RELEASED UNDER THE AIA – UNCLASSIFIED INFORMATION
DIVULGUÉ EN VERTU DE LA LAI – RENSEIGNEMENTS NON CLASSIFIÉS

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

RELEASED UNDER THE AIA – UNCLASSIFIED INFORMATION
DIVULGUÉ EN VERTU DE LA LAI – RENSEIGNEMENTS NON CLASSIFIÉS

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

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 and for protecting privacy.

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, to OCSEC's Director of Operations and reviewer entitled *RE: R&D Scope Statement* and dated June 30, 2006.

RELEASED UNDER THE AIA – UNCLASSIFIED INFORMATION
DIVULGUÉ EN VERTU DE LA LAI – RENSEIGNEMENTS NON CLASSIFIÉS

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 acquisition[3] and implementation[4] 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
:o 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 and how CSEC determines, scopes, plans, conducts and manages its 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.

RELEASED UNDER THE AIA – UNCLASSIFIED INFORMATION
DIVULGUÉ EN VERTU DE LA LAI – RENSEIGNEMENTS NON CLASSIFIÉS

5. how and how CSEC is developing 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 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 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

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: and policies concerning the acquisition, use and retention of personal information about Canadians.

RELEASED UNDER THE AIA – UNCLASSIFIED INFORMATION
DIVULGUÉ EN VERTU DE LA LAI – RENSEIGNEMENTS NON CLASSIFIÉS

When criterion 4 was developed some time ago, it was not clear to OCSEC that 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 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 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 can be found under the section entitled *IT Security Use of* 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 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 system. We also received briefings and demonstrations of the , 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.

All of CSEC's Second Party[7] partners also work with version of it.

[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.

RELEASED UNDER THE AIA – UNCLASSIFIED INFORMATION
DIVULGUÉ EN VERTU DE LA LAI – RENSEIGNEMENTS NON CLASSIFIÉS

s.15(1)
s.16(2)(c)

The basic function of (and its predecessor) is to

This complex process has already been documented in a recent OCSEC report titled *OCSEC Review of the Ministerial Directive on the March 9, 2005* . 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 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*).
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,
This report focuses on CSEC's activities using under part (a) of its mandate

VIII. 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 development activities undertaken by Canadian Forces personnel at ; 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 ictivities 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 to undertake all three of its mandated activities. This report will focus on CSEC's activities using under part

RELEASED UNDER THE AIA – UNCLASSIFIED INFORMATION
DIVULGUÉ EN VERTU DE LA LAI – RENSEIGNEMENTS NON CLASSIFIÉS

s.15(1)
s.16(2)(c)
s.23

(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 is found in subsection 273.64(1) of the *NDA*.

As CSEC may intercept private communications when undertaking activities under part (a) of its mandate while using a ministerial authorization is also required (s. 273.65 of the *NDA*). The *Ministerial Authorization* ((dated December 19, 2005 and valid for the year 2006, the period under review) authorizes CSEC 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* dated March 9, 2005) which governs CSEC's 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 , 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

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

RELEASED UNDER THE AIA – UNCLASSIFIED INFORMATION
DIVULGUÉ EN VERTU DE LA LAI – RENSEIGNEMENTS NON CLASSIFIÉS

s.15(1)
s.16(2)(c)
s.23

Canadian Forces personnel at Pursuant to this demonstration, questions were raised concerning these two activities, particularly CSEC's These issues have been examined and explained in the 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 ministerial authorization (MA), permitting such interception. CSEC uses 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,

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

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

> *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]

[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 ntitled *P & T review Additional Questions*..

RELEASED UNDER THE AIA – UNCLASSIFIED INFORMATION
DIVULGUÉ EN VERTU DE LA LAI – RENSEIGNEMENTS NON CLASSIFIÉS

s.15(1)
s.16(2)(c)

RELEASED UNDER THE AIA – UNCLASSIFIED INFORMATION
DIVULGUÉ EN VERTU DE LA LAI – RENSEIGNEMENTS NON CLASSIFIÉS

s.15(1)
s.16(2)(c)

Recommendation

Criterion 2

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

- *ensures, with respect to any 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),

- -

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 [12]

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

RELEASED UNDER THE AIA – UNCLASSIFIED INFORMATION
DIVULGUÉ EN VERTU DE LA LAI – RENSEIGNEMENTS NON CLASSIFIÉS

s.15(1)
s.16(2)(c)

Tasking

Finding 2

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

Targeting

CSEC defines *target* as follows:

[13] Briefing given to OCSEC by CSEC's Associate Director, SIGINT entitled (on 17 November 2006.

[14] *Ibid.*

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

A0345037_11-000011

RELEASED UNDER THE AIA – UNCLASSIFIED INFORMATION
DIVULGUÉ EN VERTU DE LA LAI – RENSEIGNEMENTS NON CLASSIFIÉS

s.15(1)
s.16(2)(c)

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."

Finding 3

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

Finding 4

RELEASED UNDER THE AIA – UNCLASSIFIED INFORMATION
DIVULGUÉ EN VERTU DE LA LAI – RENSEIGNEMENTS NON CLASSIFIÉS

s.15(1)
s.16(2)(c)
s.23

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

RELEASED UNDER THE AIA – UNCLASSIFIED INFORMATION
DIVULGUÉ EN VERTU DE LA LAI – RENSEIGNEMENTS NON CLASSIFIÉS

s.15(1)
s.16(2)(c)

is one of the measures CSEC has put in place to protect the privacy of Canadians.

This also ensures that belong to foreign entities located outside Canada.

Finding 5

RELEASED UNDER THE AIA – UNCLASSIFIED INFORMATION
DIVULGUÉ EN VERTU DE LA LAI – RENSEIGNEMENTS NON CLASSIFIÉS

s.15(1)
s.16(2)(c)

IX.

Background

X. 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 analyst and the manager (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.

RELEASED UNDER THE AIA – UNCLASSIFIED INFORMATION
DIVULGUÉ EN VERTU DE LA LAI – RENSEIGNEMENTS NON CLASSIFIÉS

Criterion 1

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

- *conducts its 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).*

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 Of note are the *Ministerial Directive on the* the *Ministerial Directive on the Privacy of Canadians*, the *Ministerial Authorization* the ministerial authorization and the *Ministerial Authorization*

2006 (KLONDIKE).

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.

Finding 6

CSEC uses 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:

RELEASED UNDER THE AIA – UNCLASSIFIED INFORMATION
DIVULGUÉ EN VERTU DE LA LAI – RENSEIGNEMENTS NON CLASSIFIÉS

s.15(1)
s.16(2)(c)

- *ensures, with respect to any 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 users can find guidance as to the logistics of using the on web page. The respective team leaders arrange for their analysts to have access to

SIGINT Use of

According to a CSEC analyst, is used daily for two main purposes: to

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

RELEASED UNDER THE AIA – UNCLASSIFIED INFORMATION
DIVULGUÉ EN VERTU DE LA LAI – RENSEIGNEMENTS NON CLASSIFIÉS

s.15(1)
s.16(2)(c)

Finding 7

helps CSEC (SIGINT) protect the privacy of Canadians

CSEC policy recognizes that are personal information. OPS-1: *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities* (August 2005 and December 2006) defines

---

[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; demonstration and interview with a analyst, November 17, 2006.

RELEASED UNDER THE AIA – UNCLASSIFIED INFORMATION
DIVULGUÉ EN VERTU DE LA LAI – RENSEIGNEMENTS NON CLASSIFIÉS

Furthermore, the Privacy Commissioner's office has repeatedly found that an can be considered personal information about Canadians if it can be associated with an identifiable individual.

OCSEC believes this issue deserves further examination and may pursue it at a later date.

IT Security Use of

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

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

RELEASED UNDER THE AIA – UNCLASSIFIED INFORMATION
DIVULGUÉ EN VERTU DE LA LAI – RENSEIGNEMENTS NON CLASSIFIÉS

s.15(1)
s.16(2)(c)

---

may use from time to time in order to accomplish their operational activities.

Measures to protect the privacy of Canadians

RELEASED UNDER THE AIA – UNCLASSIFIED INFORMATION
DIVULGUÉ EN VERTU DE LA LAI – RENSEIGNEMENTS NON CLASSIFIÉS

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 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 team leader, the SOPs did not receive corporate approval because was a new pilot project and the SOPs only applied to a small number of personnel. The reviewed SOPs explained

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 activities and that set out measures to protect the privacy of Canadians.

Finding 9

The that was reviewed demonstrates that 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*,

[34] Section 7, ORG-1: *CSE Policy Framework*, 2005.
[35] E-mail from CSEC's Director, to OCSEC reviewer entitled *SOPs* and dated February 1, 2007.

RELEASED UNDER THE AIA – UNCLASSIFIED INFORMATION
DIVULGUÉ EN VERTU DE LA LAI – RENSEIGNEMENTS NON CLASSIFIÉS

Finding 10

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

The practice at CSEC is to

Finding 11

CSEC did not give corporate approval to policy or procedures describing the process

[36] Dated 03 January 2006.
[37] See OPS 1-1: ,
2006.
[38] *Ibid.*, section 2.4.
[39] E-mail from CSEC's Director, to OCSEC reviewer entitled *SOPs* and dated February 1, 2007.

RELEASED UNDER THE AIA – UNCLASSIFIED INFORMATION
DIVULGUÉ EN VERTU DE LA LAI – RENSEIGNEMENTS NON CLASSIFIÉS

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 CSEC first recognized an operational need for a

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,

Initially, however, was acquired by SIGINT

[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, to OCSEC Director of Operations dated April 14, 2008.

RELEASED UNDER THE AIA – UNCLASSIFIED INFORMATION
DIVULGUÉ EN VERTU DE LA LAI – RENSEIGNEMENTS NON CLASSIFIÉS

compared and evaluated other Before acquiring CSEC tried out, products.[43]

Finding 12

After research and assessment, CSEC planned to and acquired to support its SIGINT and IT Security mandates.

XI. CONCLUSION

This review focussed on CSEC's use of technology that contributes to the protection of the privacy of Canadians, and complies with paragraph 273.64(2)(b) of the *National Defence Act*. It only examined the related operational activities to the extent necessary to understand how these technologies were being employed and what measures, if any, had been implemented in their use to protect the privacy of Canadians. Two types of technologies were studied,

The review found that CSEC complied with the law in the areas that were examined. Please see Annex C for a list of all findings and recommendation. The acquisition, implementation and use of these technologies permits CSEC to fulfill its legislated mandates and helps it protect the privacy of Canadians by identifying personal information.

The review also 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. CSEC has informed us that since the review took place, this has been addressed in the new policy instruments and their approval process.

[42] E-mail from CSEC Liaison to OCSEC Review Analyst dated July 12, 2007 entitled *Request for Information 11* -

RELEASED UNDER THE AIA – UNCLASSIFIED INFORMATION
DIVULGUÉ EN VERTU DE LA LAI – RENSEIGNEMENTS NON CLASSIFIÉS

s.15(1)
s.16(2)(c)

RELEASED UNDER THE AIA – UNCLASSIFIED INFORMATION
DIVULGUÉ EN VERTU DE LA LAI – RENSEIGNEMENTS NON CLASSIFIÉS

ANNEX A

List of Interviewees

Associate Director,	SIGINT
Director,	
IT Security,	
Manager, IT Security,	
Acting Manager,	
Team Leader,	
Analyst	
Team Leader,	
Director,	
Team Leader,	
Manager,	
SIGINT analyst	
Manager, SIGINT	

RELEASED UNDER THE AIA – UNCLASSIFIED INFORMATION
DIVULGUÉ EN VERTU DE LA LAI – RENSEIGNEMENTS NON CLASSIFIÉS

ANNEX B

The terminology applied to 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

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

RELEASED UNDER THE AIA – UNCLASSIFIED INFORMATION
DIVULGUÉ EN VERTU DE LA LAI – RENSEIGNEMENTS NON CLASSIFIÉS

s.15(1)
s.16(2)(c)

RELEASED UNDER THE AIA – UNCLASSIFIED INFORMATION
DIVULGUÉ EN VERTU DE LA LAI – RENSEIGNEMENTS NON CLASSIFIÉS

s.15(1)
s.16(2)(c)

s.15(1)
s.16(2)(c)

RELEASED UNDER THE AIA – UNCLASSIFIED INFORMATION
DIVULGUÉ EN VERTU DE LA LAI – RENSEIGNEMENTS NON CLASSIFIÉS

s.15(1)
s.16(2)(c)

ANNEX C

Recommendations and Findings

Recommendation

Findings

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

2. CSEC associates its tasking of 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.

5. Based on our observations, to comply with its statutory obligations to protect the privacy of Canadians.

6. CSEC uses while undertaking their mandated activities.

7. helps CSEC (SIGINT) protect the privacy of Canadians

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

9. The that was reviewed demonstrates that respects the instructions in its policy instruments.

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

RELEASED UNDER THE AIA – UNCLASSIFIED INFORMATION
DIVULGUÉ EN VERTU DE LA LAI – RENSEIGNEMENTS NON CLASSIFIÉS

s.15(1)
s.16(2)(c)

11. CSEC did not give corporate approval to policy or procedures describing the process IT Security reports.

12. After research and assessment, CSEC planned to and acquired :o support its SIGINT and IT Security mandates.