



Communications Security  
Establishment Canada

Centre de la sécurité  
des télécommunications Canada

TOP SECRET/COMINT/CEO

s.15(1)  
s.21(1)(a)  
s.21(1)(b)

P.O. Box 9703  
Terminal  
Ottawa, Canada  
K1G 3Z4

C.P. 9703  
Terminus  
Ottawa, Canada  
K1G 3Z4

Your file / Votre dossier

Our file / Notre dossier  
CSEC/108-08

NOV 3 2008

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

Dear Minister:

Enclosed is a proposed response to the September 16, 2008 letter that you recently received from the Communications Security Establishment (CSE) Commissioner, Mr. Charles D. Gonthier. The Commissioner's letter refers to your July 3, 2008 correspondence regarding two of his recent reviews, namely, *Collection and Use of Metadata and Support to the Canadian Security Intelligence Service*.

In his letter, the Commissioner delineates two issues of disagreement with the Communications Security Establishment Canada (CSEC) management response to the above-mentioned reviews. The first issue is related to CSEC's current practice, ministerial direction and CSEC policy on accounting for private communications.

. CSEC fully complies with this requirement.

His office has advised us that they will undertake a review of this issue. We will fully support this review and await the Commissioner's recommendations before assessing next steps.

The second issue relates to the determination and application of the relevant authority when CSEC conducts specific activities in relation to information provided by federal law enforcement and national security agencies. Specifically, the Commissioner has questioned whether, in some instances, CSEC applied the appropriate part of its mandate

Canada

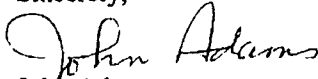
TOP SECRET/COMINT/CEO

~~TOP SECRET/COMINT/CEO~~


This issue remains the subject of continued engagement between CSEC and the Commissioner's office. Recent discussions are contributing to a better understanding of CSEC's current practices and the application of its mandate.

I will be pleased to keep you apprised of our progress in addressing these issues with the CSE Commissioner and his staff.

Sincerely,

  
John Adams  
Chief

I concur:

  
Margaret Bloodworth  
National Security Advisor to the Prime Minister  
and Associate Secretary to the Cabinet

TOP SECRET/COMINT/CEO

Office of the Minister  
of National Defence



Cabinet du ministre  
de la Défense nationale

Ottawa, Canada K1A 0K2

~~TOP SECRET/COMINT/CEO~~

The Honourable Charles D. Gonthier, C.C., Q.C.  
Communications Security Establishment Commissioner  
P.O. Box 1984  
Station "B"  
Ottawa, Ontario  
K1P 5R5

Dear Mr. Gonthier:

Thank you for your letter of 16 September 2008 concerning your recent reviews of the Communications Security Establishment Canada (CSEC) on the *Collection and Use of Metadata* and *Support to the Canadian Security Intelligence Service*. It is clear that two issues remain the subject of continued engagement between your office and CSEC.

I understand that you and Mr. Adams, Chief, CSEC, are planning regular discussions to address issues of mutual interest. I have asked Mr. Adams to include the issues raised in your letter as a point of discussion during your next meeting. Additionally, I have asked Mr. Adams to keep me apprised of your discussions.

Sincerely,

The Honourable Peter G. MacKay, P.C., M.P.  
Minister of National Defence

Canada

Communications Security  
Establishment Commissioner



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

Commissaire du Centre de la  
sécurité des télécommunications

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

s.21(1)(a)

s.21(1)(b)

~~TOP SECRET/COMINT/CEO~~

16 September 2008

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

CSE / CST  
Chief's Office / Bureau du chef  
08-152  
SEP 17 2008  
File / Dossier \_\_\_\_\_

Dear Mr. MacKay:

Thank you for your correspondence dated July 3, 2008 (enclosed for reference), concerning the reports I submitted to you in January 2008 on the Communications Security Establishment Canada's (CSEC) *Collection and Use of Metadata* and on *Support to the Canadian Security Intelligence Service (CSIS)*. Your letter also conveyed CSEC's responses to these reports. The responses contain two points with which I disagree – accounting for private communications, and legal guidance concerning parts (a) and (c) of CSEC's mandate. I am writing to clarify these matters.

With respect to my report on CSEC's *Collection and Use of Metadata* and the first recommendation dealing with accounting for private communications, it is accurate that CSEC's current practice is consistent with ministerial direction and CSEC policy.

I have instructed my staff to examine this issue in greater detail.

With respect to the second recommendation in my report on CSEC's *Collection and Use of Metadata*, and the second recommendation in my report on CSEC's *Support to CSIS*, I want to re-emphasize that I in fact agree with Justice Canada's interpretation and guidance respecting parts (a) and (c) of CSEC's mandate, as was stated in the conclusion of the report on *Support to CSIS* and again in my public annual report which was submitted to you in May, this year. What I question is which part of the mandate should be used as the proper authority in certain cases. This is important because it determines the legal requirement (e.g. ministerial authorization vs. a court warrant) in cases where activities may be "directed at" a Canadian; it also determines which agency

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

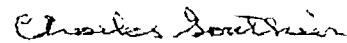
- 2 -

is responsible for the information and how the information collected should be handled. As indicated in CSEC's response, this matter has been the subject of on-going discussions between CSEC and my officials for many months, most recently at a meeting last week. As a result of that meeting, I have asked my staff to pursue this issue.

I am pleased that CSEC agreed with the first and third recommendations in my report on CSEC's *Support to CSIS*.

If you have any questions or comments, I trust you will let me know.

Yours sincerely,



Charles D. Gonthier

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

Att.

JUL 03 2008

~~TOP SECRET/~~  
~~COMINT/~~

Minister  
of National Defence



Ministre ~~Canadian Eyes Only~~  
de la Défense nationale

Ottawa, Canada K1A 0K2

The Honourable Charles D. Gonthier, C.C., Q.C.  
Communications Security Establishment Commissioner  
90 Sparks Street, Suite 730  
P.O. Box 1984, Station "B"  
Ottawa, Ontario  
K1P 5R5

Office of the Communications  
Security Establishment Commissioner  
  
29 2008  
  
Bureau du Commissaire du Centre  
de la sécurité des télécommunications

Dear Mr. Gonthier:

I am writing in response to two reports you sent to my office. The first report, dated 9 January 2008, is entitled *Ministerial Directive, Communications Security Establishment, Collection and Use of Metadata, March 9, 2005*. The second report, dated 16 January 2008, is entitled *Report to the CSE Commissioner on CSE Support to CSIS, Phase I: Mandate (a)*.

I am pleased to note that, during the course of both of these reviews, your office did not observe or report on any unlawful activity on the part of the Communications Security Establishment Canada (CSEC).

CSEC's responses to the recommendations presented in these reports are outlined in the accompanying enclosures. I am pleased that CSEC's actions to address many of the recommendations are concluded and others are in progress.

Sincerely,

Peter G. Mackay  
Minister of National Defence

Enclosures: 2

OCSEC-	BCCST-
Original:	2200-44
Copies:	2200-45
Rec. #:	1271
Date:	1 Aug 08

Canada

~~TOP SECRET/~~  
~~COMINT/~~  
~~Canadian Eyes Only~~

s.15(1)  
s.16(2)(c)  
s.21(1)(a)  
s.21(1)(b)

ANNEX A:  
CSEC Response to Recommendations in the OCSEC Report Entitled  
*Ministerial Directive, Communications Security Establishment,  
Collection and Use of Metadata, March 9, 2005*

Recommendation no. 1: Accounting for Private Communications

"CSE should re-examine and re-assess its current position and practice that requires that only those private communications recognized be accounted for."

Legally, there is no requirement under the SIGINT Ministerial Authorizations, the Ministerial Directive nor the *National Defence Act* to account for private communications.

CSEC's current position and practice of accounting is consistent with what is required by the Minister for accountability purposes.

---

<sup>1</sup> OPS-1-6,

~~TOP SECRET/~~  
~~COMINT/~~  
Canadian Eyes Only

s.15(1)  
s.16(2)(c)  
s.21(1)(a)  
s.21(1)(b)

Recommendation no. 2:

"CSE should re-examine and re-assess the legislative authority used to  
conduct its activities

This matter has been the subject of ongoing discussions with OCSEC regarding parts (a) and (c) of its mandate. OCSEC has forwarded a discussion paper on this topic to CSEC to which a response has been provided. However,

CSEC will continue working with OCSEC to address the different interpretations with a completion date of May 2008.

CSEC is to re-examine and re-assess the management direction regarding these activities. Policy is being revised to clarify approval authorities for these activities and will be completed by July 2008. In addition, practices have been modified to better document the case-by-case rationales regarding the appropriateness of part (a) of the mandate for these activities.



~~TOP SECRET/  
COMINT/  
Canadian Eyes Only~~

s.15(1)  
s.21(1)(a)  
s.21(1)(b)

**ANNEX B:  
CSEC Response to the Recommendations in the OCSEC Report Entitled  
*Report to the CSE Commissioner on CSE Support to CSIS, Phase I: Mandate (a)***

Recommendation no. 1: Complete Requests for Information (RFIs)

"CSE should consider re-examining CSIS RFIs

and in accordance with  
an investigation or warrant under Section 12 of the *CSIS Act*, and linked to a  
Government of Canada Requirement."

and over the course of the two  
and a half years of this review, CSEC has amended its policies and procedures to address  
the issues raised. Those changes have been implemented.

Recommendation no. 2: Application of parts (a) and (c) of mandate

"In accordance with Recommendation no. 1 above, as well as with  
Recommendation no. 2 from the RCMP Phase II review, CSE should re-  
examine its interpretation and application of mandates (a) and (c):

and the interpretation of parts  
(a) and (c) of CSEC's mandate has been the subject of ongoing discussions with OCSEC.  
OCSEC has forwarded a discussion paper on this topic to CSEC to which a response has  
been provided. Further discussions are planned with OCSEC in May to address the  
different interpretations.

Recommendation no. 3: Review and Update CSEC-CSIS MoU

"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."

CSEC agrees to work with CSIS in order to update the MoU, aiming for completion  
by the end of 2008.

08-00791  
Chron



Communications Security  
Establishment Canada

Centre de la sécurité  
des télécommunications Canada

P.O. Box 9703  
Terminus  
Ottawa, Canada  
K1G 3Z4

C.P. 9703  
Terminus  
Ottawa, Canada  
K1G 3Z4

~~TOP SECRET/~~  
~~COMINT/~~  
Canadian Eyes Only

Your File Votre référence

Our file Notre référence  
CSEC/052-08

MAY 26 2008

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

Dear Minister:

I am writing to seek your approval to the attached response to two reports you received from the CSE Commissioner. The first report, dated 9 January 2008, was entitled *Ministerial Directive, Communications Security Establishment, Collection and Use of Metadata, March 9, 2005*. The second report, dated 16 January 2008, was entitled *Report to the CSE Commissioner on CSE Support to CSIS, Phase I: Mandate (a)*.

I am pleased to note that during the course of these reviews, the Commissioner did not observe or report on any unlawful activity on the part of Communications Security Establishment Canada (CSEC) or its staff. There are five recommendations contained in the reports.

As the Commissioner has already noted in his letter to you, there was a delay in completing the reports due to issues at both the Office of the CSE Commissioner (OCSEC) and CSEC. These reports, which are not an easy read, are particularly complex compared to previous reports owing to the subject matter, which added to the time required OCSEC to complete the review and for CSEC to respond to its recommendations. Due to these delays, many of the observations noted during the course of the review have already been addressed.

CSEC's proposed response to both reports' recommendations is attached as annexes to this letter. Below are CSEC's views concerning points raised by the Commissioner in his letters to you but not included or referenced in the recommendations.

Canada

TOP SECRET/  
COMINT/  
Canadian Eyes Only

~~TOP SECRET/  
COMINT/  
Canadian Eyes Only~~

s.15(1)  
s.21(1)(a)  
s.21(1)(b)  
s.23

### Legal Issues

In these reviews, two recommendations from the Commissioner relate to the interpretation of the CSEC mandates. In his view, some activities undertaken by CSEC under part (a) of the mandate (foreign intelligence) should have been undertaken under part (c) of the mandate (provision of technical and operational assistance to law enforcement and security agencies).

The Commissioner indicated in his letter to you that OCSEC has shared a discussion paper on this topic with CSEC. In particular, the discussion paper suggested that

My organization has provided a response to this discussion paper and is awaiting a reply.

In the meantime, CSEC will continue to conduct its activities in a manner consistent with the legal advice provided by the Department of Justice.

### Ministerial Directives

In his letter to you, the Commissioner suggested that a number of Ministerial Directives issued prior to the amendments to the *National Defence Act* which provides CSEC with its legislated mandate, are still in force and should be reviewed to ensure they are consistent with the legislation. As noted in the response to previous reviews, I agree with the Commissioner and have committed to revisiting these three Ministerial Directives by the end of the year.

### Policy Issues

The Commissioner has noted that some CSEC operational policies and procedures, in particular the consistent use of terminology, could benefit from improved inter-policy consistency. CSEC will review and update the terminology used in policies and procedures, in order to improve consistency, by September 2008. Additional management direction will be provided to address any potential gaps identified by the Commissioner.

~~TOP SECRET/  
COMINT/  
Canadian Eyes Only~~

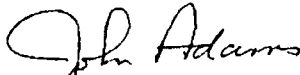
~~TOP SECRET/~~  
~~COMINT/~~  
~~Canadian Eyes Only~~

Information Management

The Commissioner raises the issue of corporate records and information management in his letters to you. CSEC has already advised the Commissioner that it is implementing an electronic corporate records management system and has also improved its management of hard-copy files, especially those related to activities conducted under Ministerial Authorization. The plan is for the CSEC electronic information management system to be fully implemented by October 2008.

As always, CSEC is open to discussion with the Commissioner's office regarding any aspects of OCSEC reviews.

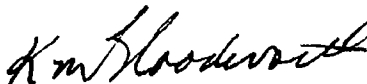
Sincerely,

  
John Adams  
Chief

Enclosures

cc. Robert Fonberg, Deputy Minister, National Defence

I concur:

  
Margaret Bloodworth  
National Security Advisor to the Prime Minister  
and Associate Secretary to Cabinet

~~TOP SECRET/~~  
~~COMINT/~~  
~~Canadian Eyes Only~~



Communications Security  
Establishment Canada

Centre de la sécurité  
des télécommunications Canada

P.O. Box 9703  
Terminal  
Ottawa, Canada  
K1G 3Z4

C.P. 9703  
Terminus  
Ottawa, Canada  
K1G 3Z4

~~TOP SECRET/  
COMINT/  
Canadian Eyes Only~~

s.15(1)  
s.16(2)(c)  
s.21(1)(a)  
s.21(1)(b)

*Your File Votre référence*

*Our file Notre référence*  
CSEC/062-08

**MAY 0 5 2008**

Mrs. Margaret Bloodworth  
National Security Advisor to the Prime Minister and  
Associate Secretary to the Cabinet  
Privy Council Office  
80 Wellington Street  
Ottawa, Ontario  
K1A 0A3

Dear *Margaret*

I am writing to provide you with the revised management response from the Communications Security Establishment Canada (CSEC) on the two reports from the Communications Security Establishment Commissioner that we discussed at our last bilateral, namely *Collection and Use of Metadata*, and *CSE Support to CSIS*. The changes to the documentation are summarized below.

On page two of the my letter to the Minister, I have provided further clarification under the "Legal Issues" section on the reasons for which

On the same page, under the "Policy Issues" section, I have now included a completion date for the policy review.

In Annex A, I have revised the CSEC management response to both OCSEC recommendations. With regard to the first recommendation on accounting for private communications,

With regard to the second recommendation on the revised response now provides a more detailed explanation however, I indicated that I am still prepared to re-examine the management direction on the activities.

**Canada**

~~TOP SECRET/  
COMINT/  
Canadian Eyes Only~~

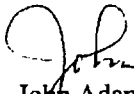
~~TOP SECRET/~~  
~~COMINT/~~  
Canadian Eyes Only

In Annex B, I made two minor changes to CSEC's responses. In response to the first recommendation, I now note that the changes have been implemented. In the response to the second recommendation on the (a) and (c) mandate, I have clarified that further discussions with OCSEC are planned in May to resolve the issue identified.

In the proposed letter of response from the Minister to the Commissioner, I have replaced "delighted" with "pleased" in the second paragraph. Lastly, I have revised the Annexes to this letter in the same manner as identified above, in order to make it consistent with the CSEC management response.

I trust that this meets with your satisfaction. Please do not hesitate to contact me for more information or to discuss further.

Sincerely,

  
John Adams  
Chief

~~TOP SECRET~~  
~~COMINT~~  
Canadian Eyes Only

TOP SECRET/COMINT/CEO

s.15(1)  
s.16(2)(c)  
s.21(1)(a)  
s.21(1)(b)

**Annex A to Excom Briefing Note**  
**Summary of Proposed Management Responses**

**To Recommendations and Findings from the OCSEC Review of the Ministerial Directive, Communications Security Establishment, Collection and Use of Metadata, March 9, 2005**

**Accounting for Private Communications** (*Recommendation no. 1*)

- *Contested.* CSEC has re-examined its current position,

There is no legal requirement under the SIGINT Ministerial Authorizations, the Ministerial Directive nor the *National Defence Act* to  
for private communications.

(*Recommendation no. 2*)

- *Accepted.* CSEC is to re-examine and re-assess the legal authority and management direction regarding activities

*OPI and target date:* SIGINT (legislative authority) and (for policy), October 2008.

**Management and** (*Finding no. 14*)

- *Accepted.* In response to past observations, SIGINT has created a separate team to address issues such as the explicit documentation and monitoring procedures.

*OPI and target date:* SIGINT - on-going with specific operating instructions to be completed by July 2008.

**Information Management** (*Finding no. 15*)

- *Accepted.* CSEC will re-examine and re-review its obligations under Government of Canada legislation and policies regarding Information Management. CSEC is actively improving its record management practices and systems through the deployment of a new electronic records and information management system and through mandatory training for all employees.

~~TOP SECRET/COMINT/CEO~~

*OPI and target date:* CIO review and CERRID deployment and training; All areas of CSEC for IM improvement. July 2008.

s.15(1)  
s.16(2)(c)  
s.21(1)(a)  
s.21(1)(b)

**of Metadata** (*Findings no. 1 and no. 13*)

- *Accepted.*

*OPI and target date:* for management instructions. December 2008.

**Improved Documentation** (*Findings no. 2, no. 8, no. 11 and no. 12*)

- *Accepted.* CSEC will document how access and develop additional documentation to guide staff.

*OPI and target date:* and CIO for documentation. September 2008.

- *Accepted.* CSEC carries out systematic review of its operational policies. The inclusion of definitions will be addressed in future updates of OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities*, expected to be completed by January 2009. Appropriate references in operational policies will be addressed as they are revised. Approval of OPS-1-10, will be completed by September 2008.

*OPI and target date:* April 2008.

- *Accepted.* CSEC will review the policy instruments and management direction related to . As the policy instruments are revised, further guidance will be provided with respect to metadata activities.

*OPI and target date:* for management direction. September 2008.



~~TOP SECRET/COMINT/CEO~~

**Annex B to Excom Briefing Note  
For Excom Discussions Purposes Only  
Details of Proposed CSEC Responses to the Recommendations and Findings from  
the OCSEC Review of the Ministerial Directive, Communications Security  
Establishment, Collection and Use of Metadata, March 9, 2005**

s.15(1)  
s.16(2)(c)  
s.21(1)(a)  
s.21(1)(b)  
s.23

**Section 1: Report Recommendations**

OCSEC Recommendation no. 1

“CSE should re-examine and re-assess its current position and practice that requires that only those private communications recognized be accounted for.”

Proposed Management Response

*Contested.* CSEC has re-examined its current position,

There is no legal requirement under the SIGINT Ministerial Authorizations, the Ministerial Directive nor the *National Defence Act* to communications for private communications.

Further information for Excom

With regard to review of metadata, and the

When dealing with a communication, CSEC maintains that the intelligence requirements. in light of Government foreign

TOP SECRET/COMINT/CEO

OCSEEC Recommendation no. 2

"CSE should re-examine and re-assess the legislative authority used to  
conduct its activities

s.15(1)  
s.16(2)(c)  
s.21(1)(a)  
s.21(1)(b)

Proposed Management Response

*Accepted.* CSEC is to re-examine and re-assess  
the legal authority and management direction regarding  
activities

*OPI and target date:* SIGINT (legislative authority) and  
(for policy), October 2008.

**Section 2: Report Findings**

**A. Positive Findings**

Finding no. 3:

Finding no. 4:

Activities

We understand that CSE is currently reviewing its activities,  
including , and that  
CSE is re-drafting OPS-1-10  
OCSEEC supports this review and will monitor  
developments.

Finding no. 5:

Based on the statements and written documentation provided by CSE,  
as defined in the metadata MD, and as  
they apply to CSE's

Finding no. 6: Activities

Based on our discussions with CSE, our previous knowledge of  
acquisition activities and on the brief examination of the  
activities

TOP SECRET/COMINT/CEO

s.15(1)  
s.16(2)(c)  
s.21(1)(a)  
s.21(1)(b)

to be guided by and support the foreign intelligence priorities of the Government of Canada.

Finding no. 7:

Before CSE it must have reasonable grounds to believe that the will yield foreign intelligence. This belief must be established by most of which is presented to CSE by

Based on our review of CSE approval request forms, we can confirm that CSE to CSE's Government of Canada intelligence requirements (GCRs), and/or the

Finding no. 9: Process for

During the period under review, CSE followed a process for receiving reviewing approving The process formally documented in June 2006, in the form of the draft OPS-1-10 procedure [Further details in Annex C of the OCSEC report].

Finding no. 10: Metadata

From our discussions with CSE staff and our examination of the documentation they provided, we are satisfied that CSE's method of metadata is an adequate means of protecting the identities of Canadians and persons in Canada.

Further, we can report that we have received assurances at this time and will not do so until an adequate means of: can be implemented.

Further information for Excom

The OCSEC report states that CSE did not However, during the period of the review, CSEC did not

**B. Findings Related to Systemic Issues**

CERRID #67374

~~TOP SECRET/COMINT/CEO~~

s.15(1)  
s.16(2)(c)  
s.21(1)(a)  
s.21(1)(b)

Finding no. 14: Documentation of Management Monitoring

We are satisfied that the CSE managers with whom we spoke understood their responsibilities under OPS-1-8, *Management Monitoring and Policy Review Procedures to Ensure Privacy of Canadians*, and that they approached their daily work with the knowledge that their metadata activities must comply with law and policy. Our inquiries did not result, however, in receipt of any written material created by CSE managers that indicate how they explicitly address or document their responsibilities as established in OPS-1-8.

Proposed Management Response

*Accepted.* In response to past observations, SIGINT has created a separate team to address issues such as the explicit documentation and monitoring procedures.

*OPI and target date:* SIGINT Programs Requirements – on-going with specific operating instructions to be completed by July 2008.

Finding no. 15: Corporate Record Keeping and Information Management

We suggest that CSE consult GoC legislation and policies regarding corporate record keeping and information management and ensure that it is in compliance.

Proposed Management Response

*Accepted.* CSEC will re-examine and re-review its obligations under Government of Canada legislation and policies regarding Information Management. CSEC is actively improving its record management practices and systems through the deployment of a new electronic records and information management system and through mandatory training for all employees.

*OPI and target date:* CIO for ; review and CERRID deployment and training; All areas of CSEC for IM improvement. July 2008.

Further Information for Excom

~~TOP SECRET/COMINT/CEO~~

s.15(1)  
s.16(2)(c)  
s.21(1)(a)  
s.21(1)(b)

Transitory records are only required for a limited time to complete a routine action or to prepare a subsequent record. An employee must dispose of or delete transitory records, including e-mail messages and attachments, once they have served their purpose. The sheer volume of transitory records can impede CSE's ability to manage official records.

**C. Findings/Issues Unique to this Review**

Finding no. 1: MD Step (2)

The [redacted] was unable to provide us with documentation

Finding no. 13:

CSE [redacted] metadata activities it conducts pursuant to the authority and rules of the governing MD.

Proposed Management Response (Findings no. 1 and no. 13 are related)  
*Accepted.*

*OPI and target date:* December 2008.

Further Information for Excom

SIGINT [redacted] of metadata activities (i.e., [redacted] as defined in the MD.

CERRID #67374

~~TOP SECRET/COMINT/CEO~~

s.15(1)  
s.16(2)(c)  
s.21(1)(a)  
s.21(1)(b)

Finding no. 2: MD Step (3):

Finding no. 8: Formal Documentation to

CSE has not drafted any formal documentation

There are no written methodology or process materials to guide personnel in ensuring compliance with the authorities of the *NDA* and the metadata MD. However, OPS-1-6 provides general guidance with regard to activities.

Proposed Management Response (Findings no. 2 and no. 8 are related)

*Accepted.* CSEC will document how access and develop additional documentation to guide staff.

OPI and target date: for documentation. September 2008.

Finding no. 11: Definitions of Metadata Activities

OPS-1 does not include definitions of or any references to

~~TOP SECRET/COMINT/CEO~~

s.15(1)  
s.16(2)(c)  
s.21(1)(a)  
s.21(1)(b)

Also, OPS-1 has no reference to the CSE's metadata activities. operational procedures [OPS-1-6 that deal with metadata. In addition, we verified that the most current version of OPS-1, dated December 2006, does not include any reference to OPS-1-10. Given that OPS-1-10 is still in draft, and that it is the only formal guidance available to CSE employees, [of the OCSEC review]

Proposed Management Response

*Accepted.* CSEC carries out systematic review of its operational policies. The inclusion of definitions will be addressed in future updates of OPS-1, expected to be completed by January 2009. Appropriate references in operational policies will be addressed as they are revised. Approval of OPS-1-10 will be completed by September 2008.

*OPI and target date:* January 2009.

Finding no. 12: Operational Procedures for Metadata Activities

The operational procedures metadata activities.

Proposed Management Response:

*Accepted.* CSEC will review the policy instruments and management direction related to As the policy instruments are revised, further guidance will be provided on respecting metadata activities.

*OPI and target date:* for management direction. September 2008.



Communications Security  
Establishment Canada

Centre de la sécurité  
des télécommunications Canada

**TOP SECRET/  
COMINT/  
Canadian Eyes Only**

P.O. Box 9703  
Terminal  
Ottawa, Canada  
K1G 3Z4

C.P. 9703  
Terminus  
Ottawa, Canada  
K1G 3Z4

s.15(1)  
s.21(1)(a)  
s.21(1)(b)

Your File Votre référence

Our file Notre référence

CSEC/00-08

19 September 2012

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

Dear Minister:

I am writing in response to the report from the Office of the CSE Commissioner (OCSEC) dated 9 January 2008, on the review of the *Ministerial Directive, Communications Security Establishment, Collection and Use of Metadata, March 9, 2005*.

I am pleased to note that during the course of the review, OCSEC did not observe or report on any unlawful activity on the part of the Communications Security Establishment Canada (CSEC). The report includes two recommendations and fifteen findings. Seven of the findings reflect positively on CSEC's policies and practices, while the remaining eight require some action from CSEC.

As mentioned by OCSEC, we are engaged, in ongoing discussions with OCSEC to resolve disagreements on part (a) (foreign intelligence) versus part (c) (technical and operational support to law enforcement and security agencies) of our mandate. I will keep you informed of the outcome of those discussions.

Below is a summary of the CSEC management responses to the report.

Accounting for Private Communications

OCSEC has recommended that CSEC re-examine and re-assess its current position and practices as they relate to the collection of data for SIGINT processing. They noted that staff should account for private communications. Since there is no legal requirement under the SIGINT Ministerial Authorizations, the Ministerial Directive nor the *National Defence Act* communications for private communications

**Canada**

**TOP SECRET/  
COMINT/  
Canadian Eyes Only**



~~TOP SECRET/~~  
~~COMINT/~~  
~~Canadian Eyes Only~~

s.15(1)  
s.16(2)(c)  
s.21(1)(a)  
s.21(1)(b)

OCSEC recommends that CSEC re-examine and re-assess the legislative authority used to conduct activities. CSEC is to re-examine and re-assess the legal authority and management direction regarding activities

Specifically, CSEC wishes to state that activities : and are used only for foreign intelligence purposes.

Management and

OCSEC has noted that management understood their responsibility to : that may impact on the privacy of Canadians. However, as noted by OCSEC, CSEC will endeavour to improve the explicit documentation of these activities.

Information Management

In response to an OCSEC finding, CSEC will re-examine and re-review its obligations under Government of Canada legislation and policies regarding Information Management. CSEC is actively improving its record management practices and systems through the deployment of a new electronic records and information management system and through mandatory training for all employees. I wish to note, however, that certain SIGINT activities create and/or utilize information that would be deemed transitory records and may not, therefore, be retained as per the expectations of OCSEC in this report.

of Metadata

OCSEC notes the need to explicitly :

Improved Documentation

OCSEC has noted a number of areas where CSEC can improve documentation such as operational policies and detailed guidance to staff. In response, CSEC will develop additional documentation related to:

- 1 ;
- guidance to staff;

~~TOP SECRET~~  
~~COMINT~~  
~~Canadian Eyes Only~~

**TOP SECRET/  
COMINT/  
Canadian Eyes Only**

- policies related to protecting the privacy of Canadians and ensuring legal compliance; and
- procedures related to

s.15(1)

s.16(2)(c)

As always, CSEC is open to discussions with the Commissioner's office regarding the points they have raised.

I have also enclosed, for your consideration, a draft letter of response to the Commissioner.

Sincerely,

*(Leave 5 blank lines for signature)*

John Adams  
Chief

Enclosure

cc: Robert Fonberg, Deputy Minister, National Defence  
Margaret Bloodworth, National Security Advisor to the Prime Minister

**TOP SECRET  
COMINT  
Canadian Eyes Only**

TOP SECRET/COMINT/CEO

s.21(1)(a)

s.21(1)(b)

### ExCom Briefing Note

## OCSEC Review of the Ministerial Directive, Communications Security Establishment, Collection and Use of Metadata, March 9, 2005

### Issue for Decision

To agree on CSEC's response to the recommendations and the findings from the Office of the CSE Commissioner's (OCSEC) review on the collection and use of metadata.

### Background

The purpose of this OCSEC review was to assess CSEC's compliance with the Ministerial Directive covering the collection and use of metadata, and with the laws of Canada in such collection. The review was also conducted to ascertain whether CSEC was complying with its own operational policies, procedures, and practices.

During the course of the review, OCSEC did not observe or report on any unlawful activity on the part of CSEC. However, OCSEC did note that this is a preliminary report and they believe that the use of metadata will require further detailed examination.

The final report to the Minister contains some factual references and analysis that CSEC contests and believes could lead to incorrect conclusions.

OCSEC has recently changed their approach to reporting on the outcomes of their review activities. Historically, OCSEC reports would include a number of findings linked to specific recommendations. This is the first report to take a different approach. It contains only two recommendations. Additionally, it includes 15 *findings* that are not linked to specific recommendations.

We have categorized the findings into three groups: 1) *positive for CSEC* and requiring no further action; 2) *ongoing systemic* issues that CSEC is addressing; and 3) issues *unique* to this particular review.

### Recommendations

It is recommended that the Chief's letter to the Minister include, in addition to the normal management response to OCSEC's recommendations, a summary of the points and analysis with OCSEC's statements, specifically the mandate "a" versus "c" issue.

That the proposed CSEC responses to OCSEC recommendations and findings be accepted.

Communications Security  
Establishment Commissioner



Commissaire du Centre de la  
sécurité des télécommunications

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

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

<b>CSE / CST</b>
Chief's Office / Bureau du chef
JAN 10 2008
File / Dossier <u>8-110067</u>

~~TOP SECRET/COMINT/CEO~~  
(with attachment)

09 January 2008

The Honourable Peter G. 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 advise you of the results of a review by my office of CSE's metadata activities carried out under a ministerial directive (MD) dated March 9, 2005. The review focused on those metadata activities undertaken by CSE in support of its foreign intelligence mandate articulated in Part V.1, paragraph 273.64(1)(a) of the *National Defence Act (NDA)*, and referred thereafter as mandate (a), for the period April 1, 2005 to March 31, 2006.

The objective of the review was to assess CSE's compliance with the ministerial directive and with the laws of Canada, including the *NDA*, and also the *Privacy Act*, which governs the collection, use and disclosure of personal information. My office also set out to assess whether these metadata activities conformed with CSE's operational policies, procedures and practices. The review was undertaken under my general authority articulated in paragraph 273.63(2)(a) of the *NDA*.

By way of background, metadata can be broadly characterized as *data about data*. In the context of the ministerial directive under review, however, metadata is

s.15(1)

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

s.15(1)  
s.21(1)(a)  
s.21(1)(b)

-2-

CSE acquires, analyzes, retains and uses metadata

This was my office's first examination of CSE's collection and use of metadata as governed by ministerial directive. Due to the complexity and breadth of the activities it authorizes, this is a preliminary report. As is my practice, I provided officials at CSE an opportunity to review and comment on this report, prior to finalizing and forwarding it to you. There was much discussion between CSE and my office regarding specific issues, several of which I describe briefly below. I believe that some of these will require further examination.

Legal issues

My office questions whether CSE appropriately undertook certain activities as principal under its (a) mandate rather than under its (c) mandate.

Discussions of this matter between my office and CSE will be pursued outside the framework of this report because it affects other areas currently under review by my officials.

My office has been advised that CSE is re-examining its metadata activities, as well as its policy entitled OPS-1-10, *Procedures for Metadata Analysis*. I support this review, and depending on its outcome, my office may conduct a more in-depth examination of these activities.

-3-

Lastly, since my office has now observed that some of CSE's :

s.15(1)  
s.21(1)(a)  
s.21(1)(b)

metadata activities, I believe that CSE must re-examine and re-assess its current position and practice that require that only those private communications recognized be accounted for. I suggest that those persons involved in the metadata activity as defined in the MD and as it applies to should also be responsible for accounting for all private communications they observe and handle.

Policy issues

CSE policy and procedures need to be amended, finalized and possibly augmented in order to better guide and support metadata activities. In particular, CSE has indicated that it is reviewing its use of terminology to ensure consistency and to avoid confusion.

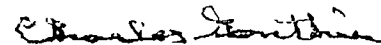
Corporate Records Management

I am of the opinion that CSE ought to be in a position to account for its metadata activities, up to and including any disclosures of Canadian identifiers made to clients and partners under the *Privacy Act*. Any future metadata reviews conducted by my office will pay particular attention to the documentation CSE is able to provide in order to facilitate an accurate assessment of its compliance with the authorities established in the *NDA*, the metadata MD, and related policies and procedures.

My report, attached, contains 15 findings and two recommendations dealing with the matters I have summarized for you in this letter.

I will continue to monitor the issues raised in the report. If you have any questions or comments, I will be pleased to discuss them with you at your convenience.

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/CEO~~

**OCSEC Review of the  
*Ministerial Directive, Communications Security Establishment,  
Collection and Use of Metadata, March 9, 2005***

**January 2008**

s.15(1)  
s.21(1)(a)  
s.21(1)(b)

---

## I. AUTHORITIES

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

On March 9, 2005, the Minister of National Defence signed a ministerial directive (MD)<sup>1</sup> to the Chief CSE describing how the Minister expects CSE to collect, use metadata<sup>2</sup> acquired in support of its foreign intelligence acquisition programs (mandate (a)), as well as for its computer systems and networks protection programs (mandate (b)) as they relate to malicious cyber activity. Included in the MD is a statement that activities undertaken pursuant to the MD are subject to review by the CSE Commissioner.<sup>3</sup> This is OCSEC's first such review. A copy of the MD can be found at Annex A.

CSE acquires, analyzes, retains and uses metadata

## III. OBJECTIVES

For this first metadata review, our objective was to identify and understand the nature of CSE's metadata activities and to assess their compliance with the ministerial directive and with the laws of Canada, including the *NDA*, and also the *Privacy Act*, which governs the collection, use and disclosure of personal information. We also set out to assess whether these activities conformed with CSE's own operational policies, procedures and practices.

## IV. SCOPE

In scoping out this review, OCSEC chose to focus on only those metadata activities undertaken by CSE in support of its foreign intelligence mandate (mandate (a)) and which did not require a ministerial authorization (MA), for the period April 1, 2005 to March 31, 2006. However, subsequent to discussions with CSE respecting the draft report's observations and findings, OCSEC recognized that certain metadata activities are

---

<sup>1</sup> Ministerial Directive [MD], *Communications Security Establishment, Collection and Use of Metadata*, dated March 9, 2005. See copy at Annex A.

<sup>2</sup> "Metadata" is defined below in Section IX - Background.

<sup>3</sup> Ministerial directive, paragraph 10.



not limited to what is authorized under the metadata MD and must also be considered in the context of MAs. Therefore, this was taken into consideration, as appropriate, in revising the report.

s.15(1)  
s.21(1)(a)  
s.21(1)(b)

## V. LINES OF ENQUIRY

This review included the following lines of enquiry:

- (a) the legal authorities and guidance governing metadata activities;
- (b) how metadata activities are determined, scoped and planned;
- (c) how they are conducted and managed;
- (d) how acquired metadata is retained, used and
- (e) how acquired Canadian identities are retained, used, and protected.

## VI. CRITERIA

We assessed CSE compliance against the criteria (expectations) that CSE would:

- 1) conduct its metadata activities based on :
  - a) whether the activity was within its legislative mandate and complied with the ministerial directive;
  - b) legal analysis and guidance on, for example, specific metadata activities described in the MD, metadata collection metadata versus collection and interception;
  - c) assessment(s) of whether the activity would produce metadata of foreign intelligence value; and
  - d) foreign intelligence priorities of the Government of Canada (specifically, those provided to CSE by its GoC clients);
- 2) have approved plans, a methodology and processes that guided its activities and were consistent with its legislative mandate and the ministerial directive;
- 3) have processes to identify, and measures to protect, metadata that identified Canadians;
- 4) have formal procedures that guided metadata activities, including the acquisition, retention, use and reporting of metadata, consistent with the *NDA* and the MD;
- 5) have the means to record, track, and account for of metadata that identified Canadians; and
- 6) have the means to determine if its metadata activities had been conducted as per its mandate, the ministerial directive and approved procedures.

s.15(1)  
s.16(2)(c)  
s.21(1)(a)  
s.21(1)(b)

## VII. LIMITATIONS OF THE REVIEW

Soon after commencing our review, it became evident that most of CSE's  
involved the collection, retention and use of metadata.  
As a result, we limited the focus of this first metadata review to generally identifying  
CSE's mandate (a) metadata activities, understanding CSE's own legal framework for  
conducting these activities, determining when and if metadata  
and observing, where possible, some metadata  
acquisition.

The majority of our observations and findings are based on our review of  
metadata activities.

we focussed our attention on CSE's  
We did not examine similar activities undertaken in CSE

metadata activity This review is  
preliminary and OCSEC will determine at a later date whether an in-depth review of  
is necessary as we have been advised by CSE that it is currently  
examining this activity.

## VIII. METHODOLOGY

A variety of documentation was examined, beginning with the 2005 ministerial directive,  
followed by policies and procedures, and then legal guidance issued to CSE by the  
Department of Justice (DoJ). We consulted CSE managers and personnel responsible for  
metadata activities, and received several briefings during the review. CSE provided both  
verbal and written answers to our questions.

We obtained a briefing and an on-site demonstration of

While this activity area is common  
the activities we observed fell within CSE's  
and were identified as

We also examined a selection  
of requests for

We paid particular attention to those CSE policies  
and practices instituted to protect the privacy of Canadians in the acquisition, use  
of metadata.

---

## IX. BACKGROUND

### What is Metadata?

There are many different definitions in the public domain of what constitutes metadata. According to CSE,

Basically, metadata is *data about data*. In the context of the ministerial directive under review, however,

In our briefings, CSE identified the following examples of metadata it collects:

### What is a Metadata Activity?

The ministerial directive of March 9, 2005 identifies activities: which are defined below. The MD also sets out general guidelines for CSE's collection, use and of metadata.

---

<sup>5</sup> The ministerial directive of March 9, 2005 defines metadata as

s.15(1)  
s.16(2)(c)  
s.21(1)(a)  
s.21(1)(b)

---

We learned that

The MD defines as:

---

<sup>6</sup> OPS-1-10, *Procedures for Metadata Analysis*

s.15(1)  
s.16(2)(c)  
s.21(1)(a)  
s.21(1)(b)  
s.23

We learned that CSE

CSE's GoC clients, such as the Canadian Security Intelligence Service (CSIS) or the Royal Canadian Mounted Police (RCMP),

supported by a DoJ legal opinion.<sup>8</sup>

This activity is

During the period April 1, 2005 to March 31, 2006, CSE received requests from  
of its GoC clients: We were provided  
documentation For the most part,

information on this subject. Annex C contains more detailed

For this reason, these metadata activities as defined in the  
MD do not require ministerial authorization.<sup>12</sup>

<sup>7</sup> See draft procedures known as OPS-1-10, *Procedures for Metadata Analysis*.

<sup>1</sup> is also found in a statement made in his correspondence to the  
Minister of National Defence when the former Chief, CSE indicated that "...

s.15(1)  
s.16(2)(c)  
s.21(1)(a)  
s.21(1)(b)  
s.23

---

### How Metadata is Obtained

The accessing and processing of data, including metadata, is at the very root of CSE's signals intelligence (SIGINT) acquisition mandate. In order for us to understand metadata acquisition, the sequence of SIGINT acquisition was described to us during a meeting with CSE officials on February 26, 2007 using the following terminology: acquire, collect, and intercept. These terms are not defined in the *National Defence Act*, the ministerial directive, or in CSE's operational policies and procedures. However, based on the information provided to us by CSE, we understand their meaning is as follows.

**Acquire/Collect:** *Used synonymously to indicate interception.*<sup>13</sup>

During our review, we learned that through its \_\_\_\_\_ as described above, CSE does in fact acquire both the metadata \_\_\_\_\_

Essentially, the SIGINT acquisition process begins when CSE \_\_\_\_\_

At the same time, \_\_\_\_\_

---

<sup>13</sup>The MD does not distinguish between these various terms and, in his general and broad direction to CSE, the Minister has adopted the terms *acquired* and *acquisition*.

performed under ministerial authorization. See Annex D for more details.

is

s.15(1)  
s.16(2)(c)  
s.21(1)(a)  
s.21(1)(b)

We learned that CSE's

However, according to CSE,

CSE's

knowledge is based on

as described above.

**Access to Metadata**

As described above, CSE

collects metadata

<sup>16</sup> CSE also has

<sup>17</sup> CSE comments on "OCSEC Dratt Review Report of the Ministerial Directive on the Collection and Use of Metadata" at page 3, sent by e-mail to OCSEC Director of Operations from CSE on September 25, 2007.

<sup>18</sup> *Ibid.*

## X. FINDINGS

The findings documented below were derived from:

- documentation received from CSE, including PowerPoint presentations, and ;
  - briefings and discussions held with CSE personnel at various levels;
  - the demonstration of
- and
- answers received from CSE to verbal and written questions.

To reiterate, the metadata activities identified in the MD and known as as it applies to collection, and were the areas of focus for this initial metadata review. The criteria used to assess the activities were that CSE would:

- 1) conduct its metadata activities based on :
  - a) whether the activity was within its legislative mandate and complied with the ministerial directive;
  - b) legal analysis and guidance on, for example, specific metadata activities described in the MD, metadata collection metadata versus collection and interception;
  - c) assessment(s) of whether the activity would produce metadata of foreign intelligence value; and
  - d) foreign intelligence priorities of the Government of Canada (specifically, those provided to CSE by its GoC clients);
- 2) have approved plans, a methodology and processes that guided its activities and were consistent with its legislative mandate and the ministerial directive;
- 3) have processes to identify, and measures to protect, metadata that identified Canadians;
- 4) have formal procedures that guided metadata activities, including the acquisition, retention, use and reporting of metadata, consistent with the *NDA* and the MD;
- 5) have the means to record, track, and account for metadata that identified Canadians; and
- 6) have the means to determine if its metadata activities had been conducted as per its mandate, the ministerial directive and approved procedures.



s.15(1)  
s.16(2)(c)  
s.21(1)(a)  
s.21(1)(b)  
s.23

Criterion 1 a):

*CSE conducted its metadata activities based on:*

*(a) whether the activity was within its legislative mandate and complied with the ministerial directive.*

The National Defence Act

<sup>19</sup> CSE derives its legislative authority to collect and use metadata for foreign intelligence purposes from its mandate found at paragraph 273.64(1)(a) of the *National Defence Act* (mandate (a)):

**273.64(1)** The mandate of the Communications Security Establishment is

- (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;

Metadata is one type of information acquired from the global information infrastructure during the SIGINT collection process, as envisaged by this authority.

The Ministerial Directive

The MD defines metadata, guides its collection and use for  
and directs CSE, among other things,  
metadata

In his direction to CSE, the Minister has also outlined four (4) steps CSE must take during the conduct of its metadata activities in order to protect the privacy of Canadians.<sup>20</sup>

**Step (1)** states that metadata

(We noted that the phrase "CSE reports" was not further described in the MD.)

**Step (2)** states that CSE's \_\_\_\_\_ must be satisfied that certain criteria, "outlined in CSE Operational Procedures," are met before

<sup>20</sup> Ministerial directive, page 2, paragraph 7.

**Step (3)**

s.15(1)  
s.16(2)(c)  
s.21(1)(a)  
s.21(1)(b)

And finally, **Step (4)**

For our review of CSE's compliance with steps (1) and (2), we asked CSE to provide us with any reports completed during the review period that related directly to

We could anticipate that some of these reports would include metadata that had been : as described in step (1) above, and that the might have received requests for (as per step (2)). We asked for an accounting of all requests made during our review period, including the number of requests, the type of metadata requested, and to whom it was released (see Annex C).

***Finding no. 1: MD Step (2)***

The was unable to provide us with documentation that

Details:

From our reading of Step (2) as set out in the MD, we expected that CSE would have metadata back to the following:

- the request ;
- the resulting and,
- the resulting CSE report, if any,

However, we found that this is not the case.

We were advised that while the

<sup>21</sup> Source: E-mail dated April 3, 2007, from Manager, staff and forwarded from

s.15(1)  
s.16(2)(c)  
s.21(1)(a)  
s.21(1)(b)

Further, we learned that when a requests

As a result, it is not possible to draw a line between a metadata activity

**Observation no. 1:**

CSE should be able to draw a clear line between a foreign intelligence priority, a metadata activity

CSE should be able to provide all of the following information: and the *Privacy Act* authority

OCSEC may, as part of a future metadata review, assess the extent to which and examine any such cases for compliance with paragraph 7, Step (2) of the MD.

***Finding no. 2: MD Step (3): Limits on Access at CSE***

CSE provided us with verbal assurance that access to CSE's metadata has been limited to certain personnel. Our follow-up inquiries did not reveal any further information on or how CSE assures itself and the Minister that it has complied with this direction.

***Finding no. 3: MD Step (4): Limits on Sharing with Allies***

We examined sample documents provided by CSE that showed that metadata

1

April 3, 2007 to OCSEC Senior Analyst, with the subject: "FW: Classified Report: OCSEC Review: Metadata MD - Some last minute follow-up issues."

<sup>22</sup> *Ibid.*

<sup>23</sup> Reference: OCSEC's Phase 2 review of CSE support to the RCMP, sent to the Minister of National Defence on 16 June 2006 and entitled: *Report to the CSE Commissioner on CSE's Support to Law Enforcement: Royal Canadian Mounted Police (RCMP), Phase II: CSE Mandate (a)*. See page 16 of the report, which begins a discussion of CSE's handling of personal information under its (a) mandate.

s.15(1)  
s.16(2)(c)  
s.21(1)(a)  
s.21(1)(b)  
s.23

Details:

As part of our review, CSE provided us with two one-page printouts of sample |  
metadata. For copies, see Annex E. These printouts represented metadata that had  
been acquired during our review period. As already  
stated, metadata is acquired

The metadata, which related to had been

i. The metadata had not been but CSE advised us  
that it did not

We understand, however, that CSE is  
under the project name, . For more details,  
please see Criterion 3, page 24.

Criterion 1 b)

*CSE conducted its metadata activities based on:*

*(b) legal analysis and guidance on, for example, specific metadata activities  
described in the MD, metadata collection . metadata  
versus collection and interception.*

Our findings fall under three headings:

We reviewed

s.15(1)  
s.16(2)(c)  
s.21(1)(a)  
s.21(1)(b)  
s.23

**Observation no. 2:**

So while metadata is indeed "data about data",

An in-depth examination by OCSEC of the

of the positions they established with some of the metadata activities undertaken by CSE. We did, however, compare some

We understand that, because of the very nature of the work, some of CSE's

examine these activities during a demonstration However, we were able to briefly  
we received at in November 2006. The demonstration was instructive.

(a)

---

<sup>24</sup> The . uses the phrase

s.15(1)  
s.16(2)(c)  
s.21(1)(a)  
s.21(1)(b)  
s.23

We were able to observe \_\_\_\_\_ activity during our visit to \_\_\_\_\_. These activities are undertaken pursuant to both the Metadata ministerial directive and the \_\_\_\_\_ ministerial authorization, as it is possible that a private communication could be intercepted.

Based on the demonstrations we were given, \_\_\_\_\_ In response to a question, \_\_\_\_\_ indicated that, as a matter of course,

\_\_\_\_\_, CSE's operational procedures indicate that these activities may include \_\_\_\_\_ and the acquisition of private communications.

This raised questions, particularly when considered along with another statement that appears in the \_\_\_\_\_ at paragraph 2 on page 11:

s.15(1)  
s.16(2)(c)  
s.21(1)(a)  
s.21(1)(b)  
s.23

**Recommendation no. 1:**

**CSE should re-examine and re-assess its current position and practice that requires that only those private communications recognized by be accounted for.**

Details:

Based on the \_\_\_\_\_, that states that

\_\_\_\_\_ CSE has advised, consistent with the conditions in the \_\_\_\_\_ MA,

Furthermore, CSE indicated that

However, OCSEC maintains that

An in-depth examination of CSE's \_\_\_\_\_ to ensure conformity to OPS-1-6 and other relevant policies was beyond the scope of this review exercise. OCSEC may conduct a detailed review of \_\_\_\_\_ in future.

---

25

*supra* note 10 at page 10.

s.15(1)  
s.16(2)(c)  
s.21(1)(a)  
s.21(1)(b)  
s.23

(b)

An in-depth examination of CSE's  
this preliminary review.

activities was beyond the scope of

**Finding no. 4:**

We understand that CSE is currently reviewing its

activities, including  
and that CSE is re-drafting  
is to be done".<sup>27</sup>

OPS-1-10 "to ensure that there is clarity in how  
OCSEC supports this review and will monitor developments.

Details:

Depending on the outcome of CSE's re-examination of its  
OCSEC may conduct a more detailed review of

activities,

to answer, among others, the following questions:

- Could
- Is CSE's (a) mandate the appropriate authority to conduct  
in the context of a criminal or national security investigation  
of a Canadian in Canada?
- Could a  
clients? | to CSE's

<sup>26</sup> Metadata Operations Under the National Defence Act, *supra* note 10 at page 6.

was not part of this review.

This activity

<sup>27</sup> *Supra*, note 17 at page 5.



s.15(1)  
s.16(2)(c)  
s.21(1)(a)  
s.21(1)(b)

Criteria 1 c) and d):

*CSE conducted its metadata activities based on:*

- c) assessment(s) of whether the activity would produce metadata of foreign intelligence value; and*
- d) foreign intelligence priorities of the Government of Canada (specifically, those provided to CSE by its GoC clients).*

We learned from CSE that its \_\_\_\_\_ and its \_\_\_\_\_ activities, were either conceived on the basis of, and/or focussed on, the foreign intelligence priorities established annually by a committee of Ministers. In direct support of these priorities, we understand that CSE continues to update its \_\_\_\_\_<sup>28</sup> which is generated in-house and which guide CSE's foreign intelligence metadata activities. CSE advised that the \_\_\_\_\_ is also endorsed by senior Government of Canada clients and stakeholders external to CSE.

***Finding no. 5:***

Based on the statements and written documentation provided by CSE, \_\_\_\_\_ activities as defined in the metadata MD, and as they apply to CSE's \_\_\_\_\_ program, appear to be supported by an assessment of available information and a formal statement of why their planned efforts can be expected to result in access to foreign intelligence of value to, and in support of, foreign intelligence priorities.

***Finding no. 6:***

Based on our discussions with CSE, our previous knowledge of \_\_\_\_\_ acquisition activities, and on the brief examination of the \_\_\_\_\_ activities as demonstrated by \_\_\_\_\_ CSE's activities respecting metadata acquired from \_\_\_\_\_ appear to be guided by \_\_\_\_\_ and support the foreign intelligence priorities of the Government of Canada.

Details:

As we noted on page 9 of this report, CSE

During this initial stage, CSE is not specifically targeting foreign entities *per se* - an entity being as defined at section 273.61 of the *NDA*:

---

<sup>28</sup> The \_\_\_\_\_ is described in detail in the classified report entitled: *Report to the CSE Commissioner on an External Review of CSE Activities Conducted Under Ministerial Authorization*, dated 28 February 2005, which was provided to the Minister of National Defence on the same date.

s.15(1)  
s.16(2)(c)  
s.21(1)(a)  
s.21(1)(b)

A person, group, trust, partnership or fund or an unincorporated association or organization and includes a state or a political subdivision or agency of a state.

CSE is, in fact, In the case  
of :

advised that this We were

During a previous review of CSE's activities,<sup>29</sup> OCSEC was provided with  
copies of what are called .

On this occasion, for our metadata review, we did not ask CSE to provide copies of any  
such since this area of activity would have been covered by other OCSEC  
reviews of CSE's activities conducted under ministerial authorization.

We can confirm, however, that some of the assessment information in

***Finding no. 7:***

Before CSE commences a it must have  
reasonable grounds to believe that the  
This belief must be established by

For further details, please refer to Annex C.

<sup>29</sup> See the classified report entitled *A Report to the CSE Commissioner on an External Review of CSE Activities Conducted under Ministerial Authorization*, dated 28 February, 2005.

s.15(1)  
s.16(2)(c)  
s.21(1)(a)  
s.21(1)(b)

Based on our review of  
that CSE

we can confirm

Criterion 2:

*CSE had approved plans, a methodology and processes that guided its activities and were consistent with its legislative mandate and the ministerial directive.*

Our discussions indicated that CSE undertakes within the context of its operational priorities established at the beginning of each year. These priorities are driven by GoC intelligence priorities and by complementary requirements of clients and partners. We did not receive any documentation during this review, however, that indicates that CSE drafts specific annual objectives for these metadata activities as part of a formal annual planning document. CSE indicated that this is the case because these activities

are linked to the GoC intelligence priorities.

***Finding no. 8:***

CSE has not drafted any formal documentation to instruct activities undertaken in response to . There are no written methodology or process materials to guide personnel in ensuring compliance with the authorities of the *NDA* and the metadata MD. However, OPS-1-6 provides general guidance with regard to activities.

Details:

activities are undertaken in response to written .

To our knowledge, however, there is no formal written documentation available for CSE personnel that supports these requests and which articulates methodologies or processes. We believe this type of information should be available to personnel, possibly as formal standard operating procedures, so that they can assure themselves that the activities they

<sup>30</sup> CSE

<sup>31</sup> *Supra* note 17 at page 5.

s.15(1)  
s.16(2)(c)  
s.21(1)(a)  
s.21(1)(b)

undertake, and that undoubtedly vary from time to time, comply with the law, ministerial directives and policy.

***Finding no. 9:***

During the period under review, CSE followed a process for receiving, reviewing and approving. The process was formally documented in June 2006, in the form of the draft OPS-1-10 procedures. A more detailed discussion of our findings regarding OPS-1-10 can be found in Annex C.

Details:

We were provided with documentation that related to requests to In every instance, the documentation consisted of a were accompanied by a CSE addendum that:

- assessed whether could be expected to produce foreign intelligence;
- identified the foreign intelligence priority and objectives; and
- identified what measures CSE would take to protect privacy.

From this documentation, we can confirm that these requests were subject to a process of internal review and managerial approval. Not all documentation, however, was provided or available for our review. Please see section XI regarding corporate records keeping at page 30 for further discussion on this matter.

This preliminary examination did raise one other fundamental issue that has been identified in previous reviews and that will require further study.<sup>32</sup> CSE undertook these using their mandate (a) authority (i.e. paragraph 273.64(1)(a) of the NDA).

<sup>32</sup> See in particular OCSEC's Phase 2 review of CSE support to the RCMP, sent to the Minister of National Defence on 16 June 2006 and entitled: *Report to the CSE Commissioner on CSE's Support to Law Enforcement: Royal Canadian Mounted Police (RCMP), Phase II: CSE Mandate (a)*.

s.15(1)  
s.16(2)(c)  
s.21(1)(a)  
s.21(1)(b)

CSE explained to us that :

Our examination of the

However, we continue to question whether CSE's authority to

should be authorized under paragraph 273.64(1)(a) or paragraph 273.64(1)(c) of the *NDA* (also known as mandate (c)).

In each of these instances, CSE

During discussions on the draft report in November 2007, CSE indicated 1

Discussion of this matter will be pursued with CSE outside the framework of this report because it affects other areas currently under review by OCSEC.

<sup>33</sup> CSE "Comments on OCSEC 2<sup>nd</sup> Draft Review Report of the Ministerial Directive on the Collection and Use of Metadata" at page 6, sent by e-mail to OCSEC Director of Operations from CSE on December 6, 2007.

<sup>34</sup> *Ibid.*

s.15(1)  
s.16(2)(c)  
s.21(1)(a)  
s.21(1)(b)

---

**Recommendation no. 2:**

**CSE should re-examine and reassess the legislative authority used to conduct its activities**

**Criterion 3:**

*CSE had processes to identify, and measures to protect, metadata that identified Canadians.*

***Finding no. 10:***

From our discussions with CSE staff and our examination of the documentation they provided, we are satisfied that CSE's method is an adequate means of protecting the identities of Canadians and persons in Canada.

Further, we can report that we have received assurances that CSE

**Details:**

As described above, CSE is able to

however, is used as the starting point for both the implementation and assessment of privacy measures.

s.15(1)  
s.16(2)(c)  
s.21(1)(a)  
s.21(1)(b)

**Observation no. 3:**

The \_\_\_\_\_ as described above will safeguard the privacy of  
Canadians and persons in Canada

Criterion 4:

*CSE had formal procedures that guided metadata activities, including acquisition, retention, use and reporting of metadata consistent with the NDA and MD authorities.*

According to CSE, the MD is the principal document guiding CSE's acquisition and use of metadata. For our review period from April 2005 to March 2006, this was complemented by OPS-3-5, entitled \_\_\_\_\_

These procedures were available for those persons cleared for and involved in \_\_\_\_\_ activities, including those described in the metadata MD.

Other formal written guidance for personnel involved in metadata activities was introduced incrementally during the months that followed. By August 2005, OPS-1, CSE's principal policy on protecting privacy and ensuring lawfulness, was re-issued with revisions that included a definition of metadata as well as definitions for the principal activities described in the March 2005 metadata MD. By December 2005, and to coincide with applications for new SIGINT ministerial authorizations, two more procedures provided metadata guidance:

- OPS-1-6, \_\_\_\_\_ and,
- \_\_\_\_\_

Subsequent to the period of review, in June 2006, CSE released draft procedures, OPS-1-10, entitled: *Procedures for Metadata Analysis* \_\_\_\_\_ It was included as part of the review since it represented the sole guidance for \_\_\_\_\_ activity.

As part of our review, we examined these policies and procedures in more detail to determine how they guided metadata activities.

s.15(1)  
s.16(2)(c)  
s.21(1)(a)  
s.21(1)(b)

OPS-1: Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities, dated 31 August 2005

**Finding no 11:**

OPS-1 does not include definitions of or any references to CSE's metadata activities. Also, OPS-1 has no reference to the operational procedures (noted above) that deal with metadata. In addition, we verified that the most current version of OPS-1, dated December 2006, does not include any reference to OPS-1-10.<sup>36</sup> Given that OPS-1-10 is still in draft, and that it is the only formal guidance available to CSE employees, the (For discussion of OPS-1-10, please see Annex C).

Details:

OPS-1 includes the definition of metadata (as it appears in the MD), outlines metadata in relation to CSE's (b) mandate and its use for the protection of GoC computer systems and networks, and refers to metadata again in relation to both its mandate (b) and its mandate (a) SIGINT reporting and release authorities.

In the section of OPS-1 titled *Retention* metadata is dealt with briefly at para. 6.15, *Metadata Collected Under Mandate A*. The reader is referred to the metadata MD which, according to OPS-1, "outlines rules regarding collection, use and of metadata collected by CSE."

In relation to metadata retention, paragraph 6.15 directs readers to OPS-1-11, entitled *Retention Schedules for SIGINT Traffic*, dated 11 March 2004. According to OPS-1-11, metadata collected by CSE .

<sup>37</sup> In written answers to questions received from CSE dated December 6, 2006, we were advised that currently,

CSE plans to

Other Operational Procedures

**Finding no. 12:**

The operational procedures do not provide adequate guidance respecting metadata activities.

<sup>36</sup> This statement remains true even upon examining the current December 2006 version of OPS-1.

<sup>37</sup> OPS-1-11, para. 2.4 *Traffic Acquired under Section 273.64(1)(a) of the NDA*.



s.15(1)  
s.16(2)(c)  
s.21(1)(a)  
s.21(1)(b)

Details:

As outlined above, the subject of metadata has been incorporated into the following operational procedures:

- a) OPS-1-6, *Procedures*
- b) OPS-3-5, *Procedures; and,*
- c) OPS-3-7, *Procedures.*

These three deal specifically with foreign intelligence collection methods and programs, but were pertinent to our review since metadata activities form part of these methods and programs.<sup>38</sup> From our examination, we noted that each procedure includes definitions and standard (but limited) guidance on metadata activities identified as collection, use and retention.

Metadata Collection

The guidance given for metadata *collection* is noteworthy for it is identical in each procedure and consists of one sentence:

*Metadata may be collected for*

No other guidance for this activity is present in these documents. Further, in the absence of any definition, we had to question what "collected" was to mean in this particular context. From our reading of the documents, we concluded that "collected" should be read in its broadest sense so as to complement the authorities and activities of the metadata MD.

Metadata Use

Each of the three OPS documents has a brief paragraph called *Using Metadata*. It is similarly worded in each procedure and is a reiteration of paragraph 8 of the metadata MD (see Annex A).

The MD definition of \_\_\_\_\_ is included in the \_\_\_\_\_ documents.

s.15(1)  
s.16(2)(c)  
s.21(1)(a)  
s.21(1)(b)

The \_\_\_\_\_ procedures<sup>39</sup> have no discussion or identification of what activities would fall within the definition of \_\_\_\_\_

The \_\_\_\_\_ procedures deal with activities that would likely fall within the definition, i.e. those referred to as \_\_\_\_\_. These activities are not linked or cross-referenced to the definition, however.

**Observation no. 4:**

Policies and procedures should be clarified to explain the differences between \_\_\_\_\_

All three of these OPS procedures deal similarly with \_\_\_\_\_. In each instance, the MD definition is included, and \_\_\_\_\_ is noted as a metadata use. There are no other rules or guidance given for this activity in these documents,

**Observation no. 5:**

It is our practice during reviews to examine CSE's policies and procedures which must both interpret and guide those activities provided for under the authority of the *NDA*. Paragraph 4 of the metadata MD directs CSE to "...apply procedures for the use and retention of metadata acquired through its program consistent with CSE's existing procedures to protect the privacy of Canadians." As outlined in the foregoing paragraphs, we have noted deficiencies in CSE's OPS-1 policy and its \_\_\_\_\_ procedures in relation to metadata activities as described in the March 2005 metadata MD.

**Criterion 5:**

*CSE had the means to record, track, and account for \_\_\_\_\_ of metadata that identified Canadians.*

***Finding no. 13:***

Findings no. 2 and no. 3 on page 13 of this report also apply to this criterion. Also, please see the section on Corporate Records Management on page 30.

<sup>39</sup> Reference OPS-3-5 and OPS-3-7, respectively.  
<sup>40</sup> Reference OPS-1-6, paragraphs 3.1 and 3.2, respectively.

s.15(1)  
s.16(2)(c)  
s.21(1)(a)  
s.21(1)(b)

CSE does

pursuant to the authority and rules of the governing MD.

Criterion 6:

*CSE had the means to determine if its metadata activities had been conducted as per its mandate, ministerial directive and approved procedures.*

***Finding no. 14:***

We are satisfied that the CSE managers with whom we spoke understood their responsibilities under OPS-1-8, *Management Monitoring and Policy Review Procedures to Ensure Privacy of Canadians*<sup>41</sup>, and that they approached their daily work with the knowledge that their metadata activities must comply with law and policy.

Our inquiries did not result, however, in receipt of any written material created by CSE managers that indicate how they explicitly address or document their responsibilities as established in OPS-1-8.

Details:

In 2004, CSE issued a new directive known as OPS-1-8. OPS-1-8 deals with CSE management's review and accounting of, among other things, its SIGINT activities, including those known as metadata activities. There are at least four (4) separate references in the document related to management monitoring of the use of metadata. From these references, we wanted to understand:

- a) the monitoring and review of management controls on activities (ref. para. 2.2);
- b) how SIGINT operational areas have developed and instituted management monitoring to ensure that operational policies on the use of metadata are respected on an on-going basis (ref. para. 4.4);
- c) how SIGINT operational areas have developed and instituted management monitoring to ensure retention schedules are followed for metadata used / retained (ref. para. 4.7); and
- d) how management monitoring ensures metadata activities are in compliance with policies and procedures, (ref. para. 2.1).

---

<sup>41</sup> Metadata is also dealt with in

however, that it fell outside the purview of this review.

Our inquiries indicated,

s.15(1)  
 s.16(2)(c)  
 s.21(1)(a)  
 s.21(1)(b)

The wording of the policy directs SIGINT operational areas to "develop and institute Management Monitoring" to ensure that the above-noted areas comply with law and policy, including the *NDA*, the *Privacy Act* and OPS-1. Level 4 managers in SIGINT operational areas and in the Operational Policy division are responsible for management monitoring.

We are satisfied that the CSE managers with whom we spoke understood their responsibilities under OPS-1-8 and that they approached their daily work with the knowledge that their metadata activities must comply with law and policy. In addition, we know from previous reviews and discussions with CSE managers that the organization's Audit, Evaluation and Ethics branch conducts periodic compliance assessments in different operational activity areas within CSE.

Our inquiries did not result, however, in receipt of any written material created by CSE managers that indicate how they explicitly address or document their responsibilities as established in OPS-1-8. In one written response received from CSE, we were advised that "In order to ensure the privacy of Canadians, the management monitors the use of by following the process set forth in OPS-1-10".<sup>42</sup> We were not provided with any further information as to what is meant by "management monitors."

## XI. Corporate Record Keeping

In the MD, the Minister has established a general framework for the collection and use of metadata which includes rules to which CSE must adhere. In addition, the Minister has advised CSE that metadata activities will be subject to review by the CSE Commissioner.

Records creation and retention is one means by which CSE can assure compliance with the metadata framework and can account for its activities as authorized.

During our review, we learned that some metadata activities are of such a nature that they do not always lead, or lend themselves, to the creation of records or documents that can be subsequently examined. This is particularly true of some of the activities

While we understand that some metadata analysis may not involve record keeping, the following two statements made by CSE in response to our requests for various documentation during our review raised questions:

Other than for those

<sup>42</sup>Consistent with OCSEC's review methodology, OPS-1-10 will be subject to further examination when future metadata reviews are undertaken.

s.15(1)  
s.16(2)(c)  
s.21(1)(a)  
s.21(1)(b)

During our discussions, CSE confirmed that it does not as a matter of policy or practice maintain corporate records of those activities

We were advised that some documentation may exist, but it is held at the discretion of individual employees and may be retained by them in their personal hard copy files, for example, or their CSE computers.

This does not allow for any

Further, it does not support CSE's ability to account for these activities, or for any activity, which may result.

It also does not allow for any subsequent review by the CSE Commissioner as is contemplated by the Minister in the MD governing CSE's metadata activities.

Lastly, we include one more statement made by CSE during this review and which raised questions:

Note that aside from activities  
there is no legal or policy requirement to retain records of

***Finding no. 15:***

We suggest that CSE consult GoC legislation and policies regarding corporate record keeping and information management and ensure that it is in compliance.

**XII. CONCLUSION**

This was OCSEC's first examination of CSE's collection and use of metadata as governed by ministerial directive. Due to the complexity and breadth of the activities it authorizes, this preliminary report raises some questions which we believe require further examination.

<sup>43</sup> Response received from CSE dated December 6, 2006, page 2 in reference to OCSEC's document entitled "MD on Collection and Use of Metadata: Preliminary Questions", sent to CSE via e-mail on October 4, 2006.

<sup>44</sup> Response dated March 19, 2007 in e-mail from staff to OCSEC Senior Analyst, Subject: " FW: OCSEC Review of Metadata MD / Meeting ...26 Feb 2007."

s.15(1)  
s.16(2)(c)  
s.21(1)(a)  
s.21(1)(b)

Legal issues:

As has been documented above, some of CSE's metadata activities raise issues that make us question whether CSE is always in compliance with the limits established by the *National Defence Act* regarding the directing of CSE's mandate (a) activities. Further, this review has confirmed that metadata activities

using metadata

We understand that CSE is re-examining its metadata activities, particularly  
This effort will support and inform future metadata reviews.

Any future OCSEC review will also likely examine and assess CSE's metadata activities in relation to mandate (b). While not a focus of this review, we did learn that all telecommunications data

, is also subject to processes designed to identify malicious cyber activity  
These activities, which may also include the  
are also conducted under the guidance of the metadata MD.

Since we have now observed that some of CSE's involves the conducting metadata activities, we believe that CSE should re-examine and re-assess its current position and practice that requires that only those private communications recognized be accounted for. We suggest that those persons involved in : should also be responsible for accounting for all private communications they recognize

Lastly, and further to this and previous reviews, CSE should re-examine its use and in the context of mandate (a) of the *NDA*, and section 8 of the *Privacy Act*.

Policy issues:

CSE policy and procedures should be amended, finalized and perhaps augmented in order to guide and support metadata activities In particular, OPS-1-10 should be finalized as soon as practicable and made available to all personnel engaged in

<sup>45</sup> See footnote 43.

---

Corporate Records Management:

CSE ought to be in a position to account for its metadata activities, up to and including any under the *Privacy Act*.

Future metadata reviews will pay particular attention to the documentation CSE is able to provide in order to facilitate an accurate assessment of its compliance with the authorities established in the *NDA*, the metadata MD, and all related policies and procedures.

Our two (2) recommendations are repeated below:

**Recommendation no. 1:**

**CSE should re-examine and re-assess its current position and practice that requires that only those private communications recognized be accounted for.**

**Recommendation no. 2:**

**CSE should re-examine and re-assess the legislative authority used to conduct its activities**

# Annex A



~~TOP SECRET COMINT~~

s.15(1)

To: Chief, Communications Security Establishment

OCSEC- BCCST-
Original: 2800-9
Copies: _____
Rec. #: 221
Date: July 22, 2005

**MINISTERIAL DIRECTIVE  
COMMUNICATIONS SECURITY ESTABLISHMENT  
COLLECTION AND USE OF METADATA**

1. This Directive is issued under my authority pursuant to subsection 273.62 (3) of the *National Defence Act*.
2. For the purpose of the CSE foreign intelligence acquisition programs:
  - a) "*metadata*" means information associated with a telecommunication to identify, describe, manage or route that telecommunication or any part of it:
  - b)
  - c)
3. CSE will collect and use metadata under foreign intelligence acquisition programs according to principles enunciated in this Ministerial Directive. Any amendment to this Ministerial Directive will require my personal approval.

~~TOP SECRET COMINT~~

~~TOP SECRET COMINT~~

s.15(1)

4. CSE will apply procedures for the use and retention of metadata acquired through its program consistent with CSE's existing procedures to protect the privacy of Canadians.

In the fulfillment of its mandate as set out in paragraphs 273.64 (1) (a) and (b) of the National Defence Act, CSE                      any metadata acquired in the execution of its foreign intelligence acquisition programs

6. CSE will :        metadata, acquired through its foreign intelligence acquisition program                      to maximize its mandate activities as set out in the National Defence Act,                      Such will be subject to strict conditions to protect the privacy of Canadians, consistent with these standards governing CSE's other programs.

7. CSE must take the following steps to protect the privacy of Canadians:

(1)

(2)

(3)

(4)

~~TOP SECRET COMINT~~

s.15(1)

8. The metadata acquired in the execution of the CSE's foreign intelligence acquisition programs shall be used strictly for:
  - a)
  - b)
  - c)
9. The metadata acquired in the execution of CSE foreign intelligence acquisition programs
10. Activities undertaken pursuant to this Ministerial Directive will be subject to review by the CSE Commissioner as part of his mandate.
11. This Ministerial Directive replaces the Annex to the Ministerial Directive, signed by the Minister of National Defence on March 15, 2004.
12. This Ministerial Directives comes into force on the date it is signed.

Dated at Ottawa this 9<sup>th</sup> day of March 2005.



The Honourable **William Graham**  
Minister of National Defence

# Annex B

**Page 69**

**is withheld pursuant to section  
est retenue en vertu de l'article**

**15(1)**

**of the Access to Information Act  
de la Loi sur l'accès à l'information**

# Annex C

s.15(1)  
s.16(2)(c)

## Review

### Background

The *Ministerial Directive [MD], Communications Security Establishment, Collection and Use of Metadata, dated March 9, 2005*, identifies activities, being .

The MD defines as:

s.15(1)  
s.16(2)(c)  
s.21(1)(a)  
s.21(1)(b)

Details:

During the period April 1, 2005 to March 31, 2006, CSE received requests to [redacted]. We can confirm that these requests were subject to a process of internal review and managerial approval. The process was not, however, formally documented until June 2006, in the form of the draft OPS-1-10 procedures (discussed below). Also, not all documentation was provided or available for our review.

We were provided with documentation that related to [redacted] requests to [redacted]. In every instance, the documentation consisted of a [redacted] were accompanied by a CSE addendum that presented the following:

- an assessment of whether a [redacted] could be expected to produce foreign intelligence;
- identified the foreign intelligence priority and objectives; and
- identified what measures CSE would take to protect privacy.

CSE encountered some difficulty in providing the [redacted] documentation we had requested in order to conduct our review. We had anticipated that CSE would have been able to provide us with the following:

In the event that [redacted] we anticipated that CSE would have been able to produce documentation that would have:



s.15(1)  
s.16(2)(c)  
s.21(1)(a)  
s.21(1)(b)  
s.23

This was not the case, however, as it was not possible to draw a line between a metadata activity

CSE did ask that we meet to allow them the opportunity to provide some of the missing details and documentation. We chose not to delay the review at this time with the expectation that we would return to review this one metadata activity in a separate, more encompassing study.

As has been documented in the full metadata MD classified report, there are a number of issues that require re-examination. We believe, for example, that will have to be studied and assessed, along with and in the context of the

In the meantime, we took the opportunity to briefly examine CSE's draft OPS-1-10 procedures, which has governed the activity since June 2006, some two to three months after our review period ended.

#### OPS-1-10

For the period under review, CSE did not have any formal procedures in place to guide CSE personnel

CSE did, however, provide us with a copy of a draft procedure dated June 2006 known as OPS-1-10, *Procedures for Metadata Analysis*  
Copy found at Annex F.

s.15(1)  
s.16(2)(c)  
s.21(1)(a)  
s.21(1)(b)

From this same document, we identified the following list of requirements that CSE personnel would have to satisfy as part of this type of activity. The relevant OPS-1-10 paragraph is noted in brackets after each requirement.

Observations:

From our examination of the documentation presented to us by CSE for the requests made prior to the release of OPS-1-10, we can make the following observations:

We would encourage CSE to continue to develop these procedures and to institute measures to record and

# Annex D

s.15(1)  
s.16(2)(c)  
s.21(1)(a)  
s.21(1)(b)

**Metadata:**

The terminology applied to metadata activities is not yet definitive within CSE's own written documentation. The following definitions, which apply generally to SIGINT acquisition, were provided to us by CSE and were important to our understanding of the collection and use of metadata as authorized by the metadata MD.

**Acquire/Collect:** *Used synonymously to indicate interception.*<sup>46</sup>

As indicated in these definitions, all data

For CSE's purposes,

---

<sup>46</sup> Briefing entitled *Metadata Review Questions* given to OCSEC by CSE on February 26, 2007.

s.15(1)  
s.16(2)(c)  
s.21(1)(a)  
s.21(1)(b)

# Annex E

**Pages 79 to / à 81  
are withheld pursuant to section  
sont retenues en vertu de l'article**

**15(1)**

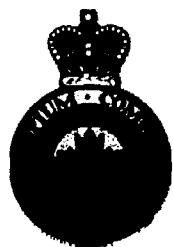
**of the Access to Information Act  
de la Loi sur l'accès à l'information**

# Annex F



s.15(1)

~~TOP SECRET//COMINT//Canadian Eyes Only~~  
June 2006  
DRAFT



OPS-1-10

**Procedures for Metadata Analysis**

~~TOP SECRET//COMINT//Canadian Eyes Only~~  
OPS-1-10  
June 2006  
**DRAFT**

---

## Table of Contents

1. Introduction .....	49
2. Process.....	51
3. Privacy Requirements .....	54
4. Roles and Responsibilities .....	58
5. Additional Information.....	60
6. Definitions.....	62
Annex 1	<b>FormError! Bookmark not defined.</b>

---

~~TOP SECRET//COMINT//Canadian Eyes Only~~  
OPS-1-10  
June 2006  
DRAFT

s.15(1)  
s.16(2)(c)

---

## 1. Introduction

---

### 1.1 Objective

These procedures describe the process CSE and CFIOG analysts must follow when conducting metadata analysis, pursuant to paragraph 273.64(1)(a) of the *National Defence Act* (*NDA*) (known as "Mandate A") in pursuit of Foreign Intelligence (FI),

Metadata analysis conducted in support of Federal Law Enforcement or Security Agencies (LESAs) to obtain Security or Criminal Intelligence (mandated under paragraph 273.64(1)(c) of the *NDA*, known as "Mandate C") is handled only in accordance with OPS-4-1, *Procedures for CSE Assistance to Canadian Federal Law Enforcement and Security Agencies*, and OPS-4-2, *Procedures for CSE Assistance under Section 12 of the CSIS Act*.

### 1.2 Authority

In accordance with these procedures, metadata analysis

for the purpose of providing FI,  
pursuant to paragraph 273.64(1)(a) of the *NDA*.

---

~~TOP SECRET//COMINT//Canadian Eyes Only~~

OPS-1-10

June 2006

**DRAFT**

s.15(1)

s.16(2)(c)

**1.3 Context and  
Limitations**

Metadata analysis  
may only be conducted  
with the authorization of , in  
accordance with these procedures, and only in  
cases where there is a reasonable belief that the  
activity will lead to Foreign Intelligence  
see 2.4).

**1.4 Application**

CSE staff, Canadian Forces Information  
Operations Group (CFIOG) staff, and any other  
parties conducting metadata analysis (

under CSE authorities are bound by  
these procedures.



~~TOP SECRET//COMINT//Canadian Eyes Only~~

OPS-1-10  
 June 2006  
**DRAFT**

s.15(1)  
 s.16(2)(c)

**2.4 FI Test**

The following questions must be addressed by analysts in metadata analysis.

Step	Considerations	If the answer is...	Then...
1	Is there a reasonable belief that  will lead to FI	YES	Analysts provide detailed rationale, using the form at Annex 1,  go to step 2.
		NO	, unless it can be done under "Mandate C" (see 1.1).
2	Will the expected FI satisfy a formal GCR (Government of Canada Requirement)?	YES	Include GCR number on form (Annex 1); submit for approval (see 2.6 below)
		NO	Do not proceed with metadata analysis.

**2.5 Documenting Rationale**

CSE Intelligence Branch and CFIOG analysts must document their rationale for believing a will lead to FI, using the form (Annex 1).

~~TOP SECRET//COMINT//Canadian Eyes Only~~  
OPS-1-10  
June 2006  
DRAFT

s.15(1)  
s.16(2)(c)

---

## 2.6 Approvals

The rationale \_\_\_\_\_ is  
presented by analysts using the form at Annex  
1,

The rationale \_\_\_\_\_ is  
( \_\_\_\_\_, is  
presented by analysts using the form at Annex  
1.

---

~~TOP SECRET//COMINT//Canadian Eyes Only~~  
OPS-1-10  
June 2006  
**DRAFT**

s.15(1)  
s.16(2)(c)

**2.7 Emergency  
Approval for**

In urgent situations (e.g. there is an imminent threat to life),

---

**3. Requirements**

---



~~TOP SECRET//COMINT//Canadian Eyes Only~~

OPS-1-10

June 2006

**DRAFT**

s.15(1)

s.16(2)(c)

**3.1 Records**

Note that:

---

**3.2 Review of  
Requirement  
for**

**Activities**

is  
subject to management monitoring, and to review  
by various government review bodies, including  
the CSE Commissioner.

---

~~TOP SECRET//COMINT//Canadian Eyes Only~~

OPS-1-10

June 2006

DRAFT

s.15(1)

s.16(2)(c)

---

### 3.3 Reporting

SIGINT reports based on metadata analysis must adhere to existing policies and procedures including:

- OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities*
  - OPS-1-1,
  - OPS-1-7, *SIGINT*.
  - OPS-4-1, *Procedures for CSE Assistance to Canadian Federal Law Enforcement and Security Agencies*
  - OPS-4-2, *Procedures for CSE Assistance under Section 12 of the CSIS Act*
  - OPS-5-2, *CSE SIGINT Reporting Procedures*
- 

3.4

---

3.5

~~TOP SECRET//COMINT//Canadian Eyes Only~~

OPS-1-10

June 2006

**DRAFT**

s.15(1)

s.16(2)(c)

---

## 4. Metadata Analysis

---

### 4.1 CSE Metadata

Metadata analysis |

requires the prior  
approval (see  
Annex )

---

~~TOP SECRET//COMINT//Canadian Eyes Only~~

OPS-1-10

June 2006

**DRAFT**

s.15(1)

s.16(2)(c)

4 Metadata analysis  
.  
2

---

## 5. Roles and Responsibilities

---

5.1

This table summarizes roles and responsibilities under these procedures.

Who	Roles
-----	-------

~~TOP SECRET//COMINT//Canadian Eyes Only~~  
 OPS-1-10  
 June 2006  
 DRAFT

s.15(1)

•	<ul style="list-style-type: none"> <li>• Approving metadata analysis</li> <li>• Seeking legal advice when required</li> </ul>
• Director, Legal Services	<ul style="list-style-type: none"> <li>• Providing legal advice, when requested</li> </ul>
•	<ul style="list-style-type: none"> <li>• Approving metadata analysis</li> <li>• Reviewing rationales for metadata analysis</li> </ul>
•	<ul style="list-style-type: none"> <li>• Reviewing rationale and, if acceptable, recommending approval to of metadata analysis</li> <li>• Emergency approval authority (see 2.8)</li> <li>• Seeking legal advice from DLS when required</li> </ul>
(for CFIOG activity)	<ul style="list-style-type: none"> <li>• Reviewing and recommending proposals to in metadata analysis</li> <li>• Reviewing forms quarterly, to ensure continued FI relevance</li> </ul>

\* Note: personnel will consult DLS only in coordination with CSE

~~TOP SECRET//COMINT//Canadian Eyes Only~~  
 OPS-1-10  
 June 2006  
 DRAFT

s.15(1)

---

## 6. Additional Information

---

**6.1  
 Accountability**

The following table outlines the accountability structure with respect to these procedures.

Who	Responsibilities
Deputy Chief SIGINT	<ul style="list-style-type: none"> <li>• Approving these procedures</li> </ul>
	<ul style="list-style-type: none"> <li>• Applying these procedures</li> <li>• Recommending changes to these procedures</li> </ul>
DG Policy and Communications	<ul style="list-style-type: none"> <li>• Approving these procedures</li> </ul>
Director, Legal Services	<ul style="list-style-type: none"> <li>• Reviewing these procedures to ensure they comply with the law</li> </ul>

~~TOP SECRET//COMINT//Canadian Eyes Only~~  
 OPS-1-10  
 June 2006  
 DRAFT

s.15(1)  
 s.16(2)(c)

<p>All CSE</p> <p>Managers involved in</p>	<ul style="list-style-type: none"> <li>Ensuring their staff have read and understood these procedures and any amendments to these procedures</li> </ul>
<ul style="list-style-type: none"> <li>CFIOG staff</li> </ul>	<ul style="list-style-type: none"> <li>Reading, understanding and complying with these procedures and any amendments to these procedures</li> </ul>
<p>Manager</p>	<ul style="list-style-type: none"> <li>Revising these procedures when required</li> <li>Responding to questions concerning these procedures</li> </ul>

**6.2 References**

- National Defence Act*
- Ministerial Directive "Privacy of Canadians", June 2001
- OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities*
- OPS-1-1,
- OPS-1-7, *SIGINT*
- OPS-5-2, *CSE SIGINT Reporting Procedures*

**6.3 Amendments**

Situations may arise where amendments to these procedures may be required because of changing or unforeseen circumstances. All approved amendments will be announced to staff and will be posted

~~TOP SECRET//COMINT//Canadian Eyes Only~~  
OPS-1-10  
June 2006  
DRAFT

s.15(1)  
s.16(2)(c)

---

---

**6.4 Enquiries**

Questions related to these procedures should be directed to operational managers, who in turn will contact staff (e-mail when necessary).

---

**7. Definitions**

---

**7.1 Canadian**

'Canadian' refers to

- a) A Canadian citizen, or
  - b) A person who has acquired the status of permanent resident under the *Immigration and Refugee Protection Act*, S.C. 2001, c. 27, and who has not subsequently lost that status under that *Act*, or
  - c) A corporation incorporated under an Act of Parliament or of the legislature of a province. (NDA)
- 

**7.2**

---



~~TOP SECRET//COMINT//Canadian Eyes Only~~  
OPS-1-10  
June 2006  
**DRAFT**

s.15(1)  
s.16(2)(c)

7.3

7.4

**7.5 Foreign  
Intelligence  
(FI)**

---

Foreign intelligence is information or intelligence about the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group, as they relate to international affairs, defence or security.

---

**7.6 Metadata**

Metadata is defined as information associated with a telecommunication to identify, describe, manage or route that telecommunication

---

~~TOP SECRET//COMINT//Canadian Eyes Only~~

OPS-1-10

June 2006

DRAFT

s.15(1)

s.16(2)(c)

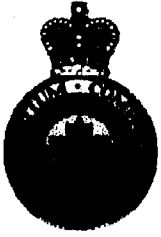
**7.7 Metadata  
Analysis**

Metadata analysis includes various types of  
SIGINT activities

---

~~TOP SECRET//COMINT//Canadian Eyes Only~~

s.15(1)



---

COMMUNICATIONS SECURITY ESTABLISHMENT  
INTELLIGENCE BRANCH

**Approval Form**