Communications Security Establishment Commissioner

The Honourable Charles D. Gonthier, C.C., Q.C.

Canada

Commissaire du Centre de la sécurité des télécommunications

L'honorable Charles D. Gonthier, C.C., c.r.

TOP SECRET/COMINT/CEO
(with attachment)
16 January 2008

The Honourable Peter G. MacKay, PC, MP
Minister of National Defence
101 Colonel By Drive
Ottawa, Ontario
K1A 0K2

Dear Mr. MacKay:

The purpose of this letter is to advise you of the results of a review by my office (OCSEC) of the lawfulness of CSE's activities in providing foreign intelligence support to the Canadian Security Intelligence Service (CSIS) under CSE's (a) mandate (*National Defence Act* (*NDA*) paragraph 273.64(1)(a)). The review was undertaken under my general authority articulated in Part V.1, paragraph 273.63(2)(a) of the *NDA*, and covered activities from April 01, 2004 to March 31, 2005 and from November and December 2006.

My office began this study in August 2005. The delays in finalizing the report were caused, in part, by other operational commitments of the OCSEC analyst conducting the review. However, the report was also delayed because my staff did not receive requested documentation from CSE in a timely manner. CSE officials have acknowledged that this was in part due to the lack of a formal system of record-keeping during the period under review, and therefore an inability on CSE's part to easily compile the required documentation. This issue is addressed in my report and CSE has committed to implementing a new corporate information management system during 2007/08. My staff have been receiving regular updates on the implementation process.

Background

As part of its (a) mandate, CSE provides regular foreign intelligence reporting to CSIS, most of which addresses general areas of interest that complement

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

and support CSIS's own mandated responsibilities. CSE also receives and responds to specific CSIS requests for intelligence-related information (RFIs), provided that the requirement is consistent with documented Government of Canada Requirements (GCRs) and CSE's National SIGINT Priorities List (NSPL). A final aspect of CSE's (a) mandate support to CSIS is that it responds to requests for the release of suppressed Canadian identities or other suppressed information contained in foreign intelligence reporting.

Overall Findings

This review was conducted by OCSEC pursuant to the Department of Justice legal opinions and its interpretation of the legislation. Overall, I am of the opinion that CSE acted within its mandate in conducting the activities it undertook and I am in accord with the advice and guidance provided by Department of Justice counsel to CSE. In some cases, however, I do not support the application of that advice. I am of the opinion that some activities undertaken by CSE based on requests for information from CSIS should have been done under mandate (c) (as an agent of CSIS) rather than mandate (a) (collection of foreign intelligence). I have recommended that CSE re-examine the application of the Department of Justice advice and asked whether additional questions need to be posed when assessing whether a request from a Government of Canada client, in this case CSIS, falls under mandate (a) or mandate (c). My officials discussed this matter with CSE in November 2007. Recently my office provided a discussion paper to CSE on this issue and will meet to review it further.

I would also note that in the previous review year I submitted two classified reports to your predecessor that had findings and recommendations applicable to, and that re-inforce some of the findings and recommendations of this review. These reports were *CSE Support to Law Enforcement: Royal Canadian Mounted Police (RCMP) Phase II: CSE Mandate (a)*[1] and *Role of the CSE's Client Relations Officers and the Operational Policy Section (D2) in the Release of Canadian Identities.*[2]

In summary, my observations, specific findings and my recommendations from this review are as follows:

Ministerial directives

Ministerial directives issued to CSE and dated June 19, 2001 preceded the passage of Part V.1 of the *National Defence Act*, and I would suggest they be reviewed to ensure they are in keeping with the mandated authorities articulated in the legislation. In response to the same observation in previous reviews, CSE has indicated that this task will be undertaken after the legislation has been amended.

[1] Submitted June 16, 2006
[2] Submitted March 30, 2007

Corporate Records

CSE has no centralized function to track or centrally locate its discussions and actions after a request for information (RFI) has been received. Accordingly, I recommend that CSE ensure its new corporate information management system, which will be implemented in 2007/2008, can capture and attribute to a centralized file all activities by individual analysts, so that the work is thoroughly documented for future reference, and that supporting documentation can be readily linked to the request or operation under which it was conducted.

Acquisition of Foreign Intelligence

CSE does not normally question how CSIS obtained the information contained in a request for information. CSE policy states it must be assured via the CSIS request that the information has been acquired lawfully. While I consider this policy to be reasonable, it does not appear to be stringently applied when processing CSIS requests. Accordingly, I recommend that CSE consider re-examining CSIS RFIs to ensure all information required under CSE policy is contained in the RFI, including the written assurance that the information was acquired lawfully, in accordance with an investigation or warrant under section 12 of the *CSIS Act*, and linked to a Government of Canada Requirement.

Mandate (a) vs. Mandate (c)

I question whether some of the activities undertaken on behalf of CSIS should have been conducted under mandate (c) rather than mandate (a), and I recommend that CSE re-examine this matter to ensure that all decisions and resulting activities are based upon criteria that have been consistently applied and are statutorily defensible. This includes clarification of the relevant mandate under which contact chaining activities should be conducted, for example, a matter dealt with in more detail in my office's review of the *Ministerial Directive, Communications Security Establishment, Collection and Use of Metadata, March 9, 2005* submitted to you on January 9, 2008.

Requests for Release of Suppressed Information

After reviewing requests for release of suppressed information in the review period, my staff determined that although CSE had followed the relevant policies and procedures in place at the time, there were a number of inconsistencies in the completion of the forms or the degree of detail provided by CSIS. Accordingly, I believe CSE should consider amending the Request for Release form to ensure it is clear to clients that all parts of the form must be completed regardless of whether any action is contemplated based on the suppressed information requested. I identified questions about the provisions for the disclosure of identities under the *Privacy Act* with a view to amending the Request for Release form to include the section of the

Privacy Act that is the appropriate authority. I note that in response to recommendations made in the reviews of *CSE Support to Law Enforcement: Royal Canadian Mounted Police (RCMP) Phase II: CSE Mandate (a);* of the *Role of the CSE's Client Relations Officers and the Operational Policy Section (D2) in the Release of Canadian Identities;* and of the *Office of Counter Terrorism,* CSE has indicated that a review was undertaken by CSE's legal counsel following consultations with the Information Law and Privacy section of the Department of Justice. Solicitor-Client Privilege

Solicitor-Client Privilege

Treatment of Requests for Information (RFIs)

My staff was concerned to note that CSE treats information provided by CSIS in the same way as any other foreign information it obtains through its own searches or through other GoC departments or collaborating agencies, i.e. as lead information that may assist CSE with subsequent targeting and tasking. In my opinion, CSE is contravening the Memorandum of Understanding between CSIS and CSE dated November 1, 1990, which indicates CSE is to consult with CSIS prior to the dissemination of any security or foreign intelligence derived from information provided by CSIS. When my staff questioned CSE on this matter, we were advised that CSIS and CSE believe consultation is not required when CSIS provides lead information used in obtaining foreign intelligence in relation to Government of Canada intelligence requirements. Accordingly, I recommend that CSE ensure that the CSIS-CSE Memorandum of Understanding is revised to reflect current practices and agreements.

As is my practice, I have provided officials at CSE an opportunity to review and comment on this report, prior to finalizing and forwarding it to you. I will continue to monitor the issues raised.

Please let me know if you have any questions or comments.

Yours sincerely,

Charles D. Gonthier

c.c. Mr. John Adams, Chief, CSE
Ms. Margaret Bloodworth, National Security Advisor, PCO
Mr. Robert Fonberg, Deputy Minister, National Defence

TOP SECRET/COMINT/Canadian Eyes Only

Report to the CSE Commissioner on

CSE Support to CSIS

Phase I: CSE Mandate (a)

January 16, 2008

I. AUTHORITY

This report was prepared on behalf of the Communications Security Establishment (CSE) Commissioner under his general authority articulated in Part V.1, paragraph 273.63(2)(a) of the *National Defence Act* (*NDA*).

II. INTRODUCTION

The purpose of this review was to examine and assess the lawfulness of CSE's activities as they relate to the provision of support to the Canadian Security Intelligence Service (CSIS) under subsection 273.64(1) of the *NDA*, and in particular paragraph 273.64(1)(a).

CSE collects foreign signals intelligence in support of the Government of Canada's (GoC) annual intelligence priorities, under the authority of paragraph 273.64(1)(a) of the *NDA* (referred to hereafter as the (a) mandate):

> *(a) 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;*

As part of its (a) mandate, CSE provides regular foreign intelligence reporting to its clients, including CSIS, most of which addresses general areas of interest that complement and support CSIS's own mandated responsibilities.

CSE also receives and responds to specific CSIS requests for intelligence-related information (also referred to as RFIs), provided that the requirement is consistent with documented Government of Canada Requirements (GCRs) and CSE's National SIGINT Priorities List (NSPL).

A final aspect of CSE's support to CSIS is that it responds to requests for the release of Canadian identities or other suppressed information contained in foreign intelligence reporting.

III. PERIOD OF REVIEW

The following report presents our findings as they relate to CSE's (a) mandate activities in support of CSIS for the period April 01, 2004 to March 31, 2005. During the review we agreed to a suggestion by CSE to also look at [redacted] RFIs actioned in the period [redacted] Where practices have changed subsequently, this will be noted.

We began this study in August 2005. The delays in finalizing the report were caused, in part, by other operational commitments of the OCSEC analyst conducting the review.

However, the report was also delayed because we did not receive requested documentation from CSE in a timely manner. CSE representatives have acknowledged that this was in part due to the lack of a formal system of record keeping during the period under review, and therefore an inability on CSE's part to easily compile the documentation we requested.

IV. OBJECTIVE

The objective of this review was to assess the lawfulness of CSE's activities under its (a) mandate, in support of CSIS.

V. LINES OF INQUIRY

The review pursued the following lines of inquiry:

- Identify and describe the nature of the CSE–CSIS relationship and the forms of assistance provided under the authority of CSE's mandate.
- Identify and examine all related authorities that govern CSE–CSIS activities conducted pursuant to CSE's mandate, and for the purposes of this review its (a) mandate, including:
  - ministerial directives;
  - memoranda of understanding;
  - legal advice and opinions; and
  - policies and procedures.
- Examine CSE's process for reviewing and accepting/denying requests for assistance made by CSIS under the authority of the (a) mandate, and identify and understand how CSE tracks and accounts for the assistance it provides CSIS.
- Identify and examine any related records, files, correspondence, and any other material such as CSE internal audits or reviews conducted in respect of CSE's assistance to CSIS.
- Examine, review and report on any other issue that may arise during the course of this study and that may impact on CSE's ability to conduct its activities lawfully and safeguard the privacy of Canadians.

VI. METHODOLOGY

To begin this review we requested and received a general briefing pertaining to the support CSE provides to CSIS. In addition, we submitted a series of written questions pertaining to support provided to CSIS by CSE under its (a), (b) and (c) mandates. In the interest of time, we advised CSE on September 6, 2006 that we would focus specifically on CSE's support to CSIS under its (a) mandate. A reassessment of the focus and time frames of support to CSIS under CSE's other mandates (b) and (c), as outlined in our original Scope Statement, will be done at a later date. We also conducted three onsite interview/information sessions with individuals working in the areas involved. During the course of this review we were advised that CSE had not conducted any internal audits or reviews specific to its support to CSIS. CSE has since advised us that various elements of SIGINT support to CSIS may have been captured in audits or evaluations pertaining to the IRRELEVANT program (November 2003 – March 2004) and Support to Lawful Access program.

We obtained a list of the CSIS Requests for Information (RFIs) during the period under review. This list included [redacted] requests for intelligence-related information, [redacted] of which were from the Counter Terrorism branch of CSIS. We chose [redacted] %) of these RFIs to review in more detail, as these appeared to be requests for information related more specifically to Canadians, or to investigations relating to Canadians. In December 2006 we received a listing of [redacted] RFIs and the related material for [redacted] of these (the documentation for one was missing); this constituted approximately half of the [redacted] we had originally chosen. CSE was unable to provide the documentation for the remaining [redacted] RFIs we had originally requested in a reasonable time frame; therefore, in the interest of avoiding any further delays, we agreed to continue the review with what CSE was able to provide.

We completed the analysis and then a draft of this report in September 2007, after which we reiterated our request for the remaining [redacted] RFIs. We received them, along with most of the related documentation, on November 29, 2007. We have included the analysis of these RFIs in an annex to this report, and results have been referred to in the conclusions.

Since [redacted] RFIs we actually received were from CSIS' Counter Terrorism branch, we arranged to meet with representatives of CSE's Office of Counter Terrorism (OCT) to determine the best way to proceed and complete this review. After our initial meeting, we decided that we would, in the interest of time, choose and review a small sampling from the [redacted] RFIs CSE provided. In addition, CSE also suggested reviewing RFIs received in the latter part of [redacted] in order to see how the process had changed from the original review period. As a result, we reviewed five RFIs from the original review period of April 2004 to March 2005, and four received between [redacted] that CSE randomly picked.

In addition, CSE had advised us that during the review period a total of [redacted] Canadian identities had been released to CSIS. Therefore, we requested the related documentation

and then reviewed [redacted] Release of Suppressed Information forms, which we were advised were the total for the review period. Most of the forms contained multiple release requests.

The findings of the above-noted review areas are described in the following section.

VII. REVIEW FINDINGS

Overall, this review found that CSE's support to CSIS under its (a) mandate during the review period was within the law, as interpreted by the Department of Justice, and followed CSE policies, as they existed during the review period. However, we did identify a number of issues, some of which we have addressed with recommendations.

It should be noted that two previous classified reports submitted to the Minister had findings and recommendations applicable to this review. These reports were *CSE Support to Law Enforcement: Royal Canadian Mounted Police (RCMP) Phase II: CSE Mandate (a),*[1] and *Role of the CSE's Client Relations Officers and the Operational Policy Section (D2) in the Release of Canadian Identities.*[2] We will not repeat findings that have already been highlighted, discussed and analyzed quite extensively in the two aforementioned reports, but simply note where they apply to this review as well. The findings of the two previous reports, as they relate to CSE's mandates (a) and (c), are the subject of ongoing discussions. This report will inform those discussions as well.

(a) Authorities

In addition to its legislated authority as identified above, CSE's foreign signals intelligence support to CSIS is guided by several supporting instruments, including:

- Three ministerial directives dated June 19, 2001:
  - *CSE Support to Law Enforcement and National Security Agencies;*
  - *Accountability Framework*; and
  - *Privacy of Canadians.*

- The CSIS–CSE Memorandum of Understanding (MOU), effective November 1, 1990, outlining the nature of operational and technical cooperation in relation to signals intelligence activities.

- Operational policies and procedures in force for the review period, including:
  - OPS-1 *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities;*

[1] Submitted June 16, 2006
[2] Submitted March 30, 2007

- OPS-1-1 *Procedures for the Release of Suppressed Information from SIGINT Reports*;
- OPS-1-7 *SIGINT Naming Procedures*;
- OPS-4-2 *Procedures for Assisting CSIS Section 12 Activities*; and
- OPS-5-9 *End-Product Sanitization/Action-on Procedures.*

The CSE personnel we interviewed have a clear understanding that their activities must respect the laws of Canada—not only the *National Defence Act,*, but also the *Criminal Code*, the *Charter,* and the *Privacy Act.*

Observation no. 1

Ministerial directives issued to CSE and dated June 19, 2001 preceded the passage of Part V.1 of the National Defence Act *and should be reviewed to ensure they are in keeping with the mandated authorities articulated in the legislation.*

In response to the same observation in previous reviews by this office, CSE has indicated that this task will be undertaken when the legislation has been amended. More specifically, CSE responded to a similar recommendation contained in the *RCMP Phase I* review in January 2005 as follows:

"**Accepted and Active.** - It is integral to CSE's plan to revisit all three of the original MDs that pre-date legislation. This work was initiated during the first quarter of FY 05/06, and the revised MDs will be ready for signature by our Minister on completion of the *Anti-Terrorism Act* review."

This matter remains outstanding as of the date of this report.

(b) Corporate Records: An Ongoing Issue

Operational files associated with any RFIs or other CSE activities vary between individual work areas in respect to their organization and completeness. CSE has advised in its written responses that there is no requirement to maintain a central file with respect to the CSE-CSIS relationship as it pertains to mandate (a). CSE's Office of Counter Terrorism (OCT) has its own centralized or shared system for recording and tracking RFIs. However, there is no requirement or centralized function to track or centrally locate information, discussions or e-mails between the CSIS and CSE analysts after an RFI has been received and during the course of the RFI cycle. This makes it difficult for CSE employees to respond to queries about why certain actions were taken, or why an approach was followed that differed from the original RFI.

It is important for accountability that all interaction between CSE's analysts and clients, especially those with investigative mandates, be documented and that records be kept centrally for such transactions. All activity by CSE should be linked to the RFI or a central corporate record, rather than to the analyst, particularly for activities that may

relate to the safeguarding of the privacy of Canadians. A recent briefing by CSE suggests that this matter will be addressed with the implementation of the new corporate information management system.

(c) Acquisition of Foreign Intelligence

When CSIS requests foreign intelligence from CSE, the RFI normally indicates [redacted] We have been advised that CSE assesses all information provided by CSIS, and seeks clarification if there are any questions or concerns. However, CSE does not normally question how CSIS obtained the information in question—the presumption is that CSIS has lawfully acquired the information that it is providing.

Observation no. 2

CSE's failure to ensure that material provided by CSIS has been lawfully acquired would appear to be contrary to the stated objective and requirements of CSE Operational Policy OPS-4-2.[3]

Recommendation no. 1:

CSE should consider re-examining CSIS RFIs to ensure all information required under OPS-4-2 is contained in the RFI, including the written assurance that the information was acquired lawfully and in accordance with an investigation or warrant under section 12 of the *CSIS Act*, and linked to a Government of Canada Requirement.

(d) Mandate (a) vs. Mandate (c)

When CSE receives an RFI from CSIS or any other GoC client department, we were advised that it assesses whether the request falls under mandate (a) by asking:

- Is the activity directed at a foreign person or entity?
- Is the foreign person or entity located outside of Canada?
- Does the expected information or intelligence relate to the capabilities, intentions or activities of the foreign person or entity? and
- Does the expected information or intelligence relate to an intelligence priority of the Government of Canada?

[3] OPS-4-2, *Procedure for Assisting CSIS Section 12 Activities,* dated July 25, 2001, states under the policy objective that the procedures contained therein are intended to "reassure CSE staff that any material provided to them by CSIS has been acquired lawfully". The procedures require that "written requests should contain whether there is a valid warrant or not, background of the CSIS operation, clear description of kind of assistance being sought, urgency of request and form the response should take".

If the answer is yes to all four questions, then CSE proceeds under mandate (a) and in accordance with CSE operational policies.

However, we suggest that additional questions may need to be included to address whether the information being provided by CSIS relates to the subject of an authorized investigation by CSIS. Additional questions would assist in determining whether the activity CSE undertakes is in fact "directed at" the person who is the subject of or associated with the information CSIS provided. Such questions could include: "Is the request part of an authorized or lawful investigation?" and "What is the intent or focus of the investigation?"

Observation no. 3

CSIS requests for information that may relate to a specific investigation or warranted activity under section 12 of the CSIS Act, *such as any* IRRELEVANT IRRELEVANT *may be more appropriately made and dealt with under CSE's (c) mandate,*[4] *as they are in fact being used by CSIS to further an authorized investigation being conducted by CSIS.*

As was indicated in the report on CSE support to the RCMP dated June 2006, and the review of the *Ministerial Directive, Communications Security Establishment. Collection and Use of Metadata, March 9, 2005*, submitted to the Minister in January 2008, CSE should be able to assess its activities in response to any client department seeking intelligence support based on foreign information obtained from, and/or linked to, persons in Canada under lawful investigation.

Whereas section.16 of the *CSIS Act* expressly states that CSIS may collect foreign intelligence *in Canada* at the request of either the Minister of National Defence or the Minister of Foreign Affairs, section 12 does not preclude CSIS from collecting this information overseas. The section 12 mandate reads:

> "The Service shall collect, by investigation or *otherwise*, to the extent that is strictly necessary, and analyse and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada and, in relation thereto, shall report to and advise the Government of Canada."

In order to meet this mandate, CSIS can request that CSE provide what for CSIS purposes is "security intelligence" about foreign persons or entities that may be related to CSIS targets under investigation in Canada.

[4] Mandate (c) (*NDA*, Part V.1, paragraph 273.64(1)(c)) authorizes CSE to "provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties."

The scope and intent of section 12 of the *CSIS Act* has been explained by current and former Directors of CSIS before parliamentary committees and in other public forums. Indeed, a former Solicitor General said during debate on the bill in 1984 that resulted in the *CSIS Act*, "There is no statutory requirement that the entire activities of the Security Intelligence Service be performed in Canada. I think that would be unduly inhibiting." As a former Director of CSIS has observed: "...the legislation authorizes us to conduct operations abroad. It wasn't in hindsight that some loophole has been discovered. The Act was designed that way in the first place to protect Canada from threats to its security."

CSIS requests for security intelligence concerning foreign entities in support of authorized section 12 investigations in Canada are therefore requests to provide operational support to a national security agency, thus requiring CSE to conduct its activities under its (c) mandate. This distinction is important because it determines how CSE handles the information it is collecting, which differs depending on whether it is acting as the principal, under mandate (a), or as the agent, under mandate (c).

In addition, by including additional questions in its criteria for determining whether an activity should be conducted under mandate (a) or (c) (such as whether or not there is an authorized investigation—which does not necessarily require a federal court warrant), the resulting answers may allow it to act under mandate (c) without resorting to determining what CSIS can or cannot do within its own mandate.

Just as is the case in section 16 activities, CSE would not be precluded from further disseminating foreign intelligence gathered at the request of CSIS for a domestic investigation. Upon sign-off by CSIS (as allowed for under the section 12 Memorandum of Understanding), that foreign intelligence could be provided to Government of Canada clients and allies that have a requirement.

This issue is further described below in the context of CSE's treatment of the RFIs we selected for detailed review.

Recommendation no. 2:

In accordance with the above-noted observation and Recommendation no. 1, as well as with Recommendation no. 2 from the RCMP Phase II review,[5] CSE should re-examine its interpretation and application of mandates (a) and (c) and ensure that all decisions and resulting activities are based upon criteria that have been consistently applied and are statutorily defensible.

[5] *RCMP Phase II*, submitted to the Minister of National Defence, June 16, 2006.

(e) Treatment of Requests for Information (RFIs)

We were advised that CSIS information and/or requests are provided to the relevant [redacted] production areas. The analysts' activities in response to that request/information might include searching various data sources for further foreign information related to the CSIS information/request, or targeting the foreign selectors to [redacted] collection sources to obtain additional foreign intelligence. In this instance the Director General Intelligence Production Group could engage other components or collection programs within CSE

Following our selection of [redacted] RFIs for review, we arranged an initial meeting with representatives of CSE's [redacted] Group), as our preliminary review of the RFIs and related end-product reporting raised a number of questions and concerns.

Evolution of the RFI Process

[redacted] Group explained that what has typically been called an RFI is in fact treated the same as any other lead information CSE may acquire on its own or through other client agencies or Second Party partners. The RFI becomes simply a starting point for the production of foreign intelligence for GoC clients and partners generally. The assigned production unit reviews the information contained in the RFI for foreign selectors. No further action is taken with any information that CSE defines as "contextual" information about Canadians. The foreign selectors are then entered into various CSE databases, first to determine if any previous reporting exists on that selector or target. Any information that may arise is then corroborated [redacted] Depending on what information is found as a result of this preliminary search, CSE may or may not target the specific selectors contained in an RFI. CSE personnel also added that they do not often get results based specifically on the lead information provided by the RFI, and if they do receive traffic it is not necessarily foreign intelligence. If CSE holds the information for a period of time, an analyst may eventually be able to develop something usable, but there is no guarantee.

We were unable to correlate the end-product reporting, which had been associated with several of the RFIs, to the information contained in the original request. CSE advised us that this results from the process the original RFI lead information undergoes as the foreign selectors are tasked. It became clear that what we thought was a linear process leading from an RFI and subsequent targeting, to appropriate Government of Canada Requirements (GCRs) / National SIGINT Priorities Lists (NSPLs) to CSE's (a) mandate and legal authorities, to an end-product report, was in fact much more complicated. CSE's analysis is what representatives referred to as a [redacted] process. The lead information/RFI is, as we previously noted, merely a starting point for a process that spreads in many different directions, sometimes producing many new leads, which are then pursued, ultimately resulting in new and different end products not necessarily related to the information that started the process.

We then inquired how CSE would respond to the original CSIS RFI, and were advised that the original Security Product Line (SPL) or CSIS-specific reporting line, no longer exists, other than when information CSE obtains is *specific to a CSIS-only requirement.* CSE advised that, in some particularly sensitive cases, [redacted] There was a short-lived attempt to segregate information received that related specifically to CSIS, but this was abandoned because of other priorities such as CSE's relationship with its four Second Party partners. CSE believes that when it is prevented from sharing intelligence, this inhibits the ability to obtain additional intelligence of value to the Government of Canada. Through the development of this "partnership" principle, CSE believes it is still getting the required information back to CSIS but just not on a one-to-one basis. CSIS receives any and all foreign intelligence information that relates to the mandated requirements it has provided to CSE, as do all other GoC departments to which CSE provides reporting.

When CSE treats information provided by CSIS in the same way as any other foreign information it obtains through its own searches or through other GoC departments or collaborating agencies, i.e. as lead information that may assist CSE with subsequent targeting and tasking, CSE appears to be contravening the Memorandum of Understanding between CSIS and CSE dated November 1, 1990. This MOU indicates CSE is to consult with CSIS prior to the dissemination of any security or foreign intelligence derived from information provided by CSIS.[6] When we questioned CSE on this matter, we were told that the provisions of the MOU are invoked when CSIS makes a formal request for assistance (usually technical) under CSE's (c) mandate. However, we were advised by CSE that they and CSIS believe this is not required when CSIS provides lead information used in obtaining foreign intelligence in relation to GCRs.

Recommendation no. 3:

CSE should review the Memorandum of Understanding between CSE and CSIS, dated November 1, 1990, relating to information/intelligence exchange and operational support (section 12 activities), to ensure it reflects current practices and agreements.

We asked if CSE would treat information or requests received from CSIS differently if CSE was aware that the information related to a section 12 investigation that CSIS was conducting under a warrant. CSE advised us that it would depend on the wording of the RFI and whether it dealt with a group or an individual. As mentioned previously, CSE advised that the Canadian content or identifiers contained in an RFI are considered contextual and not acted upon. However we were provided with [redacted] examples where

[6] CSIS-CSE MOU dated November 1, 1990 – Appendix C, Section A, #5(a) & (b), Section D - #14(a) & (b).

CSE, in response to a CSIS RFI, sought specific permission through an internal process of review and managerial approval, to contact chain [redacted] in order to obtain foreign intelligence; [redacted]

In [redacted] of the above-noted examples, CSE commenced the activity at the specific request of CSIS using information supplied by CSIS. [redacted] were not acquired by CSE as part of its own foreign intelligence collection activities. [redacted] Further, Department of Justice counsel to CSE, in May and September 2004, noted that, Solicitor-Client Privilege Solicitor-Client Privilege

Observation no.4

The foregoing supports the recommendation made in the review of the Ministerial Directive, Communications Security Establishment, Collection and Use of Metadata, March 9, 2005, *submitted to the Minister on January 2008, that CSE should re-examine and reassess the legislative authority used to conduct its contact chaining activities commencing with* [redacted] *particularly those supplied by clients, including law enforcement and security agencies engaged in ongoing criminal and national security investigations.*

Such re-examination, as suggested in the recent Metadata review, would require that attention be given to the meaning of, for example, "directed at" (paragraph 273.64(2)(a), *NDA*), intercepted information (paragraph 273.64(2)(b), *NDA*), and metadata (both foreign and [redacted] that is incidentally obtained versus that which is supplied by a client.

In addition, it was found that while the above [redacted] cases were well documented, the CSE policy governing contact chaining was not instituted until June 2006. [redacted] This policy was marked as a draft policy. To date an approved final policy has not been issued.

In the absence of the above-noted policy during the review period covered by this report, we questioned under which authority CSE was able to seek and obtain management approval to conduct such activity, and we were provided with copies of draft policies and memoranda from 2003. None dealt specifically with the section 12 situations described above; one memorandum indicated that [redacted] should not be undertaken in the absence of a legal opinion.

The activity of contact chaining [redacted] is dealt with in greater detail in the above-noted OCSEC review of the *Ministerial Directive on the Collection and Use of Metadata*, which was completed and sent to the Minister in January 2008. The circumstances described in the present review support the findings made in the Metadata review that contact chaining will have to be studied and assessed, along with and in the context of the October 2003 Department of Justice legal opinion that deals with the Solicitor-Client Privilege We were informed in late August 2007 that CSE suspended contact chaining [redacted] pending the outcome of internal discussions.

RFIs Reviewed By OCSEC

As previously noted, we chose [redacted] RFIs provided to us by CSE, as each had a very clear Canadian content angle. In addition, some had related end-product reporting. The CSE Tracking – Requirements and RFIs sheet provided to us indicated that for two RFIs, special authorization had been sought and granted to contact chain [redacted] and two were de-tasked as they either very clearly contained [redacted] and/or there was insufficient information provided by CSIS for CSE to determine if the [redacted]

CSE representatives from the Office of Counter Terrorism (OCT) described to us the process CSE would follow in dealing with the above-noted RFIs. The first RFI we dealt with had been processed by the project leader from OCT we were meeting with, and therefore the CSE process was very easily explained and found to be in order.

The other RFIs were not so straightforward, as the employee who was helping us could only second-guess in some areas what approach the analyst who had handled the RFI would have taken. It was explained that although all the same tools/databases are available to everyone working in OCT, each analyst can approach the information differently and subsequently come up with different information or different directions to go in. This, along with the [redacted] process described earlier, explains why some of the EPRs we reviewed that were shown as being related to a specific RFI did not resemble the information contained in the RFI.

Observation no. 5

It is problematic from a corporate accountability perspective that the end product may not relate to the GCR that was given in the first instance. In such instances, CSE's systems and policies do not require that a separate tracking be kept and that the "new" GCR that is being met be provided.

(f) CSE Requirement Tracking Forms

We observed that the information contained in CSE's Requirement Tracking Forms for the period under review was incomplete. We would expect that CSE policies and

procedures would indicate a requirement for analysts to complete tracking forms in order to account for actions taken and results obtained. However, we found that CSE analysts were identified by first names only, if at all, and the column for CSE file number/office assigned was invariably blank. CSE representatives provided us with a copy of the current tracking sheet used within OCT, which provides for greater detail. It is a continuing problem, however, that completion of tracking forms is somewhat of a voluntary process, as the fields contained on the form are not mandatory insertions dictated by the software system used. When the forms are not completed, there is a gap in the accountability chain, because there is no way of ensuring RFIs have been handled appropriately from beginning to end.

Observation no. 6

It was not always possible to draw a line from the authorities and requirements of legislation and policy, to CSE practices and the actual activities undertaken in response to a request from CSIS.

All RFIs we reviewed were written requests/e-mails from CSIS. Some of the RFIs were very detailed, whereas others were more general in what they requested. In keeping with CSE policy (OPS-4-2), we would expect to see consistency in the amount of information required and provided before CSE actions any request.

(g) Requests for Release of Suppressed Information

As previously noted, CSE advised us that during the period under review CSIS had requested and received [redacted] releases of suppressed information about Canadian identities contained in foreign intelligence reporting. We received copies of [redacted] Requests for Release of Suppressed Information. Most of these obviously contained requests for more than one identity.

After reviewing each of these requests and subsequent releases we determined that although CSE had followed the policies and procedures governing the release of suppressed information in place during the period of this review, there were a number of inconsistencies in the completion of the forms or the degree of detail provided by CSIS.

These inconsistencies or omissions of detail occurred most notably in sections:

- F.2 – if there is an actual or potential violation of a Canadian law, cite the law;
- F.3 - [redacted]
- G – indicate what action, if any, is being contemplated based on the information.

We noted that when section F.1 of the forms provided to us indicated that the CSIS rationale for requesting the information was that it related to Cabinet Confidence or Cabinet Confidenc and Cabinet Confidence section F.2 requesting CSIS to

cite the Canadian law which would potentially or actually be violated, was in all instances blank. This supports similar findings contained in a recent review, *Role of the CSE's Client Relations Officers and the Operational Policy Section (D2) in the Release of Canadian Identities.*[7]

The policy governing this (OPS-1-1, *Procedures for the Release of Suppressed Information in SIGINT Reports*)[8] requires that the client be explicit with respect to the requirement for suppressed information. We expected that completion of this field would be mandatory and that it would be incumbent upon those processing these forms in D2 to ensure they contained all the required information; if not, we would have expected the form to be returned to the client for proper completion.

While many of the forms clearly articulated the relationship between the information being requested and the operating program or activity at CSIS under which the request was being made, many others did not. Again, we would have expected the officials in D2 to ensure this information was complete and if not, to return the forms.

Section G of the form requires that the client indicate what action, if any, is being contemplated based on the information being provided. Although many explanations provided by CSIS were thorough, others were not, and on [redacted] forms the section was left blank or did not provide a response which addressed the question at all. Again, this is contrary to OPS-1-1, specifically Sections 3.4 and 3.6.

Observation no. 7

CSE should consider amending the Request for Release of Suppressed Information form to ensure it is clear to all GoC clients requesting suppressed information, that Section G of the form must be fully completed regardless of whether any action is contemplated based on the suppressed information requested.

CSE policy also refers to legislative authorities such as the *Privacy Act* when dealing with releases of suppressed information contained in end-product reporting. Both the RCMP Phase II and OCT reviews included a discussion of the issue of the release or disclosure of Canadian identities under the *Privacy Act* and what section of that Act would apply. It was noted that the disclosure of identities under paragraph 8(2)(a) (consistent use) of the *Privacy Act* would be appropriate for CSE clients having a foreign intelligence mandate, such as DFAIT. However, for a national security agency such as CSIS, paragraph 8(2)(e) (release to an investigative body) may be the more appropriate section under which to disclose the information to CSIS, as it is receiving the identity information under its section 12 mandate.

[7] Submitted to Minister of National Defence March 30, 2007.
[8] *Ops-1-1, Procedures for the Release of Suppressed Information from SIGINT Reports,* effective date 11 February 2003; last modified 3 January 2006.

CSE has advised us that, in this regard, a review was undertaken by CSE's legal counsel following consultations with colleagues from the Information Law and Privacy section of the Department of Justice and Solicitor-Client Privilege
Solicitor-Client Privilege

Our last point with respect to the release of suppressed information contained in foreign intelligence reports to CSIS relates to the multiple releases of the same identity to different individuals within the agency. OPS-1-1 allows individuals within the client department, in this case CSIS, to share the released suppressed information with other individuals should it be required. The onus is on CSIS to ensure that information is only shared with those having the need to know it. This issue was also raised in the CRO review and noted as Recommendation #4. CSE's response, dated May 7, 2007, indicated that it has accepted this recommendation with modifications. Existing procedures governing the release of identities will be re-examined to ensure consistency of application when receiving multiple requests from a given organization, and CSE will review, process and file each request individually. CSE has advised that it will also address the statistical consistency issue by tabulating only the release of identity information to a given organization, and not to the individual within the organization.

The above-noted matters were also contained in the CRO report of March 2007 and analyzed in detail; therefore we did not repeat the process for the purpose of this report. However, we did meet with a representative of Operational Policy Branch to ask questions related to a sampling of some forms that contained the above-noted issues. It was explained that since the time of this review CSE has implemented new procedures whereby releases that are authorized by newer members of D2 will be reviewed by a more senior member of the unit. In addition, the D2 manager now conducts monthly reviews of a random sample of releases to ensure policy is being complied with. Future OCSEC reviews will monitor this, as appropriate.

VIII. CONCLUSION

This review was conducted by OCSEC pursuant to the Department of Justice legal opinions and its interpretation of the legislation. Overall, we agreed that CSE was within its mandate to conduct the activities it had undertaken, and we also agreed with the relevant advice and guidance provided by Department of Justice counsel to CSE. We disagreed, however, with the application of that advice and believe that some activities undertaken by CSE based on requests for information from CSIS should have been done under mandate (c) (as an agent of CSIS) rather than mandate (a) (collection of foreign intelligence). We discussed this matter with CSE in November 2007, subsequent to requesting their comments as to the factual accuracy of a draft report of this review, as is our practice.

We agreed with CSE on the importance of examining each request on a case-by-case basis. We also found it helpful during discussions that CSE agreed on the importance of

terminology and its consistent use. We believe, however, that the disagreement over application of legal advice reinforces our recommendation that CSE re-examine the application of the Department of Justice advice, and also that additional questions may need to be asked when assessing whether a request from a Government of Canada client, in this case CSIS, falls under mandate (a) or mandate (c). This is consistent with a recommendation made in the OCSEC report on CSE's Support to Law Enforcement: RCMP Phase II in June 2006.

Included in Annex A to this report is a summary of information obtained from the additional RFIs we initially requested in September 2006, but which were not available to us until November 2007. In reviewing the additional RFIs we have drawn the same conclusions as noted above. Although we have not reached a common agreement or interpretation in this matter with CSE at the time of concluding this report, we have in the interim prepared a discussion paper on the subject of CSE's interpretation and use of mandates (a) and (c) that has been forwarded to CSE for review. We anticipate having further discussions on this matter in the near future.

SUMMARY OF RECOMMENDATIONS

Recommendation no. 1:

CSE should consider re-examining CSIS RFIs to ensure all information required under OPS-4-2 is contained in the RFI, including the written assurance that the information was acquired lawfully and in accordance with an investigation or warrant under section 12 of the *CSIS Act*, and linked to a Government of Canada Requirement.

Recommendation no. 2:

In accordance with Recommendation no. 1 above, as well as with Recommendation no. 2 from the RCMP Phase II review,[9] CSE should re-examine its interpretation and application of mandates (a) and (c) and ensure that all decisions and resulting activities are based upon criteria that have been consistently applied and are statutorily defensible.

Recommendation no. 3:

CSE should review the Memorandum of Understanding between CSE and CSIS, dated November 1, 1990, relating to information/intelligence exchange and operational support (section 12 activities), to ensure it reflects current practices and agreements.

[9] *RCMP Phase II*, submitted to Minister of National Defence, June 16, 2006

Annex A

On November 29, 2007, we received the remaining [redacted] RFIs and resulting reporting associated with each RFI, which were outstanding at the time we completed the draft of this report. These RFIs corresponded to the original review period of April 1, 2004 to March 31, 2005.

These RFIs were accompanied by a detailed chart entitled *CSE Activity on Selected Messages from CSIS.* [redacted] of these RFIs appeared straightforward; however, we noted that, in addition to the [redacted] RFIs previously noted in this report, [redacted] contained in [redacted] of the newly-provided batch were used by CSE for contact chaining.

In [redacted] RFIs reviewed, Canadians were the subject of and/or connected to CSIS investigations. CSIS requested "assistance" and each RFI contained CSIS caveats indicating that the "information was loaned in confidence," "was for internal use only," "was the property of CSIS," and that "the information was from sensitive sources."

We requested the "Selector Identification and tracking approval forms to [redacted] contact chain [redacted]" for each of the above-noted [redacted] RFIs, and received them on December 13, 2007.

Resulting reporting from the contact chaining [redacted] included reports in which [redacted] were suppressed but were subsequently requested by and provided to CSIS. We did not ascertain which other CSE clients or allies might have requested and received the suppressed identifiers from the reporting.

This in turn indicates that although initially CSE uses telephone numbers and e-mail addresses [redacted] as metadata for the purpose of [redacted] to collect foreign intelligence, the information can subsequently be put to other uses. That is, the original [redacted] can become part of the content of an end-product report and, although suppressed in accordance with CSE policy, can be requested and released to clients and allies.

The client, in this instance CSIS, is providing information identifying a Canadian, which results from a section 12 investigation, to CSE. [redacted] We believe that this is the same as Solicitor-Client Privilege Solicitor-C as described in the Department of Justice opinion to CSE, dated October 2003, and therefore should be conducted under CSE's (c) mandate.