

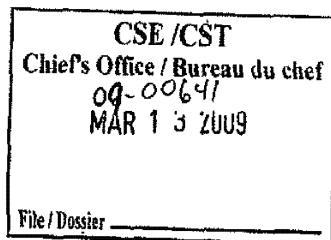
Communications Security
Establishment Commissioner

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



Commissaire du Centre de la
sécurité des télécommunications

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



TOP SECRET/COMINT/CEO
(with attachment)

12 March 2009

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

Dear Mr. MacKay:

The purpose of this letter is to advise you of the results of a review by my office of the Communications Security Establishment Canada's (CSEC) [REDACTED] network analysis and prioritization (NA&P) and [REDACTED] activities. This is a follow-up to my January 2008 review report of CSEC's metadata activities carried out under a ministerial directive dated March 9, 2005. I have enclosed, for your convenience, a copy of my previous letter informing you of the results of the 2008 review. That review raised questions respecting access to the content of communications, which may include private communications, by [REDACTED] operators involved in NA&P and [REDACTED] activities. I had mentioned to you in my letter of 16 September 2008 that I would examine this issue in greater detail because there was disagreement between CSEC and my office respecting these activities and specifically with recommendation #1 that stated:

CSE should re-examine and re-assess its current position and practice that requires that only those private communications recognized by intelligence analysts be accounted for. (p.17)

The main objective of this follow-up review was to determine whether that recommendation should be maintained, amended or discarded. Subsequent to this review, the results of which are discussed below, I am withdrawing recommendation #1 of my 2008 Metadata Review Report.

P.O. Box/C.P. 1884, Station "B"/Succursale «B»
Ottawa, Canada
K1P 5R5
(613) 992-3044 Fax: (613) 992-4096

According to CSEC, only analysts responsible for producing foreign intelligence reports are capable of determining whether a private communication has foreign intelligence value. Therefore, CSEC maintains that only foreign intelligence analysts should be responsible for accounting for those communications. The review assessed whether, during a NA&P and [REDACTED] activity, a [REDACTED] operator who observes a private communication should be required, as a measure to protect the privacy of Canadians, to record and to report the fact that a private communication was observed, even though the operator may not be in a position to assess the foreign intelligence value of the private communication.

The review was undertaken under my general authority articulated in subsection 273.65(8) and paragraph 273.63(2)(a) of the *National Defence Act (NDA)*, and reflected in paragraph 6 of the ministerial authorization authorizing the interception of private communications under CSEC's [REDACTED] program. Our methodology included first-hand observation of the activities by [REDACTED] operators.

Based upon the information reviewed and the interviews conducted, CSEC conducts its [REDACTED] NA&P and [REDACTED] activities in accordance with the law and ministerial requirements.

My staff found that, based on current practices as observed in October 2008, [REDACTED] NA&P and [REDACTED] activities involve a very low risk to privacy. It was determined that [REDACTED] operators primarily analyse the metadata of communications and when, in rare cases, they must access the content of communications, it is for technical purposes. It was concluded that [REDACTED] operators conduct different and less intrusive activities than those of CSEC foreign intelligence analysts and therefore have a different and lesser potential to affect the privacy of Canadians.

Furthermore, my staff found that [REDACTED] operators take sufficient measures to protect the privacy of Canadians. [REDACTED] operators and CSEC personnel are aware of operational policies and procedures in place that provide direction respecting the protection of the privacy of Canadians. I am pleased to note that the CSEC's new associated operational policy contains additional guidance respecting the protection of the privacy of Canadians. Managers routinely and closely monitor compliance with these policies and procedures.

Therefore, as I have stated above, I am withdrawing recommendation #1 of my 2008 Metadata Review Report. I have no expectation that CSEC will take any action respecting this subject in the context of [REDACTED] operators' NA&P and [REDACTED] activities.

However, as my predecessors and I have repeatedly indicated, ambiguities in the *NDA* continue to result in a lack of clarity or differences of interpretation between CSEC and my office regarding certain sections of the *NDA*. For example, as described in the attached report, ambiguities relating to the term "interception", which is not defined in the *NDA*, raised questions respecting whether [REDACTED] operators may be conducting

analysis of intercepted communications. Amendments to the *NDA* are needed in order to clarify this ambiguity, amongst others, and allow CSEC to continue conducting their mandated activities, while protecting the privacy of Canadians.

My report, attached, contains seven findings dealing with the matters I have summarized for you in this letter.

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

Yours sincerely,



Charles D. Gonthier

c.c. Mr. John Adams, Chief, CSEC
Ms. Marie-Lucie Morin, National Security Advisor, PCO
Mr. Robert Fonberg, Deputy Minister, National Defence

TOP SECRET//COMINT//CEO

**A Review of Recommendation No. 1 from the January 2008
Review Report respecting CSEC's Ministerial Directive on the
Collection and Use of Metadata**

**CSEC's [REDACTED]
Network Analysis and Prioritization and [REDACTED] Activities**

12 March 2009

TABLE OF CONTENTS

I. AUTHORITIES	1
II. INTRODUCTION	1
III. OBJECTIVES	2
IV. SCOPE	2
V. CRITERIA.....	2
VI. METHODOLOGY	3
VII. BACKGROUND	4
Network Analysis and Prioritization	5
[REDACTED]	5
SIGINT Development Operations and [REDACTED]	6
Collection.....	10
[REDACTED]	11
VIII. FINDINGS	12
A) Legal Requirements	12
Legal Advice.....	12
Private Communications/Personal Information about Canadians.....	13
B) Ministerial Requirements	15
C) Policies and Procedures	16
i) Appropriateness of policies and procedures.....	16
ii) Awareness of personnel	16
iii) Management control framework.....	17
IX. CONCLUSION	17
ANNEX A - Interviewees	19
ANNEX B - Findings	20
ANNEX C - [REDACTED] & SIGINT Development Tools.....	21
ANNEX D - Demonstration, October 31, 2008	22

I. AUTHORITIES

This review is conducted under the authority of the CSE Commissioner as articulated in Part V.1, subsection 273.65(8) and paragraph 273.63(2)(a) of the *National Defence Act* (NDA), and reflected in paragraph 6 of the ministerial authorization (MA) authorizing the interception of private communications under a foreign intelligence (FI) collection program known as [REDACTED]

II. INTRODUCTION

The Commissioner's January 2008 review report of CSEC's metadata activities raised questions respecting access to the content of communications, which may include private communications (PCs), by [REDACTED] operators involved in network analysis and prioritization (NA&P) [REDACTED] and signals intelligence development (SIGINT development)) and [REDACTED] conducted under CSEC's authorities.

Specifically, recommendation #1 of the Metadata Review Report stated:

CSE should re-examine and re-assess its current position and practice that requires that only those private communications recognized by intelligence analysts be accounted for (p.17).

CSEC is of the view that only analysts responsible for producing FI reports are capable of determining whether a PC has FI value. Therefore, CSEC maintains that only FI analysts can assess whether PCs should be retained or destroyed and be responsible for accounting for those communications. This review is a focused follow-up to CSEC's response to and Commissioner's office-CSEC discussions respecting recommendation #1 of the Metadata Review Report. The review assesses whether, during a NA&P and [REDACTED] activity, a [REDACTED] operator who observes a PC should be required, as a measure to protect the privacy of Canadians, to record and to report the fact that a PC was observed, even though the operator may not be in a position to assess the FI value of the PC.

CSEC's NA&P and [REDACTED] activities are conducted under the authority of:

- paragraph 273.64(1)(a) of the NDA;
- the [REDACTED] MA¹ and the ministerial directive (MD) respecting Metadata.²

¹ The most recent [REDACTED] MA is effective December 23, 2008 to December 22, 2009.

² *Ministerial Directive, Communications Security Establishment, Collection and Use of Metadata*, effective March 9, 2005.

III. OBJECTIVES

The objectives of the review were to assess:

- whether CSEC's [REDACTED] NA&P and [REDACTED] activities complied with the law;
- the extent to which CSEC protects the privacy of Canadians in carrying out the activities; and, specifically,
- whether recommendation #1 of the Commissioner's Metadata Review Report should be maintained, amended or discarded.

IV. SCOPE

In addition to acquiring detailed knowledge of [REDACTED] NA&P and [REDACTED] activities, the review examined:

- the authorities, policies,³ and procedures under which [REDACTED] NA&P and [REDACTED] activities operate and any conditions imposed on the activities;
- the "analysis" of [REDACTED] intercepted communications and other activities conducted by [REDACTED] operators; including the volume and nature of the communications accessed by the operators;
- the nature of the [REDACTED] operators' interaction with CSEC officials respecting the communications accessed by the operators; and
- the number of PCs typically accessed by [REDACTED] operators during a certain period of time.

V. CRITERIA

We expected that:

A) Legal Requirements

- CSEC conducts its [REDACTED] NA&P and [REDACTED] activities in accordance with the *NDA*, the *Canadian Charter of Rights and Freedoms*, the *Privacy Act*, the *Criminal Code*, and any other relevant legislation and Justice Canada advice.⁴

³ Namely, CSEC's policy OPS-1-13, *Procedures for Canadian [REDACTED] Activities*, effective on December 23, 2008. OPS-1-13 superseded OPS-1-6, *Canadian [REDACTED] Procedures*, effective December 23, 2007 and is an amalgamation of the former OPS-1-6, OPS-3-5, [REDACTED] *Procedures* and OPS-3-7, [REDACTED] *Procedures*.

⁴ Namely, the legal opinion provided to the Chief of CSEC by the Deputy Minister of Justice and Deputy Attorney General of Canada dated June 6, 2005 respecting Solicitor-Client Privilege [REDACTED]

Solicitor-Client Privilege [REDACTED]

B) Ministerial Requirements

- CSEC conducts its [REDACTED] NA&P and [REDACTED] activities in a manner that is in accordance with ministerial direction, namely the expectations and approval framework outlined in the [REDACTED] MA and the MD respecting Metadata;

C) Policies and Procedures

- i) CSEC has appropriate policies and procedures that guide [REDACTED] NA&P and [REDACTED] activities;
- ii) CSEC has personnel who are aware of and comply with the policies and procedures; and
- iii) CSEC has an effective management control framework to maintain the integrity of [REDACTED] NA&P and [REDACTED] activities, including appropriately accounting for important decisions and information.

VI. METHODOLOGY

This was our first detailed examination of [REDACTED] NA&P and [REDACTED] activities, following the overall review of activities conducted under the MD respecting Metadata. The aim was to acquire detailed knowledge of the activities of [REDACTED] operators, to answer the questions set out in the scope section above and to meet the specific objective of this focused review. Observing first-hand the activities of the [REDACTED] operators was necessary to validate CSEC's suggestions that the reporting recommended by the Commissioner was not necessary because the operators' activities involve only a low risk to privacy and that the reporting would be onerous.⁵

On October 17, 2008, CSEC provided us with an overview briefing respecting [REDACTED] NA&P and [REDACTED] activities. On October 27 and 31, we observed the conduct of NA&P and [REDACTED] activities at the [REDACTED] site [REDACTED] and interviewed [REDACTED] operators and the [REDACTED] Tasking Manager (which are employees of the Canadian Forces) as well as personnel from CSEC. A list of interviewees, by position title, is enclosed at Annex A. Annex D describes the demonstration observed on October 31.

Applicable written and electronic records, files, correspondence and other documentation relevant to the [REDACTED] NA&P and [REDACTED] activities were examined, including policies and procedures, and legal advice.

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 findings.

⁵ Discussion with CSEC's Director, SIGINT Requirements and CSEC's Manager, External Review and Policy Management, October 2, 2008.

VII. BACKGROUND

The Commissioner's [REDACTED] review reports of February 2005 and December 2008 and the Metadata Review Report provide detailed background information respecting [REDACTED] activities.

As of October 2008, Canadian [REDACTED] collection activities at [REDACTED]
[REDACTED]

As of October 2008, [REDACTED] personnel were as follows: [REDACTED] SIGINT development operators ([REDACTED] operators, [REDACTED] SIGINT development supervisor, [REDACTED] training staff ([REDACTED] [REDACTED] tasking manager (the tasking manager normally works [REDACTED] but may work extended periods [REDACTED] to lend assistance in all aspects of operations); and technical support staff (these staff are responsible to maintain the equipment and the software; they do not conduct [REDACTED] or SIGINT development activities). We reviewed a copy of a generic work description for an [REDACTED] SIGINT development operator.

During a typical day, [REDACTED] operators may conduct [REDACTED] SIGINT development, and collection activities. At one time CSEC had sufficient personnel to assign them specific duties as either an [REDACTED] or a SIGINT development operator. However, due to the current limited number of [REDACTED] operators, all operators may be involved in any of the activities.

[REDACTED] collection activities involve targeting foreign communications [REDACTED] [REDACTED] as well as conducting research and analysis of global information networks, to produce FI of value to the Government of Canada (GC). [REDACTED] and SIGINT development are the two key research and analysis activities.⁶ NA&P includes [REDACTED] and SIGINT development and the work [REDACTED] operators do [REDACTED] as we observed on October 27 and 31, 2008.⁷ [REDACTED] operators conduct analysis [REDACTED] of the communications. [REDACTED] are important for CSEC analysts (from the Directorate General Intelligence) and CSEC's [REDACTED] to determine if a signal should be investigated further or proposed for collection.

⁶ Section 2.1 of OPS-1-13, *Procedures for Canadian [REDACTED] Activities*, effective December 23, 2008.

⁷ CSEC response to OCSEC questions, November 28, 2008, CSEC CERRID #170168, page 2.

Network Analysis and Prioritization

The MD on the Collection and Use of Metadata, March 2005, defines network analysis and prioritization as: "...the method developed to understand the global information infrastructure, from information derived from metadata, in order to identify and determine telecommunication links of interest to achieve the Government of Canada foreign intelligence priorities. This method involves the acquisition of metadata, the identification of [REDACTED] the determination of the [REDACTED]

[REDACTED] the determination of the [REDACTED]

[REDACTED] This definition

also appears in section 9.18 of OPS-1-13.

Operations

In short, [REDACTED] operations are aimed at [REDACTED]

[REDACTED] that may be

of FI interest.

Section 2.2 of OPS-1-13 defines [REDACTED] Ops as:

[REDACTED] Ops activities [REDACTED]

[REDACTED] SIGINT

development activities.

Section 9.6 of the former and now defunct OPS-1-6 stated:

[REDACTED] Ops are aimed at [REDACTED]

[REDACTED]
[REDACTED] This
information is used to populate technical databases. Traffic [REDACTED]
[REDACTED]

We find the new description of [REDACTED] Ops in OPS-1-13 to be a more detailed and accurate reflection of the activities that we observed and therefore to be an improvement from the previous definition of [REDACTED] Ops in the former OPS-1-6. We note in particular that the new description in OPS-1-13 contains additional guidance respecting the protection of the privacy of Canadians, e.g., care is taken to avoid Canadian traffic, and access to content must be limited.

We observed [REDACTED] Ops [REDACTED]. As a first step, [REDACTED]
[REDACTED]

SIGINT Development Operations and [REDACTED]

In short, SIGINT development and [REDACTED] operations involve analyzing [REDACTED]
[REDACTED] communications [REDACTED]
[REDACTED] If the results do not
indicate possible Canadian content, then [REDACTED] operators will run sample collection
of the [REDACTED] DNI/DNR⁸ [REDACTED] If there is a selector match, then a SIGINT
development report is generated alerting CSEC and the second party community of the
potential to collect FI [REDACTED]


⁸ Dialed Number Recognition (DNR) generally refers to phone and fax communications. Digital Network Intelligence (DNI) refers to [REDACTED] communications, e.g., e-mails.

Section 2.3 of OPS-1-13 describes SIGINT development operations as:

SIGINT Development [REDACTED]



Once analysis has been completed, any recognized private communications must be purged from the system. [REDACTED]



[REDACTED] Access to this data must be limited to those

[REDACTED] SIGINT Development analysis.

We find the new descriptions of SIGINT development and [REDACTED] in OPS-1-13 to also be a more detailed and accurate reflection of the activities observed by us and therefore to be an improvement from the previous descriptions in the former OPS-1-6. We note that the new description in OPS-1-13 contains additional guidance respecting the protection of the privacy of Canadians, e.g., [REDACTED]

obtained, [REDACTED] can not take place on [REDACTED] access to data must be limited. We also note that the new description in OPS-1-13 indicates that “no annotation [of PCs] is necessary since there is no requirement to account for private communications that are viewed only technically by collection staff,” which is exactly the question this review set out to answer, i.e., whether CSEC should re-examine and re-assess its current position and practice that requires that only those PCs recognized by intelligence analysts be accounted for.

CSEC acknowledged that there is some overlap in the [REDACTED] and SIGINT development activities. [REDACTED]

Annex C identifies [REDACTED] as part of SIGINT development and [REDACTED] activities.

In the context of our metadata review, CSEC officials indicated that, as part of SIGINT development and [REDACTED] activities, [REDACTED] it is part of the operators “day jobs” to make certain the information obtained is “good stuff”. We sought clarification respecting whether such statements were consistent with the former OPS-1-6 that stated that [REDACTED]

However, during this review, CSEC clarified that previous statements were in part based on dated information. [REDACTED]

Past [REDACTED] and historical data inform [REDACTED] operators as to which [REDACTED]

⁹ CSEC response to OCSEC questions, November 28, 2008, CSEC CERRID #170168 – v2A, page 6.

[REDACTED]

CSEC indicated that [REDACTED] operators err on the side of caution; if an operator observes that a communication [REDACTED]

[REDACTED]

We asked in what circumstances, other than [REDACTED] if any, would a [REDACTED] operator examine traffic content? In response, CSEC indicated:

[REDACTED]

We also asked whether any SIGINT development activities were undertaken on [REDACTED] and whether any such activities occurred in the past. In response, CSEC indicated: [REDACTED]

[REDACTED]

A supervisor creates a weekly report respecting [REDACTED] and SIGINT development operations. If any of the activities involved information about a Canadian or PCs, the supervisor verifies that the entry for those activities was properly identified in [REDACTED]

[REDACTED]

"Strong" selectors relate to metadata identifiers of FI targets (e.g., telephone numbers, e-mail or IP addresses). [REDACTED]

[REDACTED]

¹⁰ CSEC response to OCSEC questions, November 28, 2008, CSEC CERRID #170168 – v2A, page 5.

¹¹ CSEC response to OCSEC questions, November 28, 2008, CSEC CERRID #170168 – v2A, page 7.

[REDACTED]

If a selector "hits", operators produce a SIGINT development Report primarily to alert CSEC and [REDACTED] Second Parties [REDACTED] containing FI of interest is available [REDACTED] Sometimes reports are also forwarded to FI analysts responsible for the area in question, based on the subject of the report.

We reviewed examples of the three types of SIGINT development reports. The only difference between the types of reports was the type of activity being reported: (1)

[REDACTED]

[REDACTED] National SIGINT Priorities List (NSPL) requirements. We had no questions respecting the reports.

CSEC indicated that [REDACTED] stored on the [REDACTED] operators' hard drives as well as [REDACTED] stored in [REDACTED] are automatically deleted after [REDACTED] However, if a [REDACTED] operator observes, based on metadata, that the [REDACTED] could potentially be associated with a Canadian communication or contain information about a Canadian, then the operator is to immediately delete the [REDACTED] through a manual process.

CSEC indicated that metadata obtained by [REDACTED] is currently stored for approximately [REDACTED] after which time the storage device becomes full and older data is overwritten.

Collection

In addition to NA&P and [REDACTED] activities, [REDACTED] operators receive and implement taskings for collection from CSEC's [REDACTED] section (collection activities are, however, outside of the scope of this review). Pre-taskings are also conducted [REDACTED] and SIGINT development operations for possible tasking. For clarity, the decision to [REDACTED] not [REDACTED] operators.

At the beginning and end of a typical day, [REDACTED] operators [REDACTED]

[REDACTED]

[REDACTED] Operators may conduct [REDACTED] or SIGINT development [REDACTED]

A solid black image with no visible content.



VIII. FINDINGS

A) Legal Requirements

CSEC's NA&P and [REDACTED] activities are conducted under the authority of:

- paragraph 273.64(1)(a) of the *NDA*¹⁴;
- the [REDACTED] MA; and
- the MD respecting Metadata.

NA&P and [REDACTED] activities are undertaken pursuant to both the [REDACTED] MA, as it is possible that CSEC may intercept a PC, and the MD respecting Metadata.

Legal Advice

We examined and discussed with CSEC officials the 2005 Justice Canada legal opinion referenced in the Metadata Review Report.¹⁵

We requested any additional legal advice that CSEC may have received respecting its decision to limit MA reporting requirements to intelligence analysts who prepare FI reports. CSEC indicated that it is not aware of any such advice and indicated that an examination of the evolution of the requirements in MAs over time would illustrate CSEC's decision-making respecting this issue. An examination of the changes in the MAs does not however provide a justification for why only certain CSEC personnel need to account for the PCs they observe and handle.

Following the observations [REDACTED] we agree with CSEC's assertion that the analysis conducted by [REDACTED] operators is technical in nature and not focused on the

¹³ CSEC response to OCSEC questions, November 28, 2008, CSEC CERRID #170168, page 3.

¹⁴ Paragraph 273.64(1)(a) of the *National Defence Act* mandates CSEC "to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence priorities."

¹⁵ Legal opinion provided to the Chief of CSEC by the Deputy Minister of Justice and Deputy Attorney General of Canada dated June 6, 2005 respecting Solicitor-Client Privilege [REDACTED] page 10.

content of the [REDACTED]/intercepted communications. Rather, the focus is on [REDACTED]

Communications are not viewed in a meaningful way; it is not analysis respecting whether CSEC should use the intercepted information. Therefore, we also agree that, based on current practices, [REDACTED] operators conduct different and less intrusive activities than those of CSEC FI analysts and therefore have a different and lesser potential to affect the privacy of a Canadian.

However, given the ambiguities relating to the term "interception", which is not defined in the *NDA*, it can be argued that [REDACTED] operators may be conducting analysis of intercepted communications. Therefore, it would follow that operators should be required to report the number of times a PC is accessed, just as CSEC FI analysts are required to do (even though the number of PCs accessed has been shown to be [REDACTED]).

Private Communications/Personal Information about Canadians

Paragraph 273.64(2)(b) of the *NDA* requires that "activities carried out under paragraphs (1)(a) and (b), shall be subject to measures to protect the privacy of Canadians in the use and retention of intercepted information."

Given that [REDACTED] operations [REDACTED] only target foreign [REDACTED] by design, the chance of obtaining a two-end Canadian communication is [REDACTED] and the chance of obtaining a one-end Canadian communication is [REDACTED]

As indicated above, "[i]t is [REDACTED] operators' practice to *always* delete a [REDACTED] that contains a possible or confirmed link to Canada (including metadata that suggests the possibility of Canadian content) and to *always* indicate so in [REDACTED]"¹⁶ (emphasis added). CSEC indicated that such "...practices respecting a [REDACTED] that contains a possible or confirmed link to Canada are based on an interpretation of the requirements of the *National Defence Act*."¹⁷

We asked whether, following the analysis of the metadata of a communication that contains a possible link to Canada, [REDACTED] operators may subsequently examine the [REDACTED] in order to confirm or to rule out a link to Canada.

Specifically, we asked whether [REDACTED] operators always, out of caution [REDACTED]

[REDACTED]¹⁸ In response, CSEC indicated [REDACTED] operators [REDACTED] indicates a possible or confirmed link to Canada. The policy is designed to permit operators to examine the content of the communication in cases where there is no indication, at the metadata level, of a possible

¹⁶ CSEC response to OCSEC questions, November 28, 2008, CSEC CERRID #170168- v2A, page 4.

¹⁷ Interview with [REDACTED] operator, October 31, 2008, and CSEC response to OCSEC questions, November 28, 2008, CSEC CERRID #170168- v2A, page 4.

¹⁸ For the purposes of this report, PI includes information about an incorporated body in Canada.

or confirmed link to Canada.”¹⁹ CSEC’s response is consistent with what we observed [REDACTED] on October 31, 2008.

We also asked whether [REDACTED] operators ever take another [REDACTED] of the same [REDACTED] containing a possible link to Canada, in order to confirm or to rule out a link to Canada. In response, CSEC indicated [REDACTED]

[REDACTED] No further analysis is conducted on the [REDACTED]
Operators do not currently have the [REDACTED]²⁰

CSEC provided a non-exhaustive list of potential causes that might make a [REDACTED] operator suspect, as occurred during the October 31 demonstration, that a [REDACTED] has a possible link to Canada (and to identify the [REDACTED] as such in [REDACTED])

-
-
-
-
-
-
-
-
-
-



Finding no. 1: Private Communications/Personal Information about Canadians

Based on current practices as observed in October 2008, [REDACTED] operators take sufficient measures to protect the privacy of Canadians in the conduct of network analysis and prioritization and [REDACTED] activities.

¹⁹ CSEC response to OCSEC questions, November 28, 2008, CSEC CERRID #170168 – v2A, page 5.

²⁰ CSEC response to OCSEC questions, November 28, 2008, CSEC CERRID #170168 – v2A, page 5.

²¹ CSEC response to OCSEC questions, November 28, 2008, CSEC CERRID #170168 – v2A, page 2.

Finding no. 2: Private Communications/Personal Information about Canadians

Based on current practices as observed in October 2008, [REDACTED] operators' practices respecting network analysis and prioritization and [REDACTED] activities appear to relate to a strict interpretation of the *National Defence Act*.

We observed the practice that [REDACTED] operators always stop at the analysis of metadata and delete a [REDACTED] that contains a possible link to Canada. We appreciate CSEC's comments that there are not sufficient resources [REDACTED] to conduct detailed analysis of all [REDACTED] that may relate to Canada. We also recognize how the current practice is beneficial to helping to ensure that the privacy of Canadians is protected. However, as described by CSEC, the current NA&P and [REDACTED] practices mean that CSEC may lose an opportunity to obtain FI of value as [REDACTED]

Finding no. 3: Compliance with the Law

Based upon the information reviewed and the interviews conducted, CSEC conducts its [REDACTED] network analysis and prioritization and [REDACTED] activities in accordance with the law.

B) Ministerial Requirements

There is no explicit requirement in the [REDACTED] MA to have any person other than an analyst who prepares an FI report to account for PCs. The MD respecting Metadata has no requirements respecting accounting for PCs. In this respect, the current practice of [REDACTED] operators not to account for PCs is consistent with ministerial requirements.

Finding no. 4: Ministerial Requirements

Based upon the information reviewed and the interviews conducted, CSEC conducts its [REDACTED] network analysis and prioritization and [REDACTED] activities in accordance with the [REDACTED] MA and the MD respecting Metadata.

The Commissioner's [REDACTED] review reports of February 2005 and December 2008 and the Metadata Review Report of January 2008 provide assessments of CSEC's compliance with other ministerial requirements respecting [REDACTED] and metadata.

C) Policies and Procedures

i) OCSEC expected that CSEC would have appropriate policies and procedures that guide [REDACTED] NA&P and [REDACTED] activities

As indicated above, we find the descriptions of NA&P and [REDACTED] activities in the recent (December 2008) OPS-1-13 to be a more detailed and accurate reflection of the activities we observed and therefore to be an improvement from the previous descriptions in the former OPS-1-6. We are pleased to note that the new descriptions in OPS-1-13 contain additional guidance respecting the protection of the privacy of Canadians. For example, the practice of [REDACTED] operators to delete a [REDACTED] that contains a possible or confirmed link to Canada is now included in the new OPS-1-13.

Finding no. 5: Operational Policies

Operational policies and procedures for [REDACTED] network analysis and prioritization and [REDACTED] activities are in place and provide direction to CSEC officials respecting the protection of the privacy of Canadians, and no information or documentation was found to indicate that any actions of [REDACTED] operators or CSEC personnel contravene the policies and procedures.

ii) OCSEC expected that CSEC personnel would be aware of and complied with the policies and procedures for [REDACTED] NA&P and [REDACTED] activities

[REDACTED] operators must complete significant training - three months of classroom and six months of on the job training - before being considered qualified. We examined the agendas for the course beginning in January 2009. Training includes relevant policies, namely OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE[C] Activities*²² and OPS-1-13. As part of the training, operators receive 10 binders of reference materials. Operators must repeat the training if they have been out of the environment for more than 36 months. Personnel who return from a deployment within this timeframe are retrained (on the job training). CSEC indicated that operators work an average of 1-2 years before leaving [REDACTED] to assume other duties.

The [REDACTED] operations centre contains a number of large wall charts to assist operators in tracking such things as current FI priorities of the GC, and ongoing collection/tasking requirements. Copies of the OPS policies and the National SIGINT Priorities List²³ are available to [REDACTED] operators. We reviewed a copy of a working aid developed for [REDACTED] operators ([REDACTED] operators' workflow chart).

²² The most recent version of OPS-1 was effective on December 23, 2008.

²³ The National SIGINT Priorities List (NSPL) is a document which consists of two tiered lists, the Standing Issues and the Watching Briefs, which define the GC's FI priorities - source: Canadian SIGINT Operation Instruction CSOI-1-1, July 17, 2008.

Finding no. 6: Operational Policies

██████ operators and managers and CSEC personnel interviewed and observed were aware of relevant policies and their application to ██████ network analysis and prioritization and ██████ activities.

The people with whom we spoke were forthcoming and demonstrated a professional approach to the activities under review.

iii) OCSEC expected that CSEC would have an effective management control framework to maintain the integrity of ██████ NA&P and ██████ activities, including appropriately accounting for important decisions and information

The materials reviewed and the interviews conducted demonstrated that CSEC managers routinely and closely monitor ██████ network analysis and prioritization and ██████ activities. For example, as indicated above, a supervisor creates a weekly report respecting ██████ and SIGINT development operations. If any of the activities ██████ the supervisor verifies that the entry in ██████ for those activities was properly identified and that the associated ██████ were destroyed.

Finding no. 7: Management Control Framework

██████ operators and managers and CSEC personnel routinely and closely monitor ██████ network analysis and prioritization and ██████ activities to make certain the activities comply with its governing authorities.

CSEC has initiated, in accordance with the provisions of its OPS-1-8 policy (Active Monitoring), periodic reviews of compliance with its OPS-1 policy, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities*, including for ██████ activities. It is anticipated that this effort has contributed favourably to the degree of understanding and consistency that ██████ operators and CSEC analysts apply to the direction provided in the OPS-1 policy. CSEC's Directorate of Audit, Evaluation and Ethics will finalize an audit of OPS-1-8 in 2009-2010.²⁴

IX. CONCLUSION

The objectives of the review were to assess:

- whether CSEC's ██████ NA&P and ██████ activities complied with the law;
- the extent to which CSEC protects the privacy of Canadians in carrying out the ██████ NA&P and ██████ activities; and, specifically,

²⁴ Discussion with CSEC's Director General of Audit, Evaluation and Ethics as part of a brief respecting "CSEC Policy System Annual Update", December 8, 2008.

- whether recommendation #1 of the Commissioner's Metadata Review Report should be maintained, amended or discarded.

Based upon the information reviewed and the interviews conducted, CSEC conducts its [REDACTED] network analysis and prioritization and [REDACTED] activities in accordance with the law and ministerial requirements.

However, given the ambiguities relating to the term "interception", which is not defined in the *NDA*, it can be argued that [REDACTED] operators may be conducting analysis of intercepted communications. Therefore, it would follow that operators should be required to report the number of times a PC is accessed, like CSEC FI analysts are required to do, even though the number of PCs accessed has been shown to be [REDACTED]

Given that [REDACTED] operations [REDACTED] only target foreign [REDACTED] by design, the chance of obtaining a two-end Canadian communication is [REDACTED] and the chance of obtaining a one-end Canadian communication is [REDACTED]. In very few cases (according to CSEC, approximately [REDACTED] of the time), [REDACTED] operators may examine the content of [REDACTED]

[REDACTED] Since 2001, less than [REDACTED] and less than [REDACTED] have been identified as having potential [REDACTED] content (12 of [REDACTED] clearly relate to [REDACTED] that have been [REDACTED] communications and [REDACTED] entries relate to [REDACTED] communications).²⁵ Therefore, based on current practices as observed in October 2008, [REDACTED] network analysis and prioritization and [REDACTED] activities involve only a [REDACTED] risk to privacy.

[REDACTED] operators take sufficient measures to protect the privacy of Canadians in the conduct of network analysis and prioritization and [REDACTED] activities. [REDACTED] operators and CSEC personnel are aware of operational policies and procedures in place that provide direction respecting the protection of the privacy of Canadians. Managers routinely and closely monitor compliance with the policies and procedures.

In view of the above, therefore, the Commissioner is withdrawing recommendation #1 of the 2008 Metadata Review Report that stated: "CSE should re-examine and re-assess its current position and practice that requires that only those private communications recognized by intelligence analysts be accounted for" (p.17). We have no expectation that CSEC take any action respecting this subject in the context of [REDACTED] operators' network analysis and [REDACTED] activities.

A list of findings is enclosed at Annex B.

²⁵ Presentation by CSEC's Director, [REDACTED] October 17, 2008, slide #7.

ANNEX A - INTERVIEWEES

[REDACTED] Tasking Manager
[REDACTED] SIGINT development Supervisor
Two [REDACTED] SIGINT development Operators
Director, [REDACTED]
Director, SIGINT Requirements
Manager, SIGINT Programs Oversight and Compliance
Senior Policy and Review Advisor, External Review and Policy Management

ANNEX B - FINDINGS

Finding no. 1: Private Communications/Personal Information about Canadians

Based on current practices as observed in October 2008, [REDACTED] operators take sufficient measures to protect the privacy of Canadians in the conduct of network analysis and prioritization and [REDACTED] activities.

Finding no. 2: Private Communications/Personal Information about Canadians

Based on current practices as observed in October 2008, [REDACTED] operators' practices respecting network analysis and prioritization and [REDACTED] activities appear to relate to a strict interpretation of the *National Defence Act*.

Finding no. 3: Compliance with the Law

Based upon the information reviewed and the interviews conducted, CSEC conducts its [REDACTED] network analysis and prioritization and [REDACTED] activities in accordance with the law.

Finding no. 4: Ministerial Requirements

Based upon the information reviewed and the interviews conducted, CSEC conducts its [REDACTED] network analysis and prioritization and [REDACTED] activities in accordance with the [REDACTED] MA and the MD respecting Metadata.

Finding no. 5: Operational Policies

Operational policies and procedures for [REDACTED] network analysis and prioritization and [REDACTED] activities are in place and provide direction to CSEC officials respecting the protection of the privacy of Canadians, and no information or documentation was found to indicate that any actions of [REDACTED] operators or CSEC personnel contravene the policies and procedures.

Finding no. 6: Operational Policies

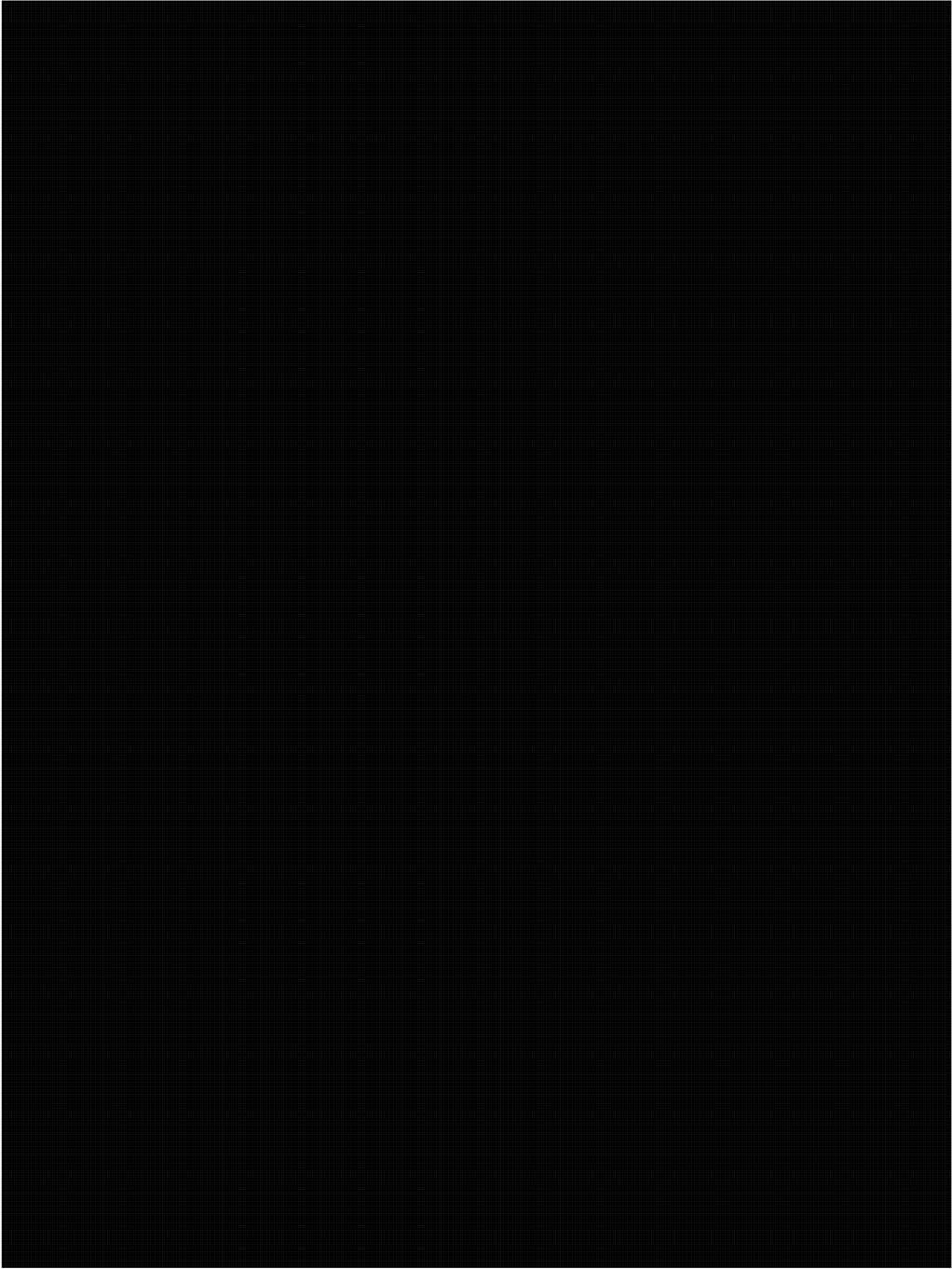
[REDACTED] operators and managers and CSEC personnel interviewed and observed were aware of relevant policies and their application to [REDACTED] network analysis and prioritization and [REDACTED] activities.

Finding no. 7: Management Control Framework

[REDACTED] operators and managers and CSEC personnel routinely and closely monitor [REDACTED] network analysis and prioritization and [REDACTED] activities to make certain the activities comply with its governing authorities.

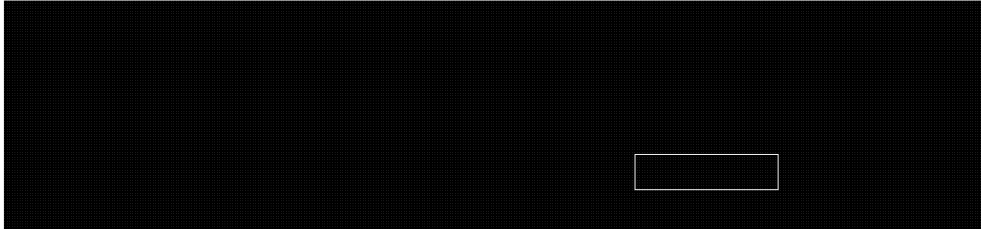
ANNEX C - [REDACTED] & SIGINT DEVELOPMENT TOOLS

The following is a non-exhaustive list of tools (software), grouped by function, that a

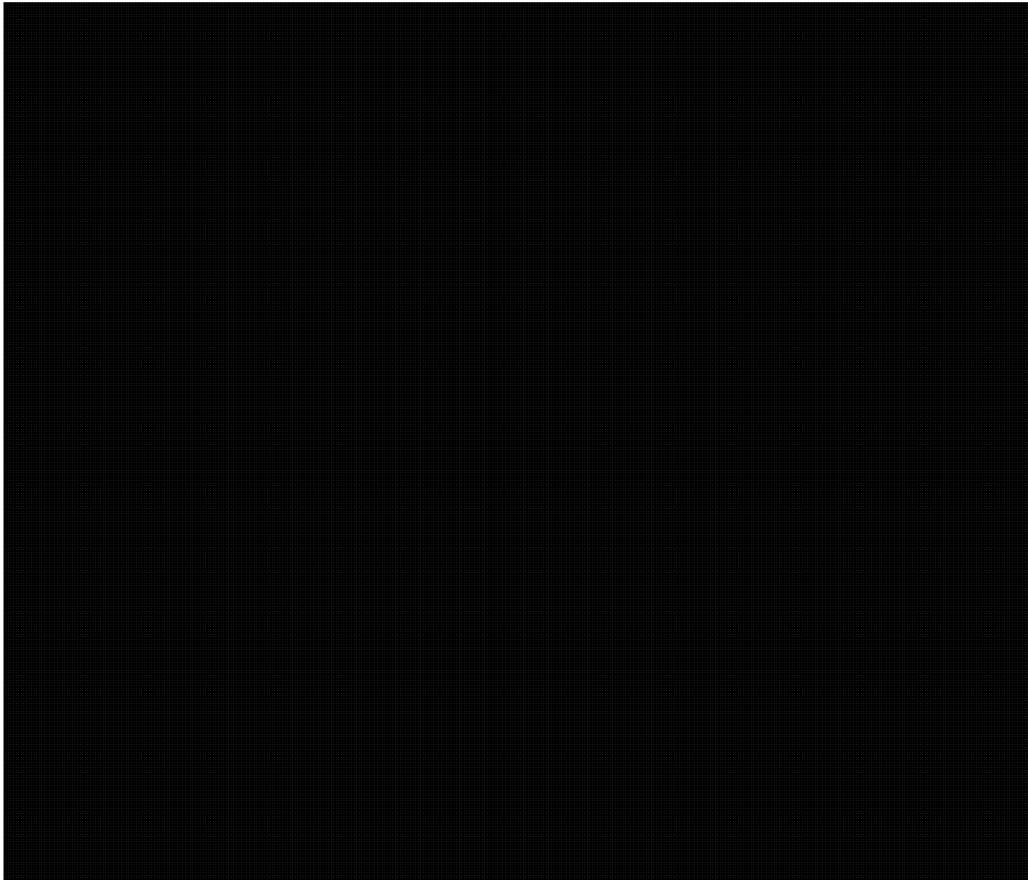


ANNEX D – [REDACTED] & SIGINT DEVELOPMENT DEMONSTRATION,
OCTOBER 31, 2008

The following is a high-level description of the [REDACTED] and SIGINT development activities that we observed [REDACTED] on October 31, 2008.



SIGINT Development



1

