Communications Security Establishment Commissioner

The Honourable Jean - Pierre Plouffe, C.D.

Commissaire du Centre de la sécurité des télécommunications

L'honorable Jean - Pierre Plouffe, C.D.

TOP SECRET // SI // CEO

Our file # 2200–84

March 31, 2014

The Honourable Robert Nicholson, P.C., Q.C., M.P.
Minister of National Defence
101 Colonel By Drive
Ottawa, ON K1A 0K2

Dear Minister:

The purpose of this letter is to provide you with the results of my annual combined review of the Communications Security Establishment's (CSEC) foreign signals intelligence (SIGINT) ministerial authorizations (MAs) and intercepted private communications (PCs) for the period of December 1, 2012, to November 30, 2013. This review was undertaken under my general authority as articulated in Part V.1, paragraph 273.63(2)(*a*) of the *National Defence Act* (*NDA*), as well as under my specific authority found in subsection 273.65(8) of the *NDA*. Subsection 273.65(8) of the *NDA* requires me to review CSEC activities carried out under MAs "to ensure they are authorized and report annually to the Minister on the review". This annual review is one way that I fulfill this part of my mandate.

The purpose of this review was to: ensure that the activities conducted under the MAs were authorized; identify any significant changes — for the year under review, compared with previous years — 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 the PCs unintentionally intercepted by CSEC for compliance with the law.

In past years, my office examined samples of intercepted PCs as part of this annual review. This year, for the first time, my office examined all of the PCs that CSEC used in End Product Reports or retained at the end of the MA period for use in future reporting, for compliance with the law and for protection of the privacy of Canadians. This led me to a number of findings and recommendations.

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

I found that the 2012–2013 SIGINT MAs met the conditions for authorization set out in the *NDA*. The format of the 2012–2013 SIGINT MAs and associated request memoranda was significantly different than that used in 2011–2012. These changes were positive and resulted in documents that are more properly aligned with the purpose of the MAs — to shield CSEC from potential liability under Part VI of the *Criminal Code* in the event that CSEC unintentionally intercepts PCs as part of SIGINT collection — and that are clear and comprehensive. In addition, CSEC made changes to some technology used for some of its SIGINT collection activities, the impact of which may be examined in subsequent in-depth reviews by my office.

With one exception, revised versions of CSEC operational policies did not contain major amendments that would have significantly changed the conduct of activities under MA authorities. However, to ensure proper accountability for sensitive activities, **I recommend** that CSEC promulgate detailed guidance, as soon as possible, regarding the additional approvals required for certain activities relating to the [redacted] program and to CSEC operations [redacted]

It is a positive development that, while CSEC made significant changes to how it counts "collected communications" that it reports to the Minister for its SIGINT collection activities, CSEC continues to use the same method as in previous years to count and report recognized PCs, which will enable a more accurate comparison between the overall number of collected communications and the number of intercepted PCs.

Overall, in 2012–2013, the volume of communications collected through CSEC's SIGINT activities [redacted] while the number of recognized PCs unintentionally intercepted by CSEC remained very small. All End Product Reports based on PCs contained foreign intelligence relating to international affairs, defence or security. Based on the information reviewed and the interviews conducted, in 2012–2013, all PCs that were recognized by CSEC were intercepted unintentionally, and all but one of those used or retained were essential to international affairs, defence or security, as required by the *NDA*. In one case, an analyst recognized and appropriately flagged that a communication was a PC; however, that communication did not pertain to the analyst's target set, and, contrary to policy, the analyst incorrectly marked it for retention even though the analyst did not assess whether the communication was essential.

Contrary to policy, one analyst viewed and recognized 18 PCs during the period under review, but did not annotate them until several weeks later. As a result of this example, as well as others, **I recommend** that CSEC analysts immediately annotate recognized PCs for essentiality to international affairs, defence or security, as required by the *NDA*, or, if not essential, for deletion.

A number of analysts retained PCs that had once been, but were no longer, essential to international affairs, defence or security; despite regular written reminders to review and mark for deletion any PCs that were no longer essential, these PCs were retained — in some cases, for several months — until just before the expiration of the MAs and prior to associated reporting to the Minister. As a result, **I recommend** that CSEC analysts regularly assess, at a minimum quarterly, whether the ongoing retention of a recognized PC not yet used in an End Product Report is strictly necessary and remains essential to international affairs, defence or security or whether that PC should be deleted.
I also recommend that CSEC make available to you more comprehensive information regarding the number of collected communications and intercepted PCs that it acquires and retains throughout an MA period, in order to enhance accountability.

As a result of one example in which an analyst retained PCs pending further advice, **I recommend** that CSEC promulgate guidance regarding the protection of privacy and the handling of intercepted communications of a targeted foreign entity located outside Canada that include [redacted] of a Canadian or person in Canada as part of those intercepted communications.

Finally, I found that CSEC made further progress in implementing a recommendation from the *2010–2011 Review of Foreign Signals Intelligence Ministerial Authorizations and Intercepted Private Communications*, regarding reporting to the Minister on the number of one-end Canadian communications acquired through [redacted] activities [redacted] in a manner similar to what CSEC does for recognized PCs intercepted under the other SIGINT collection programs.

CSEC officials were provided an opportunity to review and comment on the results of the review, for factual accuracy, prior to finalizing the enclosed report.

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

Yours sincerely,

Jean-Pierre Plouffe

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

Enclosure

Communications Security Establishment Commissioner

The Honourable Jean - Pierre Plouffe, C.D.

Commissaire du Centre de la sécurité des télécommunications

L'honorable Jean - Pierre Plouffe, C.D.

TOP SECRET // SI // CEO

Our File # 2200–84

Annual Combined Review of Foreign Signals Intelligence Ministerial Authorizations and Intercepted Private Communications for 2012–2013

March 31, 2014

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

TABLE OF CONTENTS

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 six of the 2012–2013 ministerial authorizations (MAs) authorizing the interception of private communications (PCs) — as defined in section 183 of the *Criminal Code*[1] — under foreign signals intelligence (SIGINT) collection activities known as [redacted] and [redacted] collection,[3] as well as paragraph seven of the 2012–2013 MA authorizing the interception of PCs under SIGINT collection activity known as [redacted] collection.[4]

II. INTRODUCTION

In the previous MA period (2011–2012), the Communications Security Establishment Canada (CSEC) conducted its SIGINT collection activities under six MAs: [redacted] interception activities [redacted] interception activities [redacted] interception activities done in support of the Government of Canada (GC) mission in Afghanistan; and [redacted] interception (as it was termed for that period).

CSEC restructured the SIGINT MAs for the 2012–2013 period to make clear that they applied to classes of activities rather than to specific collection programs. Since MAs are not program approval mechanisms, CSEC explained that consolidating them according to classes of activities better aligned the approval process with the scheme outlined in the *NDA*.[5] CSEC also restructured the MA request memoranda for 2012–2013 to better describe how mandated classes of activities risk interception of PCs and how CSEC mitigates this risk. This has minimized unnecessary duplication, thereby reducing the number of SIGINT MAs from six to three. According to CSEC, the intent of this new approach is to provide the Minister of National Defence (the Minister) with a more

[1] According to section 183 of the *Criminal Code*, "private communication" means any oral communication, or any telecommunication, that is made by an originator who is in Canada or is intended by the 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.

[redacted]

[5] Section 273.65(1) of the *NDA* states "The Minister may, for the sole purpose of obtaining foreign intelligence, authorize the Communications Security Establishment in writing to intercept private communications in relation to an activity or class of activities specified in the authorization."

comprehensive understanding of both the value and the applicable risk of intercepting PCs associated with each class of activity.[6]

As a result of this restructuring, CSEC now conducts three distinct SIGINT collection activities under ministerial authority: [redacted] collection (which includes the same class of activities included in the 2011–2012 MAs for [redacted] interception activities conducted in support of the GC mission in Afghanistan, and interception activities [redacted]); and [redacted] collection (which includes the same class of activities included in the 2011–2012 MAs for [redacted] and for interception activities conducted in support of the GC mission in Afghanistan). Under subsection 273.68(1) of the *NDA*, MAs cannot be in effect for a period of more than one year, but may be renewed.

Rationale for conducting this review

Subsection 273.65(1) of the *NDA* permits the Minister to authorize CSEC in writing — for the sole purpose of obtaining foreign intelligence (FI), and only if the Minister is satisfied that specific conditions set out in subsection 273.65(2) of the *NDA* have been met — to intercept PCs (including solicitor-client communications) in relation to an activity or class of activities specified in the MA. The MAs set out a formal framework for dealing with PCs that have been intercepted unintentionally through SIGINT activities, and shield CSEC from the prohibition respecting the interception of PCs found in Part VI of the *Criminal Code*.[7]

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 conducted on the 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 or retain only those PCs that are essential to international affairs, defence or security. In this annual review, the Commissioner's office examined *all* of the PCs that were intercepted, recognized and retained by CSEC at the end of the MA period to assess whether those PCs met this essentiality test.

[6] CERRID #1103590: *CSEC Strategic Policy Update for the Period of January 2010 to December 2012.*
[7] CSEC operational policy documents contain detailed guidance related to the handling of PCs.

III. OBJECTIVES

The purpose of this combined review of the three SIGINT MAs and intercepted PCs was to:

1. ensure that the activities conducted under the MAs were authorized;

2. identify any significant changes — for the year under review, compared with previous years — to the MA documents themselves and to CSEC activities or class of 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 the resulting PCs unintentionally intercepted for compliance with the law and for protection of the privacy of Canadians.

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, occurring either within the review period or from year to year.

IV. SCOPE

This review covered the three SIGINT MAs in effect from December 1, 2012, to November 30, 2013.

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, for example, 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 collected communications and the number of recognized PCs unintentionally intercepted under the MAs; and

5. all recognized PCs retained at the end of the MA period, to assess whether those communications were retained by CSEC in compliance with the law, and whether CSEC protected the privacy of Canadians in the use and retention of that intercepted information.

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 or class of activities and the impact of these changes on the risk to non-compliance and on the risk to privacy were made in the context of the Commissioner's standard review criteria, that is, the Commissioner expected CSEC to:

- conduct its activities in accordance with legal and ministerial requirements;
- have appropriate policies and procedures in place to provide sufficient direction respecting ministerial requirements, including the protection of the privacy of Canadians;
- 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 measures to ensure that the integrity of 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 interviews with several CSEC employees 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 that came into effect following last year's combined review, and included examination of the documents listed in the Scope section of this report.

In addition, for the first time, the Commissioner's office examined all PCs from the 2012–2013 MA period that were used for CSEC End Product Reports (EPRs) and all retained PCs from the 2012–2013 period that had not yet been used in reports, in order to determine if they were retained in accordance with the law and with CSEC policy. In previous reviews of this kind, the Commissioner's office reviewed samples of these retained PCs. The Commissioner's office also examined all EPRs produced by CSEC containing information derived from PCs from the 2012–2013 MA period, along with

associated transcripts, as well as key metrics relating to the interception of PCs and to the privacy of Canadians.

VII. BACKGROUND

Paragraph 273.64(1)(*a*) of the *NDA* authorizes CSEC to acquire and use information from the global information infrastructure for the purpose of providing FI, in accordance with GC intelligence priorities.

The *NDA* states that 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*].

Paragraph 273.65(2)(*d*) of the *NDA* requires that an intercepted PC shall be used or retained only if it is essential to international affairs, defence or security.

Under subsection 273.65(5) of the *NDA*, the Minister may include in an MA any conditions that he considers advisable to protect the privacy of Canadians. While this review encompasses three 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 following ministerial directives (MDs):
   - *Ministerial Directive on Accountability Framework*,[8]
   - *Ministerial Directive on Privacy of Canadians*,[9] and
   - *Ministerial Directive on Collection and Use of Metadata*;[10]

[8] For the period under review, the MD on *Accountability Framework* issued November 20, 2012, was in effect.
[9] For the period under review, the MD on *Privacy of Canadians* issued November 20, 2012, was in effect.
[10] For the period under review, the MD on *Collection and Use of Metadata* issued November 21, 2011, was in effect.

2. in addition to the MDs listed above, [redacted] and [redacted] activities are to be conducted in strict compliance with program-specific MDs;[11]

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 maintain an automated directory of selectors that it believes relate to foreign entities located outside Canada;[12]

5. CSEC is to report to the Minister, within four months following 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 when any serious issue arises in the implementation of the MA, such as a sustained substantial decrease in the value of the FI or any sustained major increase in the number of recognized PCs or solicitor-client communications intercepted pursuant to the MA;

7. CSEC is to support and assist the CSE Commissioner in the conduct of reviews; and

8. the activities shall be subject, at 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 CSEC Activities*;[13] and

   - specific policies and operational instructions relating to each of the three SIGINT collection activities.[14]

[11] For [redacted], for the period under review, the MD on [redacted] *Operations* issued November 20, 2012, was in effect; for [redacted] for the period under review, the MD on [redacted] *Program* issued November 20, 2012, was in effect, as well as [redacted] MDs on [redacted] (CSEC requests approval for these [redacted] MDs annually at the same time as for the [redacted] MA).

[12] In the previous MAs, CSEC was to "establish and maintain" an automated directory of selectors. Because these directories were already established prior to the MA period under review, the 2012–2013 MAs refer simply to "maintaining" an automated directory of selectors. This requirement applies to the [redacted] Collection and [redacted] MAs, but does not apply to [redacted] activities.

[13] For the period under review, the OPS-1 policy issued December 1, 2012, was in effect.

[14] For activities conducted under the [redacted] MA, OPS-3-1, *Operational Procedures for* [redacted] *Activities*, issued December 11, 2012, was in effect. For activities conducted under the [redacted] Collection and [redacted] MAs, OPS-1-13, *Operational Procedures Related to Canadian* [redacted] *Collection Activities*, issued December 5, 2012, was in effect.

VIII. FINDINGS

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

i) Ministerial authorizations

Finding no. 1: Ministerial Authorizations

The 2012–2013 foreign signals intelligence ministerial authorizations met the conditions for authorization set out in the *National Defence Act*.

Finding no. 2: Ministerial Authorizations and Associated Request Memoranda

The format of the 2012–2013 foreign signals intelligence ministerial authorizations and associated request memoranda to the Minister of National Defence was significantly different than that used in 2011–2012; these changes were positive and resulted in documents that are more properly aligned with the purpose of the ministerial authorizations — to shield CSEC from potential liability under Part VI of the *Criminal Code* — and that are clear and comprehensive.

For the year 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*, namely, that:

- interception will be directed at foreign entities located outside Canada;
- the information to be obtained could not reasonably be obtained by other means;
- the expected FI value of the information that would be derived from the interception justifies it; and,
- satisfactory measures are in place to protect the privacy of Canadians and to ensure that PCs will only be used or retained if they are essential to international affairs, defence or security.

The memoranda followed a consistent format: outlining the legislative basis for the MA scheme; describing the particular class of activities being authorized; detailing the conditions to be satisfied as described in the *NDA* and explaining the ways in which CSEC has satisfied these conditions; and outlining additional relevant operational policies and MDs that apply to the proposed collection activities. They provided the Minister with useful details about collection activities and how they could be employed to satisfy GC intelligence requirements. The inclusion of more detailed contextual information than had been provided in past memoranda is a positive development.

As mentioned in the introduction, the MAs themselves were consolidated according to three distinct classes of activities. In previous years, some had been based on classes of

activities (e.g., [redacted]), but others were based on specific collection programs (e.g., [redacted]) or collection activities [redacted] (e.g., interception activities conducted in support of the GC mission in Afghanistan). The new approach of organizing MAs solely according to classes of activities is more in line with the approval scheme set out in subsection 273.65(1) of the *NDA*, whereby the Minister "may, for the sole purpose of obtaining foreign intelligence, authorize the Communications Security Establishment in writing to intercept PCs in relation to an *activity or class of activities* specified in the authorization" (emphasis added). The MAs shield CSEC from potential liability under Part VI of the *Criminal Code* in the event that they unintentionally intercept PCs in the course of undertaking foreign SIGINT collection. The MAs do not act as a mechanism to approve specific collection programs, which follow separate processes outlined in operational policy.

The new format had the potential to preclude CSEC from providing information about specific collection programs to the Minister in as much detail as they had done in previous years, since the Minister was no longer authorizing a particular collection program, but rather a class of activities. It is positive to note that, in the memoranda accompanying each of the MAs, CSEC broadly outlined the types of intelligence priorities that were to be satisfied through each MA, and gave examples of the type of intelligence that past activities had yielded. It is particularly positive that CSEC attached an annex to the [redacted] collection MA memorandum, which provides information about specific collection programs, current and prospective operations, and [redacted] of CSEC activities. These collection programs are particularly sensitive, and it is appropriate that the Minister continue to be informed of developments, regardless of whether he is approving the actual programs or the class of activities that they employ. The Commissioner's office will continue to monitor this as part of future reviews.

In addition to changes made to the format and structure of the MAs, there were several notable changes to the content of the MAs and their associated memoranda, for example:

- For the previous period, all MAs except the [redacted] MA referred to "interception" rather than "collection" in their titles (e.g. [redacted] interception"). Now all three of them refer to "collection activities" (e.g., [redacted] collection"). The Commissioner's office questioned CSEC about the change in terminology in the titles of the MAs, and CSEC noted that, as part of the overall restructuring process, some of the language used in previous MAs was also reconsidered. CSEC noted that the term "collection" refers to a process whereby CSEC [redacted] a metadata repository. "Interception" occurs when [redacted] has been selected by CSEC based on specific criteria, and is sent from the [redacted] to CSEC traffic repositories. Since the classes of activities specified in the authorizations (e.g., [redacted] are [redacted] collection activities, and since interception [redacted] has taken place, CSEC argues that it is more accurate for the MAs to refer to collection activities, rather than interception activities.[15] The Commissioner's

[15] E-mail from Senior Policy and Review Advisor, External Review, November 1, 2013.

office accepts this explanation, since subsection 273.65(1) of the *NDA* allows the Minister to authorize CSEC "to intercept private communications in relation to an activity or class of activity specified in the authorization." In the 2012–2013 MAs, the classes of activities are the collection programs specified in the MAs.

- Similarly, in paragraph 2 of the 2012–2013 [redacted] MA, the Minister authorizes CSEC to "engage in foreign intelligence collection activities described as [redacted] *that risk* the interception of private communications" (emphasis added), while paragraph 3a) states "This Ministerial Authorization authorizes CSE to intercept private communications for the sole purpose of obtaining foreign intelligence." The two other MAs contain language that is nearly identical to this latter statement, rather than the former.

  The Commissioner's office questioned CSEC about the difference in language between the [redacted] MA and the two others, and CSEC indicated that the language in the [redacted] MA was changed to ensure greater clarity. Through [redacted] activities, CSEC collects data [redacted] and, thus far, [redacted] activities have [redacted] resulted in an intercepted PC. Nevertheless, CSEC finds it prudent to request MAs annually for this activity, in the event that PCs are unintentionally intercepted as part of [redacted] collection. Since the other activities authorized under MA are more likely to result in the unintentional interception of PCs, the language in those MAs stayed consistent with language used in previous years.[16] The Commissioner's office accepts this response, as the change in language is not likely to have an impact on compliance with the law and policy.[17]

- Paragraph 3a) of the [redacted] MA states "[t]his Ministerial Authorization authorizes CSE to intercept private communications for the sole purpose of obtaining foreign intelligence." However, unlike the other two MAs, it did not follow this by stating that the foreign intelligence would be obtained "in accordance with the Government of Canada intelligence priorities." When asked about the omission, CSEC noted that "[t]he exclusion of the language 'in accordance with the Government of Canada intelligence priorities' was an oversight and it should have been included in the 2012–2013 [redacted] MA."[18] The 2012 MD on [redacted] explicitly states that the Minister expects CSEC to "select intelligence targets for these [redacted] operations in accordance with Government of Canada intelligence priorities." Nevertheless, it would be helpful for clarity's sake and for consistency with language found in the *NDA* if future [redacted] MAs

[16] *Ibid.*

[17] CSEC's response is consistent with changes made to the definitions of "collection" and "interception" in *OPS-1-13 Operational Procedures Related to Canadian [redacted] Collection Activities*, released December 5, 2012. Collection: For the purposes of these procedures, collection has two meanings. With respect to private communications, collection is the process of acquiring data as it [redacted] the GII and [redacted] With respect to all other communications, collection is the process of acquiring data as it [redacted] the GII, [redacted] and subsequently forwarding it to the traffic repository. Interception: For the purposes of these procedures, interception occurs when a private communication is selected from [redacted] and is forwarded to the traffic repository.

[18] E-mail from Senior Policy and Review Advisor, External Review, November 1, 2013.

contained explicit reference to conducting operations in accordance with GC intelligence priorities.

- Paragraph 5b(ii) of the [redacted] MA states "if the analyst believes that a solicitor-client communication may contain foreign intelligence, then the analyst shall annotate that communication for retention and forthwith bring the communication to the attention of his/her director or supervisor (via the reporting chain)." This represents a lower level of reporting than is mandated in the other two MAs, as well as in OPS-1, all of which require that a director (rather than a supervisor) ultimately be informed in these cases. The Commissioner's office pointed out this inconsistency and CSEC noted that it will be corrected in future MAs, to clarify that directors will need to be informed in such cases.

- The [redacted] MA now lists the 2011 MD on *Collection and Use of Metadata* on the list of MDs that apply to [redacted] activities. It was not included in the previous [redacted] MA, although the MD applied to all metadata activities and therefore was in effect in any case. Nevertheless, it is positive that, for clarity, CSEC added it to the [redacted] MA explicitly.

- Both the [redacted] and [redacted] MAs state that CSEC "shall maintain an automated directory of selectors which it is satisfied relates to foreign entities located outside Canada." Previous versions stated that CSEC would "establish and maintain" a list of selectors. CSEC explained that these lists had already been established; therefore the language would have been redundant. This requirement does not apply to [redacted] activities.[19]

- Paragraph 3 of [redacted] MA states "*in cases where access to a [redacted] is required*, where [redacted] has been obtained and, where CSE has grounds to suspect that the [redacted] of potential foreign intelligence value, this authorization will allow CSE to work [redacted] for the purpose of obtaining foreign intelligence." The italicized portion was not included in the previous year's MA. CSEC noted that the additional language "was added for clarity to avoid confusion or future conflicts of interpretation. Where [redacted] of interest is generally conducted covertly, [redacted] Thus, the additional language found in paragraph 3 highlights [redacted]

[19] During the review, the Commissioner's office was informed that the [redacted] program has begun incorporating [redacted] into its operations. This raises the question of whether incorporating a list of selectors could be helpful for [redacted] in the future. The Commissioner's office may explore this as part of a future review of the [redacted] program, which is currently on the Commissioner's office's work plan.

[redacted] is concerned."[20] This is a positive clarification on CSEC's part.

- As part of the restructuring of the SIGINT MAs, activities previously conducted under the Afghanistan MA were covered by the [redacted] MA for the 2012–2013 period. The Commissioner's office asked whether collection activities in Afghanistan were now being conducted strictly under the [redacted] MA, or whether they could take place under other MAs as well. Because MAs apply to classes of activities, they give broad authority to undertake these classes of activities anywhere, so long as the activities themselves are not directed at Canadians or people in Canada, and so long as they are conducted for the sole purpose of obtaining FI, in accordance with GC priorities. As such, activities in Afghanistan could be undertaken under any of the three MAs. The former Afghanistan MA was absorbed into both the 2012–2013 [redacted] MAs. This occurred because CSEC had previously established both [redacted] collection [redacted] Afghanistan, under the Afghanistan MA, in support of the Canadian mission. [redacted] at the end of Canada's combat operations in 2011. During the review period, CSEC continued to maintain [redacted] For the reporting year, the only activities in Afghanistan that CSEC reported on occurred under the [redacted] MA.

In summary, the memoranda were restructured and add further detail about how the various SIGINT collection activities contribute to CSEC's overall mission. The new MA format reduces administrative burden and provides for an approval process that is better aligned with the purpose of MAs as set out in the *NDA,* namely, to shield CSEC from potential liability under Part VI of the *Criminal Code*. Most importantly, it does not reduce CSEC reporting requirements to the Minister: statistics are still required; CSEC must still report when any serious issue arises in the implementation of the MAs. As part of future annual reviews, the Commissioner's office will continue to monitor SIGINT MAs and accompanying memoranda to ensure, among other things, that the new format does not detract from information provided to the Minister on specific collection programs. The Commissioner's office will also monitor CSEC efforts to address minor deficiencies and inconsistencies in the MA documents identified in this review.

[20] E-mail from Senior Policy and Review Advisor, External Review, November 1, 2013.
[21] The Second Parties are CSEC's four SIGINT partners: the U.S. National Security Agency (NSA), the U.K. Government Communications Headquarters (GCHQ), the Australian Signals Directorate (ASD), and the New Zealand Government Communications Security Bureau (GCSB).

ii) Policies and procedures

Finding no. 3: Policies and Procedures

With one exception, revised versions of CSEC operational policies did not contain major amendments that would have significantly changed the conduct of activities under MA authorities.

The Commissioner's office reviewed amendments made to CSEC operational policies and MDs in effect for the period under review. The MDs on *Accountability Framework, Privacy of Canadians,* [redacted] *Operations* and [redacted] were all updated prior to the start of the MA period, but did not contain major amendments that would have significantly changed the conduct of activities under MA authorities. Similarly, updated versions of OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities* (revised effective December 1, 2012) and OPS-3-1, *Operational Procedures for* [redacted] *Activities* (revised effective December 11, 2012) will not significantly change the conduct of activities under MA authorities. However, amendments made to OPS-1-13, *Operational Procedures Related to Canadian* [redacted] *Collection Activities* (revised effective December 5, 2012) may alter approvals required for certain sensitive operations, which are explained in greater detail below. Revisions made to policies will be examined in further detail as part of future reviews of specific programs by the Commissioner's office.

The Commissioner's office reviewed updated policy guidance issued by CSEC on December 5, 2012, in the form of *OPS-1-13 Operational Procedures Related to Canadian* [redacted] *Collection Activities*. Since the Minister is no longer approving specific [redacted] collection programs through MAs, but is rather authorizing the interception of PCs in relation to broad classes of activities, the office wanted to see if procedures for approving sensitive collection programs like [redacted] or [redacted][22] had been strengthened or had changed in any way. The guidance found in this latest version of OPS-1-13 is less clear than guidance in previous versions regarding what role the Minister plays in approving new collection [redacted] under these programs. Given the sensitive nature of these activities, and their potential [redacted] it is critical that the Minister be accountable for approving new collection [redacted] under these programs, and that the new MA format not detract from any pre-existing authority the Minister had with respect to [redacted] or [redacted]

Since the Minister is now approving an overall collection activity [redacted] through MAs, rather than signing off on a specific collection program ([redacted] or [redacted]), it makes it even more important that clear approval processes exist in operational policy for sensitive activities under [redacted] and [redacted] consistent with Cabinet direction.

The Commissioner's office asked CSEC why the new version of OPS-1-13 contained general and less defined information about the approval process for [redacted]

[22] [redacted] refers to CSEC's collection program [redacted]

CSEC indicated that more general direction simplified and shortened the new version of OPS-1-13, while allowing for detailed guidance to be revised more readily, should the need arise.[23] We also asked for detailed guidance provided by the Director, SIGINT Requirements, regarding additional approval for [redacted] and [redacted] In a written response, CSEC indicated that draft guidance was being worked on, but that it had not yet been finalized for approval.[24]

Recommendation no. 1: Policies and Procedures

To ensure proper accountability for sensitive activities, CSEC should promulgate detailed guidance, as soon as possible, regarding the additional approvals required for certain activities relating to the [redacted] program and to CSEC operations [redacted]

iii) Technology

Finding no. 4: Technology

In 2012–2013, CSEC made some changes to technology used for some of its foreign signals intelligence collection activities, the impact of which may be examined in subsequent in-depth reviews of these activities.

[redacted] MA

- CSEC continued to expand the [redacted] program, and engaged in ongoing [redacted] that will continue to be the program's focus over the next twelve months.[25] In addition, CSEC is working to expand [redacted] capabilities, enabling analysts to better identify and prioritize collection sources, in line with current intelligence priorities.

- [redacted] initiative that will see a complete overhaul to the [redacted] collection [redacted] Developers are redesigning and implementing [redacted] that will further minimize risks of unintentional collection, while providing analysts with more refined and relevant traffic.

[23] E-mail from Senior Policy and Review Advisor, External Review, March 3, 2014.
[24] E-mail from Senior Policy and Review Advisor, External Review, March 7, 2014.
[25] The [redacted] program (also known as the "[redacted]" program) refers to CSEC [redacted]

[redacted] MA

For [redacted] collection:

- Digital Network Intelligence (DNI) processing has been upgraded, while Dialed Number Recognition (DNR) processing remains unchanged.[26]
- A [redacted] collection capability was added at Masset.

For the [redacted] program:

- [redacted] in August 2013.
- [redacted] in April 2013.
- [redacted] was not operational at the beginning of the MA period, [redacted] in May 2013.

For [redacted]

- [redacted] in August 2013. Sustained collection started in September 2013.

[redacted] MA

- According to CSEC, there were no significant changes to the collection technologies implemented during the review period for [redacted] activities. However, CSEC did indicate that there are [redacted] capabilities of collecting foreign [redacted] activities.
- There were [redacted] operations ([redacted]) initiated during the reporting period.[27]

The Commissioner's office noted that the cover name [redacted] had previously been used to refer to a [redacted] set up under MA authority in the 2011–2012 period. CSEC indicated that [redacted] used to refer to [redacted] but now it refers to the capability [redacted] in question is now referred to as

[26] Digital Network Intelligence metadata is metadata associated with [redacted] communications (e.g., e-mail address). Dialled Number Recognition metadata generally refers to telephone and fax routing information (e.g., telephone number or fax number).

[27] [redacted] are approved by the Chief's delegate, the Chief or the Minister.

[redacted] while [redacted] refers to the overall program. According to CSEC, these names were established to avoid confusion in the event that [redacted][28]

The Commissioner's office has no immediate questions or concerns about these [redacted] capabilities based on CSEC's description. Their impact may be examined as part of future, in-depth reviews of SIGINT activities.

Privacy Picker tool

During the review period, CSEC finalized and launched a tool called Privacy Picker, which was made available within the [redacted] in September 2013. The Privacy Picker was designed to assist analysts in choosing the appropriate privacy annotation or marking for traffic items, in accordance with OPS-1 policy. Many of the annotations use similar combinations of letters, making it difficult for analysts to remember them and apply them correctly 100% of the time. The Privacy Picker asks analysts a series of basic questions about a piece of traffic being annotated, and based on the answers, automatically generates an annotation for the traffic item. Then it asks the analyst to confirm whether they would like this annotation to be applied to the traffic item. As such, the final decision regarding the appropriate annotation to apply continues to rest with analysts. While the Privacy Picker is not foolproof, since it requires analysts to answer a group of questions accurately, it does reduce the potential for human error in the annotation process. CSEC stated that the tool also saves analysts time in determining the appropriate annotation or marking to apply to traffic items. CSEC has informed the Commissioner's office that feedback from analysts has been very positive thus far. The Commissioner's office also views the implementation of the Privacy Picker as a positive step that is likely to assist analysts in appropriately annotating private communications and communications that contain information about Canadians.

[redacted] tool

During the period under review, CSEC made a new [redacted] feature available to all [redacted] users. The so-called [redacted] was developed to reduce analyst workload, as it had been discovered that analysts were relying on sources and tools outside of the [redacted] to obtain additional information about traffic items, often pertaining to the [redacted] of targets. In fiscal year 2012–2013, CSEC's SIGINT Systems Development unit began work on improving analysts' traffic results, including [redacted] The [redacted] was part of this process and became available to all [redacted] users in July 2013. The [redacted] ensures that when a user's search results are loaded into [redacted], a [redacted] about the traffic items, including the [redacted] In the [redacted] system, [redacted] which is displayed next to the traffic item. Analysts can choose to use this feature by activating it in their "preferences".

[28] E-mail from Senior Policy and Review Advisor, External Review, February 18, 2014.

Additional, more specific [redacted] data is also available to analysts through toolbar options, and users can control and customize which data they want to view. It is still the analyst's responsibility to validate the results of the automated search and correlation of [redacted] data. The feature is generally accurate, but it is not correct 100% of the time. [redacted] represents a positive development in that it assists analysts in recognizing communications that [redacted]

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

Finding no. 5: Metrics Relating to Interception and to the Privacy of Canadians (1)

It is a positive development that, while CSEC made significant changes to how it counts "collected communications" that it reports to the Minister for its foreign signals intelligence collection activities, it continues to use the same method as in previous years to count and report recognized private communications, which will enable a more accurate comparison between the overall number of collected communications and the number of intercepted private communications (that is, "traffic files").

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

1. the total volume of collected communications during the period in which the MAs were in force;

2. the total volume of recognized PCs unintentionally intercepted during the period in which the MAs were in force;

3. the total volume of recognized PCs unintentionally intercepted and destroyed during the period in which the MAs were in force;

4. the total volume of recognized PCs unintentionally intercepted and used or retained on the basis that they are essential to international affairs, defence or security during the period in which the MAs were in force;

5. the total volume of recognized PCs unintentionally intercepted, retained and subsequently used in finished CSEC reports during the period in which the MAs were in force; and

6. the total volume of recognized PCs unintentionally intercepted and subsequently retained, during the period in which the MAs were in force, that were recognized as seeking, formulating or delivering legal advice.

In previous years, the number of collected communications reported by CSEC as part of the annual review of SIGINT MAs and intercepted PCs was based on the number of "data items" captured in CSEC systems. According to CSEC, a data item is considered a [redacted]

Beginning in the 2012–2013 MA period, CSEC began counting the volume of collected communications as the number of traffic files rather than the number of data items. CSEC believes that traffic files are more representative of the number of communications collected, and are therefore a better metric. It is important to note that, due to the fact that a traffic file is generally [redacted] this change in metric results in a [redacted] figure for the overall number of collected communications during the period under review.

As such, the Commissioner's office requested that CSEC provide statistics according to both volumes of traffic files and volumes of data items. This allowed for a direct comparison of volumes of collected communications from the 2012–2013 period with volumes from previous periods, using the same metric. The result is that, since the previous MA period, collection activity has [redacted] by about [redacted]% for [redacted] and by about [redacted]% for [redacted], and has [redacted] by about [redacted]% for [redacted]

Given the change in metric relating to the number of collected communications, we asked CSEC whether it also changed the way in which it accounts for intercepted PCs. CSEC provided the Commissioner's office with a written response indicating that the organization has not changed the methodology for the way in which it accounts for intercepted PCs. Since intercepted PCs were already counted as traffic files, direct year-over-year comparisons of volumes of intercepted PCs are possible without adjusting the metrics. The change in metric also renders CSEC statistics more accurate in their comparison of the total number of collected communications with the number of intercepted private communications, as both figures are now based on traffic files.

Finding no. 6: Metrics Relating to Interception and to the Privacy of Canadians (2)

Overall, in 2012-2013, the volume of communications collected by CSEC's foreign signals intelligence collection activities [redacted] while the number of recognized private communications unintentionally intercepted by CSEC remained very small.

The Commissioner's office observed the following respecting the metrics relating to collection and to the privacy of Canadians (these metrics represent CSEC's reported volumes of data items because doing so allows for a direct year-over-year comparison):

- The total number of communications collected under the [redacted] MA [redacted] from [redacted] in 2011–2012, to [redacted] in 2012–2013 (according to the new traffic file metric, the figure for 2012–2013 is [redacted]).
- The total number of communications collected under the [redacted] MA [redacted] significantly from [redacted] in 2011–2012, to [redacted] in 2012–2013 (according to the new traffic file metric, the figure for 2012–2013 is [redacted]).
- The total number of communications collected under the [redacted] MA [redacted] significantly from [redacted] in 2011–2012 to [redacted] in 2012–2013 (according to the new traffic file metric, the 2012–2013 figure is [redacted]).[29]

The Commissioner's office asked CSEC for an explanation as to why the volumes had shifted so significantly in the case of [redacted] and [redacted] collection. In its response, CSEC noted that "[d]ue to the nature of SIGINT collection (i.e., [redacted], volume fluctuations are inevitable and the exact causes of these fluctuations are difficult to record accurately."[30]

CSEC went on to list some, but admittedly not necessarily all, of the factors that may have contributed to the fluctuations in metrics. According to CSEC, changes that occurred for some of the [redacted] could be contributing factors to the overall [redacted] in volume among [redacted] collection activities:

- [redacted] in the reporting period;
- [redacted] in the reporting period;
- [redacted] and [redacted] part-way through the reporting period; and

[29] 2011–2012 figures for [redacted] collection include total volumes of communications collected under both the 2011–2012 [redacted] MA and the 2011–2012 [redacted] MA, since these programs are now captured under the [redacted] MA (figures for the 2011–2012 [redacted] MA, which also now falls under the [redacted] MA, were not provided in 2011–2012, since sustained collection had not yet begun). 2011–2012 figures for [redacted] collection include both the 2011–2012 MA on Interception Activities Conducted in Support of the Government of Canada Mission in Afghanistan and the 2011–2012 [redacted] MA, since these programs are now captured under the [redacted] MA. This provides an accurate basis for comparing year-over-year developments.

[30] E-mail from Senior Policy and Review Advisor, External Review, February 20, 2014.

- [redacted] during the MA period [redacted]

According to CSEC, for [redacted] collection activities, [redacted] collection asset was likely a key contributor to the [redacted] in the number of collected communications."[31] The Commissioner's office is currently undertaking an in-depth review of the [redacted] program, and may examine the [redacted] in collected communications for [redacted] collection activities in further detail as part of that review.

The overall number of recognized PCs unintentionally intercepted by CSEC under the 2012–2013 MAs [redacted] from the previous MA period (from [redacted] in 2011–2012, to [redacted] in 2012–2013). All of the recognized PCs that were intercepted by CSEC in 2012–2013 were done so under the [redacted] MA.

In 2012–2013, CSEC destroyed most recognized PCs unintentionally intercepted ([redacted] PCs). CSEC retained 66 recognized PCs, [redacted] from [redacted] in 2011–2012. Of these 66, 41 were used in reporting and 25 were retained for future use. There were no recognized solicitor-client communications unintentionally intercepted by CSEC in 2012–2013.

In its annual strategic policy update briefing to the Commissioner's office, CSEC noted that the new MA rationalization does not reduce reporting requirements to the Minister. The Commissioner's office will monitor future reporting to the Minister, including the Ministerial Authorization Year-End Report for 2012–2013, to see whether volumes of intercepted communications continue to be reported according to collection program as well as collection activity. Such reporting will ensure that the Minister remains apprised of developments in programs that were formerly the subject of specific MAs, but that now fall within broader categories of activity. Reporting by collection program can also provide an opportunity to explain any significant changes to the programs or to volumes of intercepted communications, and how these changes relate to or impact GC intelligence priorities.

In addition to the reasons outlined above, the Commissioner's office will also monitor future reporting to the Minister, including the *Ministerial Authorization Year-End Report for 2012–2013*, to determine if the new way in which CSEC counts intercepted communications will affect messaging to the Minister. It will be important for CSEC to clearly explain the impact that the change in metric will have on year-over-year comparisons of data volumes.

Beyond the changes to MA format from the previous reporting period, and changes to the way CSEC counts intercepted communications, the Commissioner's office identified some broader issues with the way CSEC accounts for and reports PCs. The figure for the number of PCs retained that is reported to the Minister only reflects those PCs that are retained following the expiry of the MA period (i.e., beyond November 30 of that year).

[31] *Ibid.*

PCs that are retained for a portion (even a large portion) of the year, but deleted prior to the MA expiry are counted as "deleted" PCs, although it is possible that they had been retained for nearly one year. The year-end figures do not indicate how long CSEC retains PCs throughout the year.

The Commissioner's office asked CSEC whether there is a way to assemble statistics showing how many PCs are annotated and retained for a period of time, but deleted prior to the expiry of the MA (and therefore not reflected in the year-end statistics that the Minister sees). CSEC responded by stating that they are discussing the use of a business intelligence tool called [redacted] as a way to determine the number of traffic items marked as PCs throughout the year but not kept or used in reports.[32]

The issue with the way PCs are reported to the Minister became clear to the Commissioner's office when it came time to review retained PCs for compliance with law and policy. During a briefing by SIGINT Programs Oversight and Compliance (SPOC) on November 15, 2013, the Commissioner's office was told that, as of November 4, CSEC had annotated 40 PCs for retention and that, while this number was likely to change slightly by November 30, it would not change significantly. However, when the final list of retained PCs was provided to the Commissioner's office on December 4, only 13 PCs were marked as having been retained. CSEC subsequently informed the Commissioner's office that between November 4 and November 30, 30 of the 40 PCs originally annotated for retention had their annotations changed from INCA (which means they would be retained) to INCAN (which means they would be deleted), while three new PCs had been annotated for retention since the original November 4 list was compiled.[33] Of the 30 PCs that had been marked for deletion, 21 belonged to one analyst working on one file. The fact that 75% of the PCs marked as essential as of November 4 had their annotations changed to non-essential in the final two weeks of the MA period was a cause for further investigation. As a result, the Commissioner's office made a decision to examine all 30 of the PCs that had been marked for deletion in the lead-up to the end of the MA period to better understand the reason behind the timing, in

[32] [redacted] is a business intelligence tool, used to measure all stages of the SIGINT End to End Process. First implemented in 2010, [redacted] data is used by teams within SIGINT to support evidence-based decision making for SIGINT and CSEC executives, and for external reporting requirements. [redacted] is currently linked to four SIGINT systems: [redacted] With these systems linked, SIGINT teams can track metrics on reporting, traffic, targeting and selectors, as well as SIGINT training data. According to CSEC, [redacted] is expected to be linked to other SIGINT systems and applications but implementation will depend on resources, operational requirements and senior management direction.

[33] 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 four applicable privacy annotations in such a case: INCA (one-end located in Canada), OUCA (one-end Canadian outside Canada), INCAS (in Canada/Solicitor Client Privilege), and OUCAS (outside Canada/Solicitor Client Privilege). 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, and OUCASN. Intercepted communications containing information about Canadians, but which do not have intelligence value, are annotated as IACN.

addition to examining all 13 PCs that were retained at year-end.[34] Because PCs that are annotated for deletion remain in the system for an additional [redacted] the Commissioner's office was able to view these before they were destroyed.

In examining the PCs that had been annotated for deletion, the Commissioner's office found that it was not uncommon for SIGINT analysts to hold on to PCs that were no longer relevant, sometimes for several months, prior to annotating them for deletion. As of October 2013, SPOC sends out quarterly reminders via e-mail to managers whose analysts have retained PCs but have not yet reported on them. Prior to that time, SPOC sent monthly reminders, based on [redacted] reporting, to managers. The purpose of these e-mails is to remind analysts to review their holdings and annotate for deletion any traffic that is unlikely to be used in an EPR or no longer meets the criteria for retention, as set out in OPS-1, paragraph 3.3.[35] These reminders are meant to reduce the risk that analysts would retain PCs for any longer than is strictly necessary. The reminders include a list of analysts who have unused INCA traffic, but only include traffic that was marked for retention since the previous reminder had been sent. For example, a traffic item annotated in January would appear in the February reminder, but not in the March reminder. The Commissioner's office obtained copies of the messages that were sent to analysts during the 2012–2013 period. Despite SPOC's reminders, many analysts retained PCs long after they should have annotated them for deletion. The fact that so many PCs were deleted in the two weeks prior to the expiry of the MAs suggests that the obligation to report on PCs retained at the end of the MA period acts as an incentive for analysts to delete PCs at that time.

Obliging CSEC to provide quarterly statistics on the number of retained PCs (but still report annually on them) may provide further incentive for analysts to delete PCs as soon as they are no longer essential, rather than waiting until the end of the MA period.

A quarterly breakdown of figures would also provide the Minister with a more accurate picture of how CSEC retains and uses PCs in the course of its work throughout the year, and would thus enhance CSEC accountability to the Minister.

There was one instance in which a PC had sat in the Consolidated Traffic Repository (CTR) for five years, even though it was no longer relevant. Clearly, the quarterly reminders, and in this case even the end-of-year reminders by SPOC were not always effective in getting analysts to comply with retention policies for PCs. However, the prospect that retained PCs would be reported to the Minister, and that analysts marking these PCs for retention would have to meet with the Commissioner's office to explain

[34] Some of the 13 traffic files that were initially annotated and retained as PCs during the 2012–2013 MA period were annotated as PCs in error. These annotations were subsequently changed by CSEC analysts when it was found that the files did not in fact constitute PCs.

[35] According to paragraph 3.3 of OPS-1, PCs, the communications of a Canadian located outside Canada, or a communication that contains information about Canadians may be retained if it: is FI as defined in the *NDA* using specified criteria; is essential to protect the lives or safety of individuals of any nationality, using specified criteria; or, contains information on serious criminal activity relating to the security of Canada using specified criteria.

their rationale as part of this review seemed to encourage the deletion of non-essential PCs at the end of the MA period.

The issue of PCs lingering in CSEC systems when they no longer meet criteria for essentiality is linked to other problems identified by the Commissioner's office, which are discussed in more detail later in this report.

Recommendation no. 2: Metrics Relating to Interception and to the Privacy of Canadians

CSEC should make available to the Minister more comprehensive information regarding the number of collected communications and intercepted private communications that it acquires and retains throughout an MA period, in order to enhance accountability to the Minister.

Lack of clarity in policy regarding obligation to annotate recognized PCs

Finding no. 7: Essentiality of Used or Retained Private Communications (1)

Contrary to policy, one analyst viewed and recognized 18 private communications during the period under review, but did not annotate them until several weeks later.

Following the review by the Commissioner's office of all PCs annotated for retention as of the end of the 2012–2013 MA period, as well as the review of PCs annotated for deletion during the final two weeks of the MA period, CSEC informed us that there were other PCs that we may be interested in viewing. This was because an analyst, who had viewed PCs during the MA period, had only annotated them for retention in December, following the expiry of the 2012–2013 MAs. As such, CSEC would be accounting for them in their 2012–2013 statistics as part of their Ministerial Authorization Year-End Report, since they were intercepted under the authority of the 2012–2013 [redacted] MA.

The Commissioner's office interviewed the analyst, as well as the manager and team leader involved in this particular case. CSEC explained that the analyst had recognized 18 PCs over the course of several days, beginning November 19, 2013, in the context of target development pertaining to an [redacted] operation. The team at CSEC was still building its target set, and would not fully understand the relevance of these e-mails until further information could be gathered to compare against it. This follow-up information, the Commissioner's office was told, was not available until after the expiry of the 2012–2013 [redacted] MA.

Since the analyst who had captured the PCs was not sure if they would end up being relevant, a decision was taken to not annotate them at all. The rationale was that, if they had been annotated as INCA (having foreign intelligence value), the system would retain

them for [redacted] following the date of annotation. The analyst explained that, if the team had been unable to gather the appropriate intelligence in the ensuing weeks to validate the PCs as having intelligence value, she did not want the system to unnecessarily retain them for a prolonged period of time. Conversely, if the analyst had annotated the PCs as INCAN (not having intelligence value), the system would have automatically destroyed them after [redacted] In that case, if the team had been able to gather the appropriate intelligence in the ensuing weeks to validate the PCs as having intelligence value, but that this process took longer than [redacted] the system would have already destroyed the PCs and any potential information of interest to emerge from them.

Recommendation no. 3: Essentiality of Used or Retained Private Communications (1)

CSEC analysts should immediately annotate recognized private communications for essentiality to international affairs, defence or security, as required by the *National Defence Act*, or, if not essential, for deletion.

The Commissioner's office believes that the analyst in the case above acted in good faith, and was legitimately interested in appropriately protecting the privacy of Canadians. However, there was another possible course of action in this case which was not explored. For example, the analyst would have been within her right to mark the PCs as INCA (having intelligence value), since it would be necessary in the ensuing weeks to compare these PCs against further intelligence to better understand the nature of the target set. While the rationale for not doing so, highlighted above, was that a PC marked INCA is retained by the system for [redacted] (and retention would be undesirable if information gathered in the ensuing weeks did not validate the PCs as having intelligence value), it would have been possible for the analyst to revisit the original marking and change it to INCAN at any future point in time.

This would have been the preferred option from the point of view of accountability. By not marking the PCs in the first instance, the overall statistics on the number of recognized PCs were rendered inaccurate. Ideally, the PCs in question would have been annotated immediately as INCA, pending the receipt of additional information to aid in reporting. If this additional information had not come the following month, the analyst would have been able to change the original marking from INCA to INCAN.

CSEC policy guidance on retaining PCs is found in OPS-1, Section 2.8:

> If analysts whose functions are directly related to the production of foreign intelligence reports recognize that SIGINT traffic is a private communication, a communication of Canadians located outside Canada, or contains information about Canadians, and which is not essential to international affairs, defence or security, then they must, upon recognition, annotate this traffic for deletion. Private communications and communications of Canadians located outside Canada deemed

> essential to international affairs, defence, or security must also be annotated appropriately.

This explicitly states that PCs that are not relevant need to be annotated for deletion immediately upon recognition. However, while it seems to imply that analysts should immediately annotate PCs that are deemed essential, it leaves room for interpretation. This leaves open the possibility that analysts could encounter PCs and not immediately assess their essentiality and the appropriate annotation. The risk in not immediately annotating a recognized PC is that CSEC may be acting contrary to the *NDA* requirement "to ensure that private communications will only be used or retained if they are essential to international affairs, defence or security." It also creates an accountability gap whereby the Minister is not informed of certain PCs (because they are not systematically tracked or accounted for), and it skews the figures that the Minister is provided with at the end of the MA period regarding retained PCs. As such, analysts should immediately annotate recognized PCs and take steps to validate original assumptions or decisions about relevance. These steps can include consultation with team members or with other analysts who may have a higher level of expertise on a given target or set of traffic.

2. Essentiality of retained private communications

> ***Finding no. 8: Essentiality of Used or Retained Private Communications (2)***
>
> Based on the information reviewed and the interviews conducted, in 2012–2013, all private communications that were recognized by CSEC were intercepted unintentionally, and all but one of those used or retained were essential to international affairs, defence or security, as required by the *National Defence Act*.

The Commissioner's office's examination involved several meetings with analysts and team leaders, as well as an overview briefing on the [redacted] which is a program that CSEC uses to organize, view and mark raw traffic from the CTR.

As stated above, the Commissioner's office even examined some PCs deleted between November and December because the discrepancy in number had been so great between the SPOC meeting and when we received the list. The Commissioner's office reviewed an additional 18 PCs that had been viewed in November 2013, but not marked as PCs until December. These interviews provided a number of insights into how to improve CSEC accountability to the Minister. As such, viewing all retained PCs was a very valuable exercise, and yielded results that sampling would likely not have yielded.

The PCs were retained by several different reporting areas, and related to a number of GC intelligence priorities, including Cabinet Confidence

Cabinet Confidence

With one exception, all retained PCs had a clear link to GC intelligence priorities, and CSEC's National SIGINT Priorities List. The Commissioner's office found that all PCs that were recognized by CSEC were intercepted unintentionally, and all but one of those used or retained were essential to international affairs, defence or security, as required by

the *NDA*. That said, in addition to the issues outlined above, a number of inconsistencies of practice were identified in the review of intercepted PCs, which are the subject of subsequent findings as explained below.

Finding no. 9: Essentiality of Used or Retained Private Communications (3)

In one case, an analyst recognized and appropriately flagged that a communication was a private communication; however that communication did not pertain to the analyst's target set, and, contrary to policy, the analyst incorrectly marked it for retention even though the analyst did not assess whether the communication was essential to international affairs, defence or security, as required by the *National Defence Act*.

One analyst had marked a PC as INCA (essential) when he recognized it as a PC within a search query, even though he could not determine whether or not it was relevant. This analyst explained that traffic pertaining to another analyst's files had come up during one of his search queries in the [redacted] system. Because he recognized the PC, he felt that he had to annotate it as such. However, since he was not in a position to determine its essentiality (i.e., whether it constituted foreign intelligence under the *NDA*), and he did not want to delete traffic that another analyst may have found to be essential, the analyst marked it as essential. However, he did not inform the analyst who would have been in a position to determine its essentiality that he had pulled the traffic, and the PC was retained in the system. This action was not in line with CSEC policy. Sections 3.3 of OPS-1 states that a recognized PC may be retained if it is foreign intelligence as defined in the *NDA* using specific listed criteria; if it is essential to protect the lives or safety of individuals of any nationality, using specific listed criteria; or if it contains information on serious criminal activity relating to the security of Canada using specific listed criteria. Section 3.4 goes on to state that information that does not relate to one of the criteria listed in Section 3.3 must be annotated for deletion in traffic databases if recognized. Since the analyst in this case was admittedly not in a position to determine essentiality based on the criteria established in OPS-1, the analyst violated CSEC policy by annotating the PC for retention. The PC should have been annotated for deletion pending assessment by the appropriate analyst, who could have made an informed determination regarding essentiality.

Recommendation no. 4: Essentiality of Used or Retained Private Communications (2)

CSEC analysts should regularly assess, at a minimum quarterly, whether the ongoing retention of a recognized private communication not yet used in an End Product Report is strictly necessary and remains essential to international affairs, defence or security or whether that private communication should be deleted.

Finding no. 10: Essentiality of Used or Retained Private Communications (4)

A number of analysts retained private communications that had once been, but were no longer, essential to international affairs, defence or security; despite regular, written reminders to review and mark for deletion any private communications that were no longer essential, these private communications were retained — in some cases, for several months — until just before the expiration of the ministerial authorizations and prior to associated reporting to the Minister.

One analyst had kept more than 13 PCs from earlier in the MA period (as early as December and continuing through the spring). These PCs related to [redacted] to Canada, and were pertinent e-mails at the time of interception. However, the individuals involved in that [redacted] and therefore these PCs were no longer essential, since they would not be used as the basis for future reports. The analyst recognized that she should have deleted these PCs, in accordance with CSEC policy, when it became clear that they were no longer essential to ongoing intelligence collection and that they would not form the basis of future reporting. The quarterly e-mails sent by SPOC did not have the desired effect of ensuring that this analyst would delete PCs that were no longer essential. The analyst responded to prompting at the end of the MA period, when the consequences of retaining a PC were that it would be counted among statistics provided to the Minister, and that the Commissioner's office would review the retained PC for compliance with the law and with CSEC policy.

Requiring CSEC to report quarterly figures for retained PCs to the Minister (even if the report itself remains annual) could strengthen compliance with retention and deletion obligations on the part of CSEC analysts. The Commissioner's office asked whether the [redacted] system was equipped (or could be configured) to provide statistics of this kind. SPOC initially indicated that it would be possible to provide these types of statistics using currently available tools, but that CSEC does not track this data systematically at the present time. Following further inquiries, CSEC noted that [redacted] would only be able to provide these kinds of statistics following several months of software development.

Recommendation no. 5: Foreign Targets and [redacted]

CSEC should promulgate guidance regarding the protection of privacy and the handling of intercepted communications of a targeted foreign entity located outside Canada that include [redacted] of a Canadian or person in Canada as part of those intercepted communications.

Another issue arose pertaining to this same analyst's work. One of the [redacted] she had retained was a [redacted] which was apparently [redacted] however, [redacted] of the communication [redacted] The analyst asked SPOC for

guidance as to how to treat the material, and held onto it for many months during the review period, pending guidance (but apparently did not receive any guidance).

In her interview, this analyst explained that a foreign selector outside Canada was targeted, which [redacted] The analyst asked SPOC for guidance and kept the traffic pending a decision from SPOC, which never arrived. The traffic was then deleted at the end of the MA period. As situations like this implicate the privacy of Canadians and are likely to arise in the future, it is recommended that CSEC promulgate guidance regarding situations in which [redacted] While these situations may be atypical, the privacy interest involved in them is considerable nonetheless.

Finding no. 11: Essentiality of Used or Retained Private Communications (5)

All End Product Reports based on private communications contained foreign intelligence relating to international affairs, defence or security.

During the 2012–2013 MA period, CSEC issued [redacted] EPRs that were derived from information contained in 41 unintentionally intercepted private communications. These reports related to GC intelligence priorities in such areas as Cabinet Confidence Cabinet Confidence

The Commissioner's office reviewed all CSEC reports issued during the 2012–2013 MA period that were based, in whole or in part, on intercepted PCs. The Commissioner's office found that all of the reports contained foreign intelligence relating to international affairs, defence or security. The Commissioner's office had no questions with respect to these reports.

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

Finding no. 12: CSEC activities in response to a previous recommendation of the Commissioner on accountability and [redacted]

CSEC made further progress in implementing a recommendation from the 2010–2011 *Review of Foreign Signals Intelligence Ministerial Authorizations and Intercepted Private Communications*, regarding reporting to the Minister of National Defence on the number of one-end Canadian communications acquired through [redacted] in a manner similar to what CSEC does for recognized private communications intercepted under the other foreign signals intelligence collection programs.

Information on [redacted] was not included in the *Ministerial Authorization Year End Report for 2011–2012*, but was included in the Chief's Annual Report to the Minister, issued in December 2013. It is a significant positive development that CSEC has begun reporting on this metric. CSEC informed the Commissioner's office that a significant

amount of technical work and training had been undertaken in 2012 to enable the marking of recognized one-end Canadian e-mails acquired through the [redacted] program.[36] SPOC began meeting with the SIGINT Systems Development office in March 2012 to effect this change, and the new marking requirement was incorporated into analyst training on annotations in September 2012. CSEC also informed the Commissioner's office that use of the new marking across the SIGINT organization began in December 2012.

The statistics that were provided in the Chief's Annual Report reflected the period from December 1, 2012, to March 31, 2013. The 2013–2014 Annual Report will provide statistics for the full fiscal year of April 1, 2013, to March 31, 2014.

IX. CONCLUSION

This combined review of SIGINT MAs encompassed the 2012–2013 [redacted] collection and [redacted] MAs.

The purpose of this review was to:

- ensure that the MAs were authorized, and 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 all of the PCs unintentionally intercepted for compliance with the law and for protection of the privacy of Canadians

The 2012–2013 SIGINT MAs met the conditions for authorization set out in the *NDA*.

The format of the 2012–2013 SIGINT MAs and associated request memoranda to the Minister of National Defence was significantly different than that used in 2011–2012; these changes were positive and resulted in documents that are more properly aligned with the purpose of the MAs — to shield CSEC from potential liability under Part VI of the *Criminal Code* — and that are clear and comprehensive.

With one exception, revised versions of CSEC operational policies did not contain major amendments that would have significantly changed the conduct of activities under MA authorities.

In 2012–2013, CSEC made some changes to technology used for some of its SIGINT collection activities, the impact of which may be examined in subsequent in-depth reviews of these activities.

[36] E-mail from Senior Policy and Review Advisor, External Review, November 1, 2013.

It is a positive development that, while CSEC made significant changes to how it counts "collected communications" that it reports to the Minister for its SIGINT collection activities, it continues to use the same method as in previous years to count and report recognized PCs, which will enable a more accurate comparison between the overall number of collected communications and the number of intercepted PCs (that is, "traffic files").

Overall, in 2012–2013, the volume of communications collected by CSEC's SIGINT collection activities [redacted] while the number of recognized PCs unintentionally intercepted by CSEC remained very small.

Contrary to policy, one analyst viewed and recognized 18 PCs during the period under review, but did not annotate them until several weeks later.

Based on the information reviewed and the interviews conducted, in 2012–2013, all PCs that were recognized by CSEC were intercepted unintentionally, and all but one of those used or retained were essential to international affairs, defence or security, as required by the *NDA*.

In one case, an analyst recognized and appropriately flagged that a communication was a PC; however that communication did not pertain to the analyst's target set, and, contrary to policy, the analyst incorrectly marked it for retention even though the analyst did not assess whether the communication was essential to international affairs, defence or security, as required by the *NDA*.

A number of analysts retained PCs that had once been, but were no longer, essential to international affairs, defence or security; despite regular, written reminders to review and mark for deletion any PCs that were no longer essential, these PCs were retained — in some cases, for several months — until just before the expiration of the MAs and prior to associated reporting to the Minister.

All EPRs based on PCs contained FI relating to international affairs, defence or security.

CSEC made further progress in implementing a recommendation from the 2010–2011 *Review of Foreign Signals Intelligence Ministerial Authorizations and Intercepted Private Communications*, regarding reporting to the Minister on the number of one-end Canadian communications acquired through [redacted] activities ([redacted]) in a manner similar to what CSEC does for recognized PCs intercepted under the other SIGINT collection programs.

This review contains five recommendations:

1. To ensure proper accountability for sensitive activities, CSEC should promulgate detailed guidance, as soon as possible, regarding the additional approvals required for certain activities relating to the [redacted] program and to CSEC operations [redacted]

2. CSEC should make available to the Minister more comprehensive information regarding the number of collected communications and intercepted PCs that it acquires and retains throughout an MA period, in order to enhance accountability to the Minister;

3. CSEC analysts should immediately annotate recognized PCs for essentiality to international affairs, defence or security, as required by the *NDA*, or, if not essential, for deletion;

4. CSEC analysts should regularly assess, at a minimum quarterly, whether the ongoing retention of a recognized PC not yet used in an EPR is strictly necessary and remains essential to international affairs, defence or security or whether that PC should be deleted; and

5. CSEC should promulgate guidance regarding the protection of privacy and the handling of intercepted communications of a targeted foreign entity located outside Canada that include [redacted] of a Canadian or person in Canada as part of those intercepted communications.

A list of recommendations and findings is enclosed at Annex A. A list of interviewees is at Annex B.

Jean-Pierre Plouffe, Commissioner

ANNEX A — Recommendations and Findings

Recommendation no. 1: Policies and Procedures

To ensure proper accountability for sensitive activities, CSEC should promulgate detailed guidance, as soon as possible, regarding the additional approvals required for certain activities relating to the [redacted] program and to CSEC operations [redacted]

Recommendation no. 2: Metrics Relating to Interception and to the Privacy of Canadians

CSEC should make available to the Minister more comprehensive information regarding the number of collected communications and intercepted private communications that it acquires and retains throughout an MA period, in order to enhance accountability to the Minister.

Recommendation no. 3: Essentiality of Used or Retained Private Communications (1)

CSEC analysts should immediately annotate recognized private communications for essentiality to international affairs, defence or security, as required by the *National Defence Act*, or, if not essential, for deletion.

Recommendation no. 4: Essentiality of Used or Retained Private Communications (2)

CSEC analysts should regularly assess, at a minimum quarterly, whether the ongoing retention of a recognized private communication not yet used in an End Product Report is strictly necessary and remains essential to international affairs, defence or security or whether that private communication should be deleted.

Recommendation no. 5: Foreign Targets and [redacted]

CSEC should promulgate guidance regarding the protection of privacy and the handling of intercepted communications of a targeted foreign entity located outside Canada that include [redacted] of a Canadian or person in Canada as part of those intercepted communications.

Finding no. 1: Ministerial Authorizations

The 2012–2013 foreign signals intelligence ministerial authorizations met the conditions for authorization set out in the *National Defence Act*.

Finding no. 2: Ministerial Authorizations and Associated Request Memoranda

The format of the 2012–2013 foreign signals intelligence ministerial authorizations and associated request memoranda to the Minister of National Defence was significantly different than that used in 2011–2012; these changes were positive and resulted in documents that are more properly aligned with the purpose of the ministerial authorizations — to shield CSEC from potential liability under Part VI of the *Criminal Code* — and that are clear and comprehensive.

Finding no. 3: Policies and Procedures

With one exception, revised versions of CSEC operational policies did not contain major amendments that would have significantly changed the conduct of activities under MA authorities.

Finding no. 4: Technology

In 2012-2013, CSEC made some changes to technology used for some of its foreign signals intelligence collection activities, the impact of which may be examined in subsequent in-depth reviews of these activities.

Finding no. 5: Metrics Relating to Interception and to the Privacy of Canadians (1)

It is a positive development that, while CSEC made significant changes to how it counts "collected communications" that it reports to the Minister for its foreign signals intelligence collection activities, it continues to use the same method as in previous years to count and report recognized private communications, which will enable a more accurate comparison between the overall number of collected communications and the number of intercepted private communications (that is, "traffic files").

Finding no. 6: Metrics Relating to Interception and to the Privacy of Canadians (2)

Overall, in 2012-2013, the volume of communications collected by CSEC's foreign signals intelligence collection activities [redacted] while the number of recognized private communications unintentionally intercepted by CSEC remained very small.

Finding no. 7: Essentiality of Used or Retained Private Communications (1)

Contrary to policy, one analyst viewed and recognized 18 private communications during the period under review, but did not annotate them until several weeks later.

Finding no. 8: Essentiality of Used or Retained Private Communications (2)

Based on the information reviewed and the interviews conducted, in 2012–2013, all private communications that were recognized by CSEC were intercepted unintentionally, and all but one of those used or retained were essential to international affairs, defence or security, as required by the *National Defence Act*.

Finding no. 9: Essentiality of Used or Retained Private Communications (3)

In one case, an analyst recognized and appropriately flagged that a communication was a private communication; however that communication did not pertain to the analyst's target set, and, contrary to policy, the analyst incorrectly marked it for retention even though the analyst did not assess whether the communication was essential to international affairs, defence or security, as required by the *National Defence Act*.

Finding no. 10: Essentiality of Used or Retained Private Communications (4)

A number of analysts retained private communications that had once been, but were no longer, essential to international affairs, defence or security; despite regular, written reminders to review and mark for deletion any private communications that were no longer essential, these private communications were retained — in some cases, for several months — until just before the expiration of the ministerial authorizations and prior to associated reporting to the Minister.

Finding no. 11: Essentiality of Used or Retained Private Communications (5)

All End Product Reports based on private communications contained foreign intelligence relating to international affairs, defence or security.

Finding no. 12: CSEC activities in response to a previous recommendation of the Commissioner on accountability and [redacted]

CSEC made further progress in implementing a recommendation from the 2010–2011 *Review of Foreign Signals Intelligence Ministerial Authorizations and Intercepted Private Communications*, regarding reporting to the Minister of national Defence on the number of one-end Canadian communications acquired through [redacted] activities ([redacted]) in a manner similar to what CSEC does for recognized private communications intercepted under the other foreign signals intelligence collection programs.

ANNEX B — Interviewees

The following CSEC employees provided information or facilitated the review:

Manager, [redacted] Office of Counter-Terrorism
Manager, [redacted]
Manager, SIGINT Programs Oversight and Compliance
Senior Mission Management Officer, SIGINT Programs Oversight and Compliance
Team Leader, [redacted]
Analyst, [redacted]
Analyst, [redacted]
Analyst, [redacted]
Analyst, [redacted]
Analyst, [redacted]
Analyst, [redacted]
Analyst, [redacted]
Analyst, [redacted]
Analyst, [redacted] Office of Counter-Terrorism
Analyst, [redacted] Office of Counter-Terrorism (2)
Analyst, [redacted] Office of Counter-Terrorism (3)
Analyst, [redacted] Office of Counter-Terrorism (4)
Analyst, [redacted] Office of Counter-Terrorism (5)
Analyst, [redacted] Office of Counter-Terrorism (6)
Analyst, [redacted] Office of Counter-Terrorism (7)
Senior Policy and Review Advisor, External Review
Senior Policy and Review Advisor, External Review (2)