

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)**

11 June 2008

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) acquisition and implementation of technology that contributes to the protection of the privacy of Canadians under subsection 273.64(2) of the *National Defence Act (NDA)*, for the period August 17, 2006 to December 31, 2007. Two types of technologies were studied, one a signals intelligence acquisition system named [REDACTED] and the other an analytical dataset named [REDACTED]. Although CSEC's operational activities leading to the use of these technologies were not a part of the scope of this review, some were examined in order to understand how these technologies were being employed.

The objective of the review was to assess CSEC's compliance with the laws of Canada and whether measures were in place to protect the privacy of Canadians. My office also set out to assess whether these activities conformed with CSEC's operational policies, procedures and practices. The review was undertaken under my general authority articulated in paragraph 273.63(2)(a) of the *NDA*.

By way of background, [REDACTED] is a signals intelligence acquisition system developed for the purpose of acquiring, processing and collecting digital network intelligence (i.e. all Internet traffic such as e-mails and [REDACTED] communications. CSEC currently uses the system for [REDACTED] acquisition. [REDACTED] is a commercial product offering [REDACTED] data and services. [REDACTED] is the process of determining [REDACTED]

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

Both of CSEC's business lines (signals intelligence (SIGINT) and information technology security (IT Security)) use [REDACTED] for specific purposes. CSEC uses these technologies to fulfill their legislated mandates.

The review found that CSEC complied with the law in the areas that were examined. I am also pleased to note that CSEC took measures to protect the privacy of Canadians. For example, in order to comply with its statutory obligations as stated in paragraph 273.64(2) of the *NDA*, CSEC modified [REDACTED] in order to comply with the "Metadata First" regime it had instituted for all its [REDACTED] collection systems. This regime requires CSEC to [REDACTED]

Hence, the Metadata First requirement is one of the measures CSEC has put in place to protect the privacy of Canadians as it ensures that at least one of the communicators, i.e. the foreign communicator, is the target CSEC is looking for. Moreover, the acquisition, implementation and use of [REDACTED] helps CSEC protect the privacy of Canadians by identifying potential private communications (as defined in section 183 of the *Criminal Code*), as well as personal information.

Furthermore, the review found that special attention should be brought to the development of IT Security policy instruments so as to ensure that CSEC's guidance in this regard is up to date, formalized and corporately approved. I am pleased to note however that, subsequent to the completion of this review, CSEC has revised some of its policy instruments and their approval process to address this issue. It was also observed that CSEC's SIGINT and IT Security business practices are different as regards accounting for personal information (e.g. Canadian IP addresses) identified through analysis. Although CSEC has provided me with explanations for this inconsistency, I believe the matter deserves further examination and I have instructed my staff to continue discussions with CSEC in this regard.

One recommendation ensued as regards CSEC requests for [REDACTED] ministerial authorizations. As you may be aware, since the promulgation of the omnibus *Anti-Terrorism Act* in December 2001 there have been extensive discussions between CSEC and my office regarding the interpretation of certain sections of the *NDA*, particularly section 273.65 relating to ministerial authorizations. It has been the practice of my office to review CSEC's activities carried out under ministerial authorization and to conclude as to their lawfulness in light of the interpretation of the applicable legislative provisions by the Department of Justice.

In this instance, since CSEC may intercept private communications when undertaking [REDACTED] activities under part (a) of its mandate while using [REDACTED] a ministerial authorization was required. It was observed that when seeking a ministerial authorization, the Chief, CSEC requests the authority to intercept private communications while conducting collection/interception activities. These

activities are described in the request, as well as other activities known as metadata activities (i.e. research and analysis such as [REDACTED] SIGINT development and Network Analysis and Prioritization). I found this to be confusing as the Minister only authorizes the interception of private communications acquired through the class of activities described as [REDACTED] *interception* (as defined in the legal guidance received by CSEC). Therefore, I recommend that CSEC re-evaluate how it describes the [REDACTED] activities in its request for a ministerial authorization so as to clearly identify which activity the Minister of National Defence is authorizing when signing a [REDACTED] ministerial authorization.

My report, attached, contains 12 findings and one recommendation 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, CSE
Ms. Margaret Bloodworth, National Security Advisor, PCO
Mr. Robert Fonberg, Deputy Minister, National Defence

TOP SECRET/COMINT/Canadian Eyes Only

Report to the CSE Commissioner on Protecting Privacy:
Review of CSEC's Acquisition and
Implementation of Technology per Subsection 273.64(2)
of the *National Defence Act*

11 June 2008

I. AUTHORITIES

This report was prepared on behalf of the Communications Security Establishment Commissioner under his general authority articulated in Part V.1, paragraph 273.63(2)(a) of the *National Defence Act (NDA)*.

II. INTRODUCTION

The Communications Security Establishment Canada (CSEC)¹ provided the Office of the CSE Commissioner (OCSEC) with a general briefing on its research and development (R&D) program. Provided at our request, this preliminary briefing was to serve as a means for OCSEC to scope out its first formal review of R&D activities.

OCSEC was advised that CSEC allocates funds and conducts basic research, applied research and experimental development activities. Both its signals intelligence (SIGINT) and its information technology security (IT Security) groups conduct R&D activities, coordinated by the Chief Technology Officer. Contrary to our initial expectations, however, we also learned that no R&D activity is specifically dedicated to creating measures to protect the privacy of Canadians. Rather, CSEC ensures that any technology applied and implemented as a result of an R&D project, conforms to its statutory obligations to protect the privacy of Canadians.

During the briefing, CSEC cited two such technologies known by the names [REDACTED] and [REDACTED] is a [REDACTED] signals [REDACTED] system that [REDACTED]. During the briefing, we learned that CSEC chose not to use the system immediately because it did not comply with CSEC's rules for targeting based on metadata selection and for protecting privacy.

[REDACTED] is the name of a commercial [REDACTED] data. CSEC has [REDACTED] to the [REDACTED] dataset and first used it operationally in [REDACTED] to [REDACTED]. CSEC advised us that by reviewing [REDACTED] data, it will [REDACTED] and use this to inform CSEC's collection. For example, if a Canadian [REDACTED] is identified through the use of [REDACTED] information, this information will help CSEC avoid inadvertent targeting of Canadians.

While CSEC clarified during subsequent discussions that neither of these two systems should be considered as specifically R&D related, it was agreed that they are "certainly privacy related".²

¹ The Communications Security Establishment's (CSE) name was changed to Communications Security Establishment Canada effective September 27, 2007, in order to comply with the Government of Canada's Federal Identity Program.

² E-mail from CSEC's Manager, External Review and Policy Compliance to OCSEC's Director of Operations and reviewer entitled *RE: R&D Scope Statement* and dated June 30, 2006.

Based on the information received, on discussions with CSEC regarding the nature of R&D activities, and taking into account that CSEC usually considers privacy implications in its application and implementation phase rather than in its R&D phase, OCSEC determined that CSEC's R&D programs were not the appropriate focus for a review at this time. Rather, the focus of the review would be on privacy and on how CSEC's acquisition³ and implementation⁴ of technologies satisfied, in practice, the legislative requirement to protect the privacy of Canadians under par. 273.64(2)(a) and (b) of the *National Defence Act*.

III. OBJECTIVES

OCSEC examined and assessed CSEC's acquisition and implementation of [REDACTED] and [REDACTED] to determine whether they comply with the laws of Canada and contribute to the protection of the privacy of Canadians, for the period August 17, 2006 to December 31, 2007.

IV. LINES OF ENQUIRY

This review included the following lines of enquiry:

1. which of CSEC's legal authorities governed the operational need that led to the acquisition and implementation of these technologies;
2. how CSEC assessed and tested for privacy risks associated with the implementation of these technologies;
3. how CSEC identifies and generally describes the extent to which protecting privacy forms part of its planning process in developing or purchasing technology or technological systems for the collection, use or retention of intercepted information;
4. the operational uses of the [REDACTED] dataset and how CSEC determines, scopes, plans, conducts and manages its [REDACTED] activities;

³ For clarification, in this context, the term « acquisition » includes how CSEC identified its operational need to purchase or receive a new technology and the corresponding mandated authority it was intended to satisfy. It does not include management issues such as CSEC's contracting practices, financial control and accountability and life-cycle management.

⁴ For clarification, in this context, the term « implementation » includes both the use of the technology as well as any modification that may have occurred to make it operable and, in CSEC's assessment, lawful.

5. how [REDACTED] differs from its predecessor used [REDACTED] and how CSEC is developing [REDACTED] to comply with its rules for targeting and protecting the privacy of Canadians;
6. how information about Canadians acquired by these systems is (or would be) retained, used, shared and protected.

V. CRITERIA

We expected that in planning, assessing and deciding whether to implement technological systems, CSEC:

- 1- conducts its [REDACTED] and [REDACTED] activities based on such factors as:
 - whether the operational activity complies with CSEC's legislated authorities found in paragraphs 273.64(1)(a), (b) and/or (c) of the *National Defence Act*;
 - whether it falls under the authority of and complies with ministerial direction;
 - whether it falls under the authority of a valid ministerial authorization(s);
- 2- ensures, with respect to any [REDACTED] and [REDACTED] activities carried out under paragraphs 273.64(1)(a) or (b) of the *National Defence Act*, that:
 - these activities would not be directed at Canadians or any person in Canada; and,
 - these activities would be subject to measures to protect the privacy of Canadians in the use and retention of intercepted information;
- 3- has approved plans, processes and privacy-risk assessments to determine whether systems being considered for development or acquisition comply with its legislative mandate and internal policies;
- 4- In respect of [REDACTED]
 - a. ensures the conducted activities respect legislated authorities;
 - b. has a formalized methodology, including an internal approval framework, in place in order to conduct the activities;
 - c. has the means to determine if its activities have been conducted as per its authorities;
 - d. has measures in place to protect the privacy of Canadians: in particular, processes to identify Canadians and policies concerning the acquisition, use and retention of personal information about Canadians.

When criterion 4 was developed some time ago, it was not clear to OCSEC that [REDACTED] was but an analytic “tool” used by CSEC to help it undertake its mandated activities. Therefore, some of the sub-criteria are not quite pertinent with respect to CSEC’s use of [REDACTED] because the review focussed on the technologies used, and not on CSEC’s operational activities leading to the use of these technologies. Accordingly, it is understood that CSEC will use [REDACTED] when undertaking its operational activities in accordance with its legislated authorities. Discussion of the measures CSEC has in place to protect the privacy of Canadians as relates to [REDACTED] can be found under the section entitled *IT Security Use of [REDACTED]* starting at page 18.

VI. METHODOLOGY

A variety of documentation was examined, including CSEC policies and procedures and legal guidance issued to CSEC by Justice Canada. CSEC managers and personnel responsible for undertaking activities with [REDACTED] and [REDACTED] were interviewed and OCSEC received several briefings throughout the review. CSEC provided both verbal and written answers to our questions. A list of interviewees, by position title, is attached at Annex A.

We obtained briefings and an on-site demonstration of the [REDACTED] collection system. We also received briefings and demonstrations of the [REDACTED] data set, as used by both the SIGINT and IT Security groups. We paid particular attention to those CSEC policies and practices instituted to protect the privacy of Canadians in the acquisition, use and disclosure of personal information about Canadians.

VII. [REDACTED]

[REDACTED] is a [REDACTED] SIGINT acquisition system [REDACTED] for the purpose of acquiring, processing and collecting digital network intelligence (DNI)⁵ communications.⁶

[REDACTED] All of CSEC’s Second Party⁷ partners [REDACTED] or a [REDACTED] version of it.

⁵ DNI traffic includes all Internet traffic such as e-mail, [REDACTED]

⁷ CSEC’s Second Party SIGINT partner agencies are the Government Communications Headquarters (GCHQ) in the United Kingdom, the NSA in the United States, the Defence Signals Directorate (DSD) in Australia and the Government Communications Security Bureau (GCSB) in New Zealand.

The basic function of [REDACTED] (and its predecessor) is to [REDACTED]

[REDACTED] This complex process has already been documented in a recent OCSEC report titled *OCSEC Review of the Ministerial Directive on the Collection and Use of Metadata, March 9, 2005* [Metadata Review]. For ease of reference, Annex D of that report, which details the process, has been re-printed as Annex B of this report.

CSEC's mandated activities are found at subsection 273.64(1) of the *NDA*. The [REDACTED] system is predominantly used by CSEC in the context of its foreign intelligence (FI) and assistance mandates (respectively, paragraphs 273.64(1)(a) and (c) of the *NDA*). [REDACTED] can also be used for information technology security (IT Security) purposes under part (b) of CSEC's mandate. The system is used by CSEC in the performance of a number of its mandated activities, some of which (but not all) require additional authorization from the Minister. This report focuses on CSEC's activities using [REDACTED] under part (a) of its mandate

VIII. [REDACTED] FINDINGS

The findings documented below were derived from:

- documentation received from CSEC, including PowerPoint presentations and legal opinions;
- briefings and discussions held with CSEC personnel at various levels;
- the demonstration of [REDACTED] SIGINT development activities undertaken by Canadian Forces personnel [REDACTED]; and
- answers received from CSEC to verbal and written questions.

The findings are assessed based on the criteria (expectations) enumerated above.

Criterion 1

We would expect that in planning, assessing and deciding whether to implement technological systems, CSEC:

- *conducts its [REDACTED] activities based on such factors as:*
 - *whether the operational activity complies with CSEC's legislated authorities found in paragraphs 273.64(1)(a), (b) and/or (c) of the National Defence Act;*
 - *whether it falls under the authority of and complies with ministerial direction;*
 - *whether it falls under the authority of a valid ministerial authorization(s).*

As mentioned above, CSEC uses the [REDACTED] to undertake all three of its mandated activities. This report will focus on CSEC's activities using [REDACTED] under part

(a) of its mandate. Paragraph 273.64(1)(a) of the *NDA* states that CSEC's mandate is "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." Activities carried out under paragraph 273.64 (1)(a) shall not be directed at Canadians or any person in Canada and shall be subject to measures to protect the privacy of Canadians in the use and retention of intercepted information (subsection 273.64(2) of the *NDA*).

Finding 1

CSEC's authority to conduct its activities using [REDACTED] is found in subsection 273.64(1) of the *NDA*.

As CSEC may intercept private communications when undertaking [REDACTED] activities under part (a) of its mandate while using [REDACTED] a ministerial authorization is also required (s. 273.65 of the *NDA*). The *Ministerial Authorization on [REDACTED] [REDACTED] Interception* (dated December 19, 2005 and valid for the year 2006, the period under review) authorizes CSEC "to intercept private communications [...] acquired through the class of activities described as [REDACTED] interception [...] for the sole purpose of obtaining foreign intelligence that is in accordance with the Government of Canada intelligence priorities."

CSEC also receives guidance from the *Ministerial Directive on the Collection and Use of Metadata* (dated March 9, 2005) which governs CSEC's collection and use of metadata under foreign intelligence acquisition programs. It dictates certain steps to be followed by CSEC in order to protect the privacy of Canadians.

The *Ministerial Directive on the Privacy of Canadians* (dated June 19, 2001) directs the Chief, CSEC to ensure that CSEC does not target the communications of Canadians, to adopt procedures to minimize the inadvertent collection of such communications, and to ensure that, in using and retaining information, CSEC takes all possible measures and implements appropriate policies to protect the privacy of Canadians.

CSEC receives further guidance from its OPS 1-6 procedure entitled *Canadian [REDACTED] Procedures*.

Also of note is the *Canadian-U.S. COMINT Agreement*, signed in 1949. This agreement is of a general nature and covers most matters relating to the signals intelligence relations between CSEC and NSA. Appendixes E and H of the agreement promote cooperation and exchange between Second Party partners. An example of this cooperation is the fact that CSEC [REDACTED]
[REDACTED]

While conducting this review, we received a demonstration of [REDACTED]
[REDACTED] signals intelligence (SIGINT) development activities undertaken by

Canadian Forces personnel [REDACTED]. Pursuant to this demonstration, questions were raised concerning these two activities, particularly CSEC's [REDACTED] extraction and interception of metadata while using [REDACTED]. These issues have been examined and explained in the Metadata Review report and are pertinent to this review.

Ministerial Authorization

Under subsection 273.65(1) of the *NDA*, the Minister may authorize CSEC to intercept private communications for the sole purpose of obtaining foreign intelligence. On December 19, 2005 the Minister of National Defence signed a [REDACTED] interception ministerial authorization (MA), permitting such interception. CSEC uses selectors to target communications of foreign entities of intelligence interest located outside Canada. According to the Deputy Minister of Justice and Deputy Attorney General of Canada, Solicitor-Client Privilege [REDACTED] Solicitor-Client Privilege [REDACTED]

[REDACTED] allows CSEC to conduct both its metadata activities and its interception/collection activities. As mentioned above, metadata activities are authorized by the *NDA* and governed by the *Ministerial Directive on the Collection and Use of Metadata*. According to CSEC, an MA is not necessary to conduct those metadata activities described in the ministerial directive, such as network analysis and prioritization and contact chaining.⁹ CSEC has explained that network analysis and prioritization as defined in the ministerial directive basically constitutes [REDACTED] SIGINT development activities.¹⁰ CSEC undertakes [REDACTED] collection/interception activities under the authority of paragraphs 273.64(1)(a) or (c) of the *NDA* and the [REDACTED] MA.

The [REDACTED] interception ministerial authorization signed in December 2005 was in effect during the period under review and specified the following:

I therefore authorize the Communications Security Establishment, with the assistance of the Canadian Forces Information Operations Group where necessary, to intercept, [REDACTED] private communications acquired through the class of activities *described as* [REDACTED] *Interception* [REDACTED] *in the request for Ministerial Authorization* dated 5 December 2005, for the sole purpose of obtaining foreign intelligence that is in accordance with the Government of Canada intelligence priorities. [Emphasis added]

Solicitor-Client Privilege [REDACTED]

⁹ Details can be found at page 7 of OCSEC's Metadata Review report.

¹⁰ E-mail dated July 16, 2007 from CSEC Liaison to OCSEC reviewer attaching responses from CSEC's Manager, SIGINT Programs Oversight and Compliance entitled *P & T review - Additional [REDACTED] Questions..*

The Minister is authorizing the interception of private communications acquired through the class of activities described as [REDACTED] *interception*. Therefore, it is expected that the activity described in the request for ministerial authorization signed by the Chief, CSEC would constitute interception only, and be in accordance with the legal guidance CSEC has received. However, the request clearly describes not only collection/interception activities, but also metadata activities (i.e. research and analysis such as [REDACTED], SIGINT development and Network Analysis and Prioritization). The request states:

Under this authority, CSE hereby requests a Ministerial Authorization to *intercept* [REDACTED] private communications in relation to [REDACTED] *Interception* activities directed at foreign entities located abroad.

[REDACTED] activities involve *targeting* foreign communications [REDACTED] [REDACTED] to produce foreign intelligence of value to the Government of Canada. [REDACTED] activities also involve *research and analysis* of global information networks in support of CSE's foreign intelligence mandate. For *collection*, specific [REDACTED] are targeted to collect the communications of foreign entities of interest, which are then forwarded to CSE for assessment and reporting. For *research and analysis*, CSE acquires all the signals [REDACTED] for a limited period of time and analyzes their [REDACTED]

It is possible that in carrying out this class of activities, CSE will intercept communications that either terminate or originate in Canada, which constitute private communications pursuant to the *Criminal Code*. A Ministerial Authorization is therefore necessary to allow CSE to conduct its [REDACTED] *collection* activities. [Emphasis added]

Although the request accurately reflects CSEC's activities in practice, it is unclear whether the Minister is authorizing the interception of private communications acquired only through CSEC's [REDACTED] collection/interception activities or whether he is authorizing the interception of private communications acquired through both CSEC's [REDACTED] collection/interception *and* metadata activities. As mentioned previously, it is the Department of Justice's opinion that Solicitor-Client Privilege [REDACTED] Solicitor-Client F

Recommendation

That CSEC re-evaluate how it describes the [REDACTED] activities in its request for a ministerial authorization so as to clearly identify which activity the Minister of National Defence is authorizing when signing a [REDACTED] ministerial authorization.¹¹

Criterion 2

We would expect that in planning, assessing and deciding whether to implement technological systems, CSEC:

- *ensures, with respect to any [REDACTED] activities carried out under paragraphs 273.64(1)(a) or (b) of the National Defence Act, that:*
 - *these activities would not be directed at Canadians or any person in Canada; and,*
 - *these activities would be subject to measures to protect the privacy of Canadians in the use and retention of intercepted information.*

Tasking and Targeting Procedures

Before CSEC undertakes any tasking and targeting (defined below), it must ensure that a foreign intelligence requirement is associated to the [REDACTED] CSEC wishes to task, as well as to the selector CSEC wishes to target. Paragraph 273.64(1)(a) of the *NDA* specifies that CSEC's acquisition and use of information from the global information infrastructure must be in accordance with the Government of Canada's intelligence priorities. CSEC receives the Government's intelligence priorities yearly and from those, establishes its own detailed list of foreign intelligence priorities named the National SIGINT Priorities List (NSPL). The NSPL is based on consultation with CSEC's key Government of Canada clients and is approved by Government. CSEC also creates and manages an internal document called the Government of Canada Requirements (GCR) list in order to organize and map requirements as they are received from clients. This list is more detailed and allows CSEC to track requirements to the NSPL.¹²

¹¹ In practice, CSEC drafts both the MA as well as the MA justification letter for the Minister (s. 2.4 of CSEC's ORG 2-1 – *Procedures for Obtaining and Handling Ministerial Directives and Ministerial Authorizations*, dated 4 Aug 2005). Thus, CSEC identifies and explains the activities or class of activities the Minister is being asked to authorize. The Chief, CSEC presents the MA package to the Minister, who then considers the package, and if he agrees, approves and signs the MA. After the MA is signed, CSEC undertakes what has been authorized.

¹² E-mail dated February 25, 2008 from CSEC liaison to OCSEC reviewer entitled *Addendum to Privacy and Technology Review Responses*.

Tasking

CSEC's SIGINT Programs, [REDACTED] is responsible for tasking Canadian [REDACTED] collection [REDACTED]. In a briefing provided to OCSEC on November 17, 2006,¹³ CSEC defined *task* as follows: "One 'tasks' a [REDACTED]" When CSEC identifies [REDACTED] it wishes to task, an Activity Authorization Request form is required. The form specifies the intelligence and collection requirements, the [REDACTED] as well as some targeting and collection handling procedures. In the one Activity Authorization Request form presented to OCSEC, the intelligence and collection requirements provided the justification for putting a specific [REDACTED] and related the activity with GCR and NSPL requirements. We were assured that [REDACTED] ensures all the information in the form is complete and conforms to the [REDACTED] MA. Also, several directors must approve the request before it is actioned [REDACTED] (including [REDACTED]). According to CSEC officials, logs are kept to indicate when the [REDACTED] why, by whom, and when it is removed. Verification of the forms and the logs was outside the scope of this review but will be examined in future reviews.

Finding 2

CSEC associates its tasking of telecommunications data to a foreign intelligence requirement in compliance with part (a) of its mandate.

Targeting

CSEC defines *target* as follows: "One 'targets' a selector to a [REDACTED] [sic] a [sic] [REDACTED] or dictionary to collect only 'hit' (wanted) data".¹⁴ As mentioned above, CSEC will choose and input selectors (i.e. a name, an Internet protocol (IP) address, an e-mail address or a telephone number) in a dictionary for the purpose of identifying traffic that relates to national foreign intelligence requirements. This constitutes targeting. There are two types of targeting: DNI, which relates to Internet communications and includes text such as e-mail, and Dialed Number Recognition (DNR), which relates to phone and facsimile. [REDACTED] is responsible for both types of targeting at Canadian collection sites including [REDACTED]. Thus, the targeting process is transparent to the [REDACTED] operators. [REDACTED] only, however, it is also used for the [REDACTED] such as of [REDACTED]¹⁵

¹³ Briefing given to OCSEC by CSEC's Associate Director, SIGINT Programs, entitled *Overview of Tasking and Targeting and its Application to [REDACTED]* on 17 November 2006.

¹⁴ *Ibid.*

¹⁵ Answer provided by Associate Director, SIGINT Programs by e-mail from CSEC Liaison to OCSEC reviewer, entitled *P & T Review // ** Answers* dated 6 November 2006.

Selectors used to collect one-end foreign communications traffic must also meet the definition of metadata in the *Ministerial Directive on the Collection and Use of Metadata*. Consequently, a selector can only be used to collect/intercept communications if it is foreign and relates to the external component of communications. We were assured by the DNI team leader that all DNI selectors are associated with a valid foreign intelligence target located outside Canada.¹⁶ Selectors must be approved by the DNI team before they are inputted in [REDACTED]. The team verifies that the selectors relate to a foreign target and are linked to a GCR. Targets can, however, be very broad or general in nature. A target may also be an entity. Section 273.61 of the *NDA* defines *entity* as meaning "a person, group, trust, partnership or fund or an unincorporated association or organization and includes a state or a political subdivision or agency of a state."

When asked how he determines that selectors are foreign, the DNI team leader stated that many selectors that are likely to relate to a Canadian or a person in Canada [REDACTED] do not go through the system such as [REDACTED]. He also stated that the content of communications is often used [REDACTED]. For example, [REDACTED] are used.¹⁷ The analyst must know the foreign entity to be targeted, why that entity is being targeted and its location.

In order to determine that [REDACTED] selectors are not directed at Canadians, the DNR Team Leader stated that he confirms nationality indicators and the validity of foreign phone numbers as well as ensures that selectors are associated with a GCR.

Analysts will verify that [REDACTED] is producing proper traffic by examining the traffic (metadata and content) generated by the selectors.

Finding 3

Based on the information received, CSEC takes measures to ensure that its targeting is not directed at Canadians.

Finding 4

[REDACTED]

¹⁶ Verification of this process was also beyond the scope of this review but will be examined in future reviews.

[REDACTED]

Criterion 3

We would expect that in planning, assessing and deciding whether to implement technological systems, CSEC:

- *has approved plans, processes and privacy-risk assessments to determine whether systems being considered for development or acquisition comply with its legislative mandate and internal policies.*

When OCSEC received the introductory briefing on CSEC's Research and Development branch, we learned that no R&D activity is specifically dedicated to creating measures to protect the privacy of Canadians. Rather, CSEC ensures that any technology that is applied and implemented for SIGINT acquisition complements and conforms to its statutory obligations to protect the privacy of Canadians.

For example, when the [REDACTED] system was first installed in 2005, it did not become operational immediately due to privacy and targeting compliance issues identified by CSEC. For instance, CSEC had instituted a "Metadata First" regime for all its [REDACTED] collection systems. It required CSEC to select communications traffic by running its programmed dictionary selectors at the metadata (routing information) first. [REDACTED] At that time, [REDACTED] This was not permitted under the *NDA* as interpreted by the Department of Justice.¹⁸ CSEC modified the [REDACTED] system in order to meet these legal requirements and amended its policy accordingly.

CSEC's rules on targeting found at section 4.1 of OPS 1-6, *Canadian [REDACTED] Procedures* (2005) operationally describe the requirement:

Based on legal advice obtained from the Department of Justice, Solicitor-Client
Solicitor-Client Privilege

The Metadata First regime was set up initially as a privacy measure applying to a sensitive collection program known as [REDACTED] because of legal and privacy issues

¹⁸ Department of Justice legal opinion to the Chief, CSEC dated January 23, 2004 entitled Solicitor-Client Privilege

regarding the content of communications. For example, CSEC [REDACTED] would acquire traffic containing the selector [REDACTED]

[REDACTED] The Metadata First requirement ensures that at least one of the communicators, i.e. the foreign communicator, is the target CSEC is looking for.

The Metadata First requirement is one of the measures CSEC has put in place to protect the privacy of Canadians. [REDACTED]

[REDACTED] This also ensures that selectors belong to foreign entities located outside Canada.

Thus, [REDACTED] software had to be [REDACTED] before it could become operational. First, [REDACTED] had to be [REDACTED] to provide CSEC with a [REDACTED] to comply with the Metadata First requirement.

Secondly, a joint [REDACTED]
[REDACTED]
[REDACTED] A fault in the system did not permit this operation to function properly and was consequently fixed.¹⁹

Finally, a [REDACTED]
[REDACTED] This would have affected approximately [REDACTED] % of CSEC's targeting. This too was resolved with changes to software.

Finding 5

Based on our observations, CSEC modifies its interception/collection technology, if required, to comply with its statutory obligations to protect the privacy of Canadians.

¹⁹ CSEC described [REDACTED] as follows: [REDACTED] is [sic] the [sic] [REDACTED] is done by the [REDACTED] Where possible (i.e., [REDACTED] the [REDACTED]
[REDACTED]
[REDACTED] based on information related to [REDACTED] etc. so that the [REDACTED] within the [REDACTED] are then forwarded to traffic repositories for analytic use." E-mail from CSEC Liaison to OCSEC reviewer entitled *P&T Review - Additional [REDACTED] Questions*, dated July 16, 2007.

IX. [REDACTED]

Background

[REDACTED] is a USA-based company that offers [REDACTED] and services. [REDACTED] is the process of determining the [REDACTED] [REDACTED] has [REDACTED] It is possible to determine [REDACTED] because every computer [REDACTED] has access to [REDACTED] [REDACTED] has a data collection network that captures information about [REDACTED] [REDACTED] which it stores in a database. That information is extracted to better understand [REDACTED] Then, [REDACTED] network analysts look at the raw data and determine how each [REDACTED] Once a given [REDACTED] has been identified, [REDACTED] can [REDACTED]²⁰

Confidence levels indicate the relative likelihood that the specified [REDACTED] estimate is correct. [REDACTED] assigns a number to represent the confidence level for [REDACTED] A [REDACTED] number indicates a high likelihood of a correct [REDACTED] assignment. This level is based on the precision, completeness, certainty and consistency of the data used to determine [REDACTED]

CSEC has been using this commercial product since [REDACTED] through a [REDACTED] [REDACTED] Both CSEC business lines (SIGINT and information technology security (IT Security)) use [REDACTED] in their daily activities.

X. [REDACTED] FINDINGS

The findings documented below were derived from:

- documentation received from CSEC, including PowerPoint presentations and graphs;
- briefings and discussions held with CSEC personnel at various levels;
- the demonstrations of [REDACTED] activities undertaken by a SIGINT [REDACTED] analyst and the manager of [REDACTED] (IT Security); and
- answers received from CSEC to verbal and written questions.

The findings are assessed based on the criteria (expectations) enumerated in section V above.

²⁰ www.[REDACTED].com.

Criterion 1

We would expect that in planning, assessing and deciding whether to implement technological systems, CSEC:

- conducts its [REDACTED] activities based on such factors as:
 - whether the operational activity complies with CSEC's legislated authorities found in paragraphs 273.64(1)(a), (b) and/or (c) of the National Defence Act;
 - whether it falls under the authority of and complies with ministerial direction;
 - whether it falls under the authority of a valid ministerial authorization(s).

[REDACTED] is an analytical dataset used in support of all three of CSEC's mandated activities articulated in paragraphs 273.64(1)(a), (b) and (c) of the *NDA*. Therefore, most of CSEC's ministerial directives and ministerial authorizations will apply to the operational activity undertaken, including the use of [REDACTED]. Of note are the *Ministerial Directive on the Collection and Use of Metadata*, the *Ministerial Directive on the Privacy of Canadians*, the *Ministerial Authorization on [REDACTED] Interception*, the [REDACTED] ministerial authorization [REDACTED] and the *Ministerial Authorization on the protection of Computer Systems and Networks of the Government of Canada: Communications Security Establishment and Department of National Defence 2006 [REDACTED]*

Some of these guiding authorities have been described above (see section VIII, Criteria 1) and those descriptions apply here as well. It should be noted however, that this review focussed on the technologies used, and not on CSEC's operational activities that lead to the use of these technologies. Thus, [REDACTED] use in the context of the [REDACTED] MA has been examined more closely in OCSEC's report entitled *A Review of CSE Signals Intelligence Activities Conducted under Ministerial Directive and Authorization - [REDACTED]* [REDACTED]. Also, although CSEC would have used [REDACTED] while undertaking activities under the IT Security MAs listed above, since the MAs were suspended by the Chief, CSEC in October 2006 and subsequently investigated by CSEC, these operational activities were not examined in depth.

Finding 6

CSEC uses [REDACTED] for analytical purposes while undertaking their mandated activities.

Criterion 2

We would expect that in planning, assessing and deciding whether to implement technological systems, CSEC:

- ensures, with respect to any [REDACTED] activities carried out under paragraphs 273.64(1)(a) or (b) of the National Defence Act, that:
 - these activities would not be directed at Canadians or any person in Canada; and,
 - these activities would be subject to measures to protect the privacy of Canadians in the use and retention of intercepted information.

Both SIGINT and IT Security [REDACTED] users can find guidance as to the logistics of using the dataset on CSEC's [REDACTED] Intranet web page. The respective team leaders arrange for their analysts to have access to [REDACTED]. While prior approval to conduct a query is not required,²¹ authentication and user identification is needed to access the database.

SIGINT Use of [REDACTED]

According to a CSEC [REDACTED] analyst, [REDACTED] is used daily for two main purposes: to [REDACTED] metadata and to perform target development.

[REDACTED]

CSEC [REDACTED] with some collection systems in order to [REDACTED] metadata, thus identifying [REDACTED]. For example, [REDACTED] is [REDACTED] with [REDACTED]. [REDACTED] refers to the [REDACTED] and [REDACTED]. Currently, [REDACTED] equipment is [REDACTED] which [REDACTED] traffic using [REDACTED] and [REDACTED]. The communications that are [REDACTED] are not subjected to the techniques used to detect foreign [REDACTED] activities. Only those communications where either the [REDACTED] and scanned for foreign [REDACTED] activities.²² Information gained from cyber threat detection is used to produce foreign intelligence related to foreign [REDACTED] activities, as well as to provide technical data to CSEC's IT Security group to assist them in developing defensive measures to protect Canadian computer networks.

[REDACTED] analysts also search the [REDACTED] dataset to identify the [REDACTED]. This activity assists with target development and general network research. In pursuing such research, [REDACTED] analysts must also ensure that activities are not directed at Canadians. The [REDACTED] dataset can therefore be used to [REDACTED]. [REDACTED] ensure that Canadians are not targeted. This is a second type of [REDACTED] that is done.

²¹ *Infra*, note 22.

²² Response from CSEC [REDACTED] analyst sent by e-mail dated October 23, 2006, from CSEC Liaison to OCSEC reviewer entitled *P&T Review / Answers to Queries*.

In addition, CSEC uses [REDACTED] to identify data [REDACTED]. CSEC uses [REDACTED] to identify this data prior to making it available to SIGINT analysts in its metadata repository [REDACTED]. In [REDACTED] the name of the [REDACTED] will be encrypted, but the [REDACTED] will not. The analyst views the information in encrypted form.²³ Metadata associated with known foreign targets is not encrypted. In some circumstances, known foreign targets using [REDACTED] associated with [REDACTED] which have been identified as being [REDACTED] will not be encrypted.²⁴ For this to occur, analysts are required to demonstrate how they know that the target is foreign [REDACTED].

Target Development

[REDACTED] is also used for target development. [REDACTED] are identified through the daily work of [REDACTED] or intelligence analysts as they conduct SIGINT development work on their target's [REDACTED]. Through everyday traffic analysis, analysts will attempt to [REDACTED] of their targets by [REDACTED] and highlighting the way [REDACTED]. CSEC analysts using [REDACTED] will likely seek further information to determine more precisely [REDACTED] or to confirm the [REDACTED] information. Should additional information be obtained, it is possible for the analysts to input it in the [REDACTED] query results page. CSEC modified the [REDACTED] interface in order to be able to insert information from additional analysis conducted that either changes or corrects the original [REDACTED] information. With these measures, analysts can ensure they are not targeting Canadian [REDACTED].

Finding 7

[REDACTED] helps CSEC (SIGINT) protect the privacy of Canadians by identifying Canadian [REDACTED].

However, CSEC (SIGINT) does not record the number of Canadian [REDACTED] having been identified by [REDACTED] "because they cannot be targeted, and there is no requirement to account for them in any way".²⁵ According to the [REDACTED] analyst interviewed, it is not [REDACTED] purpose to record the number of identified Canadian [REDACTED]. There is no need to record the discarded Canadian [REDACTED].²⁶

CSEC policy recognizes that [REDACTED] are personal information. In fact, section 1.2 of OPS-1: *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities* (August 2005 and December 2006) defines "Canadian Identity

²³ Analysts with an operational need-to-know have access to the encrypted metadata. However, access to unencrypted metadata is restricted to less than [REDACTED] analysts.

²⁴ *Supra*, note 22.

²⁵ E-mail dated February 22, 2008 from CSEC liaison to OCSEC reviewer entitled *Privacy and Technology Review -- Responses* (see question 8).

²⁶ *Supra*, note 22; [REDACTED] demonstration and interview with a CSEC [REDACTED] analyst, November 17, 2006.

Information” as including [REDACTED] Furthermore, the Privacy Commissioner’s office has repeatedly found that an [REDACTED] can be considered personal information about Canadians if it can be associated with an identifiable individual.

It is interesting to note that the SIGINT business line does not account for the personal information it has identified, but that the IT Security business line does (see below for more details). According to CSEC, the difference is due to one of mandate:

ITS information is collected as a result of activities observed on Canadian networks. This is an entirely different environment from that which holds for SIGINT collection conducted under mandate A.

SIGINT’s MAs require that it track its recognition, use and retention of private communications. We do this through annotations of traffic, which is annotated for deletion or for retention if the traffic is to be used in an end-product report. Information about Canadians is suppressed; requests for idsents must be justified before they are released.

Metadata, however, is not considered to be a communication and therefore cannot be a private communication. For this reason, there is no need to account for metadata that is recognized as pertaining to a Canadian. The MD that governs the use of metadata requires that CSE alter any metadata known to be associated with Canadians when it is reported. In addition, SIGINT is not allowed to share its [REDACTED] DNI metadata with allies unless it has altered the data in such a way as to render impossible the identification of the persons to whom the metadata relates.²⁷

OCSEC acknowledges that SIGINT and IT Security collection are different but still questions why SIGINT does not account for the personal information it has identified. Both types of collection are subject to MAs which require CSEC to account for private communications and both collect metadata. [REDACTED] contained in metadata are considered to be “Canadian identity information” in CSEC operational policies and personal information about Canadians. The only policy found which directs CSEC to track information about Canadians that is used, retained or shared is OPS 1-14: *Procedures for Computer Network Defence (CND) Activities* (June 2005) (section 2.9). SIGINT policy does not address this issue. OCSEC believes this issue deserves further examination and may pursue it at a later date.

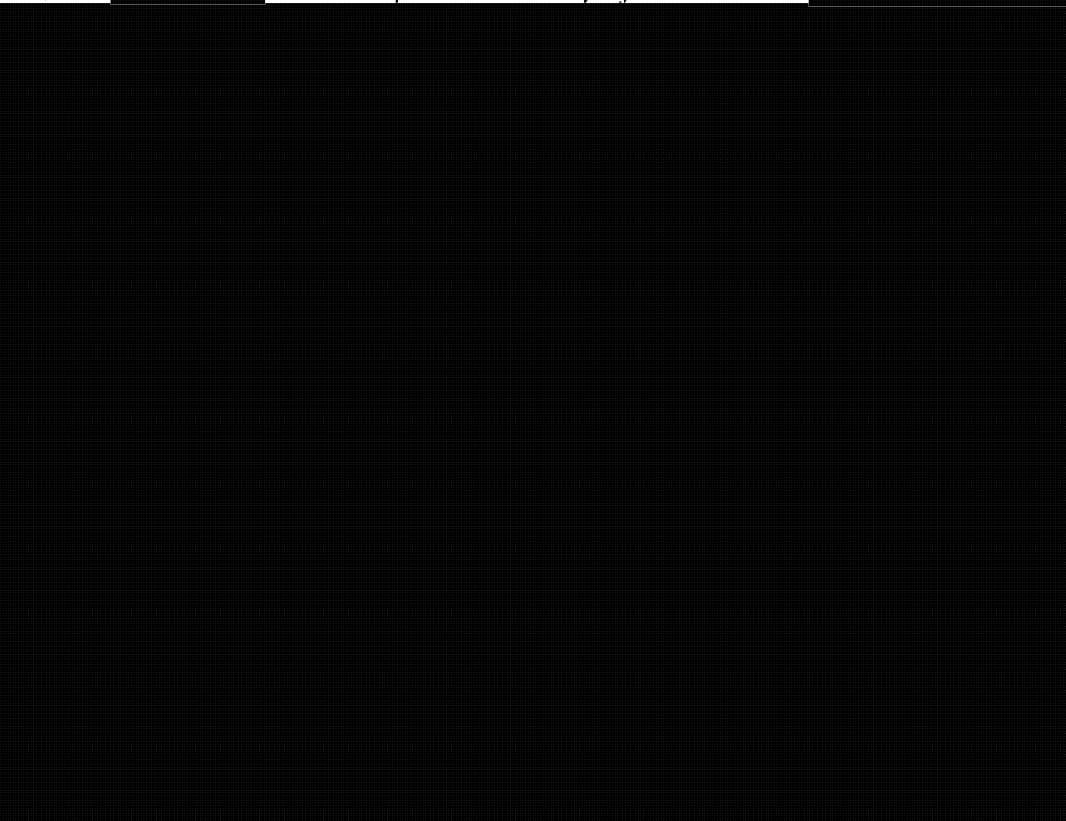
IT Security Use of [REDACTED]

CSEC’s Threat and Vulnerability Analysis Center (N Group) uses [REDACTED] in support of its [REDACTED] and other part (b) mandate activities related to the protection of the Government of Canada’s computer systems and networks. All of N Group’s subgroups

²⁷ E-mail dated February 22, 2008 from CSEC liaison to OCSEC reviewer entitled *Privacy and Technology Review – Responses* (see question 7).

██████████²⁸ may use ██████████ from time to time as an analytical tool in order to accomplish their operational activities.

CSEC's ██████████ team is responsible for the project codenamed ██████████



Measures to protect the privacy of Canadians

As previously mentioned, SIGINT does not account for the personal information (Canadian ██████████) identified through ██████████. This however, is not the case for IT Security. When conducting ██████████ operations, only those private communications, including metadata extracted from private communications or information about Canadians, deemed essential in identifying, isolating or preventing harm to Government of Canada computer systems or networks will be used or retained.³¹ N Group must track

²⁸ ██████████ undertakes Security Posture Assessments (SPA) and Active Network Security Testing (ANST) for client departments. ██████████ CSEC's ██████████ group, and ██████████ will use ██████████ from time to time, particularly when undertaking ██████████ activities.

²⁹ *Memorandum for the Minister of National Defence, Request for Ministerial Authorization – Protection of Government of Canada Computer Systems and Networks: Communications Security Establishment, dated June 2006 and signed by the Chief, CSEC and the Deputy Minister of National Defence, at page 3.*

³⁰ Section 2.9, OPS 1-14: *Procedures for Computer Network Defence (CND) Activities*, dated 14 June 2005.

³¹ Section 2.1, OPS 1-14: *Procedures for Computer Network Defence (CND) Activities*, 14 June 2005.

private communications and information about Canadians that is used, retained or shared.³² Information about Canadians will only be included in reports if essential to the understanding of the information and will be suppressed. A master log of private communications, including metadata extracted from private communications, which are used in reports must be kept.³³ Also, a [REDACTED] Oversight Committee reviews reports and decides whether there is a requirement to further distribute them (to SIGINT or to CSEC's partners). For most of these specific activities, OPS 1-14: *Procedures for Computer Network Defence (CND) Activities* refers to Standard Operating Procedures (SOPs) for further details.

While forming a necessary component of the controls under which CSEC operations are conducted, SOPs are not subject to the same standardized formats and processes as operational policy instruments and can take the form of e-mails or memoranda to staff. It is the responsibility of managers to ensure that the SOPs provided to their staff are effective, up to date, and consistent with higher level policies and procedures.³⁴ The SOPs reviewed were drafted in October and November of 2006, and encapsulated pre-existing staff direction in the form of the operational CONOPs, management emails, etc. They were sent in standard policy form to the Director of N Group on 17 November 2006.³⁵ As of February 2007, they were undated, still in draft form and had not received corporate approval. According to the Cyber lab's team leader, the SOPs did not receive corporate approval because [REDACTED] was a new pilot project and the SOPs only applied to a small number of personnel. The reviewed SOPs explained how and where to maintain the appropriate logs. The organizational policies in effect during the period under review did not specify the approval framework for operational instructions (i.e. SOPs). However, Annex 3 of the most recent version of ORG-1: *CSE Policy Framework* (December 2007), states that instructions must be reviewed for consistency with operational policy and procedures and receive corporate approval.

Finding 8

IT Security has policies and procedures in place to guide CND activities and that set out measures to protect the privacy of Canadians.

Finding 9

The [REDACTED] Report Tracking Tool that was reviewed demonstrates that N Group respects the instructions in its policy instruments.

³² Section 2.9, OPS 1-14: *Procedures for Computer Network Defence (CND) Activities*, 14 June 2005.

³³ Sections 3.1 and 3.2, OPS 1-14: *Procedures for Computer Network Defence (CND) Activities*, 14 June 2005.

³⁴ Section 7, ORG-1: *CSE Policy Framework*, 2005.

³⁵ E-mail from CSEC's Director, Corporate and Operational Policy to OCSEC reviewer entitled [REDACTED] SOPs and dated February 1, 2007.

Finding 10

During the period under review, CSEC did not give corporate approval to the [REDACTED] Standard Operating Procedures.

The practice at CSEC is to suppress information about Canadians that is included in both SIGINT and IT Security reports. According to section 1.5 of OPS 1-1: *Procedures for the Release of Suppressed Information from SIGINT Reports*,³⁶ suppressed information is defined as:

[...]information excluded from a SIGINT end-product report because it may reveal the identity of a Canadian or Allied entity. This information is stored in a limited-access database and is in most cases replaced in the report by a generic term.

Suppressed information includes, but is not limited to, personal identifiers such as names, passport information, [REDACTED] email addresses, phone numbers and *IP addresses*, as well as context identifiers such as [REDACTED] [Emphasis added]

The procedure to release suppressed information found in SIGINT reports is documented in CSEC's policies.³⁷ CSEC's [REDACTED] is the authority for releasing information suppressed from SIGINT reports. This authority has been delegated in writing to the Operational Policy Section.³⁸ However, the Operational Policy Section is not responsible for releasing information suppressed from IT Security reports to clients. In fact, there is no *corporately approved* policy or procedures which describe the process to release suppressed information in IT Security reports. However, the draft [REDACTED] *Information Handling SOP* (section 1.11) states that requests for suppressed identities for Canadian information or information about Second Party partners will be submitted to N Group and subject to the Director of N Group's approval. According to CSEC's Director, Corporate and Operational Policy, to date, "there have not been any external requests for Canadian identity information in [REDACTED] operations".³⁹

Finding 11

CSEC did not give corporate approval to policy or procedures describing the process to release suppressed information found in IT Security reports.

³⁶ Dated 03 January 2006.

³⁷ See OPS 1-1: *Procedures for the Release of Suppressed Information from SIGINT Reports*, 03 January 2006.

³⁸ *Ibid.*, section 2.4.

³⁹ E-mail from CSEC's Director, Corporate and Operational Policy to OCSEC reviewer entitled [REDACTED] *SOPs* and dated February 1, 2007.

We understand however, that since the review took place, CSEC has included IT Security in its operational policy structure, assigning Q group to lead its development. CSEC has implemented an IT Security operational policy framework compartmentalized by IT Security pillar (Sophisticated Cyber Defence, Enterprise Security Architecture, Secure Technologies, Enablers and Joint Operations) and by policy document categories (IT Security Policy, Procedures, Standards, Guidelines and Instructions).⁴⁰ These centralized efforts to develop and approve IT Security policy instruments should benefit CSEC's overall efforts to protect privacy. CSEC has also advised us that the issues raised in findings 10 and 11 above have been addressed in new policy instruments and their approval process.⁴¹

Criterion 3

We would expect that in planning, assessing and deciding whether to implement technological systems, CSEC:

- *has approved plans, processes and privacy-risk assessments to determine whether systems being considered for development or acquisition comply with its legislative mandate and internal policies.*

Before purchasing the subscription for the [REDACTED] database, CSEC first recognized an operational need for a tool [REDACTED]. Both the SIGINT and the IT Security business lines required the analytic dataset to help fulfill their mandates. The development and/or acquisition of a technology by SIGINT is driven by the need to develop and/or [REDACTED] capabilities to access/obtain information from the global information infrastructure to meet GoC intelligence requirements. Also, CSEC must maintain the capability to collect and [REDACTED] the same technologies used by their targets. As for IT Security, the development and/or acquisition of the technology supports CSEC's part (b) mandate activities related to the protection of the Government of Canada's computer systems and networks, such as cyber-threat protection and advanced intrusion detection.

Initially, however, [REDACTED] was acquired by SIGINT "in order to address the need to [REDACTED] for various purposes—e.g., [REDACTED] [REDACTED]

⁴⁰ Power Point presentation entitled *IT Security Policy, Standards and Relations (Q2A)*, IT Security Fundamentals Course, 6 November 2007.

⁴¹ *CSEC Comments on OCSEC Draft Review on: "Review of CSEC's Acquisition and Implementation of Technology per Subsection 273.64(2) of the National Defence Act"*, sent by e-mail from CSEC Director, Corporate and Operational Policy to OCSEC Director of Operations dated April 14, 2008.

Finding 12

XI. CONCLUSION

⁴³ See *A History of Commercial [REDACTED] Services at CSEC*, prepared by a CSEC [REDACTED] analyst, dated June 22, 2007 and *Commercial [REDACTED] Services - [REDACTED]* prepared by CSEC's [REDACTED] March 2006.

One recommendation is set forth concerning requests for [REDACTED] ministerial authorizations. It was observed that when seeking a ministerial authorization, the Chief, CSEC requests authority to intercept private communications while conducting collection/interception activities. These activities are described in the request, as well as other activities known as metadata activities (i.e. research and analysis such as [REDACTED] SIGINT development and Network Analysis and Prioritization). This is confusing as the Minister only authorizes the class of activities described as [REDACTED] *interception* (as defined in the legal guidance received by CSEC). Therefore, we recommend that CSEC re-evaluate how it describes the [REDACTED] activities in its request for a ministerial authorization so as to clearly identify which activity the Minister of National Defence is authorizing when signing a [REDACTED] ministerial authorization.

ANNEX A

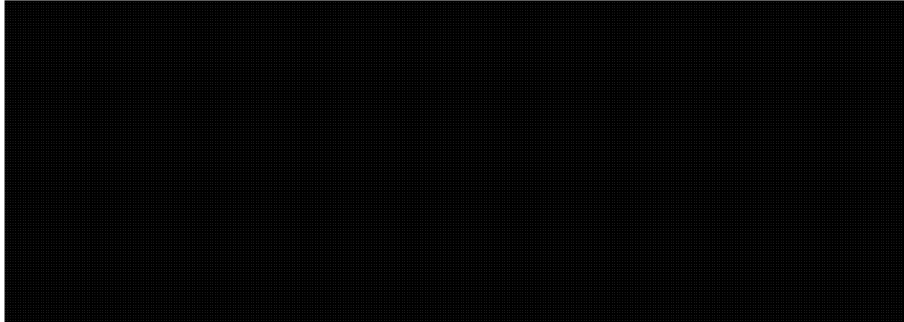
List of Interviewees

Associate Director, [REDACTED] SIGINT Programs
Director, [REDACTED] Group
IT Security, Strategic Management
Manager, IT Security, Cyber Defence Futures
Acting Manager, [REDACTED]
Team Leader, Cyberlab
Canadian Forces Information Operations Group [REDACTED]
Analyst
Team Leader, [REDACTED]
Director, Corporate and Operational Policy
Team Leader, [REDACTED]
Manager, Operational Policy
SIGINT [REDACTED] analyst
Manager, SIGINT Programs Oversight and Compliance

ANNEX B

Metadata: [REDACTED] **Process,** [REDACTED]

The terminology applied to metadata activities is not yet definitive within CSEC's own written documentation. The following definitions, which apply generally to SIGINT acquisition, were provided to us by CSEC and were important to our understanding of the collection and use of metadata as authorized by the metadata MD.



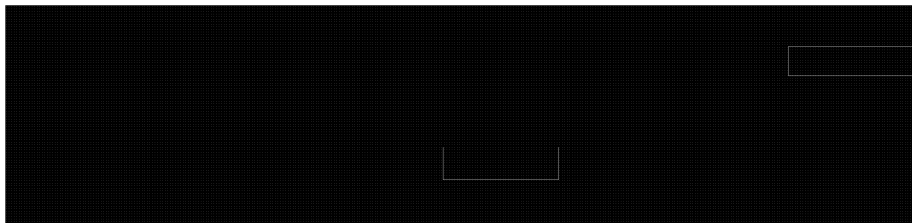
Acquire/Collect: *Used synonymously to indicate interception.*⁴⁴

As indicated in these definitions, all data is [REDACTED]

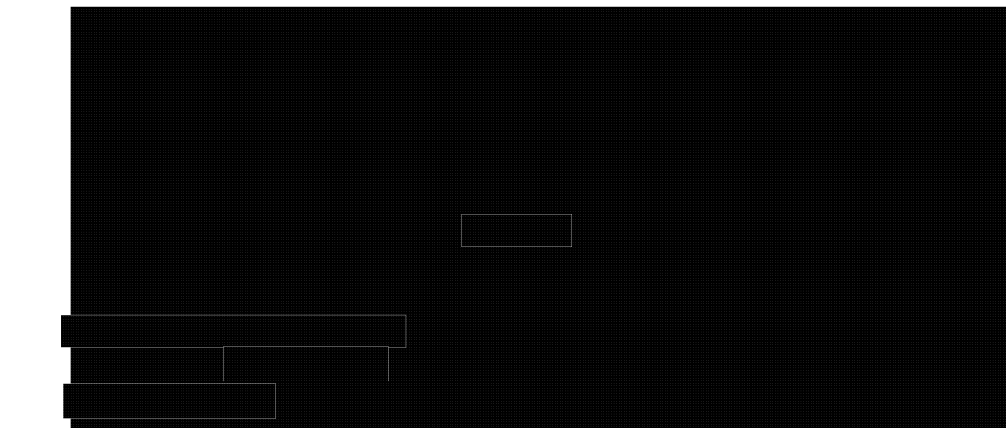


For CSEC's purposes, each communication is seen as having two distinct parts: that known as the metadata and that known as the content. The metadata portion is the focus of [REDACTED] by CSEC and which result in [REDACTED]

[REDACTED] database (see below). We understand these [REDACTED] processes to be as follows:



⁴⁴ Briefing entitled *Metadata Review Questions* given to OCSEC by CSEC on February 26, 2007.

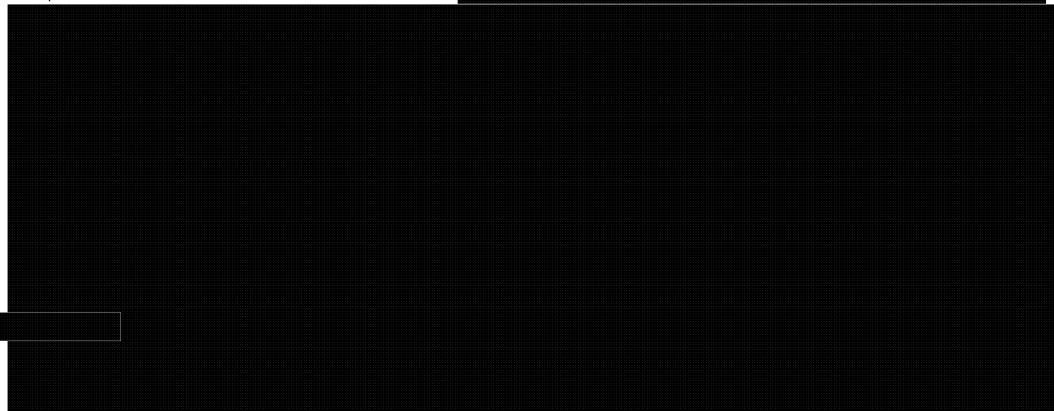


[REDACTED]

[REDACTED] is a CSEC database that stores only metadata. The metadata has been [REDACTED] from both DNR (dialled number recognition) and DNI (digital network intelligence) communications traffic. Generally, DNR traffic is that commonly known as phone or fax, while DNI refers generally to e-mails. CSEC will often refer to DNI as [REDACTED] traffic.

The source of [REDACTED] metadata is CSEC's own collection [REDACTED] and includes that acquired via [REDACTED] programme.

All CSEC-collected DNR metadata is [REDACTED]



⁴⁵Typically, foreign intelligence traffic is obtained using *selectors* that represent foreign entities of intelligence interest. Selectors are alphanumeric data such as e-mail addresses or telephone numbers that are [REDACTED] into a [REDACTED] dictionary.

⁴⁶ The communications stored in these principal information databases are accessed mainly for foreign intelligence analysis purposes.

TOP SECRET/COMINT/CEO



ANNEX C

Recommendations and Findings

Recommendation

That CSEC re-evaluate how it describes the [REDACTED] activities in its request for a ministerial authorization so as to clearly identify which activity the Minister of National Defence is authorizing when signing a [REDACTED] ministerial authorization.

Findings

1. CSEC's authority to conduct its activities using [REDACTED] is found in subsection 273.64(1) of the *NDA*.
2. CSEC associates its tasking of telecommunications data to a foreign intelligence requirement in compliance with part (a) of its mandate.
3. Based on the information received, CSEC takes measures to ensure that its targeting is not directed at Canadians.
4. [REDACTED] is a SIGINT [REDACTED] system only and is [REDACTED] of private communications, [REDACTED]
5. Based on our observations, CSEC modifies its interception/collection technology, if required, to comply with its statutory obligations to protect the privacy of Canadians.
6. CSEC uses [REDACTED] for analytical purposes while undertaking their mandated activities.
7. [REDACTED] helps CSEC (SIGINT) protect the privacy of Canadians by identifying Canadian [REDACTED]
8. IT Security has policies and procedures in place to guide CND activities and that set out measures to protect the privacy of Canadians.
9. The [REDACTED] Report Tracking Tool that was reviewed demonstrates that N Group respects the instructions in its policy instruments.
10. During the period under review, CSEC did not give corporate approval to the [REDACTED] Standard Operating Procedures.

11. CSEC did not give corporate approval to policy or procedures describing the process to release suppressed information found in IT Security reports.
12. After research and assessment, CSEC planned to and acquired [REDACTED] to support its SIGINT and IT Security mandates.