – Minister responded to Commissioner's *Metadata* and *Support to CSIS* review reports indicating that: the interpretation of parts (a) and (c) of CSEC's mandate has been the subject of ongoing discussions with OCSEC..."

September 2008 – Commissioner's office and CSEC met to discuss CSEC's application of parts (a) and (c) of CSEC's mandate using scenarios prepared by CSEC based on factual cases previously examined by the Commissioner's office during reviews. During this meeting, it became evident that CSEC's practices had changed since the *Support to CSIS* and *RCMP* reviews.

September 2008 – CSEC provided a document (CERRID #138049) identifying CSEC's new practices implemented since the reviews in January/February 2008, including: (1) a guide for CSIS on how to disclose information to CSEC in support of CSEC's FI mandate; (2) a form for how CSEC will acknowledge CSIS' messages; and (3) a CSEC form used to document how such information was used (if at all) and the context within which FI value was expected.

September 2008 – revised OPS-1-10, *Procedures for Metadata Analysis* [REDACTED] became effective.

October 2008 – CSEC recommenced contact chaining activities.

April 2009 – Terms of Reference sent to CSEC for this review.

March 2010 – CSEC's *Semi-Annual Update on Review Recommendations* indicated, regarding the status of action to address recommendation #2 of the June 2006 *Support to RCMP Mandate A* review:

CSE operations, legal, and policy staffs conferred through the summer of 2006, which included a full-day workshop on this and related issues; the results will be validated during the fall. The aim is to formalize via the new policy package on CSE support to federal law enforcement and security agencies (OPS-4-1) slated for release in the context of the CSE-RCMP MOU revision. In the meantime, any requests for specific 'reactive' intelligence support of the type referred to in the review recommendation will be dealt with on an ad hoc basis in consultation with legal staff.

NOT REVIEWED

A0000406_30-01121

Implementation not completed as of April 2010: The new policy on support to law enforcement and security agencies (revised draft of OPS-4-1 was completed in December 2009 and is almost ready for circulation) will further clarify and formalize the direction. In the interim, all requests are handled on a case-by-case basis and oversight is provided by the Director SIGINT Requirements. In cases where the Director has any doubt, advice is sought from Justice legal counsel.

NOT REVIEWED

A0000406_31-01122