

Communications Security  
Establishment Commissioner  
  
The Honourable Robert Décaray, Q.C.



Commissaire du Centre de la  
sécurité des télécommunications  
  
L'honorable Robert Décaray, c.r.

**TOP SECRET // SI // CEO**

**Our file # 2200-79**

July 17, 2013

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

Dear Mr. Nicholson:

The purpose of this letter is to provide you with the results of my review of Communications Security Establishment Canada (CSEC) signals intelligence (SIGINT) information sharing activities with its second party partners: the United States National Security Agency, the United Kingdom Government Communications Headquarters, the Australian Defence Signals Directorate, and the New Zealand Government Communications Security Bureau. The review was conducted under my authority as articulated in Part V.1, paragraph 273.63(2)(a) of the *National Defence Act (NDA)*. You will recall that on March 23, 2012, I provided you with an update on this review.

As you are aware, the Five-Eyes SIGINT alliance evolved from collaboration during the Second World War. Long-standing agreements and present-day resolutions provide the foundation for CSEC's SIGINT information sharing with the Second Parties.

The amount of foreign intelligence CSEC provides to and receives from the Second Parties is extensive. Information sharing is an essential component of CSEC SIGINT collection and other activities.

CSEC SIGINT information sharing activities with the Second Parties have the potential to directly affect the privacy and security of a Canadian person when private communications or identity information is in the shared information.

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

TOP SECRET // SI // CEO

The allies recognize each other's sovereignty and respect each other's laws by pledging not to target one another's communications. Consequently, CSEC policies and procedures state that collection activities are not to be directed at second party nationals located anywhere, or against anyone located in second party territory. Discussions in interviews and written answers suggest that CSEC conducts its SIGINT activities in a manner that is consistent with the agreements it has with its second party partners to respect the privacy of the partners' citizens, and to follow the partners' policies in this regard.

CSEC trusts that its second party partners will similarly not direct activities at Canadians or persons in Canada. It is recognized, however, that each of the Five-Eyes is an agency of a sovereign nation that may derogate from the agreements, if it is judged necessary for their respective national interests.

My update letter to you of March 23, 2012, indicated that CSEC has substantial controls and measures in place to help ensure that its SIGINT information sharing with the Second Parties is lawful and protects the privacy of Canadians.

This was the first in-depth review focused exclusively on CSEC SIGINT information sharing activities with the Second Parties. In this part of the review, I focused on the two outstanding questions contained in my update letter, namely:

- how many private communications and what volume of information about Canadians does CSEC share with and receive from the Second Parties? and
- how does CSEC assure itself that its second party partners protect private communications and information about Canadians, and that the Second Parties follow the agreements?

I assessed CSEC activities in the context of the limitations in the *NDA* for the protection of Canadians, that is, CSEC foreign intelligence activities "shall not be directed at Canadians or any person in Canada" (paragraph 273.64(2)(a) of the *NDA*) and "shall 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*).

It is accepted that sharing should be optimized, but not mandated in detail. Attempting to prescribe in agreements or policies all details respecting CSEC SIGINT information sharing with the Second Parties is not reasonable. However, I am making two recommendations to implement measures to enhance the protection of the privacy of Canadians and that relate to you as Minister of National Defence in your accountability for CSEC.

**TOP SECRET // SI // CEO**

First, I recommend that CSEC record and include in its Annual Report to the Minister information about the communications CSEC acquires from its second party partners, including the number of one-end in Canada, second party-collected communications, recognized by CSEC analysts and used or retained for foreign intelligence purposes, as well as the number of this type of communication destroyed. Strong arguments can be made that a Canadian's expectation of privacy in his/her communications would be at least the same if not greater whether the communications are unintentionally intercepted and recognized by CSEC itself or are unintentionally acquired by a second party partner and shared with CSEC as a result of using CSEC-supplied selectors.

Regularly reporting to you a wider range of statistical information relating to information shared with the Second Parties, in a manner similar to the existing ministerial authorization statistics, would support you in your accountability for CSEC by making you aware of the volume and extent of such information relating to Canadians and thereby supplement existing measures to protect the privacy of Canadians.

My second recommendation is that you issue, under your authority pursuant to subsection 273.62(3) of the *NDA*, a new ministerial directive to provide general direction to CSEC on its foreign signals intelligence information sharing activities with its second party partners, and to set out expectations for the protection of the privacy of Canadians in the conduct of those activities.

The rationale for this second recommendation is that on completion of this review, what remains unclear to me is the extent to which the Second Parties follow the agreements and protect private communications and information about Canadians in what CSEC shares with them. While CSEC and its second party partners have arrangements about how to treat information relating to respective nationals, the partners do not seek or share evidence from each other to demonstrate that these principles are in fact being followed. CSEC notes, however, that it "regularly engages Five-Eyes policy stakeholders" on the protection of the privacy of Canadians.

There are numerous recent public sources of information about controversies in second party countries, particularly in the U.S. and in New Zealand, including about alleged domestic spying by their foreign signals intelligence agencies. These events raise questions about second party practices involving private communications or information about Canadians and I have directed my office to follow developments closely.

I believe the drafting of this new directive should be informed by an in-depth analysis of the potential impact of respective national differences in legal and policy authorities on CSEC compliance with the law and the protection of the privacy of Canadians, that is, a risk assessment. I understand that such a risk assessment would not be a trivial undertaking, would take time, and would require the cooperation of the Second Parties. However, in light of recent events, I believe it is essential.

**TOP SECRET // SI // CEO**

The new directive should explicitly acknowledge the risks associated with the fact that the information shared with the Second Parties by CSEC may include the communications of Canadians and information about Canadians and that CSEC cannot for reasons of sovereignty demand that its second party partners account for any use of such information.

While outside of the scope of this review, I am suggesting that you and CSEC may consider that the new directive address IT Security information sharing with the Second Parties, as well as SIGINT information sharing.

The Commissioner's office will continue to examine the controls in place and measures taken by CSEC to help ensure that its SIGINT information sharing with the Second Parties is lawful and protects the privacy of Canadians in the conduct of specific reviews.

This review has, in addition, provided the Commissioner's office with background information on CSEC disclosures of Canadian identity information to second party partners and, starting in 2013, the office will expand the annual review of disclosures to also include a sample of such sharing.

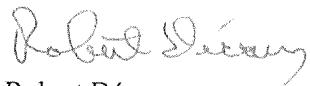
The Commissioner's office will also continue to include privacy incidents involving the second party partners in its annual review of incidents identified by CSEC.

Finally, the Commissioner's office will continue to monitor Canadian and international discussions between review bodies of different countries to review information sharing activities among their respective intelligence agencies.

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

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

Yours sincerely,

  
Robert Décaray

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

Office of the  
Communications Security  
Establishment Commissioner



Bureau du  
Commissaire du Centre de la  
sécurité des télécommunications

**TOP SECRET // SI // CEO**

**Our File # 2200-79**

**A Review of CSEC SIGINT  
Information Sharing with the Second Parties**

**July 17, 2013**

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

TABLE OF CONTENTS

I. AUTHORITIES.....	1
II. INTRODUCTION .....	1
Rationale for conducting this review.....	2
III. OBJECTIVES AND CRITERIA.....	4
IV. SCOPE.....	6
VI. METHODOLOGY .....	8
VII.BACKGROUND.....	8
Canada's National Security Policy .....	9
Five Eyes' agreements and resolutions.....	9
Authorities for SIGINT information sharing.....	12
Legal framework for SIGINT information sharing.....	12
Ministerial direction relating to SIGINT information sharing.....	14
What SIGINT does CSEC share with and receive from the Second Parties? .....	15
Liaison Officers .....	16
International cooperation between review bodies.....	17
VIII. FINDINGS AND RECOMMENDATIONS .....	17
1. How many PCs and what volume of information about Canadians does CSEC share with and receive from the Second Parties? .....	19
2. How does CSEC assure itself that its second party partners protect PCs and information about Canadians, and that the Second Parties follow the agreements? ...	21
IX. CONCLUSION .....	26
ANNEX A — Findings and Recommendations.....	30
ANNEX B — Interviewees .....	32
ANNEX C — Commissioner's update letter to the Minister of March 23, 2012.....	33

## I. AUTHORITIES

The review was conducted under the authority of the CSE Commissioner as articulated in Part V.1, paragraph 273.63(2)(a) of the *National Defence Act (NDA)*.

The review is in conformance with CSEC foreign signals intelligence (SIGINT) ministerial authorizations (MAs) authorizing the interception of private communications (PCs) — as defined in s.183 of the *Criminal Code* — under SIGINT collection activities known as [REDACTED] Collection, [REDACTED] Collection, and [REDACTED]

[REDACTED]  
The review is also in accordance with ministerial directives (MDs) on “Accountability Framework”,<sup>2</sup> “Privacy of Canadians”,<sup>3</sup> “Collection and Use of Metadata”,<sup>4</sup> “[REDACTED] Operations”,<sup>5</sup> and respecting “[REDACTED]”<sup>6</sup> that indicate that associated activities will be subject to review by the CSE Commissioner and that require CSEC to provide full support and cooperation to the Commissioner in the conduct of reviews.

## II. INTRODUCTION

CSEC's ability to fulfill its foreign signals intelligence collection mandate rests in large part on building and maintaining productive relations with foreign counterparts. CSEC's longstanding relationships with its closest allies in the United States (U.S.), the United Kingdom (U.K.), Australia and New Zealand — known as the Second Parties<sup>7</sup> or, collectively with CSEC as the Five-Eyes alliance — continues to benefit CSEC, and, in turn, the Government of Canada (GC). This cooperative alliance is a collective of interdependent organizations working together, but maintaining organizational autonomy; a number of formal structures enable the Five-Eyes partners to pursue common goals. According to CSEC, the Five-Eyes alliance is more valuable now than at any other time in history, given the increasingly complex technological challenges faced by the partners.

<sup>1</sup> Activities conducted under MAs must be undertaken in accordance with conditions set out by the Minister of National Defence in the MAs, e.g., respecting measures to protect the private communications unintentionally intercepted under the SIGINT collection programs. The most recent MAs are in effect from December 1, 2012 to November 30, 2013.

<sup>2</sup> Issued November 20, 2012.

<sup>3</sup> Issued November 20, 2012.

<sup>4</sup> Issued November 21, 2011.

<sup>5</sup> Issued November 20, 2012.

<sup>6</sup> Issued November 20, 2012.

<sup>7</sup> 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 Defence Signals Directorate (DSD), and the New Zealand Government Communications Security Bureau (GCSB).

The allies recognize each other's sovereignty and respect each other's laws by pledging not to target one another's communications. Consequently, CSEC policies and procedures state that collection activities are not to be directed at second party nationals located anywhere, or against anyone located in second party territory.<sup>8</sup> CSEC trusts that its second party partners will similarly not direct activities at Canadians or persons in Canada.

CSEC SIGINT information sharing activities with the Second Parties support part (a) of CSEC's mandate "to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence priorities".<sup>9</sup>

SIGINT information sharing activities with the Second Parties are also conducted under the authority of:

- SIGINT MAs;
- MDs on "Accountability Framework", "Privacy of Canadians", "Collection and Use of Metadata", "████████████████████ Operations", and respecting '████████████████'; and
- agreements and resolutions, namely, the *British-U.S. Communications [COMINT] Intelligence Agreement* (1946), *Canada-U.S. COMINT Agreement* (1949), ██████████, and the ██████████ (summarized on pp. 9-10).

#### *Rationale for conducting this review*

While the case of Mr. Maher Arar did not relate specifically to CSEC or to SIGINT information sharing with the Second Parties, it is an example of how Canada's closest international partners may make their own decisions in relation to a Canadian. Notwithstanding the findings of the Honourable Justice Dennis O'Connor's public inquiry report,<sup>10</sup> a formal apology and compensation to Mr. Arar by the GC, as well as requests by the former Ministers of Public Safety and Foreign Affairs that Mr. Arar be removed from a U.S. "watch list", in a January 16, 2007, open letter, the U.S. Government indicated that "the continued watch listing of Mr. Arar is appropriate".<sup>11</sup> The case of Mr. Arar demonstrates how GC information sharing with the U.S. or other partners may affect a Canadian and possibly put a Canadian in personal jeopardy.

<sup>8</sup> For example, section 6.3 of OPS-I-13, *Procedures for Canadian ██████████ and Joint CSEC-CF Activities*, December 1, 2010.

<sup>9</sup> Paragraph 273.64(1)(a) of the *National Defence Act*.

<sup>10</sup> Report of the Events Relating to Maher Arar, Analysis and Recommendations (Part I — Factual Inquiry), *Commission of Inquiry into the Actions of Canadian Officials in relation to Maher Arar*, the Honourable Dennis O'Connor, Q.C., Commissioner, September 2006.

<sup>11</sup> January 16, 2007, letter to then Minister of Public Safety Stockwell Day from former U.S. Secretary of Homeland Security Michael Chertoff and former U.S. Attorney General Alberto Gonzales accessed on May 11, 2010, from: [www.cbc.ca/news/background/arar/Chertoff-Gonzales-letter-to-Day.pdf](http://www.cbc.ca/news/background/arar/Chertoff-Gonzales-letter-to-Day.pdf).

The GC's response to the Report of the Standing Committee on Public Safety and National Security: *Review of the Findings and Recommendations Arising From the Iacobucci<sup>12</sup> and O'Connor Inquiries* highlighted GC efforts respecting the sharing of intelligence with allies:

The Government's implementation of Justice O'Connor's recommendations has also served to strengthen safeguards in relation to the exchange of information with foreign governments and agencies.

(...)

International collaboration, including the exchange of information, is critical to Canada's national security. That said, the exchange of information with foreign partners raises unique challenges — policy, legal and operational — that are examined on a case-by-case basis in the context of Canada's national security environment.

The cumulative result of successive commissions of inquiry, reports and lessons learned has been the refinement of policies and practices surrounding the exchange of information between foreign partners and Canada's national security and intelligence and law enforcement communities. (p.4)

Reports of commissions of inquiry such as the report on the terrorist bombing of Air India Flight 182 and the U.S. 9/11 commission report stress the need for all agencies involved in national security investigations to cooperate and share information with one another. It is clear that the need for information sharing is vital, but the exchange of information must have due regard for the law and protect the privacy of Canadians.

The amount of foreign intelligence (FI) CSEC provides to and receives from the Second Parties is extensive. Information sharing is an essential component of CSEC SIGINT collection and other activities. Specific controls are placed on SIGINT information sharing to ensure compliance with legal, ministerial and policy requirements. The potential impact on the privacy of Canadians of non-compliance with the law while conducting these activities could be significant. These activities may directly affect the security of a Canadian person. Past Commissioners have identified issues for follow-up and have made findings and recommendations respecting these activities. It is for these reasons that the Commissioner selected CSEC SIGINT information sharing activities with the Second Parties for review.

<sup>12</sup> Internal Inquiry into the Actions of Canadian Officials in relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin, the Honourable Frank Iacobucci, Q.C., Commissioner, October, 2008. The Iacobucci Inquiry identified a number of issues, with a particular emphasis on the GC's sharing and handling of information provided to, and received from, foreign agencies. The findings of the Iacobucci Inquiry did not relate specifically to CSEC or to SIGINT information sharing with the Second Parties.

### III. OBJECTIVES AND CRITERIA

The Commissioner's update letter to the Minister of March 23, 2012, indicated that this review had taken longer than expected for several reasons, including competing priorities of the Commissioner's office, staffing challenges at CSEC and CSEC delays in providing information. (Annex C)

The Commissioner also indicated at that time that he found that CSEC does take measures to protect the privacy of Canadians in what it shares with and receives from the Second Parties, for example:

- CSEC employees must apply CSEC privacy rules to second party-acquired communications;
- CSEC suppresses Canadian identity information in metadata and reports shared with the Second Parties;
- nationality checks and other measures help to limit the inadvertent targeting of Canadians by the Second Parties; and
- CSEC takes action to correct or mitigate privacy incidents involving the Second Parties.

There is no need to revisit in this final review report the substantial controls in place and measures taken by CSEC to help ensure that its SIGINT information sharing with the Second Parties is lawful and protects the privacy of Canadians. The working file held at the Commissioner's office contains detailed information on CSEC policies, procedures and measures taken to protect the privacy of Canadians in what it shares with and receives from the Second Parties.<sup>13</sup> The Commissioner's office will continue to examine these controls and measures in the conduct of activity and subject-specific reviews.

In addition, the evolution of CSEC policies and procedures demonstrates that CSEC respects the core principle that the allies do not treat the communications of respective nationals as they do those that the agreements define as "foreign". Examples of CSEC policies in place that document requirements and promote compliance with respective second parties' laws and policies include those relating to:

- protecting nationally sensitive information in SIGINT report (OPS-2-3, *Sensicheck Procedures*, March 30, 2004);

<sup>13</sup> Examples of measures to protect the privacy of Canadians can be found in CSEC policy OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities*. Section 2.7 of OPS-1 refers to the corrective action that must be taken in the event that a Canadian or a person in Canada is inadvertently targeted, and sections 2.8, 3.4, 3.5, and Annex 3 of OPS-1 refer to privacy annotations. Additional examples of measures to protect the privacy of Canadians in the use and retention of information can be found in OPS-1-7, *Operational Procedures for Naming in SIGINT Reports*, and OPS-1-11, *Retention Schedules for SIGINT Data* (section 1.5 notes that SIGINT data may be retained by CSEC only when required to fulfill CSEC's mandate.).

- referring to or suppressing identities in SIGINT reports (OPS-1-7, *Operational Procedures for Naming in SIGINT reports*, July 8, 2011);
- actions which might jeopardize communications intelligence sources (OPS-5-9, *End Product Sanitization/Action-On Procedures*, May 10, 2002); and
- releasing national identity information suppressed in SIGINT reports (OPS-1-1, *Procedures for the Release of Suppressed Information from SIGINT Reports*, May 8, 2008).<sup>14</sup>

The Commissioner's office will continue to verify that CSEC adheres to these policies and procedures in the conduct of activity and subject-specific reviews.

This review report focuses on the two outstanding questions contained in the Commissioner's update letter to the Minister of March 23, 2012, namely:

1. how many PCs and what volume of information about Canadians<sup>15</sup> does CSEC share with and receive from the Second Parties? and
2. how does CSEC assure itself that its second party partners protect PCs and information about Canadians, and that the Second Parties follow the agreements?

In this context, CSEC activities were assessed in the context of the limitations in the *NDA* for the protection of Canadians, that is, CSEC's FI activities "shall not be directed at Canadians or any person in Canada" (paragraph 273.64(2)(a) of the *NDA*) and "shall 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*).

At the outset of this review, it was also an objective to examine a sample of CSEC disclosures to its second party partners of Canadian identity information suppressed in CSEC and second party reports, as well as any privacy incidents identified by CSEC relating to SIGINT information sharing with the Second Parties. Since that time, the Commissioner has conducted annual reviews of a sample of disclosures to GC clients. This review has provided the Commissioner's office with background information on CSEC disclosures of Canadian identity information to second party partners and, starting in 2013, the office will expand the annual review of disclosures to also include a sample of such sharing. Also since the outset of this review, the Commissioner has conducted an annual review of all privacy incidents identified by CSEC, including incidents involving the second party partners, and the Commissioner's office will continue these reviews. Therefore, this review does not address disclosures or privacy incidents.

<sup>14</sup> CERRID # 327609-v1, September 18, 2009.

<sup>15</sup> Information about Canadians includes Canadian identity information (CII), see CSEC policy OPS-1, *Protecting the Privacy of Canadians and Ensuring legal Compliance in the Conduct of CSEC Activities*, December 1, 2012.

#### IV. SCOPE

This was the first in-depth review focused exclusively on CSEC SIGINT information sharing activities with the Second Parties.

In this part of the review, the Commissioner examined:

- the legislative framework for CSEC's provision to and receipt from the Second Parties of intercepted communications and other SIGINT information, particularly PCs and information about Canadians; and
- CSEC's due diligence respecting the activities, i.e., does CSEC take all reasonable steps to confirm that the Second Parties treat PCs and information about Canadians *consistent with* the laws of Canada and the privacy protections applied by CSEC? (The Second Parties have no *legal* obligation to treat PCs and information about Canadians in accordance with Canadian law.)

This part of the review also included follow-up of CSEC activities in response to previous findings and recommendations of Commissioners as well as issues identified by Commissioners in past reviews, namely:

- Questions in Commissioner Décarie's February 2011 *Review of CSEC activities under Foreign Intelligence Ministerial Authorizations*, that is, what is the volume of communications intercepted by CSEC for its second party partners, and what is the volume of intercepted communications that CSEC obtains from the Second Parties?;
- Finding no. 7 in Commissioner Gonthier's June 2008 [REDACTED] review report respecting accounting for shared PCs and the September 2008 response from the Minister of National Defence;<sup>16</sup> and
- Recommendation no. 5 in Commissioner Lamer's February 2005 [REDACTED] review report respecting the use and retention of recognized PCs.<sup>17</sup>

<sup>16</sup> Finding no. 7 in Commissioner Gonthier's June 2008 [REDACTED] review report was: "Reporting to the Minister the number of private communications recognized by the Second Parties and obtained as a result of CSEC collection shared with the Second Parties would enhance accountability by providing an increased understanding of the number of intercepted private communications, and would therefore enhance the protection of the privacy of Canadians." At that time, CSEC commented that "[w]hile at first blush it may appear reasonable for Second Parties to expand their monthly reporting to CSEC to include recognized PCs, these changes would require significant system adjustments and training... It is unreasonable, however, to expect SIGINT partners — who have any number of [REDACTED] of the Five Eyes — to make significant system, training and metrics adjustments to accommodate an extended Canadian requirement. The review itself notes... that it is unlikely that CSEC would follow through with any sanctions against Second Parties who failed to adhere to reporting arrangements designed to protect the privacy of Canadians, since such sanctions would 'have a significant negative effect on CSEC'. The proposed requirement to have Second Parties expand their reporting to CSEC to include statistics on recognized private communications would likely have a similar negative effect on CSEC, in that it would become too onerous for Second Parties to do business with CSEC (given that this requirement would have to apply to all CSEC collection programs). There are limits on partnership commitments."

The following review reports of Commissioners also provide useful background and contain findings and recommendations relating to CSEC SIGINT information sharing with the Second Parties: *CSEC assistance to the Canadian Security Intelligence Service (CSIS) under part (c) of CSEC's mandate and sections 12 and 21 of the CSIS Act in support of Domestic Interception of Foreign Telecommunications and Search (DIFTS) warrants and related activities* (November 2012); *SIGINT Targeting and Selector Management Activities* (March 2011); *Recommendation No. 1 from the January 2008 Review Report respecting CSEC's Ministerial Directive on the Collection and Use of Metadata — CSEC's [REDACTED] Network Analysis and Prioritization and [REDACTED] Activities* (March 2009); *[REDACTED] Phase II* (March 2008); *Review of the Ministerial Directive, Communications Security Establishment, Collection and Use of Metadata, March 9, 2005* (January 2008); and *Review of the activities of CSEC's Office of Counter-Terrorism* (October 2007).

This review excluded a detailed examination of activities undertaken by CSEC under the authority of paragraph 273.64(1)(c) of the *NDA* and pursuant to sections 12, 16 and 21 of the *Canadian Security Intelligence Service Act*. These subjects have been and will continue to be addressed in separate reviews.

This review also excluded review of “[REDACTED]” and “exceptional reporting” by CSEC and the Second Parties. This will be addressed in a subsequent review.

<sup>17</sup> Recommendation no. 5 in Commissioner Lamer's February 2005 [REDACTED] review report was: “[t]hat CSE[C] seek agreement among the second party partners on mutually acceptable measures covering the use and retention of recognized private communications intercepted through collection. The purpose would be to more formally address the intended provisions of the condition of par. 273.65(2)(d) of the *Act* [*NDA*] for those instances where Second Parties are involved. (An appropriate forum for this policy addition might be the regular Quinquepartite Reporting Policy Conference.)” CSEC's July 2005 management response was: “[n]ot accepted. This recommendation was of concern for partnership reasons. Quinquepartite partners have long-standing arrangements in place for treating Second Party identities according to the privacy policies of the respective Second Party counterpart. These agreements are well articulated through our respective documented policies and procedures, for example those related to Sensicheck, naming, sanitization of COMINT and the release of national identity information suppressed from SIGINT reports. NSA also has strict policies that limit access to non-minimized raw traffic. The allied policy documents, which are visible to CSE[C] and on which CSE[C] Operational Policy staff have frequent dealings, enable us to have confidence that partners are safeguarding the privacy of Canadians. Information is shared among sovereign nations, but there are limits to what any country can require of another. The sanction for not complying with these measures is the ability to restrict the sharing of further information. Notwithstanding, CSE[C] will continue to ensure that mention of mutual respect for privacy concerns be stated wherever appropriate in future agreements and shared policies.”

## VI. METHODOLOGY

The Commissioner's office examined relevant written and electronic records, files, correspondence and other documentation, including policies and procedures and legal advice.<sup>18</sup>

The office interviewed CSEC managers and other employees involved in the activities.

As a first step, the office documented and mapped the forms of SIGINT information sharing; related activities, processes and systems; the legislative and policy framework; and ensured a common understanding of concepts and terminology. The working file held at the Commissioner's office contains detailed information on these subjects.

Subsequently, we assessed CSEC's compliance with the criteria and developed conclusions respecting the objectives. This is the second report on the outcomes.

## VII. BACKGROUND

In April 2007, the Standing Senate Committee on National Security and Defence raised questions respecting CSEC SIGINT information sharing with the Second Parties. The Chairman of the Committee commented that: “[t]he suggestion that came up when Bill C-36 was being looked at that if the law prohibits you from listening to Canadians, you can always go to your friends, and they can listen to Canadians for you.” In response, the then Chief of CSEC responded:

...First, there is a protocol among us that we do not target each other's citizens. Second, we could not be complicit in anything they do. I could not ask my colleagues anywhere to target Canadians, because if I did that, I would be circumventing our law and thereby breaking the law. It would not happen. However, if they targeted, unbeknownst to us, and it was obviously a threat that they envisaged, possibly to Canada, I would guess that — since if it is close to Canada, it is close to the United States — they may well give us that information... we would not have known where it came from or been involved in that targeting. We cannot circumvent our laws.<sup>19</sup>

<sup>18</sup> If legal advice given to CSEC is shared with the Commissioner's office, this is done on the understanding that the sharing by CSEC of information which is subject to solicitor-client privilege does not constitute a waiver by CSEC of its privilege.

<sup>19</sup> Proceedings of the Standing Senate Committee on National Security and Defence, Issue No. 15, twenty-sixth and twenty-seventh meetings on Canada's national security policy, April 30, 2007, pp. 145 and 146.

---

Similarly, the U.S. NSA's website includes the following frequently asked question:

Couldn't NSA simply ask its allies to provide them [*sic*] with information about U.S. persons?

No. NSA is prohibited from requesting any person to undertake activities that NSA itself is prohibited from conducting.<sup>20</sup>

***Canada's National Security Policy***

Canada's *National Security Policy* (2004) recognizes the importance of sharing intelligence information:

A part of our ability to access intelligence derives from our intelligence alliances and relationships. For many years Canada has exchanged information with key allies. ... These relations are enormously beneficial to our country. Canada alone could not replicate the benefits gained through these international arrangements. But we are also a significant contributor of intelligence. These contributions are recognized and appreciated by our allies.<sup>21</sup>

The statements in the *National Security Policy* apply to CSEC's SIGINT activities; by means of CSEC's partnerships with the Second Parties, Canada is a net beneficiary of FI.

***Five Eyes' agreements and resolutions***

(The working file held at the Commissioner's office contains copies of the agreements and resolutions)

The Five-Eyes SIGINT alliance evolved from collaboration during the Second World War. Long-standing agreements and present-day resolutions provide the foundation for CSEC's SIGINT information sharing with the Second Parties.

***British-U.S. Communication Intelligence Agreement (UKUSA Agreement) (1946)***

The UKUSA Agreement is an agreement among those two parties to exchange foreign communications intelligence (COMINT, which is a component of SIGINT) and addresses matters respecting associated methods and techniques, analysis, dissemination and security. The UKUSA Agreement defines "foreign country" as "any country, whether or not its government is recognized by the U.S. or the British Empire, excluding only the U.S., the British Commonwealth of Nations and the British Empire."

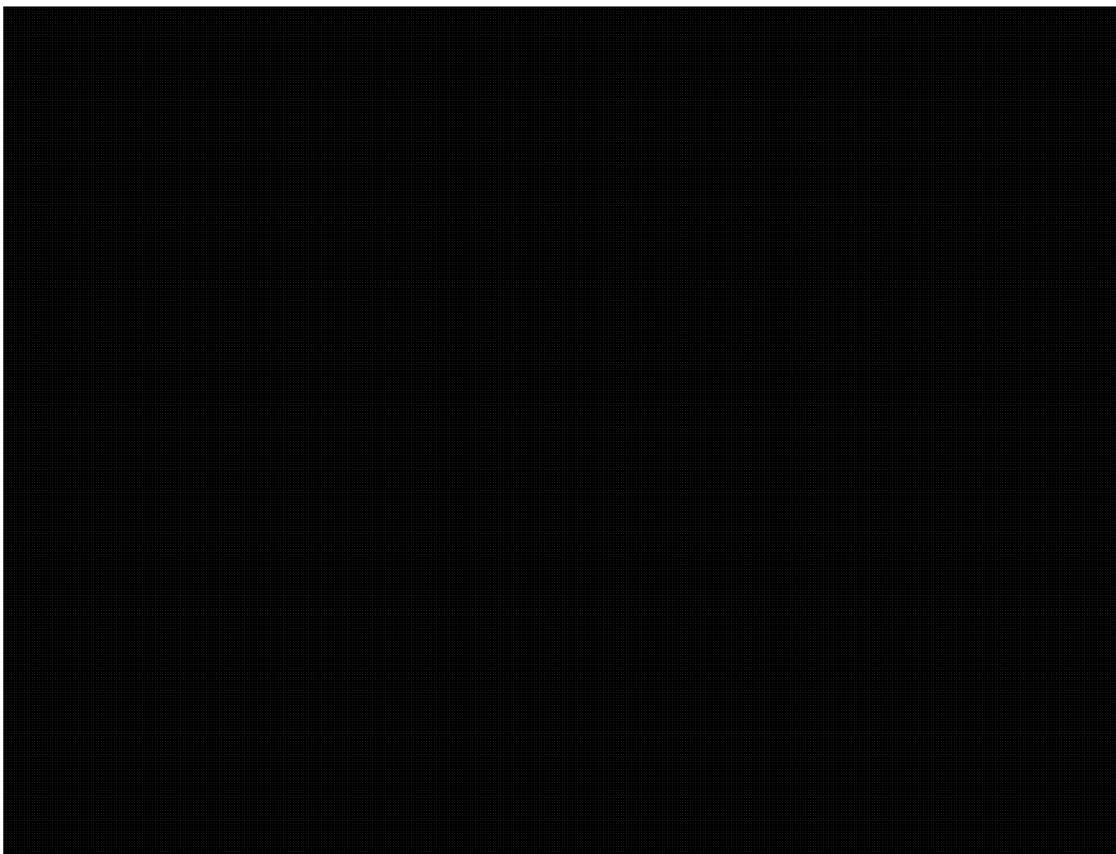
***Canada-U.S. COMINT Agreement (CANUSA Agreement) (1949)***

The CANUSA Agreement established the relationship between the Canadian Communications Research Committee (a predecessor of CSEC) and the U.S. Communication Intelligence Board (a predecessor of NSA) respecting COMINT.

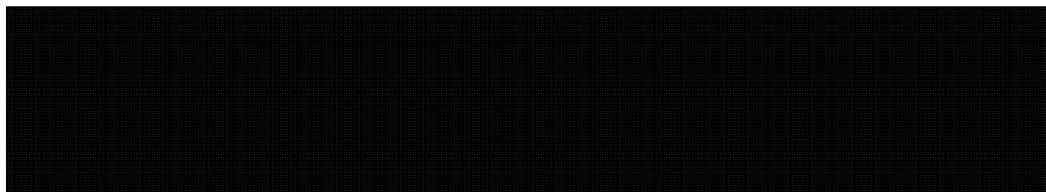
---

<sup>20</sup> <http://www.nsa.gov/sigint/faqs.shtml>, page 2 of 3, accessed April 12, 2010.

<sup>21</sup> Securing an Open Society: Canada's National Security Policy, 2004, page 17.



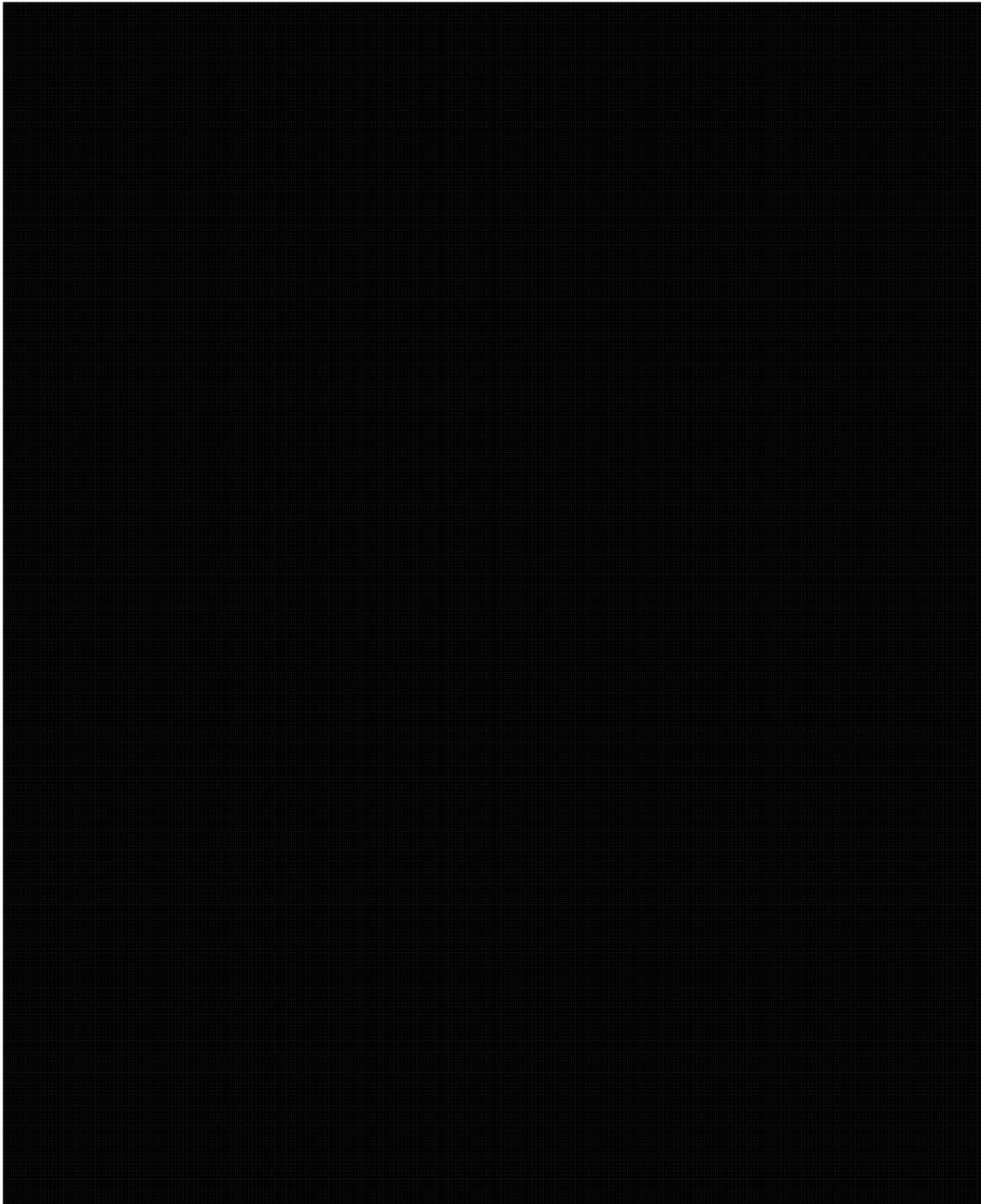
CSEC's historical relationships are reinforced through present-day resolutions.



The MD on *Collection and Use of Metadata* requires CSEC to minimize Canadian identity information prior to sharing [REDACTED] metadata with the Second Parties. CSEC has implemented processes to automatically minimize both shared Dialed Number Recognition (DNR) (e.g., telephone and fax) and Digital Network Intelligence (DNI) metadata [REDACTED] e.g., e-mail and Internet Protocol addresses).

---

<sup>22</sup> “Metadata” means: “information associated with a telecommunication to identify, describe, manage or route that telecommunication or any part of it as well as the means by which it was transmitted, but excludes any information or part of information which could reveal the purport of a telecommunication, or the whole or any part of its content.” MD on *Collection and Use of Metadata*, November 21, 2011.



5b  
x

### ***Authorities for SIGINT information sharing***

The *NDA* does not contain explicit authority or any specific limitations respecting CSEC SIGINT information sharing with the Second Parties. Such activities are implicitly authorized by the *NDA*.<sup>23</sup>

### ***Legal framework for SIGINT information sharing***

CSEC SIGINT information sharing activities with the Second Parties support part (a) of CSEC's mandate "to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence priorities".

The cooperative agreements and resolutions summarized above include a commitment by the Five-Eyes to respect the privacy of each others' citizens, and to act in a manner consistent with each others' policies relating to privacy. It is recognized, however, that each of the Five-Eyes is an agency of a sovereign nation that may derogate from the agreements, if it is judged necessary for their respective national interests.

The Commissioner's office questioned CSEC about the measures it takes to ensure that its use of information acquired by the Second Parties is in compliance with section 8 of the *Canadian Charter of Rights and Freedoms (Charter)*, the right to be secure against unreasonable search or seizure.<sup>24</sup>

CSEC responded that subsection 273.64(2)(b) of the *NDA* requires activities carried out by CSEC to be subject to measures to protect the privacy of Canadians in the use and retention of intercepted information. This provision was included in CSEC's legislation in order to satisfy section 8 of the *Charter*. The measures to protect the privacy of Canadians apply to communications traffic that are intercepted by CSEC as well as those CSEC acquires from the Second Parties using CSEC-supplied selectors. CSEC possesses many measures, such as specific policies and procedures, to protect the privacy of Canadians in the use and retention of such intercepted information.<sup>25</sup>

The Second Parties treat information according to their own domestic authorities. Although the Five-Eyes have agreements and practices in place for SIGINT information sharing with each other, the Second Parties are under no legal obligation to treat any information — including PCs and information about Canadians obtained by the Second Parties or provided to the Second Parties by CSEC — in a manner consistent with the laws of Canada and the privacy protections applied by CSEC. Likewise, CSEC has no legal obligation to protect information respecting second party nationals. It is recognized, however, that the Five-Eyes partners have a vested interest in complying with the requirements of the other partners to protect information about their respective nationals in support of continued access to

<sup>23</sup> This is in contrast to, for example, the *Canadian Security Intelligence Service Act* that sets out at paragraph 13(3) a regime for CSIS, with ministerial approval, to enter into an arrangement or otherwise cooperate with a foreign state or an institution thereof respecting threats to the security of Canada and security assessments.

<sup>24</sup> E-mail from Director of Operations to CSEC A/Manager, External Review, January 16, 2013.

<sup>25</sup> E-mail from CSEC A/Manager, External Review, January 31, 2013.

second party information. “Wilful failure to comply with this arrangement would undermine the level of trust that is fundamental to information exchange, and would have severe repercussions for the continued relationship between the partner countries.”<sup>26</sup>

The Commissioner’s office agrees with CSEC’s legal interpretation.

*Justice Canada advice*

CSEC indicated that “[it] is unaware of any foundational legal opinions or advice of general application with respect to SIGINT information sharing with the Second Parties.”<sup>27</sup>

The Commissioner’s office also requested a copy of any Justice Canada legal opinions or advice provided to CSEC respecting the agreements, resolutions or directions. CSEC responded that it was unable to provide a copy of any such advice for the following reason: “... the Commissioner’s mandate is to review CSEC activities to determine if it is in compliance with the law, [CSEC does] not believe that the signing of agreements/resolutions/strategic directions has a bearing on CSEC’s lawfulness. Rather, it is the activities that CSEC undertakes as a result of these agreements/resolutions/strategic directions that require lawful compliance and are therefore subject to review.” CSEC further indicated that if the Commissioner had “particular legal concerns regarding some of the activities [CSEC] ha[d] undertaken as a result of these agreements, [CSEC] will duly consider your Office’s request for legal opinions or advice on that particular matter.”<sup>28</sup>

The Commissioner’s office then asked for a copy of any Justice Canada legal opinions or advice provided to CSEC respecting the important similarities and any significant differences respecting how CSEC and each of the Second Parties treat and protect PCs and identity information of respective citizens under respective foreign intelligence authorities and national laws. CSEC responded that “CSEC and its Justice Counsel are unaware of any foundational legal study of general application comparing authorities and national laws between the Five-Eyes nations related to this subject.”<sup>29</sup>

In addition, the Commissioner’s office asked for a copy of any Justice Canada legal opinions or advice provided to CSEC on the specific subject of the application of MAs and MA requirements to intercepted communications acquired by CSEC from a second party source. CSEC responded that it “consults with DLS (and has done so since the *Anti-Terrorism Act* was passed). CSEC is not aware of any foundational opinion on this question.”<sup>30</sup>

In subsequent exchanges, CSEC confirmed that it does not need an MA to shield it from section 184 of the *Criminal Code* for information it acquires from its second party

<sup>26</sup> *Supra*, note 14.

<sup>27</sup> CERRID #310604-v1, July 24, 2009.

<sup>28</sup> E-mail from Senior Policy and Review Advisor, External Review, September 18, 2008.

<sup>29</sup> *Supra*, note 14.

<sup>30</sup> E-mail from Senior Policy and Review Advisor, External Review, January 31, 2013.

partners. "Private communication" and "intercept" are defined in Canadian law,<sup>31</sup> but do not apply to an interception of a communication done by a Second Party, conducted under that ally's authorities. An interception conducted by a second party partner using a CSEC supplied selector is not an interception under the *NDA* and the *Criminal Code*. Consequently, the acquisition by CSEC of a one-end Canadian communication intercepted by a Second Party and shared with CSEC is not a PC and does not trigger the application of Part VI of the *Criminal Code*.<sup>32</sup> (See pp. 17-18 for a detailed discussion on the application of MAs and MA requirements)

***Ministerial direction relating to SIGINT information sharing***

The 2012 Memoranda for the Minister requesting approval of the MAs for [REDACTED] and [REDACTED] collection activities contain indirect references to information sharing activities with the Second Parties. Respecting the condition to be satisfied that the expected FI value of the information that would be derived from the interception justifies it, the requests for MAs refer to the value of second party produced reports, shared with CSEC and based on CSEC collection. The Memoranda on [REDACTED] Collection also refers to CSEC's allied research infrastructure.

The SIGINT MAs proper do not contain any references — direct or otherwise — to information sharing with the Second Parties.<sup>33</sup>

CSEC's SIGINT information sharing activities with the Second Parties are also conducted under the authority of and specifically referred to in MDs. Significant excerpts of relevant MDs are:

***MD on Framework for Addressing Risks in Sharing Information with Foreign Entities***  
(November 21, 2011)

CSE[C]'s information sharing with Five-Eyes cryptologic partners will continue under existing policies and protocols, given the unique nature of CSE[C]'s shared and collaborative access to the Five-Eyes SIGINT enterprise. I expect CSE[C] to maintain these long-standing relationships. (p.1)

***MD on Accountability*** (November 20, 2012)

To fulfill your mandated functions, you may enter into an arrangement or otherwise cooperate with any domestic entity, foreign entity or class of foreign entities. In these cases, I expect you to maintain the appropriate security safeguards. (pp. 2-3)

<sup>31</sup> Section 183 of the *Criminal Code*.

<sup>32</sup> E-mail from Senior Policy and Review Advisor, External Review, November 28, 2012.

<sup>33</sup> In 2012-2013, CSEC adopted a new approach to requesting MAs which was intended to clarify to the Minister that he is being asked to authorize CSEC to use activities or classes of activities to pursue CSEC's mandates, when those activities risk interception of PCs.

*MD on the Collection and Use of Metadata* (November 21, 2011)

CSE[C] will share metadata, acquired through its foreign intelligence acquisition programs with international allies to maximize its mandate activities as set out in the *National Defence Act*, and strengthen Canada's partnerships abroad. Such sharing will be subject to strict conditions to protect the privacy of Canadians, consistent with these standards governing CSE[C]'s other programs. (p.2)

*MD on [REDACTED] Operations* (November 20, 2012)

I expect you to maintain efficient and effective consultative and cooperative processes with ... our SIGINT allies to carry out operations. (p.2)

*MD on [REDACTED] Program* (November 20, 2012)

CSE[C] is authorized to share information, including metadata, acquired through this program with international allies to maximize its SIGINT and ITS activities, and strengthen Canada's partnerships abroad. (p.3)

***What SIGINT does CSEC share with and receive from the Second Parties?***

CSEC shares [REDACTED] minimized DNR (e.g., telephone or fax number) and DNI (e.g., e-mail or Internet Protocol address) metadata. On account of volume, CSEC does not archive metadata shared with the Second Parties.

CSEC shares [REDACTED] traffic. These communications are targeted by CSEC for the Second Parties, using second party selectors submitted to CSEC for approval, according to CSEC policies and procedures, that is, second party selectors must be associated with foreign entities located outside Canada for the purpose of obtaining FI and in accordance with the GC intelligence priorities. CSEC retains an archived copy of all intercepted communications forwarded to the Second Parties.

CSEC shares [REDACTED] traffic collected as part of SIGINT Development (SD) activities, consisting of technical analysis such as [REDACTED] and [REDACTED]. These activities are aimed at mapping the GII and identifying signals that may be of FI interest.

The [REDACTED] tool is used by the Five-Eyes to share SD and other non-CEO information respecting targets and tradecraft. CSEC may share [REDACTED] intercepted communications, for example, for assistance in exploiting the communications and making them [REDACTED]

IRRELEVANT

CSEC also shares end-product reports (EPRs), generally excluding those designated CEO.<sup>34</sup> CEO series reports may relate to sensitive or confidential aspects of GC policy or be detrimental to economic, security and intelligence or other national interests.

The Second Parties may, with CSEC approval, pass sanitized communications intercept or CSEC reports to other SIGINT allies [REDACTED] as long as all source information is removed from the reports.

The Second Parties similarly share with CSEC metadata and [REDACTED] traffic (selected and respecting SD activities) acquired and shared in accordance with their respective legislative and policy regimes.

CSEC-approved selectors may be forwarded to second party collection teams for approval. CSEC's policies and procedures require that [REDACTED] must meet the same requirements as for targeting [REDACTED] CSEC collection [REDACTED] for example, strong selectors (metadata) must relate to a foreign entity outside Canada and to a FI priority of the GC.

The Second Parties also share EPRs in accordance with their respective legislative and policy regimes. CSEC indicated that virtually all second party-authored reporting is available to CSEC analysts (and through CSEC to GC analysts) by means of [REDACTED]<sup>35</sup> and that named and restricted distribution reports may occasionally be disseminated using a second party liaison office.

The working file held at the Commissioner's office contains detailed information on CSEC policies and procedures that guide this sharing of SIGINT information, as well as on how in technical terms CSEC shares it with the Second Parties, including information on associated systems (namely, CSEC and second party [REDACTED])

[REDACTED] CSEC's Common Traffic Repository (CTR) and [REDACTED]

The working file also contains sample metrics respecting the number of EPRs shared and related FI priorities and collection sources.

#### *Liaison Officers*

According to CSEC, the exchange of liaison officers on-site among second party agencies is one example of the distinctiveness and closeness of the relationship, more so than that of human intelligence agencies, for example, CSIS and its allied counterparts.

<sup>34</sup> In addition to CEO and Five-Eyes sharing, some reports may be shared only with select Second Parties due to national sensitivities.

<sup>35</sup> [REDACTED] is CSEC's SIGINT production and dissemination system. It is used for client requirements gathering; end-product report authoring, storage and searching (including Second Party reporting); dissemination of reports; and as a reporting feedback tool. Access to documents in [REDACTED] is strictly controlled, e.g., based on security clearance and indoctrinations, caveats, and user access permissions.

<sup>36</sup> CERRID # 298623-v1, May 25, 2009 and CERRID # 327740-v1, September 18, 2009.

According to CSEC, Canadian Special Liaison Officers (CANSLOs) and second party liaison officers play a minimal role in SIGINT information sharing. Metadata, traffic and report sharing are automated. In rare cases (e.g., named restricted distribution), CANSLOs may share metadata or reports between agencies. CSEC's SIGINT Programs Oversight and Compliance and Corporate and Operational Policy sections may be asked for advice on these rare occasions. Second party liaison officers play a similar, minimal role in information sharing.<sup>37</sup>

The Commissioner's office will examine in detail the role and activities of CANSLOs in a subsequent review.

#### ***International cooperation between review bodies***

As a general point, beyond the Second Parties, but certainly related, is a theme raised by a number of Canadian and international academics. They have referred to an "accountability gap" concerning an absence of cooperation between review bodies of different countries to review information sharing activities among their respective intelligence agencies. These researchers suggest that growing international intelligence cooperation should be matched by growing international cooperation between oversight and review bodies.<sup>38</sup> This is an area of interest for the Commissioner's office.

### **VIII. FINDINGS AND RECOMMENDATIONS**

In this second part of the review, the Commissioner examined CSEC's due diligence respecting the activities, that is, does CSEC take all reasonable steps to confirm that the Second Parties treat PCs and information about Canadians *consistent with* the laws of Canada and the privacy protections applied by CSEC?

Specifically, this review report focused on the two questions contained in the Commissioner's update letter to the Minister of March 23, 2012:

1. how many PCs and what volume of information about Canadians does CSEC share with and receive from the Second Parties; and
2. how does CSEC assure itself that its second party partners protect PCs and information about Canadians, and that the Second Parties follow the agreements?

---

<sup>37</sup> *Supra*, note 27.

<sup>38</sup> Dr. Hans Born, Senior Fellow, Geneva Centre for the Democratic Control of Armed Forces, Geneva, speaking notes for the NATO Parliamentary Assembly Session at Reykjavik, October 6, 2007. Dr. Born's paper concludes: "...we must recognise that given both the threats to security and the responses to these threats have become increasing transnational, so too must the mechanisms which scrutinise and control these responses. It is imperative that we must move towards a situation in which the power generated by international intelligence cooperation is counterbalanced by the powers of effective accountability mechanisms-narrowing the accountability gap". (page 8) See also: *The Collateral Casualties of Collaboration – The Consequence for Civil and Human Rights of Transnational Intelligence Sharing*, Craig Forcese, Associate Professor, Faculty of Law, University of Ottawa, March 5, 2009, electronic copy available at: <http://ssrn.com/abstract=1354022>.

In this context, the Commissioner assessed CSEC's activities in the context of the limitations in the *NDA* for the protection of Canadians, i.e., CSEC's foreign intelligence activities "shall not be directed at Canadians or any person in Canada" (paragraph 273.64(2)(a) of the *NDA*) and "shall be subject to measures to protect the privacy of Canadians in the use and retention of intercepted information" (paragraph 273.64(2)(b) of the *NDA*).

The unintentional interception of a PC by CSEC is a different concept than the unintentional acquisition by CSEC from a second party source of a one-end Canadian communication.<sup>39</sup>

The 2001 amendments to the *NDA* established the MA regime. MAs allow CSEC to direct its activities at foreign entities abroad, for the sole purpose of providing FI in accordance with the GC's intelligence priorities, even if doing so risks unintentionally intercepting PCs. By means of an MA, the Minister of National Defence may authorize CSEC to intercept PCs, as long as CSEC has met relevant criteria outlined in the *NDA* (e.g., implementing measures to protect the privacy of Canadians with respect to the use or retention of a PC unintentionally intercepted). SIGINT activities conducted under an MA must satisfy conditions stated in subsections 273.65(2) of the *NDA*,<sup>40</sup> and may also be subject to additional measures that the Minister considers advisable to protect the privacy of Canadians, pursuant to subsection 273.65(5) of the *NDA*, for example, to report certain information to the Minister. Without the MA regime, CSEC would be prohibited under the *Criminal Code* from unintentionally intercepting PCs; in effect, without MAs, CSEC would be rendered "deaf" in today's highly dynamic technology and threat environment.

The MA regime in Part V.1 of the *NDA* is a Canadian instrument and applies to CSEC. It has no application to the Second Parties or to their own respective sovereign regimes. The MA covers CSEC's unintentional interception of PCs, not CSEC's acquisition of FI from second party sources. This is set out in section 2.12 of OPS-1 which states:

As a result of the beneficial sharing arrangements with its SIGINT allies, CSEC acquires a considerable amount of foreign intelligence target intercept consistent with GC priorities from Second Parties. Second Parties conduct collection activities in pursuit of their own national interests and in accordance with their domestic laws.

Most of these collection assets are also managed by Second Parties who direct the collection [REDACTED] which they believe will yield intercept to meet their national intelligence requirements. CSEC, as a SIGINT partner and in accordance with its authorities, accesses this collection by proposing selectors [REDACTED]  
[REDACTED]

<sup>39</sup> For the purpose of this review, a "one-end Canadian communication" means a communication where one of the communicants is physically located in Canada or if one communicant is a Canadian physically located outside Canada.

<sup>40</sup> These conditions are addressed at the time a new MA is requested.

An interception by a Second Party (whether resulting from a CSEC-supplied selector or not) is conducted under the Second Party's own authorities. The unintentional interception of a one-end Canadian communication by a second party partner and shared with CSEC does not constitute an interception of a PC under the *NDA* and does not engage the *Criminal Code*. Canadian law does not apply in the country of the second party partner and CSEC does not require an MA for such acquisition.

It follows that the associated requirements in MAs apply only to interception conducted by CSEC under CSEC authorities using CSEC's own capabilities. For example, the MA reporting requirements do not apply to second party collection acquired by CSEC; MA reporting to the Minister is representative of communications and PCs unintentionally intercepted by CSEC using CSEC capabilities for CSEC use.

*How many PCs and what volume of information about Canadians does CSEC share with and receive from the Second Parties?*

**Recommendation no. 1: Reporting to the Minister the number of one-end in Canada, second party-collected communications**

To support the Minister of National Defence in his accountability for CSEC and as an additional measure to protect the privacy of Canadians, CSEC should record and include in its Annual Report to the Minister information about the communications CSEC acquires from its second party partners in the United States, United Kingdom, Australia and New Zealand, including the number of one-end in Canada second party-collected communications, recognized by CSEC analysts and used or retained for foreign intelligence purposes, as well as the number of this type of communication destroyed.

At the outset of this review, CSEC provided a sample of the volume of [REDACTED] traffic shared with the Second Parties for a period of two months.<sup>41</sup> The Commissioner's office asked CSEC to produce similar information for a complete year. CSEC responded: "[t]hese data are not readily available. The systems have not been designed to provide these types of metrics, so the original numbers provided were acquired through a manual process. To complete the statistics for the entire year... would be highly time-consuming."<sup>42</sup>

It is unclear how many second party-authored end product reports (EPRs) are based on PCs or contain (suppressed) Canadian identity information because the Second Parties are not required by CSEC to record and report such information to CSEC and CSEC does not examine every second party-authored EPR to determine such information.<sup>43</sup> Similarly, CSEC analysts are not required to record or report the appearance of second party nationals

<sup>41</sup> CERRID # 233229, April 16, 2009.

<sup>42</sup> CERRID # 494582, April 8, 2010. CSEC clarified that to gather information for a period of two months required one employee to work three full days.

<sup>43</sup> Determining the number of second party-authored EPRs in [REDACTED] — CSEC's SIGINT reporting production and dissemination system — containing information about Canadians could be accomplished through a time-consuming manual search. A search feature in [REDACTED] can provide a rough estimate.

in intercepted communications. CSEC does not inform the Second Parties of such occurrences.

In response to questions during this review, CSEC estimated that approximately █% to █% of the selectors in CSEC collection █ dictionaries originated from the Second Parties. However, CSEC annual and other reporting to the Minister does not provide information about the volume or contents of the communications that CSEC acquires for and sends to its second party partners. Section 7.1 of CSEC policy OPS-1-13, *Procedures for Canadian [REDACTED] and Joint CSEC-CF Activities*<sup>44</sup>, indicates: "Second Parties may acquire private and solicitor client communications [as well as information about Canadians] in traffic through CSEC collection equipment. CSEC does not count or report those communications" (p. 26).

***Finding no. 1: Shared private communications and information about Canadians***

CSEC does not count and does not report to the Minister of National Defence the number of private communications and the volume of information about Canadians that CSEC shares with and receives from its second party partners in the United States, United Kingdom, Australia and New Zealand.

Similarly, CSEC annual and other reporting to the Minister excludes information about the volume and contents of communications that CSEC receives from its second party partners.<sup>45</sup>

Strong arguments can be made that a Canadian's expectation of privacy in his/her communications would be at least the same if not greater whether the communications are unintentionally intercepted and recognized by CSEC or are unintentionally intercepted by CSEC and shared with a Second Party.

Strong arguments can also be made that a Canadian's expectation of privacy in his/her communications would be at least the same if not greater whether the communications are unintentionally intercepted and recognized by CSEC itself or are unintentionally acquired by a second party partner and shared with CSEC as a result of using CSEC-supplied selectors.

***Finding no. 2: Reporting to the Minister***

Regularly reporting to the Minister a wider range of statistical information relating to information shared with the Second Parties, in a manner similar to the existing MA statistics, would support the Minister in his accountability for CSEC and supplement existing measures to protect the privacy of Canadians.

<sup>44</sup> Issued December 1, 2010.

<sup>45</sup> When accessing or using second party-acquired communications, CSEC analysts remain subject to all of the same CSEC policies and procedures that apply to CSEC-acquired communications.

CSEC analysts currently apply SIGINT privacy annotations to communications from second party collection (acquired by the Second Parties for CSEC using CSEC selectors) in the same manner as for CSEC collection. Intercept identified as containing a PC, a communication of a Canadian located outside Canada, or information about Canadians must be annotated for deletion unless it: is FI as defined in the *NDA*; is essential to protect the lives or safety of individuals of any nationality; or contains information about serious criminal activity relating to the security of Canada.<sup>46</sup> The Commissioner's office understands that CSEC has the technical capability to report to the Minister the number of one-end in Canada (physical location) second party-collected communications, recognized by CSEC analysts and used or retained for foreign intelligence purposes, and the number of this type of communication destroyed.

The Commissioner's office will continue to examine metrics relating to SIGINT information sharing with the Second Parties in the conduct of activity and subject-specific reviews.

**1. *How does CSEC assure itself that its second party partners protect PCs and information about Canadians, and that the Second Parties follow the agreements?***

**Recommendation no. 2: New ministerial directive on CSEC foreign signals intelligence information sharing activities with its second party partners**

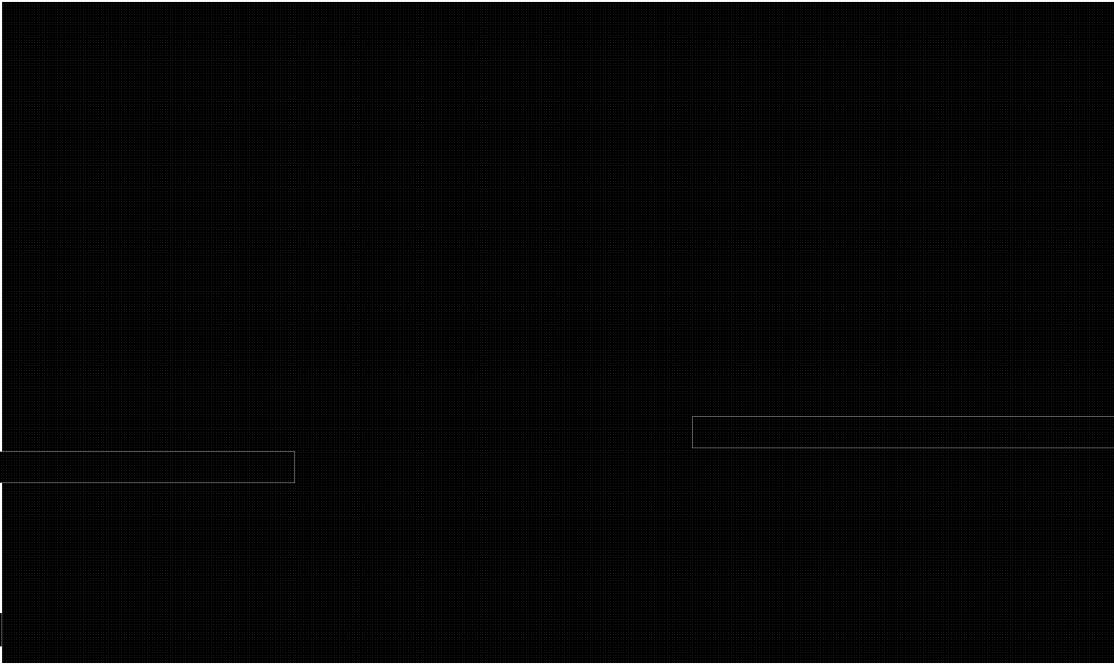
To support the Minister of National Defence in his accountability for CSEC and as a measure to protect the privacy of Canadians, it is recommended that the Minister issue, under his authority pursuant to subsection 273.62(3) of the *National Defence Act*, a new ministerial directive to provide general direction to CSEC on its foreign signals intelligence information sharing activities with its second party partners in the United States, United Kingdom, Australia and New Zealand, and to set out expectations for the protection of the privacy of Canadians in the conduct of those activities.

The Commissioner's update letter to the Minister of March 23, 2012, indicated that he found that CSEC has substantial controls and measures in place to help ensure that its SIGINT information sharing with the Second Parties is lawful and protects the privacy of Canadians.

In the conduct of this review, the Commissioner's office asked a number of questions about how CSEC treats information relating to second party nationals. Discussions in interviews and written answers suggest that CSEC also conducts its SIGINT activities in a manner that is consistent with the agreements it has with its second party partners to respect the privacy of the partners' citizens, and to follow the partners' policies in this regard.

<sup>46</sup> CSEC policy OPS-1 sets out baseline measures to ensure compliance with the law and protect the privacy of Canadians in the use and retention of intercepted information.

What remains unclear to the Commissioner's office, however, is the extent to which the Second Parties follow the agreements and protect PCs and information about Canadians in what CSEC shares with them.



In response to questions about how CSEC assures itself that the Second Parties comply with the agreements, CSEC expressed the view that:

There are a number of indicators that CSEC uses [listed below], and in fact has done so for years, that provide sufficient assurance levels that [the] Second Parties are honouring their arrangements with CSEC... While errors and oversights do occur, these are exceptions, not the rule. The fact that CSEC and the respective Second Party review and record such instances — consulting with each other as necessary in relation to specific incidents — is a further sign that Second Parties wish to deal with CSEC in good faith.

The indicators are:

- a) Identity release requests;
- b) Requests to confirm the citizenship status of possible targets;
- c) Notifications of naming violations;
- d) Regular monitoring of SIGINT EPRs for inadvertent naming violations by the Five-Eyes;
- e) Sensi-check consultations;
- f) Requests for action-on approvals; and

- 
- g) Adoption of policy requirements that are consistent with those of a Second Party partner to protect the privacy and identity information of that Second Party's nationals.<sup>47</sup>

However, while CSEC and its second party partners have agreements about how to treat information relating to respective nationals, the partners do not seek or share evidence from each other to demonstrate that these rules are in fact being followed.

During several interviews and in response to numerous written questions, CSEC was disinclined or unable to demonstrate knowledge or to provide evidence of how its second party partners treat PCs and information about Canadians. For example, CSEC would not provide the Commissioner's office with a description of or a copy of relevant extracts of second party policies on the handling of information relating to a Canadian.

CSEC also declined to identify for the Commissioner's office any specific differences — large or small — between respective partners' laws, policies and practices and how this may affect the partners' handling of PCs or information about Canadians. For example, CSEC did not answer specific questions relating to the partners' use of metadata: do the Second Parties use a common definition of metadata? If yes, what is it and where is it documented? Please explain the Second Parties respective policies respecting contact chaining [REDACTED] CSEC offered only general responses<sup>48</sup> to such questions. It suggested that review of second party authorities and activities pertain to the Second Parties and not to the lawfulness of CSEC activities, and these questions were therefore outside of the Commissioner's mandate.

In another example relating to PCs and information about Canadians, the Commissioner's office asked CSEC what assurances it has that the Second Parties apply the same policies and procedures to respective internal ("eyes only") reports that the partners apply to EPRs shared among the Second Parties. CSEC responded:

...We trust that their naming and handling procedures for internal reports are as stringent (not equally stringent, but as stringent as they need to be within the context of their own legislation — they're governed by the legal regimes under which they operate, not Canadian law)... Information is shared among sovereign nations, but there are limits to what any country can require of another. The sanction for not complying with these measures is, of course, the ability to restrict the sharing of further information.

In other than the most exceptional circumstances, Second Party internal reports (e.g., "Eyes Only", "NOFORN") are not shared with CSEC. Nor for that matter are any policies or practices related to such reports shared with CSEC. This is not surprising, as these reports and policies, by definition, are retained in the national

---

<sup>47</sup> *Supra*, note 14.

<sup>48</sup> For example, CSEC indicated: "In sum, CSEC is unaware of any differences in the Five-Eyes context that would cause it concern for sharing metadata, [REDACTED] traffic, and EPRs with Second Parties." Source: *supra*, note 42.

channels of the respective Second Party. Therefore CSEC is not in a position to state what Second Parties do in this respect.

In addition, Five-Eyes SIGINT agencies, in accordance with their own mandates and national laws, may be able to assist their domestic partners in ways that fall outside the purview of their Second Party SIGINT agreements. CSEC would not be privy to, leave alone be in a position to influence, such activities carried out by the Second Parties. IRRELEVANT

IRRELEVANT

In those exceptional instances when a Second Party shares nationally sensitive “Eyes Only” COMINT product related to a Canadian with CSEC, the product is subject to certain conditions; for example, the activity from which the product is derived could not be undertaken at the direction of, or involve prior consultation with, CSEC. Additionally, the product passed to CSEC would have to suppress any Canadian identifiers.<sup>49</sup>

The Commissioner’s office is of the view that CSEC’s suggested sanction for non-compliance — to restrict the sharing of further information with the Second Parties — seems unlikely, as it would have a significant negative effect on CSEC.

In addition, there are numerous recent public sources of information about controversies in second party countries, particularly in the U.S. and New Zealand, including about alleged domestic spying by their foreign signals intelligence agencies. These events raise questions about second party practices involving PCs or information about Canadians and the Commissioner’s office will be following developments with interest.

#### *Finding no. 3: Protection of Canadians’ privacy by the Second Parties*

Beyond certain general statements and assurances among the Second Parties, the Commissioner’s office was unable to assess the extent to which CSEC’s second party partners in the United States, United Kingdom, Australia and New Zealand follow the agreements with CSEC and protect private communications and information about Canadians in what CSEC shares with the partners.

As a result, it is recommended that the Minister issue a new ministerial directive to provide general direction to CSEC on SIGINT information sharing activities with its second party partners and to set out expectations for the protection of the privacy of Canadians in the conduct of those activities. This is particularly important in light of the Five-Eyes’ [redacted]

<sup>49</sup> *Supra*, notes 14 and 27.

The drafting of the new directive should be informed by an in-depth analysis of the potential impact of respective national differences in legal and policy authorities on CSEC compliance with the law and the protection of the privacy of Canadians, that is, a risk assessment. The Commissioner's office understands that such a risk assessment would not be a trivial undertaking, would take time, and would require the cooperation of the Second Parties. However, in light of recent events, we believe it is essential.

The new directive should explicitly acknowledge the risks associated with the fact that the information shared with the Second Parties by CSEC may include one-end Canadian communications, PCs, and information about Canadians and that CSEC can not reasonably request that its second party partners account for any use of such information.

While outside of the scope of this review, it is suggested that the Minister and CSEC may find it preferable that the new directive address both SIGINT and IT Security information sharing with the Second Parties.

The Commissioner's office will continue to examine what information relating to privacy CSEC could request the Second Parties to report to it. For example, [REDACTED]

[REDACTED] NSA is the only

Second Party agency who has requested this information.

In February 2009, CSEC's SIGINT Programs Oversight and Compliance section issued written guidance to all Director General Intelligence employees, outlining the process to be followed in the case of inadvertent targeting or naming of U.S. persons.<sup>50</sup> The Commissioner's office asked CSEC why it has not similarly formally requested that the Second Parties report to it cases of inadvertent targeting or naming of Canadians. CSEC responded that, with respect to inadvertent targeting, it believes notification of inadvertent targeting would be of questionable benefit; there is no action that CSEC would take "after the fact" as the targeting was, by definition, "inadvertent". With respect to naming, CSEC indicated that it identifies any such cases as part of its routine EPR review process, then records the incidents and follows-up with the Second Party. If a naming violation is involved, the Second Party as a rule [REDACTED]

The Commissioner's office disagrees with CSEC's assessment. The benefit would be that CSEC would have knowledge about and could inform the Minister about metrics relating to the protection of the privacy of Canadians. A significant or unusual increase in these metrics could be an indication that changes are necessary to enhance the protection of the privacy of Canadians. CSEC would not provide the Commissioner's office with the number of cases of inadvertent targeting and inadvertent naming of U.S. persons that

<sup>50</sup> *Ibid.*

<sup>51</sup> *Ibid.*

CSEC reported to the NSA indicating that "CSEC feels that this question falls outside the scope of the present review as it does not involve the lawfulness of CSEC activities."<sup>52</sup> There are a number of other examples of measures that the Second Parties *choose* to apply in return for access to each other's information, for example, the Five-Eyes added an "Intelligence Purposes Only" caveat on all U.S. COMINT and U.S. COMINT-derived documents to ensure compliance with U.S. law.<sup>53</sup>

## IX. CONCLUSION

The Five-Eyes SIGINT alliance evolved from collaboration during the Second World War. Long-standing agreements and present-day resolutions provide the foundation for CSEC's SIGINT information sharing with the Second Parties.

The amount of information provided to and received from the Second Parties is extensive. Information sharing is an essential component of CSEC SIGINT collection and other activities.

CSEC SIGINT information sharing activities with the Second Parties have the potential to directly affect the privacy and security of a Canadian person. Precision and accuracy of language in exchanges of information can be critical and affect outcomes, including how individuals are treated. The Supreme Court of Canada and the Honourable Dennis O'Connor have stressed the importance of accuracy when sharing national security information:

The need to be precise and accurate when providing information is obvious. Inaccurate information or mislabelling, even by degree, either alone or taken together with other information, can result in a seriously distorted picture... The need for accuracy and precision when sharing information, particularly written information in terrorist investigations, cannot be overstated.<sup>54</sup>

The allies recognize each other's sovereignty and respect each other's laws by pledging not to target one another's communications. Consequently, CSEC policies and procedures state that collection activities are not to be directed at second party nationals located anywhere, or against anyone located in second party territory. CSEC trusts that its second party partners will similarly not direct activities at Canadians or persons in Canada. It is recognized, however, that each of the Five-Eyes is an agency of a sovereign nation that may derogate from the agreements, if it is judged necessary for their respective national interests.

---

<sup>52</sup> *Supra*, note 42.

<sup>53</sup> *Supra*, note 14.

<sup>54</sup> *Charkaoui v Canada (Citizenship and Immigration)*, [2008] 2 SCR 326, 2008 SCC 38, p. 20, quoting from the Commission of Inquiry into the Actions of Canadian Official in Relation to Maher Arar, *Report of the Events Relating to Maher Arar: Analysis and Recommendations* (2006), p. 114.

The Commissioner's update letter to the Minister of March 23, 2012, indicated that he found that CSEC does take measures to protect the privacy of Canadians in what it shares with and receives from the Second Parties. There is no need to revisit in this final review report the substantial controls in place and measures taken by CSEC to help ensure that its SIGINT information sharing with the Second Parties is lawful and protects the privacy of Canadians. The Commissioner's office will continue to examine these controls and measures in the conduct of activity and subject-specific reviews.

Discussions in interviews and written answers suggest that CSEC also conducts its SIGINT activities in a manner that is consistent with the agreements it has with its second party partners to respect the privacy of the partners' citizens, and to follow the partners' policies in this regard. The evolution of CSEC policies and procedures demonstrates that CSEC respects the core principle that the allies do not treat the communications of respective nationals as they do those that the agreements define as "foreign".

This was the first in-depth review focused exclusively on CSEC SIGINT information sharing activities with the Second Parties. In this part of the review, the Commissioner examined:

- the legislative framework for CSEC's provision to and receipt from the Second Parties of intercepted communications and other SIGINT information, particularly PCs and information about Canadians; and
- CSEC's due diligence respecting the activities, i.e., does CSEC take all reasonable steps to confirm that the Second Parties treat PCs and information about Canadians *consistent with* the laws of Canada and the privacy protections applied by CSEC? (The Second Parties have no *legal* obligation to treat PCs and information about Canadians in accordance with Canadian law.)

This review report focuses on the two outstanding questions contained in the Commissioner's update letter to the Minister of March 23, 2012, namely:

- how many PCs and what volume of information about Canadians does CSEC share with and receive from the Second Parties? and
- how does CSEC assure itself that its second party partners protect PCs and information about Canadians, and that the Second Parties follow the agreements?

In this context, CSEC activities were assessed in the context of the limitations in the *NDA* for the protection of Canadians, i.e., CSEC's foreign intelligence activities "shall not be directed at Canadians or any person in Canada" (paragraph 273.64(2)(a) of the *NDA*) and "shall 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*).

Sharing should be optimized, not mandated in detail. Attempting to prescribe in agreements or policies all details respecting CSEC SIGINT information sharing with the Second Parties is not reasonable. However, this review resulted in two recommendations to

support the Minister of National Defence in his accountability for CSEC and as a measure to protect the privacy of Canadians:

1. it is recommended that CSEC record and include in its Annual Report to the Minister information about the communications CSEC acquires from its second party partners, including the number of one-end in Canada, second party-collected communications, recognized by CSEC analysts and used or retained for FI purposes, as well as the number of this type of communication destroyed; and
2. it is recommended that the Minister of National Defence issue, under his authority pursuant to subsection 273.62(3) of the *NDA*, a new MD to provide general direction to CSEC on its foreign signals intelligence information sharing activities with its second party partners, and to set out expectations for the protection of the privacy of Canadians in the conduct of those activities. This would also support the Minister in his accountability for CSEC and as a measure to protect the privacy of Canadians.

Acceptance and implementation of the two recommendations by CSEC would address a previous finding and a recommendation of Commissioners, namely finding no. 7 in the Commissioner's 2008 [REDACTED] review report, and recommendation no. 5 in the Commissioner's 2005 [REDACTED] review report.

The Commissioner's office will continue to examine the controls in place and measures taken by CSEC to help ensure that its SIGINT information sharing with the Second Parties is lawful and protects the privacy of Canadians in the conduct of activity and subject-specific reviews.

This review has provided the Commissioner's office with background information on CSEC disclosures of Canadian identity information to second party partners and, starting in 2013, the office will expand the annual review of disclosures to also include a sample of such sharing.

The Commissioner's office will continue to include privacy incidents involving the second party partners in its annual review of incidents identified by CSEC.

In addition, as part of activity and subject-specific reviews, the Commissioner's office will follow-up on issues identified in this report, namely:

- [REDACTED] and exceptional reporting;
- sharing of metadata and use of shared systems in support of Five-Eyes mutual efforts;
- role and activities of CANSLOs;
- metrics relating to SIGINT information sharing with the Second Parties; and

- 
- second party reporting to CSEC on information shared that relates to the privacy of Canadians.

Finally, the Commissioner's office will continue to monitor Canadian and international discussions between review bodies of different countries to review information sharing activities among their respective intelligence agencies.

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



---

Robert Décaray, Commissioner

ANNEX A —Findings and Recommendations

**Recommendation no. 1: Reporting to the Minister the number of one-end in Canada, second party-collected communications**

To support the Minister of National Defence in his accountability for CSEC and as an additional measure to protect the privacy of Canadians, CSEC should record and include in its Annual Report to the Minister information about the communications CSEC acquires from its second party partners in the United States, United Kingdom, Australia and New Zealand, including the number of one-end in Canada second party-collected communications, recognized by CSEC analysts and used or retained for foreign intelligence purposes, as well as the number of this type of communication destroyed.

**Recommendation no. 2: New ministerial directive on CSEC foreign signals intelligence information sharing activities with its second party partners**

To support the Minister of National Defence in his accountability for CSEC and as a measure to protect the privacy of Canadians, it is recommended that the Minister issue, under his authority pursuant to subsection 273.62(3) of the *National Defence Act*, a new ministerial directive to provide general direction to CSEC on its foreign signals intelligence information sharing activities with its second party partners in the United States, United Kingdom, Australia and New Zealand, and to set out expectations for the protection of the privacy of Canadians in the conduct of those activities.

*Finding no. 1: Shared private communications and information about Canadians*

CSEC does not count and does not report to the Minister of National Defence the number of private communications and the volume of information about Canadians that CSEC shares with and receives from its second party partners in the United States, United Kingdom, Australia and New Zealand.

*Finding no. 2: Reporting to the Minister*

Regularly reporting to the Minister a wider range of statistical information relating to information shared with the Second Parties, in a manner similar to the existing MA statistics, would support the Minister in his accountability for CSEC and supplement existing measures to protect the privacy of Canadians.

*Finding no. 3: Protection of Canadians' privacy by the Second Parties*

Beyond certain general statements and assurances among the Second Parties, the Commissioner's office was unable to assess the extent to which CSEC's second party partners in the United States, United Kingdom, Australia and New Zealand follow the agreements with CSEC and protect private communications and information about Canadians in what CSEC shares with the partners.

**ANNEX B — Interviewees**

The following CSEC employees provided information or facilitated the review:

A/Director General, SIGINT Programs  
Director, Corporate and Operational Policy  
A/Director, SIGINT Requirements  
A/Director, External Review and Policy Management  
Manager, Operational Policy  
Manager, External Review and Policy Management (D3)  
A/Manager, D3  
A/ Manager, D3  
Manager, SIGINT Programs Oversight and Compliance (SPOC)  
A/Manager, SPOC  
Senior Advisor, SPOC  
Senior Mission Management Officer, SPOC  
Senior Policy and Review Advisor, D3  
Senior Policy and Review Advisor, D3  
Senior Policy and Review Advisor, D3

**ANNEX C — Commissioner's update letter to the Minister of March 23, 2012**

Communications Security  
Establishment Commissioner  
The Honourable Robert O'Leary, Q.C.



Commissaire du Centre de la  
sécurité des télécommunications  
L'honorable Robert O'Leary, c.c.

**TOP SECRET//SI//CEO**  
**Our file # 2200-63**

March 23, 2012

The Honourable Peter MacKay, P.C., M.P.  
Minister of National Defence  
101 Colonel By Drive  
Ottawa, Ontario  
K1A 0K2

Dear Mr. MacKay:

The purpose of this letter is to provide you with an update on my review of CSEC's signals intelligence (SIGINT) information sharing activities with its second party partners – the U.S. National Security Agency, the U.K. Government Communications Headquarters, the Australian Defence Signals Directorate, and the New Zealand Government Communications Security Bureau. The review is being conducted under my authority as articulated in Part V.1, paragraph 273.63(2)(a) of the *National Defence Act (NDA)*.

I had committed to completing this review this year. However, it has taken longer than expected for several reasons, significantly including competing priorities of my office and of CSEC. First, I assessed that two other reviews must take priority. These reviews will, however, also address certain issues relating to SIGINT information sharing. **[REDACTED]**

**[REDACTED]** while the second review concerns CSEC's activities relating to **[REDACTED]**. You will receive my review reports on these two subjects early in the new fiscal year. The second reason relates to competing priorities of CSEC, partly reflecting CSEC responding to my shift in review priorities. However, the SIGINT information sharing review is also taking longer than expected due to staffing challenges at CSEC in support of review and delays in providing information and responses to questions from my office. This issue is the subject of discussion between my office and CSEC officials.

P.O. Box/C.P. 1084, Station 45/Suburbane 43-  
Ottawa, Canada  
K1P 5R5  
(613) 992-3044 Fax: (613) 992-4006

-2-

TOP SECRET//SI//CEO

My review of CSEC's SIGINT information sharing activities to-date has identified that the amount of foreign intelligence CSEC provides to and receives from the Second Parties is extensive; information sharing is an essential component of CSEC's SIGINT program.

Long-standing agreements and practices provide a foundation for CSEC's SIGINT information sharing with the Second Parties. These cooperative arrangements include a commitment by the Second Parties to respect the privacy of each others' citizens, and to act in a manner consistent with each others' policies relating to privacy. It is recognized, however, that each of the Second Parties is an agency of a sovereign nation that may derogate from the agreements, if it is judged necessary for their respective national interests.

Thus far, I have found that CSEC does take measures to protect the privacy of Canadians in what it shares with the Second Parties, for example: CSEC employees must apply CSEC privacy rules to second party-acquired communications; CSEC suppresses Canadian identity information in metadata and reports shared with the Second Parties; nationality checks and other measures help to limit the inadvertent targeting of Canadians by the Second Parties; and CSEC takes action to correct or mitigate privacy incidents involving the Second Parties.

However, my review has also identified important questions that I will examine, including: How many private communications of Canadians and what volume of Canadian identity information does CSEC share with and receive from the Second Parties? How does CSEC assure itself that its second party partners protect the private communications of Canadians and Canadian identity information, and that the Second Parties follow the agreements? This review also includes an examination of a sample of CSEC disclosures to its second party partners of Canadian identity information as well as relevant privacy incidents identified by CSEC.

I will complete my review and report to you on this subject in the next fiscal year. If you have any questions or comments, I will be pleased to discuss them with you at your convenience.

Yours sincerely,



Robert Décaray

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