Summary authorized, see Annex A.

Communications Security
Establishment Commissioner

The Honourable Robert Décary, Q.C.

Canada

Commissaire du Centre de la
sécurité des télécommunications

L'honorable Robert Décary, c.r.

TOP SECRET//SI//CEO

December 22, 2011

The Honourable Peter 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 provide you with the results of a review of CSEC activities relating to retention and disposal of intercepted [redacted] communications. This review was conducted under my authorities as articulated in Part V.1, paragraph 273.63(2)(*a*) and subsection 273.65(8) of the *National Defence Act* (*NDA*). Based upon the information reviewed and the interviews conducted, I concluded that CSEC conducted its retention and disposal activities in accordance with the law and ministerial direction during the period of the review.

The obligation for CSEC to take measures to protect the privacy of Canadians, as set out in paragraph 273.64(2) *(b)* of the *NDA*, extends to the retention and disposal (destruction) of intercepted [redacted] communications in the course of its mandated activities. Records creation and retention is the main means by which CSEC can assure compliance with its various requirements and account for its authorized activities. CSEC disposition of records is subject to comprehensive authorities because the unauthorized destruction of a record may result in an inability to document an activity and consequently, an inability to demonstrate compliance of that activity with legal, ministerial and policy requirements.

The primary objectives of my review were: to acquire detailed knowledge of, and document CSEC business practices respecting the retention and disposal of intercepted [redacted] communications; to assess whether CSEC activities relating to the retention and disposal of intercepted [redacted] communications were conducted in compliance with requirements set out in the law, ministerial authorities and directives, and policies and procedures; and, to assess the extent to which CSEC took steps to protect the privacy of Canadians in carrying out these activities. I paid particular attention to the retention and disposal of private communications, communications of Canadians outside Canada and information about Canadians.

I found that both CSEC's SIGINT and IT Security programs have incorporated legal, ministerial and policy considerations for retention and disposal into the digital architecture of their respective programs. CSEC information management practices are supported by this policy-based and technology-assisted approach.

CSEC takes measures - in the design of its retention and disposal systems – to promote compliance with the law and the protection of the privacy of Canadians. I found the retention and disposal periods set out in CSEC policies to be reasonable.

CSEC's policies and procedures for retention and disposal of intercepted [redacted] communications provide sufficient direction to CSEC employees respecting these activities and the protection of the privacy of Canadians. However, the use of "transitory" to describe all SIGINT intercepts in its OPS 1-11 policy, as well as the inconsistent use of certain terminology by the SIGINT and IT Security programs, are confusing and should be clarified. The Commissioner's office will follow up on CSEC efforts to address these issues.

Finally, CSEC has addressed previous associated recommendations of my predecessors to establish records management authorities and retention and disposition schedules. Specifically, I consider recommendation no. 8 of the Commissioner's 2005 review of CSEC support to the RCMP IRRELEVANT
IRRELEVANT

The enclosed report contains detailed information on my findings as well as related issues. I made no recommendations. CSEC officials were provided an opportunity to review and comment on the report, for factual accuracy, prior to finalizing it.

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

Yours sincerely,

Robert Décary

Enclosure: (1)

c.c. Mr. John Adams, Chief, CSEC

Communications Security
Establishment Commissioner

The Honourable Robert Décary, Q.C.

Canada

Commissaire du Centre de la
sécurité des télécommunications

L'honorable Robert Décary, c.r.

TOP SECRET//SI//CANADIAN EYES ONLY

Review of CSEC Retention and Disposal of Intercepted [redacted] Communications

December 22, 2011

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

TABLE OF CONTENTS

I. AUTHORITIES

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

The review encompassed CSEC processes and practices in effect for the period of April 1, 2009 to March 31, 2010.

The obligation for CSEC to take measures to protect the privacy of Canadians, as set out in paragraph 273.64(2) *(b)* of the *NDA*, extends to the retention and disposal (destruction) of intercepted [redacted] communications in the course of its mandated activities. CSEC must have appropriate measures in place for the retention and disposal of private communications, communications of Canadians located outside Canada and information about Canadians acquired through these mandated activities.

The review also derives authority from the Ministerial Directives (MDs) on Privacy of Canadians (June 19, 2001) and Collection and Use of Metadata (March 9, 2005) and the Ministerial Authorizations (MAs) authorizing the interception of private communications (PCs) – as defined in s.183 of the *Criminal Code*[1] – under Signals Intelligence (SIGINT) collection programs known as [redacted] and Interception Activities Conducted in Support of Canadian Forces Operations in Afghanistan (Afghan MA activities) as well as under the Information Technology Security (IT Security) Cyber Defence Operations (CDO) program and the Active Network Security Testing (ANST) component of the Security Posture Assessment (SPA) program. MAs current to the review period were in effect from December 1, 2010 to November 30, 2011.

Other applicable legal authorities include, namely, the *Privacy Act*, the *Library and Archives of Canada Act* (*LACA*) and judicial warrants for CSEC assistance to federal law enforcement and security agencies under paragraph 273.64(1)(*c*) of the *NDA*.

Ministerial authorities further require CSEC to support and assist the Commissioner in review exercises.

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

II. INTRODUCTION

Given that the term "interception" is not defined in the *NDA*, CSEC activities follow the June 6. 2005 legal opinion from the Deputy Minister of Justice and Deputy Attorney General of Canada to the Chief. CSEC, which states that Solicitor-Client Privilege

Solicitor-Client Privilege

In the case of SIGINT and foreign intelligence interception, paragraph 273.65(2)(*d*) of the *NDA* requires that "satisfactory measures" are in place to protect the privacy of Canadians and to ensure that private communications (PCs) will only be used or *retained* if they are essential to international affairs. defence or security" (emphasis added).

In the case of IT Security, paragraph 184(2)(e) of the *Criminal Code* permits the interception of private communications by authorized persons when engaged in activities directly related to the protection of computer systems from mischief and unauthorized use. According to the Library of Parliament summary of Bill C-14, *An Act to Amend the Criminal Code and Other Acts* (2004). this provision adds an exemption to the existing laws forbidding the interception of PCs, "in order to allow information technology managers to use "reasonable measures" to protect against data theft and the intentional transmission of computer viruses.

In the same context of protecting government computer systems or networks. paragraphs 273.65(4) (*d*) and (*e*) of the *NDA* require that "satisfactory measures are in place to ensure that only information that is essential to identify, isolate or prevent harm to Government of Canada computer systems or networks will be used or *retained*" and "satisfactory measures are in place to protect the privacy of Canadians in the use or *retention* of that information" (emphasis added).

MAs for IT Security to [redacted][4] information in order to protect government computer systems or networks allows CSEC to use or *retain* [redacted] private communication "if it is essential to identify, isolate or prevent harm to Government of Canada computer

Solicitor-Client Privilege

[3] If legal advice given to CSEC is shared with the Commissioner's office, this is done on the understanding that the sharing by CSEC of information which is subject to solicitor-client privilege does not constitute a waiver by CSEC of its privilege.

[4] In the context of IT Security operations. the term [redacted] is preferred to the term 'intercept' but has a meaning similar to the latter.

systems or networks." The MAs also require CSEC to record and report information to the Minister of National Defence, including the number of PCs intercepted that are used or *retained*.

Furthermore, the MD on Privacy of Canadians requires that:

> [...] in using and *retaining* information, CSE[C] takes all possible measures and implements appropriate policies to protect the privacy of Canadians, consistent with the *Canadian Charter of Rights and Freedoms* and the *Privacy Act*.
>
> CSE[C] may *retain* and report information on or of Canadians or Canadian corporations found in the course of its signals intelligence activities only when:
>
> - it is essential to protect the lives or safety of individuals;
> - it contains evidence of serious criminal activity; or
> - it is required to understand or exploit foreign, security and defence intelligence.
>
> In the above cases, you [the Chief, CSEC] are to ensure that the appropriate policies and procedures are in place at CSE[C] for the handling, *retention* and *destruction* of this material (emphasis added).

Retention and disposal of data are information management (IM) practices that affect all CSEC business lines. Intercepted [redacted] communications may include PCs and information about Canadians which is why CSEC IM activities are subjected to specific controls to ensure compliance with legal, ministerial and policy requirements in order to protect the privacy of Canadians.

In its *IM Strategy 2008*, CSEC noted that while information is crucial to its mission, IM practices at the time were assessed as problematic[5]. Additionally, CSEC executive management identified IM practices as a significant risk to the organization's ability to deliver fully on its mandate.[6] These assessments resulted, in part, from past Commissioners' findings and recommendations from various reviews as IM practices are crucial for CSEC to demonstrate compliance with the law and its own policies.[7]

More recently, a records management audit conducted by the CSEC Directorate of Audit, Evaluation and Ethics between September 2008 and March 2009[8] found that, without having and applying record retention and disposition schedules, the ability for CSEC to demonstrate adequate records management was compromised and that CSEC staff would benefit from additional guidance on the management of records.

[5] CSEC IM Strategy 2008.

[6] CSEC Risk Profile as assessed by ExCom June 2008.

[7] CERRID -#117344-v1 18 July 2008

[8] Audit of Records Management, Directorate of Audit, Evaluation and Ethics, Final Report, CERRID 302301

Rationale for conducting this review

Specific controls are placed on CSEC retention and disposal activities in order to ensure compliance with legal, ministerial and policy requirements. The potential impact on the privacy of Canadians could be significant, should there be an instance of non-compliance with the law while conducting these activities.

Past Commissioners made findings and recommendations respecting retention and disposal activities which require follow-up. CSEC made major changes to certain technologies and procedures relating to these activities, such as the migration of the content of multiple SIGINT databases to a common repository and the upgrading of the IT Security program cyber defence sensor infrastructure.

It is for these reasons that the Commissioner selected retention and disposal activities as a subject for review.

III. OBJECTIVES

The objectives of the review were to:

- acquire detailed knowledge of, and document CSEC business practices respecting the retention and disposal of intercepted [redacted] communications;

- assess whether CSEC retention and disposal of intercepted [redacted] communications comply with the law; and

- assess the extent to which CSEC protected the privacy of Canadians in carrying out its retention and disposal activities.

IV. SCOPE

The Commissioner's office examined:

- the legislative and policy framework;

- what intercepted [redacted] communication CSEC retains, for how long and how it is retained; when and how intercepted communications are disposed of; and in particular how CSEC retains and disposes of PCs, communications of Canadians located outside Canada, and information about Canadians;

- associated databases and systems;

- the extent to which technology is used and other efforts are applied to protect the privacy of Canadians (e.g., privacy annotations, automated schedules, deletion scripts);

- CSEC activities in response to previous associated recommendations of the Commissioner, namely;

- recommendation no. 8 of the Commissioner's review of the CSEC Support to RCMP under mandate (c) (January 7, 2005) that: "CSE[C] should develop an agreement to govern the retention/destruction of data acquired as a result of technical assistance provided to the RCMP"; and

IRRELEVANT

V. CRITERIA

A) LEGAL REQUIREMENTS

The Commissioner expected that CSEC conducts its retention and disposal activities in accordance with the *NDA*, the *Charter of Rights and Freedoms*, the *Privacy Act*, the *Criminal Code*, the *Library and Archives of Canada Act* and any other relevant legislation and Justice Canada advice.

B) MINISTERIAL REQUIREMENTS

The Commissioner expected that CSEC conducts its retention and disposal activities in accordance with ministerial direction, namely the requirements and approval frameworks outlined in the MDs on "Privacy of Canadians" and the "Collection and Use of Metadata" and the MAs allowing for the interception of PCs.

C) POLICIES AND PROCEDURES

The Commissioner expected that CSEC:

i) had appropriate policies and procedures that guide its retention and disposal activities;

ii) had personnel who are aware of and comply with the policies and procedures;

iii) had an effective management control framework to ensure that the integrity of the retention and disposal activities is maintained on a routine basis, including appropriately accounting for important decisions and information relating to compliance and the protection of the privacy of Canadians.

VI. METHODOLOGY

All applicable written and electronic records, files, correspondence and other documentation relevant to retention and disposal activities were examined, including policies and procedures and legal advice.

On June 8, 2010, CSEC provided the Commissioner's office with an overview briefing on its retention and disposal of intercepted communications.

CSEC managers and other personnel involved in retention and disposal activities were interviewed in the course of this review and provided demonstrations of retention and disposal activities.

The Commissioner's office, with the assistance of CSEC officials acting under its guidance, tested the contents of relevant databases and systems to ensure conformity with legal and ministerial requirements and associated policies and procedures with regard to retention and disposal activities.

The Commissioner's office assessed CSEC conformity with the criteria and developed conclusions respecting the objectives of this review. This is a report of the outcomes of the review.

Prior to forwarding a draft report to CSEC for comment, a meeting was held between the Commissioner's office and the CSEC personnel involved in the review to present a summary of findings.

VII. BACKGROUND

The ever increasing flow of information within the Global Information Infrastructure[9] (GII) has led to a corresponding increase in the interception and storage of communications by CSEC in the conduct of its mandated operations. In response to this and other internal challenges, CSEC initiated major technological changes such as the integration of its SIGINT intercepts from multiple databases into a Common Traffic Repository (CTR) which was completed in 2009, and the reconstitution of its IT Security program which was completed in 2008. These changes were meant to enhance the processing of this ever-increasing mass of intercepted [redacted] communications and improve CSEC ability to demonstrate compliance with the law.

As a Government of Canada (GC) institution, CSEC has a legal requirement to collect and store records. The *Access to Information Act* (*ATIA*) and the *Privacy Act* both recognize that citizens have the right, under specified conditions, to access GC records held in any form. Furthermore, federal institutions, such as CSEC, that collect and transmit personal identification data are responsible for that information throughout its

[9] The Global Information Infrastructure refers to "electromagnetic emissions, communications systems, information technology systems and networks, and any data or technical information carried on, contained in, or relating to those emissions, systems or networks" as per section 273.61 of the *NDA*.

life cycle and must protect privacy by ensuring that it cannot be breached either at rest or in motion, even when crossing department, geography or network boundaries.

These legal requirements reinforce the obligation for GC institutions like CSEC to maintain a comprehensive and complete inventory and description of their information holdings.

These requirements also make CSEC employees responsible for the preservation of official records and the disposal of transitory records, in support of CSEC IM goals. Records, whether transitory or official, required for an active request under the *ATIA*, litigation or official investigation cannot be disposed of, or deleted.

Official Record

The definition used by the CSEC Chief Information Officer (CIO) refers to a record that documents or provides evidence of CSEC's business activities. According to the CIO definition, official records include all media – paper and electronic including email messages and attachments. Examples of official records include: all briefing notes, directives, policies, final reports and recommendations; agendas and meeting minutes; work plans, schedules, assignments and performance results; all documents pertaining to the evolution of a policy; documents that lead to a decision, implement a policy or carry out an activity; and documents that require a signature (which must be printed and filed as hard copy). Official records may be kept until they meet archival status and need to be destroyed or turned over to Library and Archives Canada (LAC).

Transitory Record

Transitory records are defined in section 6.23 of the CSEC Information Management policy as a record only required for a limited time to complete a routine action or to prepare a subsequent record. They should be destroyed once they have served their purpose. These records may include e-mail messages and attachments; duplicate copies used for convenience only; information received as part of a distribution list; miscellaneous notices or memoranda on meetings and holidays; casual communications and personal messages; and widely available publications. Transitory material may be kept for a maximum period of five years.

Sub-section 12(1) of the *LACA* states that no government or ministerial record, whether or not it is surplus property of a GC institution, shall be disposed of, including by being destroyed, without the written consent of the Librarian and Archivist of Canada (LA) or of a person to whom the LA has, in writing, delegated the power to give such consent.

Instruments supporting this legislation include the Records Disposition Authority (RDA) which enables government institutions to dispose of records which no longer have operational utility, either by permitting their destruction, requiring their transfer to Library and Archives Canada (LAC), or by agreeing to their alienation from the control of the GC; and the related Records Retention and Disposition Schedules (RRDS) which set out a specific time limit for retaining records within an organization.

The focus of this review was on the retention and disposal of intercepted [redacted] communications including PCs and information about Canadians in the context of CSEC policy and technological upgrades. While these issues are common to both the SIGINT and IT Security programs, the distinct nature of their respective information and collection processes entails different practices for communications retention and disposal, which is why each program is addressed separately in this report.

While not part of the initial terms of reference, data collected (intercepted [redacted] retained and disposed under part (c) of the CSEC mandate – IRRELEVANT

IRRELEVANT

A. SIGINT Retention and Disposal Activities and Authorities

Recent changes in the technology used by the SIGINT program have allowed CSEC to incorporate some aspects of its compliance regime into the architecture of the program. Many of the controls CSEC places over its SIGINT retention and disposal practices in order to meet legal and ministerial requirements are now implemented through standardized automated processes within its operational systems. New measurable performance metrics also allow CSEC to quantify these automated compliance processes.

This was the first review of the retention and disposal of intercepted communications conducted by the Commissioner's office since the CTR became the consolidated traffic repository for Digital Network Intelligence (DNI) and fax traffic in 2009 and for Dialled Number Recognition (DNR) [redacted] traffic in March 2010.

1. Principles

The objective of the CSEC SIGINT program is to acquire and use information from the GII for the purpose of providing foreign intelligence, in accordance with the GC intelligence priorities as authorized by paragraph 273.64(1)*(a)* of the *NDA* (otherwise known as part (a) of the CSEC mandate). Intercepted [redacted] SIGINT private communications may be retained only when required to fulfill this mandate.

In pursuance of this objective, CSEC is responsible for the retention and disposal of the content of intercepted communications, collected [redacted][10] as well as selected and unselected metadata[11].

CSEC considers much of the SIGINT communications it intercepts a transitory record and does not retain it. Section 1.3 of OPS-1-11 states:

[redacted]

[11] SIGINT intercepts raw communications from the GII [redacted]

> CSE[C] is not required to retain or schedule the destruction of SIGINT data records to comply with the *LACA* since SIGINT data are considered to be transitory records. These should only be retained as long as is reasonably necessary.

2. Handling of intercepted communications under part (a) of the CSEC mandate

As noted above, intercepted SIGINT communications are considered transitory – until it is retained to fulfill the CSEC mandate.

Retained intercepted SIGINT communications are subject to controls with regard to:

- private communications;
- communications of Canadians located outside Canada; and
- information about Canadians.

These types of intercepted communications can only be kept if they meet an essentiality test defined by three conditions outlined in the MD on *Privacy of Canadians*:

- it contains foreign intelligence about capabilities, intentions or activities of a foreign entity; or
- it is essential to protect the lives of individuals of any nationality; or
- it contains information on serious criminal activity relating to the security of Canada.

Metadata is retained for [redacted] as per OPS-1-11[12].

IRRELEVANT

[12] OPS-1-11: Retention Schedules for SIGINT Data

IRRELEVANT

4. The Common Traffic Repository

CSEC SIGINT databases holding [redacted] SIGINT intercepted communications [redacted] were decommissioned and saw their contents migrated to a common platform (CTR[redacted] The CTR replaced the [redacted] database for fax intercept, the [redacted] database for [redacted] DNR communications, and the [redacted] database (also known as the [redacted] which stored all DNI including email, [redacted]

CSEC compliance requirements for retention and disposal were standardized and automated within the CTR architecture in an effort to better meet legal, ministerial and policy requirements.

CSEC users were given CTR access in mid-September 2008. The various SIGINT databases being replaced began to be partly decommissioned from that point on. The CTR was to have [redacted] before a database was decommissioned, to ensure it worked properly and prevent accidental losses.

SIGINT databases undergoing the decommissioning process were partially synchronized with the CTR during an overlap period. An automated process was used to mark traffic items as "viewed" in the CTR if an analyst had viewed it in one of the databases being decommissioned. According to CSEC, the databases being replaced by the CTR complied with CSEC retention and disposal requirements until they were fully decommissioned. Information in databases which had not reached the end of their retention schedule was migrated to the CTR for the completion of their retention period.

[redacted]

[redacted]

[redacted]

Deletion follows automated deletion scripts based on the retention schedules outlined in CSEC OPS-1-11[17], [redacted] all implemented deletion routines based upon established retention schedules. As there was [redacted] in [redacted] and [redacted] some traffic had to be [redacted] by the analyst (markings are described on p.16).

The move to a single repository also eliminated some redundancy by removing the need to annotate the same traffic item for deletion in more than one database in cases of duplicate intercepts. The CTR, in conjunction with the [redacted]

5. CTR data storage components

The CTR has [redacted] components of storage.

[redacted]

6. Organization of the file system storage

[redacted]

[17] OPS-1-11: OPS-1-11: Retention Schedules for SIGINT Data.

[redacted]

[20] In the CTR, [redacted]

The CTR [redacted]

There are two main types of directories that are used for unmarked traffic and correspond to specific retention periods – or schedules – identified in OPS-1-11[21]: one for mandate (a) data which is retained for [redacted] and referred to as [redacted] IRRELEVANT
IRRELEVANT

[redacted]

A third type, the [redacted] directory [redacted] is used for traffic that is marked for any reason. It is subdivided between traffic that is to be retained for either [redacted] Once traffic items reach their expiration date, they are individually deleted on a per item basis, [redacted]

Mandate (a)

Mandate (a) traffic marked as "having intelligence value" in the [redacted] directory [redacted] retention period) is moved to the [redacted] directory for a retention period of [redacted] In the case where mandate (a) traffic is marked as "having no intelligence value", it is moved from the [redacted] directory with the [redacted] retention period to the [redacted] directory with the [redacted] retention period, at the end of which the item will be deleted on a per item basis.

IRRELEVANT

7. Organization of database storage

Similar to the directories, the database also has a [redacted] that is used to store mandate (a) traffic that has been marked, either as "having intelligence value" or "having no intelligence value". Unmarked mandate (a) traffic is held in the [redacted] IRRELEVA
IRRELEVANT

Mandate (a)

The [redacted] partition contains mandate (a) traffic with an automatic default retention period of [redacted] Once traffic in the [redacted] is marked as "having intelligence value", it is

[21] OPS-1-11: Retention Schedules for SIGINT Data. These schedules are consistent with the [redacted] limit on the retention of metadata imposed by the Ministerial Directive.

automatically moved to the [redacted] where its default retention period is automatically updated to [redacted] from the date the marking is applied.

Traffic marked as "having no intelligence value" is moved from the [redacted] where its expiry date is updated to [redacted] from the date the marking was applied.

IRRELEVANT

8. CSEC corporate retention schedules

CSEC OPS-1-11 *Retention Schedules for SIGINT Data* policy applies to SIGINT data acquired from Canadian [redacted] sources.

SIGINT retention schedules have been established in OPS-1-11 for the purpose of satisfying the retention requirements laid out in paragraphs 273.64(2)*(b)* and 273.65(2)*(d)* of the *NDA*, by MD and CSEC operational requirements.

The automated retention periods in the CTR are consistent with the retention schedules listed in OPS-1-11, which in turn are consistent with the [redacted] limit on the retention imposed by the MD on metadata.

Mandate (a)

The retention period for mandate (a) intercepts is [redacted] unless otherwise marked. In the case where an intercept is marked as "having no intelligence value", its retention period is automatically fixed at [redacted] from the date of its marking. If the intercept is marked as "having intelligence value" the retention period is set at [redacted] from the date of the marking. LAC considers SIGINT information a transitory record, unless it is used to create an end-product report (EPR), at which time it becomes an official record and will be kept until it meets archival status and needs to be turned over to LAC. Transitory material may be kept for a maximum of [redacted]

Exceptionally, section 2.8 of OPS-1-11 states that traffic used to populate target knowledge databases [redacted] Except for metadata or a solicitor-client communication, approval to retain this material beyond the timeframe indicated in the policy, must be sought from a Director of an operational area on the recommendation of the Manager, SIGINT Oversight and Compliance.

IRRELEVANT

9. CTR annotations

Retention Annotations

The CTR default position automatically deletes unmarked data at the end of its retention period unless it is specifically marked for retention by an analyst.

Traffic can receive a marking as "having intelligence value" in the following ways:

a) an analyst marks the intercepted communications item directly by selecting a content assessment or a privacy annotation; or

b) a marking is automatically applied to the intercepted communications item when an analyst writes the related transcript in the CTR; or

c) the intercepted communications item is associated to an EPR in the [redacted] database.

Markings for retention are now affixed automatically for reported materials. The markings [redacted] (which stands for reported) [redacted] are affixed automatically when the traffic is reported [redacted] The analyst may also affix the self-explanatory [redacted] markings.

Privacy Annotations

MAs permit CSEC to unintentionally intercept one-end Canadian communications while obtaining foreign intelligence and protecting the computer systems or networks of the Government of Canada. There is a statutory requirement to destroy records with privacy annotations that have been viewed and deemed irrelevant. Records with privacy annotations may only be retained if they are relevant and essential as per OPS-1 section 3.3.

Intercepted communications with intelligence value and pertaining to a Canadian receive a retention date of [redacted] from the time the marking is applied. There are five applicable privacy annotations in such a case: INCA (one-end Canadian located in Canada), OUCA (one-end Canadian outside Canada), INCAS (in Canada/Solicitor Client Privilege), OUCAS (outside Canada/Solicitor Client Privilege) and IAC (containing information about a Canadian).

In the case of intercepted traffic with a Canadian or privacy component but no intelligence value, the markings are the same except for the addition of the letter "N" – as in "no intelligence value". The applicable annotations are: INCAN, OUCAN, INCASN, OUCASN and IACN.

10. The process by which an item is retained

Once an analyst applies a retention marking to an intercepted communications item, the system immediately and automatically makes an entry in a table to indicate the need to update the expiry date for the item; next, in an automated process that occurs [redacted] the system automatically moves the metadata from the database [redacted] placing the item in the [redacted] queue, registering the new expiry date for the traffic item with [redacted] status; then, in an automated process that occurs [redacted] the system automatically [redacted] queue from [redacted] directory, thereby removing the traffic item from the [redacted] queue. The traffic item will now be retained for a period of [redacted]

11. CTR traffic backups

The [redacted] for mandate (a) IRRELE intercepted communications marked as "having intelligence value" are backed up [redacted] and retained for [redacted] from the date of marking. The [redacted] backup system is a [redacted] commercial product called a [redacted] which is an automated system within which backup [redacted] are maintained and managed. The [redacted] can be deleted from the [redacted] sooner than [redacted] if the corresponding file on the primary file system is removed, initiated by a marking change or deletion request. This initiates an individual deletion in the [redacted] for this file on the day that the [redacted] had been removed from the primary file system. The [redacted] space is reused within the [redacted] pool.

File system backups

The [redacted] directories are backed up [redacted] The backup mechanism is not currently able to [redacted] in the [redacted] directories and a backup strategy is being developed for those directories.

Database backups

The database has [redacted] incremental backups which document changes for [redacted] and [redacted] incremental backups. Each full database backup contains the entire database contents. Full backups are performed on a [redacted] schedule and the latest of [redacted] backups are available. The [redacted] oldest backup is set as expired in the [redacted] The database carries a total backup of [redacted]

<u>12. Records disposition authority for SIGINT</u>

As previously noted (see page 9), the RDA, or Authority, is the legal agreement allowing CSEC to dispose of its official records. The SIGINT RDA identifies criteria for records to be deemed of historic or archival value in order to be preserved at LAC facilities once their retention period has ended and CSEC agrees that these records no longer have any legal or operational requirements. The RDA also allows for expired records deemed of no archival value to be destroyed.

The Commissioner's office obtained and reviewed a copy of the signed SIGINT RDA.

Mandate (a)

RDA No. 2008/003 is the authority for records generated in support of the SIGINT function. It was signed by the CSEC Chief Information Officer (CIO) and the LA on July 25, 2008.

Mandate (c)

IRRELEVANT

IRRELEVANT

13. Memoranda of Understanding

A Memorandum of Understanding (MoU) between CSEC and the RCMP signed in June 2009 states that information disclosed under this arrangement shall be administered and maintained, and disposed of in accordance with the law that applies to record retention and personal information and all applicable legislation, policies and guidelines.

IRRELEVANT

14. Retention and disposition schedules for SIGINT

Retention and disposition schedules specify the period allotted for the retention of a record or specific types of records until the time of disposal.

The rules-based configuration of the CTR has automated the application of retention and disposition schedules. Each traffic item sent to the CTR is tagged by the system with a set number of days to be retained from the moment its metadata is loaded. This fixed retention period can only be changed once an analyst applies a marking or when SIGINT Programs and Operational Compliance (SPOC) issues a request to delete the traffic item.

15. *LACA* Records Retention and Disposition Schedule

The Records Retention and Disposition Schedule (RRDS or Schedule) is a document created under the authority of the *LACA* that establishes a timetable for the life of a record from its creation through its maintenance stages until its final disposition, including the disposition action: transfer to LAC facilities, disposal or alienation. Schedules need to be established for each CSEC activity in accordance with *LACA*, CSEC Policies, MAs, MDs and MoUs.

The RDA acts as a foundational document for establishing the RRDS as it lists the criteria for identifying archival material covered by the Schedule and provides the

IRRELEVANT

complete description and purpose of holdings records as well as the type of disposition action to occur on the information identified as archival: transfer to LAC facilities, disposal or alienation.

The CSEC Information Holdings Services (IHS) is responsible for the management and safeguard of the information created by the various CSEC business lines as well as the administration of the CSEC Records Retention and Disposition Program. IHS crafts schedules in conjunction with the CSEC office of primary interest. The retention timeframes and disposition methods are developed based on the value of the information – business, administrative, financial, historical and legal – over time. The retention period must specify the duration of record custody or control by CSEC and specify a point in time when – or if – it must be transferred to the custody or control of the LAC in accordance with the terms and conditions set in the RDA.

In case of transfer to the custody and control of LAC, all CSEC records become subject to the *Access to Information Act* (*ATIA*). In such a case, LAC shall consult with CSEC on all requests for access to these records. Similarly, LAC may not destroy CSEC records in its custody and control without the prior consent of CSEC. The LA shall notify CSEC of a decision to destroy such records as CSEC has the right to repossess these records if it wishes to do so.

All CSEC branches subject to an RDA are responsible for undertaking periodic and systematic reviews of their records designated as archival for the purpose of notifying LAC that they have reached archival status.

Mandate (a)

The SIGINT RRDS was signed by CSEC stakeholders and the LA on October 6, 2010, in accordance with the *LACA*. It covers SIGINT material detailed in the corporate file plan. All numbers within a file number series (hardcopy EPR with the information attached) have been given a [redacted] disposition timeframe. The RRDS lists exceptions to the [redacted] disposition and indicates the specific disposition time that applies to these cases. The RRDS has since been implemented and, according to CSEC, SIGINT information that has met its retention limit is being handled accordingly.

Raw – or unprocessed – communications intercepts are exempted from the RRDS and is covered under OPS-1-11 retention schedules for SIGINT information, as raw data never meets archival status.

IRRELEVANT

16. Overwriting as a means of disposal

The digitization of records has given rise to difficulties in achieving destruction and can make destruction difficult to verify. The overwriting process is the best way to ensure that data has been destroyed and not simply made invisible to the user by the system.

The CTR utilizes overwriting as a means of disposal. Overwriting does not simply delete data in the regular sense of the term: new material coming into the system takes the space of material held in a storage medium such as a [redacted] thereby writing over expired data – making it no longer recoverable.

Once intercepted communications are marked for "no intelligence value" by analysts, the marked traffic may be viewed for additional [redacted] at which point it is deleted from the repository.

Data singled out for destruction is to be overwritten once it reaches its deletion date, but, according to CSEC, data awaiting deletion is usually overwritten much sooner [redacted] the overwriting process to make more room for the new incoming data. Depending on the circumstances, CSEC states that a [redacted] may be overwritten within [redacted]

Intercepted communications that have not been viewed within the scheduled time period will be overwritten by new incoming data, also according to CSEC, often in a much shorter time period than its scheduled time frame.

17. The process by which an item is deleted

Traffic items are deleted through an automated process which moves the metadata from database [redacted] It places the item to be deleted in a queue to be moved from the [redacted] directory and registers the new expiry date in a table with [redacted] status. The automated system process moves [redacted] that are in the queue from the [redacted] directory, [redacted] removing the item from the move [redacted] queue. It deletes the traffic [redacted] from expired traffic with [redacted] status and updates the expiry record from [redacted] to [redacted] [redacted] an automated process deletes the metadata for expired traffic with the [redacted] marked deleted and deletes the expiry record.

Mandate (a)

Items marked as "having no intelligence value" are queued for deletion with a date set to [redacted] from the moment the marking is applied. The system checks for marked traffic [redacted] Depending upon [redacted] when the traffic was marked and when the deletion process ran, the traffic item could have remained on the system for a further [redacted] – still well within the required [redacted] to deletion.

IRRELEVANT

18. Disposal of traffic backups

Each backup[redacted] has its expired data overwritten by the newer data. Every [redacted] the [redacted] backup system searches for the existence of the [redacted] directory and each traffic item on the CTR file system. If a traffic item has been removed from the file system, the existing backup of that traffic item and/or directory is marked as expired in this system, and gets overwritten.[redacted]

In January 2011, SSD and CIO storage services implemented a backup strategy for the [redacted] for all traffic[redacted] contained in the[redacted] directories. This strategy is separate from that of the [redacted] directories. Due to the number of files to be backed up on a [redacted] basis in the [redacted] directories, files are first grouped together into a single file based upon the date and time of arrival in the CTR. This larger group of files is then moved to the[redacted] as a single file.[redacted] management software is used to mark these files as expired, according to the original retention schedule [redacted] Once marked as expired, the[redacted] cannot recover these grouped files. The corresponding[redacted] storage [redacted] are then reused in the[redacted] storage system.

B. Information Technology Security

1. Cyber Defence Operations

The first Cyber Defence Operation (CDO) or Computer Network Defence activity, as it was then known, took place in 2003 following a request for assistance from the Department of National Defence. This undertaking required the development of new technical capabilities and concepts of operations as well as proper authorizations. An MA was sought and obtained from the Minister of National Defence in January 2004. Specific policies were subsequently drafted with a first version promulgated in June 2005.

Following this initial undertaking, similar activities were implemented with other federal department clients until October 2006 at which time CSEC suspended its IT Security activities conducted under MA following concerns of potential non-compliance with operational procedures[23], leading to an extensive reconstitution of the IT Security

[23] CSEC Report on Investigation into IT Security Compliance Relating to Operations Conducted under Ministerial Authorizations, December 11, 2006.

program policy framework along with changes to technologies and procedures. The program was officially restarted in March 2008.

Ministerial authority for CDO operations has since evolved from acquiring one individual MA related to one specific client within a specific timeframe, to a horizontal MA covering a class of activities conducted within a 12-month period during which approved activities can be conducted for multiple clients.

2. IT Security retention and disposal principles

The objective of the CSEC IT Security program is to help protect computer systems or networks, and to provide advice, guidance and service to GC institutions (i.e., "the client") as authorized by paragraph 273.64(1)*(b)* of the *NDA*, otherwise known as part (b) of the CSEC mandate.

In support of this objective, CSEC CDO installs and operates a [redacted] system which [redacted] processes and stores communications traffic entering and leaving designated client networks in order to detect, analyze and mitigate externally-based malicious activities. Because such operations may involve the interception of PCs by CSEC, a valid MA must be in force prior to the start of, and throughout an operation.

Section 3.5 of OPS 1-14 requires that all information obtained and produced by CSEC during cyber defence activities must be securely stored, with limited access.

Contrary to the SIGINT concept of operations, IT Security does not collect communications surreptitiously; it does so in response to a formal demand from a GC institution. As a first step in establishing and conducting a CDO activity, CSEC must first receive a request from a client. Once prerequisite approvals have been received from both CSEC and the client and technical issues have been addressed, CDO may install and operate a cyber defence sensor system under MA, in accordance with a MoU signed by CSEC and the client.

As per the *NDA*, and OPS 1-14, *Operational Procedures for Cyber Defence Operations Conducted under Ministerial Authorization*, the data selected for copying in the course of a CDO must not be directed at Canadians or other persons in Canada. The selection process must always be aimed at detecting, analyzing or mitigating cyber threats and the selection process must be auditable as per OPS-210-50-10, *Recognizing and Handling Private Communications and Other Data in CND Operations* allowing for the demonstration of policy compliance, if required. The copied data remains the client's property until it is retained by CSEC for further analysis, at which point CSEC becomes custodian of the data and is responsible for handling it in accordance with the proper legal, ministerial and policy requirements.

3. The cyber defence [redacted]

[redacted] at which time it was officially deployed under the MA regime.

[redacted]

[24] In the context of IT Security operations, the term [redacted] but has a meaning similar to the latter.

[redacted]

4.[redacted] infrastructure architecture and components

The [redacted] has policy requirements built into its architecture. Processes such as retention schedules and deletion scripts are automated and privacy annotation options prompt were introduced. The [redacted] configuration allows for the control of user activity for monitoring, auditing and proof of compliance purposes and the generation of reports capturing and showing qualitative and quantitative information to demonstrate proof of compliance with various CSEC requirements.

The [redacted] must offer flexibility in its implementation due to various constraints such as the [redacted]

The [redacted] infrastructure is segmented in components – or subsystems – each accomplishing a different function. The four primary architectural components are collection, detection, storage [redacted] All components operate under the same configuration, MAs and management control framework, and are subject to the same schedule and deletion scripts. This modular design makes it adaptable to various deployment requirements.

Collection subsystem

The collection subsystem is characterized by its three main functions: [redacted]

[redacted]

[25] [redacted]

[26] [redacted]

[27] [redacted]

[redacted]

Detection subsystem

The detection subsystem is responsible for [redacted]

Storage subsystem

The storage subsystem provides the CDO analysts with considerable storage for detection tool outputs such as alerts and metadata [redacted] and analyst workspace to further manipulate data. This subsystem also contains reference databases and processing components to move the data and detection results to the proper location or system for analysis.

The deletion of data (explained on p.32 below) is managed by this subsystem in accordance with applicable authorities, policies and agreements.

[redacted] ***subsystem***

[redacted]

[28] [redacted]

[29] Analyst-driven tools are executed manually by the analyst, as opposed to being executed automatically, according to a script.

[redacted]

6. The process by which an event is retained in the IT security program

The process begins when an analyst receives an alert about the identification of an event[30] in the [redacted] data. The analyst must then determine whether the event warrants further investigation.

If the analyst decides that the event is worth investigating further, he selects and transfers it from the specific [redacted] [redacted] to the CDO repository codenamed [redacted][31].

7. Relevancy test

As a next step, the analyst must determine if the alert and associated selected data are relevant to part (b) of the CSEC mandate "to provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada".

In the case where the event is deemed not relevant, it is recorded as such on the alert. No further action is taken, and the client data associated with the alert is not retained and the data in question remains under the control of the client.

If the data associated to the event is deemed relevant, the analyst must provide a rationale for the relevancy. A rationale is required whether the event contains a PC or not. There are four standard options for the rationale justifying the retention of the event:

- characteristics observed are similar to previously discovered malicious activities;
- indications exist that the computer system is attempting to affect the confidentiality, integrity or availability of a GC system;
- the event will be used to characterize normal computer behaviour for the purposes of identifying anomalous behaviour; and
- the event will be used to improve an existing detection capability.

The analyst also has the fifth option of drafting a custom rationale if the previous four are not applicable.

[30] An event is any observable occurrence in a system or network. In the specific case of [redacted] MA CDO activities, an event is an activity that triggered an alert. Multiple events that are part of the same malicious activity may be determined to comprise an incident, which may become the subject of one or more reports.

[31] The [redacted] system includes individual [redacted] codenamed [redacted] which contain "raw" [redacted] communications that may include PCs and personal information and information disclosed to CSEC under the client department's *Criminal Code* and *FAA* authorities; it also includes the CDO Personal Information Bank which contains personal information that has been used and retained for the purpose of protecting information and systems of importance to the GC. Please refer to annex C for a more detailed explanation of the various components of the [redacted] systems.

8. Identification of private communications

In the case where the alert and the associated selected data are determined relevant by the analyst, a pop-up window appears, prompting the analyst to indicate if the event contains a PC before the transfer process [redacted] to the database can be completed.

The prompt also requires the analyst to identify the number of PCs and identify a justification for retaining the PC in the rationale field of the window.

If the selected data is relevant and does not contain PC the analyst can set the PC count to zero and the rationale field in the window will be disabled and no options will be offered as they are unnecessary. If the PC count is set to a number other than zero, the rationale option becomes selectable and its drop box menu offers the following choices:

[redacted]

9. Essentiality test

In the case where the selected data contains a PC, the analyst must then determine whether the data is essential to identify, isolate or prevent harm to GC computer systems or networks. If the PC is determined to be essential, the selected data can be retained and used by CSEC.

Once the PC count and the rationale and essentiality tests have been addressed, the event is marked as retained, date stamped and moved to the [redacted] repository for further analysis.

Retained events are kept until they meet their retention date beginning at the moment of retention as the event is under client custody until active steps are taken by the analyst to retain the data. Any selected event not retained, remains [redacted] where it will be deleted according to a deletion script.

10. Analysis

The analyst uses the [redacted] system to assess the generated alerts and determine and record their relevance. It is within this environment that the analyst will assess whether the selected data contains a PC, and if so, whether it is essential and can therefore be retained. Before the selected data can be transferred to the [redacted] system, at which point it comes under CSEC ownership, the [redacted] system prompts the analyst to apply the proper privacy annotation to the data. Only once this process is done can the [redacted] data move to the [redacted] system where it can be used and retained properly and used to produce CDO reports or to develop or further refine IT Security tools. Only data under CSEC control can be used for these purposes.

11. Data storage

All [redacted]-produced CDO Reports are loaded into the Threat and Vulnerability Assessment System (TVAS) system which is used to manage report release authorization and tracking. All output of information to be disseminated outside of the CDO team must be in the form of a CDO Report and must be reviewed and approved for release prior to dissemination, in accordance with OPS-1-14 subsections 3.21 through 3.26.

12. Data disposal

Transitory data is automatically deleted via scripts based on a set schedule. Deletion scripts are run against the collection repositories on a daily basis.

As is the case for the SIGINT repository, storage space affects storage time as, according to CSEC, [redacted] communications are usually overwritten before the maximum amount of time allowed by policy is reached because the storage limit of the traffic repository is reached sooner. Only metadata is retained for its full retention period.

13. The process by which an event is deleted in IT Security

[redacted] data is deleted via the [redacted] deletion script implementation program codenamed [redacted] which runs on a [redacted] cycle and checks both the [redacted] and the database ([redacted] is launched automatically from a [redacted][32] which [redacted] the execution of the delete function at a [redacted] time and date. MoUs, MAs, and operational instructions prescribe deletion requirements, such as the retention period, while [redacted] executes the actual deletion. The data retention period is [redacted] to [redacted] ensuring the retention period of [redacted] is not overrun while allowing for extra time to verify compliance.

Client ID, MA date, MoU date, retention period and directories to monitor or exclude are configurable for [redacted] A detailed description of what specific files are monitored and the criteria used to determine data age are found in the [redacted] configuration file.

Events that are not marked to be retained, and whose retention times are identified as greater than [redacted] are automatically deleted and any information entered regarding that event is also deleted. According to CSEC, every day, [redacted] files are tested to see if either the MoU with the client or the MA are expired or whether it has gone over the retention period, in which case, the file gets deleted.

[redacted]

The [redacted] also has the ability to delete on a mass basis through the [redacted] mode of the [redacted] script. This mode will delete every single monitored file, no matter their creation date.

14. How deletion is verified

After a run, [redacted] will send a log. If the option track-success is used, every successful deletion will be logged. It will also send a log in cases where it cannot read the content of a directory or a file, or if it is unable to delete a file. As a further precaution, a script is run on the [redacted] deletion log to look for errors that could occur during the deletion process. This script looks for key words like ERROR or FAIL and sends the results to a file.

Each week, an analyst is responsible for checking [redacted] for the checks it ran and the check that was run on its deletion log, to investigate anomalies that may surface. The analyst is also responsible for checking the directory, retention period and expiry of the MA or MoU for each specified client under his or her responsibility.

The first week of each month, an analyst checks the relevant MoU and MA to ensure that they are not going to expire. The analyst also reviews the retention values to ensure that they are correct.

In the case where a file should have been deleted but was not, the analyst will delete it and send an email to IPOC describing what happened and highlight any changes to the deletion process that may be required.

Record of client data deletion

The Team Leader (TL) is responsible for recording the fact that the data for a client has been deleted. The delete checklist that is used to verify deletion is found at "Delete Check" and deletion tracking sheets for each client are stored in CERRID. The TL is responsible for filing the destruction records for each client.

15. Exceptions to [redacted]

Directories which are too large for [redacted] to monitor are excluded from its application. The data in these directories are deleted using a "find" command with the "delete" option in the [redacted] The find command is launched automatically by the [redacted] on the main System Logs servers. A find command is run weekly on the main client data directories on the [redacted] in order to verify that the client data is deleted.

Some databases have their own deletion scripts setup to remove client data from the database tables when the data expires, whether it is through expiration of the retention period, or termination of the MA or MoU.

Individuals are responsible for ensuring the deletion of their own data if it is copied from a main [redacted] server to a system which is not monitored, such as an analyst workstation.

16. Ministerial authority reporting

IT Security has an MA requirement to report on the number of PCs that are used and retained by CSEC. Once used and retained, PCs are marked as such in the CDO database. As previously noted, the [redacted] architecture allows for the number of PCs in the database to be generated for MA reporting or as required.

17. Active Network Security Testing (ANST)

While also part of the IT Security Program, the Security Posture Assessment (SPA) Active Network Security Testing (ANST) operates under a different concept than that of CDO. The CSEC ANST database, codenamed [redacted] is an exception within the mandate (b) framework to which a different set of rules applies.

ANST storage

The ANST management control framework requires that each assessment has its own [redacted] database hosted on a separate server in order to ensure data separation during concurrent assessments and facilitate the obligatory data deletion at the end of an assessment.

The data obtained from the client site in the course of an ANST activity is transferred and stored in an [redacted] database, which is classified secret and kept separate from the other IT Security systems. The [redacted] database is automatically populated from the results of the ANST activities performed and it therefore contains all of the ANST assessment data, including information on all the sessions, all actions performed as part of the assessment, the results and the information on the computers from the target network.

ANST retention

The ANST management control framework requires that, exceptionally, some information be retained as part of the ANST Assessment Client File. This includes the letter of validation, client briefings and CSEC-retained versions of final reports, the authorized target list, the active monitoring record, and business communications between the client and CSEC, all of which are subject to the IT Security RDA and retention and disposition schedule.

ANST disposal

No data is archived from [redacted] as it is all deleted at the end of an assessment as per CSEC policy OPS-210-50-14 which requires that all collected data be destroyed within [redacted] of delivery of the final report to the client. The [redacted] manager must ensure and then confirm in writing to the client that all relevant information has been destroyed.

18. Records disposition authority for IT Security

The Commissioner's office obtained and reviewed a copy of the signed IT Security RDA.

Mandate (b) Records Disposition Authority

RDA no. 2002/011 is the Authority for IT Security and it came into effect on August 19, 2002. It was signed solely by the then-National Archivist (now LA) of Canada.

Interpretation of mandate (b) RDA

Given the fact that RDA 2002/011 predates most current IT Security initiatives, CSEC sought an opinion from LAC regarding the disposition of records generated by its current cyber defence activities – specifically its SPA.

In a letter of interpretation for the RDA dated September 22, 2010, the LAC archivist responsible for the disposition of CSEC records explained that while it did not explicitly anticipate the form and nature of the activities currently carried out in the increasingly complex field of protecting the GC information infrastructure, the basic assumptions behind the mandate (b) archival appraisal and resulting terms and conditions remain valid.

According to LAC, the archival objective behind this RDA is to maintain a "high level" perspective by documenting higher level requirements and the nature of coordination within the GC required to implement effective defences against cyber attacks, thereby documenting threats and the overall direction of CSEC programs and activities developed to meet them. It is not meant to document the purely technical aspects of the program.

19. Records Retention and Disposition Schedules for IT Security

Corporate Retention Schedule

CSEC OPS-1-14 holds that retention and disposition schedules must be applied to all MA-based IT Security data, regardless of media or location. CSEC retention schedules for CDO data are found in section 5 of OPS-1-14. As ownership of the [redacted] communications determines the schedule, section 5 differentiates between data under client control, and data under CSEC control.

Data that has been either [redacted] or selected only, and not under CSEC control, is considered to be transitory and is subject to retention and detention schedules noted in the CDO MA in force which dictates that retention will be no longer than [redacted] from the date the data was [redacted] In the case of a suspension or termination of the MoU, this data will be deleted within [redacted] from notification of suspension or termination of the MoU or [redacted] from date [redacted] whichever comes first.

If the data has been used or retained by CSEC, therefore under CSEC control, then the deletion period will be in accordance with corporate retention and disposition schedule.

Used or retained data is subject to access to information requests and must be accounted for in the Personal Information Bank[33].

If a CDO MA expires and a new one has not been approved, then upon expiry of the MA, the cyber defence team must immediately cease [redacted] selecting and analyzing selected data, except for that which is already under CSEC control. If the data has been used or retained then the deletion period will be in accordance with the appropriate retention and disposition schedules.

Mandate (b) Retention and Disposition Schedule: The IT Security Functional Retention Schedule

Having specified no retention periods for records identified in RDA 2002/11when it was signed in 2002, CSEC agreed to specify retention periods for these archival records within one year of the signing of the RDA agreement. The CSEC IT Security Functional Retention Schedule was signed by the Director, Program Management and Oversight (PMO) and the LA on June 23, 2011. The schedule which reflects RDA 2002/011 terms and conditions, assigns a specific retention period and disposition for each IT Security activity with a functional file number.

CSEC stated that the Schedule has since been implemented and IT Security information that has met its retention limit is being disposed of accordingly.

Mandate (c) Retention and Disposition Schedule

IRRELEVANT

20. Retention and disposal of hard copy intercepted [redacted] communications in hard copy format under Parts (a), (b) and (c) of the CSEC mandate

Hard copy material is retained in secure filing at CSEC until it meets archival status as per the SIGINT and IT Security RDAs and RRDSs at which time they are to be turned over to the custody of LAC. LAC facilities can currently accommodate information up to the top secret level and are in the final stages of having one of their top secret vaults accredited to hold COMINT-level product.

[33] The Office of the Privacy Commissioner defines the Personal Information Bank as a listing of all personal information held by a [Canadian] government institution that has been used, is being used, or is available for use for an administrative purpose or is retrievable by a person's name, identifying number, symbol or other individual identifier. The *Privacy Act* requires that government institutions report to the public on how this personal information is handled by publishing PIB descriptions in Info Source, which is released annually by the Treasury Board Secretariat; individuals use Info Source to find out how and where their personal information is used and retained, so that they may exercise their rights of access and correction.

VIII. FINDINGS

A) LEGAL REQUIREMENTS

Finding no. 1: Compliance with the Law

Based upon the information reviewed and the interviews conducted, CSEC conducts its retention and disposal of intercepted [redacted] communications in accordance with the law.

Finding no. 2: Protection of the Privacy of Canadians

Retention and disposal periods set out in CSEC policies are reasonable.

The length of time that records having privacy implications are retained and disposed of do not unreasonably violate the privacy of Canadians.

Finding no. 3: Protection of the Privacy of Canadians

CSEC activities respecting the retention and disposal of intercepted [redacted] communications include measures to protect the privacy of Canadians, as required by law.

CSEC takes measures in the design of its systems for the retention and disposal of intercepted [redacted] communications to promote compliance with the law and the protection of the privacy of Canadians. For example:

- The integration and automation of policy requirements in the architecture of the SIGINT and IT Security storage systems help ensure that only essential intercepted [redacted] communications are retained and non-essential communications are destroyed;

- The ability of SIGINT and IT Security to generate reports which include new measurable performance metrics assists CSEC in quantifying its automated processes for a better demonstration of compliance. CSEC now has the ability to report on trends, statistical and contextual information as a complement to traditional incident-based reporting.

- The integration of information from multiple sources to a centralized storage point has made compliance reporting more reliable and consistent. Specifically, the move to a single SIGINT database has eliminated the need for analysts to manually annotate [redacted] the same communications in more than one database;

- A significant improvement in the SIGINT CTR architecture, from a compliance perspective, is that the automated default positions are set to delete instead of storing; [redacted]

- The configuration of these systems now allows for better control of user activity which has a direct impact on monitoring and auditing; and
- CSEC met the legal requirements of the *LACA* by developing and signing RDAs and RRDSs.

Finding no. 4: Follow-up to Commissioner's reviews

CSEC has addressed the previous associated recommendations of the Commissioner to establish records management authorities, and retention and disposition schedules.

IRRELEVANT

B) MINISTERIAL REQUIREMENTS

Finding no.5: Ministerial Direction

Based upon the information reviewed and the interviews conducted, CSEC conducts its retention and disposal of intercepted [redacted] communications in accordance with ministerial direction.

As noted in the section on legislative requirements, CSEC has adopted a policy-based and technology-driven approach to its information management practices. Many of the controls it places over its SIGINT and IT Security retention and disposal practices in order to meet legal and ministerial requirements have been automated and standardized.

New measurable performance metrics also allow CSEC to quantify these automated compliance processes. The configuration of the systems for both the SIGINT and IT Security programs now allows for the control of user activity and the capture of information and statistics for monitoring and auditing purposes and the generation of reports capturing and showing qualitative and quantitative information to demonstrate proof of compliance with various CSEC requirements, including the number of PCs in the database to be generated for MA reporting – or as required.

Finding no. 6: Supporting the Review by the Commissioner's Office

CSEC fully supported the conduct of this review.

During the conduct of this review, CSEC addressed in a timely fashion extensive requests from the review team for documentation, briefings and meetings with CSEC employees involved in retention and disposal activities.

C) POLICIES AND PROCEDURES

Finding no. 7: Appropriateness of Policies and Procedures

CSEC has comprehensive policies and procedures relating to the retention and disposal of intercepted [redacted] communications; however, certain language in policy should be clarified (finding no.8 and 9 refer).

The Commissioner expected that CSEC would have appropriate policies and procedures to guide its retention and disposal activities. The Commissioner's office reviewed the following policies and procedures that were in effect during the review period:

a. OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities* (dated December 1, 2010).

OPS-1 provides direction to anyone conducting activities under the CSEC mandate and authorities to ensure that the privacy of Canadians is protected in the conduct of CSEC activities by complying with the laws of Canada, complying with MDs – including, but not limited to the MD on Privacy of Canadians, the MD on Collection and Use of Metadata and the MA authorizing the interception of private communications.

b. OPS-1-8, *Active Monitoring of Operations to Ensure Legal Compliance and the Protection of the Privacy of Canadians* (March 18, 2008, December 20, 2008 and March 11, 2009)

OPS-1-8 provides direction regarding the CSEC active monitoring program, established to ensure compliance with policy instruments addressing legal compliance and protection of the privacy of Canadians in the conduct of SIGINT and IT Security operational activities under CSEC mandate and authorities.

Finding no. 8: OPS-1-11

The parts of OPS-1-11 concerning retention and disposal of transitory records and those records used in reporting are confusing and should be clarified.

c. OPS-1-11, *Retention Schedules for SIGINT Data* (October 31, 2007)

OPS-1-11 provides solid direction on retention schedules for SIGINT data. However, section 1.3 of CSEC OPS-1-11 is a source of confusion. It states that CSEC is *not* required to comply with the *LACA* in its retention or destruction scheduling of SIGINT data records since they are considered to be transitory records that should only be retained as long as is reasonably necessary. However, section 2.4 of the same policy indicates that hard copies of traffic used in SIGINT reporting must be retained [redacted] with its corresponding report and that older files must be shipped to the CSEC Information Holding Services (IHS) for permanent retention. By definition, a record held [redacted] is not transitory and its retention and disposal must necessarily comply with the *LACA*. Sections 1.3 and 2.4 should be made consistent to avoid confusion.

In spite of the statement in its section 1.3, that all SIGINT material is transitory, OPS-1-11 is consistent with the [redacted] limit on the retention of metadata imposed by MD and the automated retention schedules which do not go beyond [redacted]

Finding no. 9: Use of language by SIGINT and IT Security

To avoid confusion, the use of terminology relating to retention and disposal activities used by the SIGINT and IT Security programs should be reconciled and made consistent.

While SIGINT uses policy to define its records as transitory, IT Security policy has no specific policy defining its records as official or transitory. This situation illustrates a common challenge encountered during this review relating to policies and procedures for retention and disposal; SIGINT and IT Security programs use a common terminology with somewhat different meanings. Years of compartmentalized functions and separate application development have created an environment in which the same terms used by SIGINT and IT Security are used without a common understanding of those terms' specific definitions. A consistency in meaning of definitions pertaining to such terms as "official" and "transitory" records as well as "interception" [redacted] would be useful for compliance assessment. The absence of consistent terms can lead to confusion. Building a common terminology as part of a master information management program could remedy this situation.

d. OPS-1-13, *Procedures for Canadian* [redacted] [redacted] *and Joint CSEC-CF Activities* (December 1, 2010)

OPS-1-13 documents the procedures for Canadian SIGINT collection activities including retention and disposal guidelines.

e. OPS-1-14, *Operational Procedures for Cyber Defence Operations Conducted Under Ministerial Authorization* (March 11, 2010)

OPS-1-14 governs CSEC Cyber Defence Operations conducted under the authority of the *NDA* and a MA.

f. IRRELEVANT

g. IRRELEVANT

h.

i. OPS-210-50-02, *Instructions for Commencing and Ceasing Cyber Defence Operations* (March 19, 2010).

OPS-210-50-02 operational instructions apply to cases where data needs to be deleted after a suspension or termination.

j. OPS-210-50-06, *Active Network Security Testing (ANST) Active Monitoring* (January 6, 2010).

OPS-210-50-06 operational instructions address the requirements for conducting Active Monitoring of ANST, in response to OPS-1-8, *Active Monitoring of Operations to Ensure Legal Compliance and the Protection of the Privacy of Canadians.*

k. OPS-210-50-10, *Data Handling in Cyber Defence Operations* (July 15, 2010).

OPS-210-50-10 operational instructions provide direction in the handling of all data [redacted] by CSEC for cyber defence operations. The recognition, use, and retention of PCs, in whole or in part, and metadata associated with a PC that can identify one or both communicants or the communication itself are also addressed in these instructions as directed in OPS-1-14, *Operational Procedures for Cyber Defence Operation Conducted Under Ministerial Authorization.*

l. OPS-210-50-11, *Cyber Defence Operation (CDO): Compliance Monitoring* (March 11, 2010).

OPS-210-50-11 operational instructions address the requirements for conducting Compliance Monitoring (CM) of Cyber Defence Operations (CDO), in response to OPS-1-8, *Active Monitoring of Operations to Ensure Legal Compliance and the Protection of the Privacy of Canadians.*

m. OPS-210-50-14, *Corporate Filing Requirements in IT Security SPA & CND MA Activities* (December 1, 2008).

OPS-210-50-14 operational instructions address the requirement that all collected data be destroyed within [redacted] of delivery of the final report to the client.

n. OPS-210-50-15, *Instructions for Deployment of Tools for Cyber Defence Support* (February 8, 2010).

OPS-210-50-15 operational instructions outline the mandatory instructions for the deployment of tools for Cyber Defence Support. It sets out measures to protect the privacy of Canadians in the handling of information acquired during the course of deploying tools for Cyber Defence Support, as required by OPS-1.

Finding no. 10: Awareness of Personnel

CSEC employees interviewed and observed were aware of relevant policies and procedures and their application to the retention and disposal of intercepted [redacted] communications.

Based upon the information reviewed and the interviews conducted, the Commissioner's office was satisfied that CSEC employees complied with the policies that apply to retention and disposal activities. In interviews, CSEC employees demonstrated a solid understanding of applicable policies and procedures and their purpose.

A records management audit conducted by the CSEC Directorate of Audit, Evaluation and Ethics conducted in 2008 noted that CSEC staff would benefit from additional guidance on the management of records.

CSEC is continuing its efforts towards creating an IM/IT community competency development program. In 2009-2010, CSEC developed a Career Management Program framework and strategy, a Learning and Development strategy and curriculum for the CSEC IM/IT staff.

In its efforts to develop employee learning plans, establish career paths and streamline the hiring process, CSEC continued its efforts towards creating an IM/IT community competency development program. In 2009-2010, CSEC developed a Career Management Program framework and strategy, a Learning and Development strategy and curriculum for its IM/IT staff.

Finding no. 11: Management Control Framework

An automated management control framework has been integrated into the architecture of both the SIGINT and IT Security databases; IT Security has supplemented this with the close monitoring by designated managers of the disposal of [redacted] communications.

The Commissioner expected that CSEC had an effective management control framework to ensure that the integrity of the retention and disposal activities is maintained on a routine basis, including appropriately accounting for important decisions and information relating to compliance and the protection of the privacy of Canadians.

Here the SIGINT and IT Security programs diverge significantly. While the SIGINT program relies for the most part on its automated processes to ensure the proper disposal of intercepted communications that are no longer required, the IT Security program has supplemented the automated processes with a management control framework which has its managers routinely and closely monitoring the disposal of [redacted] communications by testing CDO databases to ensure that [redacted] communications have been properly disposed of, and documents these steps in logs that serve as further proof that these activities comply with governing authorities.

IX. CONCLUSION

Records creation and retention is the main means by which CSEC can assure compliance with its various requirements and account for its authorized activities. CSEC disposition of records is subject to comprehensive authorities as the unauthorized destruction of a record may result in an inability to document an activity and consequently, an inability to demonstrate compliance of that activity with legal, ministerial and policy requirements.

The primary objectives of this review were to assess whether CSEC activities relating to the retention and disposal of intercepted [redacted] communications were conducted in compliance with requirements set out in the law, ministerial authorities and directives and policies, and the extent to which it took steps to protect the privacy of Canadians in carrying out these activities. This review paid particular attention to the retention and disposal of PCs and personal information about Canadians.

A significant portion of this report has been committed to documenting in detail the key elements of both the SIGINT and IT Security environments relating to retention and disposal. This was done to document the technological evolution of both the SIGINT and IT Security programs in order to better set current CSEC retention and disposal practices in their proper context. This evolution has been marked by the incorporation of legal, ministerial and policy considerations into the digital architecture of both programs, reflecting a convergence of legal and technical precepts in CSEC information management practices with regard to intercepted [redacted] communications. This policy-based and technology-assisted approach is diametrically opposed to the previous model which saw systems and programs being developed on an *ad hoc* basis, with technological availability being the main impetus.

Based upon the information reviewed and the interviews conducted, the Commissioner's office has concluded that CSEC conducts its retention and disposal activities in accordance with the law and ministerial direction.

CSEC takes measures – in the design of its retention and disposal systems – to promote compliance with the law and the protection of the privacy of Canadians.

There are CSEC policies and procedures for retention and disposal of intercepted [redacted] communications activities in place which provide sufficient direction to CSEC employees respecting these activities and the protection of the privacy of Canadians. However, the use of "transitory" to describe all SIGINT intercepts in section 1.3 of OPS 1-11, as well as the inconsistent use of certain terminology by the SIGINT and IT Security functions, are confusing and should be clarified. The Commissioner's office will follow up on CSEC efforts to address these issues.

Finally, CSEC has addressed the previous associated recommendations of the Commissioner to establish records management authorities and retention and disposition schedules. Specifically, the Commissioner's office considers recommendation no. 8 of the Commissioner's 2005 Support to RCMP review IRRELEVANT IRRELEVANT

A list of findings is enclosed at Annex A.

Robert Décary, Commissioner

ANNEX A – Findings

Finding no. 1: Compliance with the Law

Based upon the information and the interviews conducted, CSEC conducts its retention and disposal of intercepted [redacted] communications in accordance with the law.

Finding no. 2: Protection of the Privacy of Canadians

Retention and disposal periods set out in CSEC policies are reasonable.

Finding no. 3: Protection of Canadians

CSEC activities respecting the retention and disposal of intercepted [redacted] communications include measures to protect the privacy of Canadians, as required by law.

Finding no. 4: Follow-up to Commissioner's reviews

CSEC has addressed the previous associated recommendations of the Commissioner to establish records management authorities and retention and disposition schedules.

Finding no. 5: Ministerial Direction

Based upon the information reviewed and the interviews conducted, CSEC conducts its retention and disposal of intercepted [redacted] communications in accordance with ministerial direction.

Finding no. 6: Supporting the Review by the Commissioner's Office

CSEC fully supported the conduct of this review.

Finding no. 7: Appropriateness of Policies and Procedures

CSEC has comprehensive policies and procedures relating to the retention and disposal of intercepted [redacted] communications; however, certain language in policy should be clarified.

Finding no. 8: OPS-1-11

The parts of OPS-1-11 concerning retention and disposal of transitory records and those records used in reporting are confusing and should be clarified.

Finding no.9: Use of language by SIGINT and IT Security

To avoid confusion, the use of terminology relating to retention and disposal activities used by the SIGINT and IT Security programs should be reconciled and made consistent.

Finding no. 10: Awareness of Personnel

CSEC employees interviewed and observed were aware of relevant policies and procedures and their application to the retention and disposal of intercepted [redacted] communications.

Finding no. 11: Management Control Framework

The management control framework has for the most part been integrated to the architecture of both the SIGINT and IT Security databases. IT Security however, has taken the extra step of supplemented the automated model with the close monitoring of disposal of [redacted] communications by designated managers.

Annex B - Interviewees

Manager, [redacted]

Supervisor, [redacted]

Team Leader, [redacted]

Acting Manager, IT Security Policy, Oversight and Compliance (IPOC)

Senior Mission Management Analyst, SIGINT Programs, Oversight and Compliance (SPOC)

Senior Policy and Review Advisor, External Review and Policy Management

Senior Policy and Review Advisor, External Review and Policy Management

Supervisor, Consolidated Traffic Repository

ANNEX C – IT Security Databases

- [redacted] a system that includes a [redacted] and [redacted] subsystems which contain [redacted] that has been used and retained for the purpose of protecting information and systems of importance to the Government of Canada;

- [redacted] an analysis database [redacted]

- [redacted]

- [redacted]

- [redacted]

- [redacted]

[redacted]