

Communications Security
Establishment Commissioner

The Honourable Robert Décary, O.C.



Commissaire du Centre de la
sécurité des télécommunications

L'honorable Robert Décary, c.r.

TOP SECRET // SI // CEO

Our File # 2200-77

March 28, 2013

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 my annual combined review of foreign signals intelligence (SIGINT) ministerial authorizations (MAs). This review covered two fiscal years: the five SIGINT MAs in effect from December 1, 2010, to November 30, 2011, as well as the six SIGINT MAs in effect from December 1, 2011, to November 30, 2012.

The purpose of this review was to: ensure that the MAs were authorized; identify any significant changes to the MA documents themselves and to CSEC activities or class of activities described in the MAs; assess the impact, if any, of the changes on the risk to non-compliance and on the risk to privacy, and, as a result, identify any subjects requiring follow-up review; and examine a sample of the resulting private communications (PCs) unintentionally intercepted for compliance with the law.

I found that the 2010-2011 and the 2011-2012 SIGINT MAs were authorized.

I found no significant changes to the scope or operation of the activities to require a follow-up in-depth review of specific activities. Changes made by CSEC in 2010-2011 and in 2011-2012 to its operational policies clarified authorities and practices and enhanced the protection of the privacy of Canadians.

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

A0000563_1-003326

In both 2010-2011 and 2011-2012, CSEC retained only those PCs essential to international affairs, defence or security. Again this year, the proportion of recognized PCs unintentionally intercepted by CSEC remained very small. CSEC destroys most recognized PCs unintentionally intercepted. In addition, it is a positive development that a new tool is being developed that will assist CSEC analysts in identifying intercepted communications that might be PCs. I will examine the impact of this new tool on privacy protection in a future review.

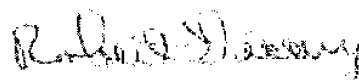
It is also a positive development that, while not a requirement in the MAs, CSEC has recognized the importance of reporting to you metrics on the number of communications intercepted by CSEC for and sent to its second party partners in the U.S., U.K., Australia and New Zealand. There are technical challenges to this but CSEC is working on a solution to provide the information. I will monitor developments.

Although not a requirement of the [REDACTED] MA, it is also a positive development that, as a measure to protect the privacy of Canadians and for accountability purposes, CSEC will enhance its reporting to you by providing information on [REDACTED]. This satisfies the outstanding recommendation from my February 2011 report on this subject.

This review contains no recommendations. CSEC officials were provided an opportunity to review and comment on the results of the review, for factual accuracy, prior to finalizing this letter.

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

Yours sincerely,



Robert Décary

c.c. Mr. John Forster, Chief, CSEC

A0000563_2-003327

Office of the
Communications Security
Establishment Commissioner



Bureau du
Commissaire du Centre de la
sécurité des télécommunications

TOP SECRET // SI // CEO

**Review of CSEC's 2010-2011 and 2011-2012
Foreign Signals Intelligence Ministerial Authorizations**

March 28, 2013

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

A0000563_3-003328

TABLE OF CONTENTS

I. AUTHORITIES	1
II. INTRODUCTION.....	1
Rationale for conducting this review.....	1
III. OBJECTIVES	2
IV. SCOPE	2
V. CRITERIA.....	3
VI. METHODOLOGY	3
VII. BACKGROUND	4
VIII. FINDINGS	6
1. Changes to the SIGINT collection activities or class of activities.....	6
i) Ministerial authorizations.....	6
ii) Policies and procedures.....	7
iii) Technology	9
iv) Metrics relating to interception and to the privacy of Canadians	10
2. Essentiality of retained private communications	12
3. CSEC's activities in response to previous recommendations of the Commissioner	13
IX. CONCLUSION	15
ANNEX A — Findings.....	16
ANNEX B — Interviewee.....	17

I. AUTHORITIES

This review was conducted under the authority of the Communications Security Establishment Commissioner (the Commissioner) as articulated in Part V.1, paragraph 273.63(2)(a) and subsection 273.65(8) of the *National Defence Act (NDA)*, and in conformance with paragraph seven of the 2010-2011 and 2011-2012 ministerial authorizations (MAs) authorizing the interception of private communications (PCs) — as defined in section 183 of the *Criminal Code* — under a foreign signals intelligence (SIGINT) collection activity known as [REDACTED] interception) as well as paragraph six of the 2010-2011 and 2011-2012 MAs authorizing the interception of PCs under SIGINT collection activities or class of activities known as Afghan MA [REDACTED]

[REDACTED]

II. INTRODUCTION

The Communications Security Establishment Canada (CSEC) conducts under ministerial authority six distinct SIGINT collection activities: Afghan MA; [REDACTED] [REDACTED] Under subsection 273.68(1) of the *NDA*, MAs cannot be in effect for a period of more than one year.

Rationale for conducting this review

Subsection 273.65(1) of the *NDA* permits the Minister of National Defence (Minister) to authorize CSEC in writing — for the sole purpose of obtaining foreign intelligence (FI), and once he is satisfied that specific conditions set out in subsection 273.65(2) of the *NDA* have been met — to intercept PCs in relation to an activity or class of activities specified in the MAs. The MAs set out a formal framework to deal with PCs unintentionally intercepted through SIGINT activities.

Subsection 273.65(8) of the *NDA* requires the Commissioner to review CSEC activities carried out under MAs “to ensure that they are authorized and report annually to the Minister on the review”. This annual review is one way the Commissioner fulfils this part of his mandate, in addition to horizontal reviews of activities common to all of the collection methods, as well as comprehensive reviews of individual MA activities.

According to paragraph 273.65(2)(d) of the *NDA*, CSEC may use and retain only those PCs that are essential to international affairs, defence or security. In this annual review, the Commissioner’s office examined a sample, selected by the Commissioner’s office of PCs intercepted and recognized by CSEC to assess whether those PCs met this essentiality test.

¹ On November 21, 2011, the Minister of National Defence approved the first MA for Interception Activities [REDACTED] for the period of December 1, 2011, to November 30, 2012.

III. OBJECTIVES

The purpose of this combined review of the six SIGINT MAs was to:

1. ensure the MAs were authorized;
2. identify any significant changes — for the years under review — to the MA documents themselves and to CSEC activities described in the MAs;
3. assess the impact, if any, of the changes on the risk to non-compliance and on the risk to privacy and, as a result, identify any subjects requiring follow-up review; and
4. examine a sample of the resulting PCs unintentionally intercepted for compliance with the law.

This review provided an opportunity to compare and contrast the activities under each of the SIGINT MAs and to identify any significant changes for each activity and for the SIGINT collection program as a whole, annually and from year to year.

IV. SCOPE

This review covered two fiscal years: the five SIGINT MAs in effect from December 1, 2010, to November 30, 2011, as well as the six SIGINT MAs in effect from December 1, 2011, to November 30, 2012.

Five principal elements relating to each of the SIGINT MAs were examined for any significant changes to the SIGINT collection activities and to PCs unintentionally intercepted:

1. the requests made to the Minister for the MAs;
2. the authorities and requirements in the MAs;
3. any significant changes to the operation of the associated activities, e.g., changes to the scope of the activities, to ministerial direction or requirements, to CSEC policies or procedures, to the technology used, or to the compliance validation framework for the activities;
4. volumes of intercepted communications and the number of PCs unintentionally intercepted under the MAs; and
5. a sample of retained PCs to assess whether those communications were retained by CSEC in compliance with the law.

Any changes were assessed for the impact on the risk to non-compliance and on the risk to privacy.

V. CRITERIA

CSEC's activities were assessed for compliance with the law and for the extent to which the activities protected the privacy of Canadians within the approach described in the Objectives and Scope sections of this report.

The assessment of any significant changes to the SIGINT collection activities and the impact of these changes on the risk to non-compliance and on the risk to privacy was made in the context of the Commissioner's standard review criteria, that is, the Commissioner expects CSEC to:

- conduct its activities in accordance with legal and ministerial requirements;
- have appropriate policies and procedures;
- have personnel who are aware of, and comply with, the policies and procedures; and
- in accordance with its policies, have an effective compliance validation framework and activities to ensure the integrity of the operational activities is maintained on a routine basis, including appropriately accounting for important decisions and information relating to compliance and the protection of the privacy of Canadians.

VI. METHODOLOGY

The Commissioner's office reviewed CSEC records, conducted an interview with a key CSEC employee and reviewed written responses provided by CSEC to specific questions. This allowed the Commissioner's office to identify any significant changes relating to the MAs and associated activities from what was in place at the time of the last comprehensive review of particular activities, as well as from last year's combined review. This included examination of the documents listed in the Scope section of this report.

The Commissioner's office also examined key metrics relating to interception and to the privacy of Canadians.

A sample of PCs used for CSEC end product reports, as well as retained PCs that had not been used in CSEC reports, were reviewed for essentiality to international affairs, defence or security.

VII. BACKGROUND

Paragraph 273.64(1)(a) of the *NDA* authorizes CSEC to acquire and use FI in accordance with Government of Canada (GC) intelligence priorities.

These activities shall:

- not be directed at Canadians or any person in Canada [paragraph 273.64(2)(a) of the *NDA*]; and
- be subject to measures to protect the privacy of Canadians in the use and retention of intercepted information [paragraph 273.64(2)(b) of the *NDA*].

The *NDA* requires that an intercepted PC shall be used or retained only if it is essential to international affairs, defence or security.

The Minister, under subsection 273.65(5) of the *NDA*, may include in an MA any conditions that he considers advisable to protect the privacy of Canadians. While this review encompasses six unique SIGINT collection activities, in general, each MA contains similar ministerial requirements and obligations:

1. CSEC is to conduct SIGINT collection activities in strict compliance with the ministerial directives (MDs) respecting:
 - *Accountability Framework*;²
 - *Privacy of Canadians*;³ and
 - *Collection and Use of Metadata*;^{4, 5}
2. the Afghan, [REDACTED] activities are to be conducted in strict compliance with program-specific MDs;⁶

² For the period under review, the MD issued June 19, 2001, was in effect; on November 20, 2012, the Minister approved a new MD on *Accountability Framework* that will be the subject of future reviews.

³ For the period under review, the MD issued June 19, 2001, was in effect; on November 20, 2012, the Minister approved a new MD on *Privacy of Canadians* that will be the subject of future reviews.

⁴ For the period under review, the MD on *Collection and Use of Metadata* issued March 9, 2005, was in effect for the 2010-2011 MAs and the MD issued November 21, 2011, was in effect for the 2011-2012 MAs.

⁵ These requirements do not apply to [REDACTED] activities.

⁶ For the Afghan MA, the MD on *Integrated SIGINT Operational Model* issued May 20, 2004; for [REDACTED] for the period under review, the MD on [REDACTED] *Operations* issued January 14, 2002, was in effect (on November 20, 2012, the Minister approved a new MD on [REDACTED] that will be the subject of future reviews); for [REDACTED] for the period under review, the MD on [REDACTED] *Program* issued March 15, 2004, was in effect (on November 20, 2012, the Minister approved a new MD on [REDACTED] *Program* that will be the subject of future reviews), as well as [REDACTED]

3. CSEC is to annotate for destruction a recognized intercepted solicitor-client communication unless it contains FI and its retention or use would be in conformity with the laws of Canada;
4. CSEC is to establish and maintain an automated directory of selectors which CSEC believes relate to foreign entities located outside Canada;⁷
5. CSEC is to report to the Minister, at the expiration of the MA or upon request, certain information respecting intercepted PCs and solicitor-client communications and the number and value of intelligence reports produced from information derived from these PCs;
6. CSEC is to report to the Minister any serious issue that arises in the implementation of the MA, such as a substantial decrease in the value of the FI or a sustained major increase in the interception of PCs or solicitor-client communications;
7. CSEC is to support and assist the CSE Commissioner in the conduct of reviews; and
8. the activities shall be subject, as a minimum, to measures to protect the privacy of Canadians, contained in CSEC's operational policies, notably:
 - OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE[C] Activities*;⁸ and
 - specific policies and operational instructions relating to each of the six SIGINT collection activities.

The most recent comprehensive reviews of the SIGINT collection activities were conducted in January 2010 for the Afghan MA, February 2009 for [REDACTED] January 2009 for [REDACTED] and June 2008 for [REDACTED]. A comprehensive review of [REDACTED] is underway; the last review of [REDACTED] was completed in March 2008.

⁷ This requirement does not apply to [REDACTED] activities.

⁸ For the period under review, the OPS-1 policy issued December 1, 2010, was in effect for the 2010-2011 MAs and the OPS-1 issued November 1, 2011, was in effect for the 2011-2012 MAs.

VIII. FINDINGS

1. Changes to the SIGINT collection activities or class of activities

i) Ministerial authorizations

Finding no. 1: Ministerial Authorizations

The 2010-2011 and the 2011-2012 signals intelligence ministerial authorizations were authorized.

Finding no. 2: Ministerial Authorizations and Associated Request Memoranda

The 2010-2011 and the 2011-2012 signals intelligence ministerial authorizations and associated request memoranda to the Minister of National Defence did not contain any significant changes.

For both years under review, the individual request memoranda to the Minister provided information and supporting reasoning that satisfied the four conditions for authorization required by subsection 273.65(2) of the *NDA*. With few minor exceptions, the rationales and explanations in the documents were consistent and contained only minor differences relating to activity-specific content.

Also for both years under review, the Commissioner's office examined each SIGINT MA and associated request memoranda for any substantial changes, additions or deletions. The changes to the documents were for the most part administrative or stylistic in nature, or related to the enhancement of existing activities, and did not indicate significant changes to the activities themselves, notably:

- In 2010-2011, CSEC changed the timing for MA requests. All approved MAs now start on December 1 and expire on November 30;
- The title of the 2011-2012 Afghan MA was changed from "Interception Activities Conducted in Support of Canadian Forces Operations in Afghanistan" to "Interception Activities Conducted in Support of the Government of Canada Mission in Afghanistan", which is a reflection of the changed nature of GC operations in Afghanistan, i.e., from a focus on military operations to broader GC activities;
- Several of the request memoranda identified changes to the collection systems such as the use of new technologies [REDACTED] and
- The request memoranda contained new references to the annual MDs on *Communications Security Establishment: Government of Canada Intelligence Priorities* (in this case, for fiscal years 2010-2011 and 2011-2012).⁹

⁹ CSEC's foreign signals intelligence collection activities must be in accordance with the GC's intelligence priorities, which are set by the Cabinet yearly and issued to CSEC in an annual ministerial directive. These priorities are disseminated and implemented by CSEC by the use of the National SIGINT Priorities List (NSPL).

In addition, in 2011-2012, the Minister approved a new MA on "CSE[C] Interception Activities [REDACTED]". Once established, this [REDACTED] would target foreign entities of FI interest [REDACTED] in particular intelligence on the [REDACTED]. The contents of the MA and associated request memorandum were consistent with the other MAs and did not raise any questions.

Under the MAs, CSEC must report to the Minister when any serious issue arises in the implementation of the MAs. CSEC indicated that there were no serious issues that arose in the implementation of any of the 2010-2011 MAs that necessitated extraordinary reporting to the Minister.¹⁰

ii) Policies and procedures

Finding no. 3: Policies and Procedures

Changes made by CSEC to its operational policies clarified authorities and practices and enhanced the protection of the privacy of Canadians.

The principal operational policies (OPS) cited in the individual MAs relating to CSEC's SIGINT collection activities are:

- OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities*;
- OPS-1-13, *Procedures for Canadian [REDACTED] and Joint CSEC-CF Activities*; and
- OPS-3-1, *Procedures for [REDACTED] Activities*.

The NSPL encompasses broad categories such as [REDACTED]

[REDACTED] The NSPL categories must be necessarily flexible to accommodate unforeseen developments, but within the scope of the GC intelligence priorities. The intelligence priorities are usually issued during the summer months and the NSPL is developed afterwards. According to CSEC, while the timing for the MA and NSPL cycles does not coincide, as noted, the NSPL categories are broad enough to avoid any conflict or hindrance.

¹⁰ E-mail from Senior Policy and Review Advisor, External Review and Policy Management, February 21, 2013. The 2011-2012 reporting to the Minister was not finalized at the time of completion of this review.

A0000563_11-003336

OPS-1

Two amendments to CSEC's cornerstone policy on compliance and privacy protection were issued during the period under review. The following summarizes the notable changes.

Amendment 9 to OPS-1 (effective December 1, 2010)

- Clarified that metadata may be searched for the purpose of providing FI, including any information related to the protection of electronic information or information infrastructures of importance to the GC that may be used for purposes of part (b) of CSEC's mandate.

IRRELEVANT

Amendment 10 to OPS-1 (effective December 1, 2011)

- Respecting limits on targeting, the words "to acquire content" were added to differentiate between [REDACTED] content and metadata collection. Metadata collection is by nature "bulk" and not [REDACTED]
- CSEC's SIGINT Programs Oversight and Compliance (SPOC) group will now notify CSEC Operational Policy (D2) of any inadvertent naming of Canadians or people in Canada.
- SPOC is now required to track all instances when an intercepted communication has been annotated for deletion because:
 - a) both originator and recipient are Canadian;
 - b) both originator and recipient are located in Canada; or,
 - c) one communicant is in Canada and the other is a Canadian abroad.
- Further clarified that SIGINT employees may search and share metadata with CSEC Information Technology (IT) Security employees.¹¹

¹¹ The 2011 update to the 2005 MD on *Collection and Use of Metadata* also authorized SIGINT to provide IT Security employees with unsuppressed foreign metadata for cyber defence purposes. Previously, SIGINT was required to follow regular identity release procedures to share unsuppressed metadata with IT Security. According to CSEC, this process was becoming increasingly problematic in the evolving cyber threat environment and resolving this issue was critical to ensuring effective cyber defence support to CSEC's clients. The Commissioner's office plans to conduct a comprehensive review of CSEC's metadata activities, including the new MD and authorities. The Commissioner's last review on metadata was completed in 2008.

- Clarified the differences between the concepts of “relevance” and “essentiality” in the context of Canadian identity information (CII).
- Clarified that CSEC IT Security can share with CSEC SIGINT data obtained from cyber defence activities. The Commissioner’s office plans to examine in a future review changes in authorities and practices respecting CSEC IT Security and CSEC SIGINT cooperation and information sharing.
- Clarified the process for handling a privacy incident identified by CSEC. The employee and supervisor involved in the incident must consult with IT Security’s Policy, Oversight, and Compliance group (IPOC) or SPOC, as appropriate, and IPOC and SPOC must consult with CSEC’s Operational Policy group, to discuss what steps should be taken. IPOC or SPOC must provide the Manager, Corporate and Operational Policy, who maintains the central file of privacy incidents, a summary of the incident and actions taken.
- Removed the definition of the term “intercept” because the existing definition was incomplete and did not reflect the wording in Cabinet Confidence

Amendment 2 to OPS-1-13 (effective December 1, 2010)

- Respecting targeting, clarified that: “...a selector can only be used to intercept a communication *where CSEC is satisfied* that it is foreign and relates to the external component of the communication ...” (emphasis added). Previously, the policy required CSEC to “believe” a selector is foreign and relates to the external component of the communication. This change mirrors the wording of paragraph 273.65(2)(a) the NDA, i.e., “[t]he Minister may only issue an authorization... if satisfied that (a) the interception will be directed a foreign entities located outside Canada” and reflects current targeting processes used by CSEC.
- Clarified the process of cyber threat detection, specifically that “collection systems [REDACTED] The previous wording, i.e., “collection systems [REDACTED] implied a chronology to the process which was not accurate.

OPS 3-1

CSEC made no amendments to OPS 3-1 during the period under review.

iii) Technology

Finding no. 4: Technology

In both 2010-2011 and 2011-2012, CSEC did not make any significant changes to the technology used for its signals intelligence collection activities.

In 2010-2011 and in 2011-2012, CSEC implemented changes [REDACTED] under the Afghan MA, and [REDACTED] that resulted in [REDACTED] collection

[REDACTED] for certain kinds of communications and an ability to collect [REDACTED] of communications. CSEC also made general enhancements and implemented "bug fixes" to the technology used for [REDACTED] collection.

Also in 2011-2012, consistent with Canada's evolving role in Afghanistan, [REDACTED]

[REDACTED] Under the [REDACTED] MA, CSEC continued development and preparation of [REDACTED] in support of [REDACTED]. This included changes to the [REDACTED] activities. CSEC also updated the [REDACTED] to provide [REDACTED] capacity.

iv) Metrics relating to interception and to the privacy of Canadians

For each of the six SIGINT collection activities, the Commissioner's office requested that CSEC provide the following key information relating to interception and to the privacy of Canadians, to permit comparison of the activities and to identify any significant changes or trends over time:¹²

1. the total number of communications intercepted by CSEC;
2. the number of intercepted communications viewed by CSEC's FI analysts;
3. the number of communications recognized as PCs; and
4. the number of recognized PCs retained by CSEC.

Finding no. 5: Metrics Relating to Interception and to the Privacy of Canadians

Overall, in 2010-2011, the volume of communications intercepted by CSEC's SIGINT collection activities [REDACTED] while the proportion of recognized private communications unintentionally intercepted by CSEC remained very small.

¹² CERRID # 890396, version 3, March 2012. Neither CSEC's annual report to the Minister on metrics for 2011-2012 nor metrics relating to the [REDACTED] MA were available at the time of completion of this review. The comparisons, changes and trends referred to in this report are based on CSEC's reports to the Minister for the 2008-2009, 2009-2010 and 2010-2011 MAs. The Commissioner's office's working file contains detailed tables and graphs illustrating the changes in metrics over time.

The Commissioner's office observed the following respecting the metrics relating to interception and to the privacy of Canadians:

- The total number of intercepted communications collected under the MA [REDACTED] in 2010-2011 (from [REDACTED] in 2009-2010 to [REDACTED] in 2010-2011). The total number of intercepted communications collected under the Afghan MA [REDACTED] (from [REDACTED] in 2008-2009 to [REDACTED] in 2009-2010, to [REDACTED] in 2010-2011). The total number of intercepted communications collected under the [REDACTED] MA also [REDACTED] with a [REDACTED] in 2009-2010 (from [REDACTED] in 2008-2009 to [REDACTED] in 2009-2010). The total number of intercepted communications collected under the [REDACTED] MA [REDACTED] in 2009-2010 (from [REDACTED] in 2008-2009, to [REDACTED] in 2009-2010, to [REDACTED] in 2010-2011). [REDACTED] is the only collection activity to experience [REDACTED] in the total number of intercepted communications (from [REDACTED] in 2008-2009, to [REDACTED] in 2009-2010, to [REDACTED] in 2010-2011).
- [REDACTED] collection results in the [REDACTED] of recognized PCs unintentionally intercepted (in 2010-2011, [REDACTED] PCs).
- The overall number of PCs unintentionally intercepted under the [REDACTED] MA [REDACTED] over the last three years; however, the number of [REDACTED] PCs retained has been [REDACTED] (from [REDACTED] in 2008-2009, to [REDACTED] in 2009-2010, to [REDACTED] in 2010-2011).
- CSEC destroys most recognized PCs unintentionally intercepted (in 2010-2011, [REDACTED] PCs). In 2011-2012, CSEC retained [REDACTED] recognized PCs. Of these, [REDACTED] were used in reporting and [REDACTED] were retained for future use.
- The only recognized solicitor-client communications unintentionally intercepted by CSEC in 2010-2011 were under the Afghan MA. All of these were destroyed.

Again this year, the Commissioner's office also sought metrics respecting the number of communications intercepted by CSEC for and sent to its second party partners.¹³ Such information was not available at this time because CSEC's systems do not automatically count that information. However, it is a positive development that, while not a requirement in the MAs, CSEC has recognized the importance of reporting to the Minister such metrics and CSEC is working on a technical solution to provide that information. According to CSEC, the solution requires significant technical work, and as a result, it is difficult for CSEC to estimate when this work may be completed.¹⁴ The Commissioner's office continues to examine this and other questions as part of an ongoing review of CSEC's SIGINT information sharing activities with its second party partners. In particular, the office is examining questions about the number of PCs and the volume of CII that CSEC shares with and receives from the Second Parties.

¹³ CSEC's second party partners are: the U.S. National Security Agency, the U.K. Government Communications Headquarters, the Australian Defence Signals Directorate, and the New Zealand Government Communications Security Bureau.

¹⁴ E-mail from Senior Policy and Review Advisor, External Review and Policy Management, March 8, 2013.

2. Essentiality of retained private communications

Finding no. 6: Essentiality of Retained Private Communications

Based upon the information reviewed and the interviews conducted, in both 2010-2011 and 2011-2012, CSEC retained only those private communications essential to international affairs, defence or security.

If a CSEC analyst whose function is directly related to the production of FI reports recognizes that an intercepted communication is a PC — including a solicitor-client communication or a communication of a Canadian located outside Canada — or contains CII, then the analyst must, upon recognition, annotate the communication. Such communications that are not essential to international affairs, defence or security must be annotated for deletion.

It is a specific objective of these annual reviews to examine a sample of PCs unintentionally intercepted and recognized by CSEC to assess whether those PCs were used in CSEC end-product reports or retained in compliance with the law, i.e., the PCs contained FI essential to international affairs, defence or security, as required by paragraph 273.65(2)(d) of the *NDA*.

The Commissioner's office reviewed all [REDACTED] end-product reports authored by CSEC in 2010-2011 and 2011-2012 that were based on PCs.¹⁵

To avoid a significant impact on CSEC operations and translators, the Commissioner's office examined only those PCs unintentionally intercepted and retained in 2010-2011 and 2011-2012 not used in reports and that originated in either English or French. The Commissioner's office examined 100% (all [REDACTED]) of the PCs retained in 2010-2011 as well as approximately 25% [REDACTED] of the PCs retained in 2011-2012 that had not been used in CSEC reports.¹⁶ The PCs examined related to different SIGINT collection

¹⁵ Namely, [REDACTED]

[REDACTED]

activities, dates, CSEC FI analysts, and tri-graphs.¹⁷ These PCs also related to different subjects, including: [REDACTED]

The Commissioner's office had no questions about CSEC's decision to use the PCs in the end-product reports examined or about CSEC's decision to retain the PCs examined that were not used in reports; the Commissioner's office accepted that all of the PCs examined contained FI essential to international affairs, defence or security.

CSEC indicated that it did not receive specific legal advice from Justice Canada counsel in relation to any individual PCs unintentionally intercepted and recognized by CSEC in 2010-2011 or 2011-2012.

In addition, it is a positive development that CSEC is testing a new tool that will assist CSEC analysts in identifying intercepted communications that might be PCs. CSEC is hopeful that the tool will positively aid analysts in the annotation process and reduce the potential for human error. At this time, CSEC is uncertain respecting when the tool will be implemented.

5. CSEC's activities in response to previous recommendations of the Commissioner

[REDACTED] and PCs

Recommendation no. 2 of the Commissioner's annual combined *Review of CSEC's Activities Under Foreign Intelligence Ministerial Authorizations* of February 25, 2011, was:

CSEC should report to the Minister the number of [REDACTED] in a manner similar to what CSEC does for recognized private communications intercepted under the other SIGINT collection programs.

CSEC did not initially accept this recommendation, and on July 5, 2011, the Minister responded to the Commissioner indicating that "pending any change in Department of Justice legal advice on this matter", he "will rely on CSEC to follow its current guidance."

¹⁷ A tri-graph is a three letter code representing the assessed nationality and function of a targeted entity.

On August 25, 2011, the Commissioner responded to the Minister indicating that in his view:

Solicitor-Client Privilege [REDACTED] respecting this subject. Knowing the number of [REDACTED] communications CSEC views or listens to that are one-end Canadian communications — in a similar way that it reports the interception of private communications — is one measure to protect the privacy of Canadians, in accordance with paragraph 273.64(2)(b) of the *NDA*, and for accountability purposes. Solicitor-Client Privilege [REDACTED] ...I continue to believe that CSEC should implement recommendation no. 2 of my report of February 25, 2011.

CSEC subsequently indicated that this recommendation was under review and on May 16, 2012, the Minister responded:

I have reflected on your additional comments with respect to Recommendation 2, and CSEC's assessment that [REDACTED] does not constitute a private communication and therefore does not trigger a legal reporting requirement. I am satisfied that CSEC has, Solicitor-Client Privilege [REDACTED]

Solicitor-Client Privilege [REDACTED] As CSEC's privacy protection measures apply equally to [REDACTED] and to intercepted communications, I am assured that should [REDACTED] contain information about Canadians, CSEC has measures in place to protect the privacy of Canadians.

Nonetheless, to support me with additional contextual information, CSEC intends to begin compiling the number of recognized one-end Canadian [REDACTED] foreign target located outside of Canada [REDACTED] acquired through the [REDACTED] program, that are retained by CSEC on the basis that they are essential to international affairs, defence or security. The Chief intends to provide the available data for the current fiscal year in CSEC's Annual Report to the Minister of National Defence, with full-year data to follow in future Annual Reports.

This response satisfies the Commissioner's recommendation. It is a positive development that, as a measure to protect the privacy of Canadians and for accountability purposes, CSEC will enhance its reporting to the Minister by providing information on [REDACTED]. The Commissioner's office will examine this reporting as part of future combined annual reviews of SIGINT MAs and in-depth reviews of [REDACTED] activities.

IX. CONCLUSION

This combined review of SIGINT MAs encompassed the 2010-2011 and 2011-2012 Afghan, [REDACTED] MAs, as well as the 2011-2012 [REDACTED] MA.

The purpose of this review was to: ensure that the MAs were authorized; identify any significant changes to the MA documents themselves and to CSEC activities described in the MAs; assess the impact, if any, of the changes on the risk to non-compliance and on the risk to privacy, and, as a result, identify any subjects requiring follow-up review; and examine a sample of the resulting PCs unintentionally intercepted for compliance with the law.

It is assessed that the 2010-2011 and the 2011-2012 SIGINT MAs were authorized.

Based upon the information reviewed and the interviews conducted, in both 2010-2011 and 2011-2012, CSEC retained only those PCs essential to international affairs, defence or security. In addition, it is a positive development that ongoing development work at CSEC is aiming to improve the annotation process for PCs through automation.

No significant changes were found to require a follow-up in-depth review of specific SIGINT MA activities. The 2010-2011 and the 2011-2012 SIGINT MAs and associated request memoranda to the Minister did not contain any significant changes. Changes made by CSEC in 2010-2011 and in 2011-2012 to its operational policies clarified authorities and practices and enhanced the protection of the privacy of Canadians. In both 2010-2011 and 2011-2012, CSEC did not make any significant changes to the technology used for its SIGINT collection activities.

Overall, in 2010-2011, the volume of communications intercepted by CSEC's SIGINT collection activities [REDACTED] while the proportion of recognized PCs unintentionally intercepted by CSEC remained very small. CSEC destroys most recognized PCs unintentionally intercepted.

It is a positive development that, while not a requirement in the MAs, CSEC has identified as a requirement the need for metrics respecting the number of communications intercepted by CSEC for and sent to its second party partners and it is working on a solution to provide this information.

Although not a requirement of the [REDACTED] MA, it is also a positive development that, as a measure to protect the privacy of Canadians and for accountability purposes, CSEC will enhance its reporting to the Minister by providing information on [REDACTED]. The Commissioner's office will examine this reporting as part of future combined annual reviews of SIGINT MAs and in-depth reviews of [REDACTED] activities.

This review contains no recommendations. A list of findings is enclosed at Annex A.


Robert Décary, Commissioner

A0000563_19-003344

ANNEX A – Findings

Finding no. 1: Ministerial Authorizations

The 2010-2011 and the 2011-2012 signals intelligence ministerial authorizations were authorized.

Finding no. 2: Ministerial Authorizations and Associated Request Memoranda

The 2010-2011 and the 2011-2012 signals intelligence ministerial authorizations and the associated request memoranda to the Minister of National Defence did not contain any significant changes requiring.

Finding no. 3: Policies and Procedures

Changes made by CSEC to its operational policies clarified authorities and practices and enhanced the protection of the privacy of Canadians.

Finding no. 4: Technology

In both 2010-2011 and 2011-2012, CSEC did not make any significant changes to the technology used for its signals intelligence collection activities.

Finding no. 5: Metrics Relating to Interception and to the Privacy of Canadians

Overall, in 2010-2011, the volume of communications intercepted by CSEC's SIGINT collection activities [REDACTED] while the proportion of recognized private communications unintentionally intercepted by CSEC remained very small.

Finding no. 6: Essentiality of Retained Private Communications

Based upon the information reviewed and the interviews conducted, in both 2010-2011 and 2011-2012, CSEC retained only those private communications essential to international affairs, defence or security.

ANNEX B – Interviewee

Senior Mission Management Officer, SIGINT Programs Oversight and Compliance

A0000563_21-003346