

## McAteer, Julie (PS/SP)

---

**From:** McAteer, Julie (PS/SP)  
**Sent:** Friday, November 18, 2016 9:57 AM  
**To:** Milech, Michael (PS/SP)  
**Cc:** DCosta, Tamara (PS/SP); McAteer, Julie (PS/SP)  
**Subject:** RE: Notices of Adjournment Proceedings Received - Avis de débat d'ajournement reçu  
**Attachments:** Late Show - Sansoucy - FC decision - Collection of information - Speeches ENG.docx;  
Late Show - Sansoucy - FC decision - Collection of information - Speeches FR.docx

Here are the ones from CSIS (mostly addressing the federal court decision).

---

**From:** Milech, Michael (PS/SP)  
**Sent:** Tuesday, November 08, 2016 2:16 PM  
**To:** McAteer, Julie (PS/SP); Leclair, Natalie (PS/SP)  
**Subject:** FW: Notices of Adjournment Proceedings Received - Avis de débat d'ajournement reçu

Still more late show excitement.

### Michael Milech

Legislative Assistant | Adjoint législatif  
Office of the Minister of Public Safety and Emergency Preparedness  
Cabinet du ministre de la Sécurité publique et de la Protection civile  
[michael.milech@canada.ca](mailto:michael.milech@canada.ca)  
613-949-9736

---

**From:** Sandhu, Gurjiven [<mailto:Gurjiven.Sandhu@lghc-lgcc.gc.ca>]  
**Sent:** Tuesday, November 08, 2016 1:42 PM  
**To:** Milech, Michael (PS/SP)  
**Subject:** Notices of Adjournment Proceedings Received - Avis de débat d'ajournement reçu

Please see below for an adjournment debate notice; our office will contact you on the day that it is scheduled. Please have a four minute speech and one minute rebuttal prepared in advance.

Veuillez consulter l'avis de débat d'ajournement ci-dessous. Notre bureau communiquera avec vous au jour prévu. Veuillez préparer un discours de quatre minutes et une réplique d'une minute.

### ADJOURNMENT PROCEEDINGS LAYOUT

---

*Divided into 3 periods of 10 minutes maximum:*

*Member raising the question — 4 minutes maximum.*

*Minister or Parliamentary Secretary replying — 4 minutes maximum.*

*Member's reply — 1 minute maximum.*

*Minister or Parliamentary Secretary's second reply — 1 minute maximum*

### DÉROULEMENT DU DÉBAT D'AJOURNEMENT

---

*Temps divisé en 3 périodes d'une durée maximale de 10 minutes:*

*Député qui soulève la question — maximum de 4 minutes.*

*Ministre ou secrétaire parlementaire qui donne la réplique — maximum de 4 minutes.*

*Réplique du député — maximum de 1 minute.*

*Seconde réplique du ministre ou du secrétaire parlementaire — maximum de 1 minute*

---

**NOTICE/AVIS**

**Sansoucy, Brigitte (NDP)**

**Saint-Hyacinthe—Bagot \ Saint-Hyacinthe—Bagot**

**Hansard, 04/11/2016, p. 6602**

Freedom of the Press

La liberté de la presse

---

**Sansoucy, Brigitte (NDP)**

**Saint-Hyacinthe—Bagot \ Saint-Hyacinthe—Bagot**

**Hansard, 04/11/2016, p. 6602**

Freedom of the Press

La liberté de la presse

**Ms. Brigitte Sansoucy (Saint-Hyacinthe—Bagot, NDP):** Mr. Speaker, for several days now, the NDP has been asking exactly how many journalists the RCMP and CSIS are spying on. When questioned about the Federal Court's decision on the collection of personal information, the director of CSIS said that he could not comment on operational details. Journalists across the country want an answer to this question. This is an opportunity for the minister to give the people a clear answer. How many journalists are being spied on?

[English]

**Hon. Ralph Goodale (Minister of Public Safety and Emergency Preparedness, Lib.):** Mr. Speaker, yesterday the director of CSIS was very clear, and the day before that the commissioner of the RCMP was very clear, in terms of the troubling issues that are being reported upon in Quebec in the last number of days. Both the commissioner and the director have said that is not happening at the federal level.

---

**Mme Brigitte Sansoucy (Saint-Hyacinthe—Bagot, NDP):** Monsieur le Président, depuis quelques jours, le NPD demande à savoir le nombre exact de journalistes qui sont sous surveillance par la GRC ou le SCRS.

Interrogé sur la décision que la Cour fédérale a rendue sur la collecte de données personnelles, le directeur du SCRS a répondu qu'il ne pouvait pas faire de commentaires sur des détails opérationnels. Les journalistes de partout au pays veulent avoir une réponse à cette question.

Le ministre a donc l'occasion de donner une réponse claire aux citoyens. Combien de journalistes sont sous surveillance?

[Traduction]

**L'hon. Ralph Goodale (ministre de la Sécurité publique et de la Protection civile, Lib.):** Monsieur le Président, au sujet des problèmes inquiétants qui ont été révélés au Québec au cours des derniers jours, le directeur du SCRS a dit très clairement hier, tout comme le commissaire de la GRC l'a fait le jour précédent, que c'est une pratique qui n'existe pas à l'échelle fédérale.

---

**Ms. Brigitte Sansoucy (Saint-Hyacinthe—Bagot, NDP):** Mr. Speaker, the only acceptable answer is "zero". However, neither the minister nor the Prime Minister can tell the people that no journalists are being spied on. When questioned about this, both the Minister of Public Safety and the Prime Minister

replied that safeguards to protect freedom of the press are in place.  
What are those safeguards?

[English]

**Hon. Ralph Goodale (Minister of Public Safety and Emergency Preparedness, Lib.):** Mr. Speaker, to correct the record so it is very clear, both the director of CSIS and the commissioner of the RCMP have said clearly the answer is “none”.

In terms of the review of the safeguards that are in place, the ministerial directives are very clear and we have already indicated, long before this controversy arose, that we are reviewing all of those directives to make sure that they safeguard the rights and interests and freedoms of Canadians.

---

**Mme Brigitte Sansoucy (Saint-Hyacinthe—Bagot, NPD):**

Monsieur le Président, la seule réponse acceptable, c'est « zéro ». Toutefois, ni le ministre ni le premier ministre ne peuvent confirmer aux citoyens qu'aucun journaliste n'est sous surveillance. Lorsqu'ils ont été interpellés à ce sujet, le ministre de la Sécurité publique et même le premier ministre nous ont répondu que des *safeguards*, soit des garde-fous, pour protéger la liberté de presse étaient toujours en place.

Quels sont ces garde-fous?

[Traduction]

**L'hon. Ralph Goodale (ministre de la Sécurité publique et de la Protection civile, Lib.):** Monsieur le Président, j'aimerais préciser les faits en disant très clairement que le directeur du SCRS et le commissaire de la GRC ont dit sans équivoque qu'aucun journaliste n'a été surveillé de la sorte.

Pour ce qui est d'examiner les garde-fous en place, les directives ministérielles sont très claires, et nous avons déjà dit, bien avant que cette controverse n'éclate, que nous examinons toutes ces directives afin de nous assurer qu'elles protègent les droits, les intérêts et les libertés des Canadiens.

**\*\*Last day for debate (projected)  
06/03/2017**

FOUR MINUTE SPEECH  
RESPONSE TO THE QUESTION FROM  
MP BRIGITTE SANSOUCY (SAINT-HYACINTHE—BAGOT)  
FREEDOM OF THE PRESS (CSIS)

- Our Government is committed to keeping Canadians safe.
- We have made it clear that we are committed to doing so in a manner that respects Canadians' rights and freedoms.
- Freedom of the press is, of course, protected by the *Charter of Rights and Freedoms* and a cornerstone of any healthy democratic society.
- As such, important questions remain with respect to the activities under review in Quebec.
- I must reiterate, however, that these activities occurred at the provincial level.
- The Director of CSIS and the Commissioner of the RCMP have made statements to this effect in recent days.
- With respect to the Canadian Security Intelligence Service, it may only act within the bounds of the

authorities set out in the *CSIS Act*, which contains important limitations and safeguards.

- CSIS may only investigate activities suspected of constituting a threat to the security of Canada. These activities are explicitly defined in law to include: terrorism, espionage, sabotage, and foreign interference.
- I would add that the definition of threats in the *CSIS Act* specifically excludes lawful protest and dissent. The Security Intelligence Review Committee, also known as SIRC, has repeatedly confirmed that the Service has not overreached in this regard.
- In fulfilling this mandate, there may, however, be instances in which the Service's lawfully authorized investigations come into contact with individuals associated with Canadian fundamental institutions.
- Any investigation that affects a fundamental societal institution such as the media, is subject to Ministerial Direction and rigorous operational policies.
- This direction recognizes the fundamental values of Canadian society and the important role of societal

institutions across a range of sectors, including the media.

- Safeguards include more senior levels of approval, special requirements for consultation, and a requirement to advise the Minister.
- A review by SIRC, summarized in its annual report for 2009-2010, recognizes that CSIS has long exercised special care if any investigation affects – or even appears to affect - fundamental institutions.
- In the same Review, SIRC found that CSIS' fundamental institutions policy and its implementation were strong.
- While the Minister has already confirmed that the investigations at issue concern activity by provincial authorities, there has been some reference to the Federal Court decision recently issued in relation to the Service's retention of associated data associated with communications lawfully intercepted under warrant.
- The recent Federal Court decision against CSIS is not related to reports of surveillance of journalists in

Quebec. Rather, it deals with the Service's retention of third party associated data collected under warrant.

- Both the Government and CSIS have accepted the Court's decision and the Minister has been assured that immediate actions have been taken to respond to the issues raised therein.

ONE MINUTE SPEECH  
RESPONSE TO THE QUESTION FROM  
MP BRIGITTE SANSOUCY (SAINT-HYACINTHE—BAGOT)  
FREEDOM OF THE PRESS

- As has been stated, we have strong safeguards in place at the federal level to protect the freedom of the press.
- The recent Federal Court decision does not speak to the surveillance of journalists. Rather, it pertains to the Canadian Security Intelligence Service's retention of associated data linked with third party communications.
- It is important to note that the associated data was collected legally through warrants. The Federal Court's concern relates to CSIS' retention of this data if it is third party and determined not to be related to a threat to the security of Canada.
- As the Minister has previously stated, both the Government and CSIS accept this ruling, and I can assure you that immediate action has been taken to address the Court's concerns, which we take seriously.

**Pages 9 to / à 13  
are not relevant  
sont non pertinentes**

## McAteer, Julie (PS/SP)

---

**From:** McAteer, Julie (PS/SP)  
**Sent:** Friday, November 18, 2016 8:33 AM  
**To:** [REDACTED]  
**Cc:** Communications Issues Management / Communications Gestion des Enjeux (PS/SP); DCosta, Tamara (PS/SP); McAteer, Julie (PS/SP)  
**Subject:** NEW TASKING: Q-602 - Due December 5, 2016 COB  
**Attachments:** Costing.doc; SOC ENG.doc; SOC FRA.doc; Q-602 - Response.docx

Good afternoon,

Please find attached new Written Question **Q-602** regarding CSIS data retention.

Attached is the appropriate template.

Reminder - Please ensure:

1. that your bilingual response is in Arial 12 font
2. to send one fax for each SOC (required in one language only)
3. that dates are written in long form (September 17, 2010 – 17 septembre 2010)
4. that the formatting for numbers/amounts is translated properly (eg. 2,589 vs 2 589 for numbers or \$2,589.00 vs 2 589,00 \$ for amounts)
5. that charts longer than one page be provided in an Excel Annex. Column headers are required to be repeated at the top of each page
6. that documents do not contain colour or shading as the content may not print or photocopy clearly.
7. that the text of the question does not repeat in the Inquiry of Ministry.

Any document not formatted properly will be returned to the originating organization for correction.

**\*\*Should you feel that another department/agency/branch/organization needs to be consulted or tasked, please advise Parliamentary Affairs within 24 hours.\*\***

**Your ADM/ADM equivalent approved bilingual response** should be sent electronically (Word document) to Tamara D'Costa and Julie McAteer **by COB on December 5, 2016**. The ADM/ADM equivalent signed Statement of Completeness (in English or French) should be sent in **PDF format**.

Feel free to contact me should you require additional information.

Have a great day!

\*\*\*\*\*

Bonjour,

Vous trouverez ci-joint la nouvelle question écrite **Q-602** concernant la conservation de données par la SCRS

Vous trouverez ci-joint le gabarit nécessaire.

Rappel – Veuillez-vous assurer :

1. que votre réponse bilingue est en police Arial 12 pt;

2. qu'une télécopie est envoyée pour chaque attestation de conformité (requis seulement dans une langue) transmise;
3. que les dates sont écrites au long (17 septembre 2010 – September 17, 2010);
4. que le format des numéros/montants est traduit correctement (p. ex. numéros – 2 589 c. 2,589; montants – 2 589,00 \$ c. \$2,589.00);
5. que les tableaux dépassant une page de longueur soient fournis en annexe dans Excel (les en-têtes de colonne doivent être répétés au haut de chaque page);
6. que les documents ne contiennent pas de couleur ni d'ombrage, car le contenu pourrait ne pas être imprimé ou photocopié clairement;
7. que le texte de la question ne se répète pas dans la Demande de renseignement au gouvernement.

**Tout document incorrectement mis en forme sera retourné à l'organisation d'origine aux fins de correction.**

**\*\*Si vous estimez qu'un(e) autre ministère/agence/secteur/organisation doit être consulté(e) ou affecté(e), veuillez en aviser les Affaires parlementaires dans un délai de 24 heures.\*\***

Veillez envoyer, par voie électronique, **votre réponse bilingue approuvée par le SMA ou un équivalent** (document Word) à Tamara D'Costa et Julie McAteer avant la **fermeture des bureaux, le 5 décembre 2016**. L'attestation de conformité (en anglais ou en français) du SMA ou de son équivalent devrait être **en format PDF**.

Si vous avez besoin de plus amples renseignements, n'hésitez pas à communiquer avec moi.

Bonne journée !!

Julie

<b>Name of organization</b>

<b>COST OF MINISTERIAL RESPONSE TO WRITTEN QUESTION, Q-</b>	
<b>Name of Parliamentarian :</b>	<b>Constituency :</b>
<b>Date of Inquiry:</b>	
<b>TOTAL COST: \$</b>	



<b>Nom de l'organisation</b>

<b>COÛT DE PRODUCTION POUR LA QUESTION ÉCRITE, Q-</b>	
<b>Nom du parlementaire:</b>	<b>Circonscription :</b>
<b>Date de la demande:</b>	
<b>COÛT TOTAL: \$</b>	

Name of organization

STATEMENT OF COMPLETENESS
RESPONSE TO WRITTEN QUESTION, Q-

Name of Parliamentarian : Constituency :
Date of Inquiry:

A) 1. Briefly describe records, analysis and consultations on which the proposed response is based:

Lead official:

2. Were publicly available documents used to draft the response? Yes No
If yes, please list titles and dates below:

B) Describe any limitations, considerations and/ or data quality statements that apply to this response (include applicable section of Access to Information Act): Yes No

C) Have information or documents relevant to this response been disclosed publicly, in any manner (e.g. access to information request or request from the Library of Parliament)? If yes, please identify relevant documents and explain any differences in the proposed response. Yes N/A

Attestation:

As the Designated Senior Official for
I attest that the information contained in the proposed response, based on the records and limitations described in this Statement of Completeness, is accurate and as complete as possible.

Signature Date
Name of Designated Senior Official Title

Nom de l'entité

ATTESTATION DE CONFORMITÉ
RÉPONSE PROPOSÉE À LA QUESTION ÉCRITE, Q-

Nom du parlementaire : Circonscription :
Date de la demande :

A) 1. Décrivez succinctement les documents, les analyses et les consultations sur lesquels se fonde la réponse.

Personne-ressource :

2. A-t-on utilisé des documents publics pour préparer la réponse? Dans l'affirmative, inscrivez ci-après les titres et les dates. Oui Non

B) Décrivez les restrictions, considérations ou énoncés sur la qualité qui s'appliquent à la présente réponse (inclure les sections applicables de la Loi sur l'accès à l'information) : Oui Non

C) Des éléments d'information ou des documents pertinents à la présente réponse ont-ils été divulgués de quelque manière que ce soit (p. ex. en réponse à une demande présentée en vertu de la Loi sur l'accès à l'information ou provenant de la Bibliothèque du Parlement)? Dans l'affirmative, énumérez les documents pertinents et expliquez toute différence par rapport aux renseignements qui figurent dans la présente réponse. Oui SO

Attestation

En tant que haut fonctionnaire désigné pour je certifie, après examen des documents et des restrictions mentionnées dans la présente attestation de conformité, que les renseignements contenus dans la réponse proposée sont exacts et aussi complets que possible.

Signature Date
Nom du haut fonctionnaire désigné Titre



# INQUIRY OF MINISTRY DEMANDE DE RENSEIGNEMENT AU GOUVERNEMENT

PREPARE IN ENGLISH AND FRENCH MARKING "ORIGINAL TEXT" OR "TRANSLATION"  
PRÉPARER EN ANGLAIS ET EN FRANÇAIS EN INDIQUANT "TEXTE ORIGINAL" OU "TRADUCTION"

QUESTION NO./N° DE LA QUESTION <b>Q-602<sup>2</sup></b>	BY / DE <b>Mr. Dubé (Beloeil—Cambly)</b>	DATE <b>November 15, 2016</b>
--	---	----------------------------------

Reply by the Minister of Public Safety and Emergency Preparedness  
Réponse du Ministre de la Sécurité publique et de la Protection civile

The Honourable Ralph Goodale, P.C., M.P.

PRINT NAME OF SIGNATORY INSCRIRE LE NOM DU SIGNATAIRE	SIGNATURE MINISTER OR PARLIAMENTARY SECRETARY MINISTRE OU SECRÉTAIRE PARLEMENTAIRE
--	--

QUESTION

With regard to the collection and retention of metadata or associated data by Canadian Security Intelligence Service (CSIS): (a) on what dates were the present or former Ministers of Public Safety informed of (i) the existence of the Operational Data Analysis Centre, (ii) the retention of metadata or associated data pertaining to third-parties or individuals who were deemed not to pose a threat, (iii) the possibility this practice could be deemed unlawful; (b) how was the information communicated for each instance in (a); (c) on what dates were the present or former Ministers of Justice informed of (i) the existence of the Operational Data Analysis Centre, (ii) the retention of metadata or associated data pertaining to third-parties or individuals who were deemed not to pose a threat, (iii) the possibility this practice could be deemed unlawful, (iv) the fact that the Federal Court had not been properly informed of this practice; (d) how was the information communicated for each instance in (c); and (e) what is the total number of Canadians whose metadata has been stored by CSIS in each year since 2006?

REPLY / RÉPONSE

ORIGINAL TEXT  
TEXTE ORIGINAL

TRANSLATION  
TRADUCTION

**Page 20**  
**is not relevant**  
**est non pertinente**

## McAteer, Julie (PS/SP)

---

**From:** [REDACTED]  
**Sent:** Wednesday, November 16, 2016 2:02 PM  
**To:** McAteer, Julie (PS/SP)  
**Cc:** [REDACTED]  
**Subject:** RE: Q-602 Constultation

That is correct!

---

**From:** McAteer, Julie (PS/SP) [mailto:julie.mcateer@canada.ca]  
**Sent:** 16-Nov-16 1:50 PM  
**To:** [REDACTED]  
**Subject:** RE: Q-602 Constultation

You mean that CSIS will take the entire question and no part has to go elsewhere correct?

---

**From:** [REDACTED]  
**Sent:** Wednesday, November 16, 2016 1:50 PM  
**To:** McAteer, Julie (PS/SP); [REDACTED] parl-affairs; [REDACTED]  
**Cc:** DCosta, Tamara (PS/SP)  
**Subject:** RE: Q-602 Constultation

Hi Julie,

The question can be answered in its entirety.

Thanks,

---

**From:** McAteer, Julie (PS/SP) [mailto:julie.mcateer@canada.ca]  
**Sent:** 16-Nov-16 1:03 PM  
**To:** [REDACTED] parl-affairs; [REDACTED]  
**Cc:** DCosta, Tamara (PS/SP); McAteer, Julie (PS/SP)  
**Subject:** Q-602 Constultation

Hello  
Please have a look at the question below and confirm which parts (if any) CSIS would be in a position to draft a response. Please confirm parts before COB today. Following this, an official tasking will follow.  
Than you

**Q-602<sup>2</sup>** — November 15, 2016 — Mr. Dubé (Beloil—Chambly) — With regard to the collection and retention of metadata or associated data by CSIS: (a) on what dates were the present or former Ministers of Public Safety informed of (i) the existence of the Operational Data Analysis Centre, (ii) the retention of metadata or associated data pertaining to third-parties or individuals who were deemed not to pose a threat, (iii) the possibility this practice could be deemed unlawful; (b) how was the information communicated for each instance in (a); (c) on what dates were the present or former Ministers of Justice informed of (i) the existence of the Operational Data Analysis Centre, (ii) the retention of metadata or associated data pertaining to third-parties or individuals who were deemed not to pose a threat, (iii) the

possibility this practice could be deemed unlawful, (iv) the fact that the Federal Court had not been properly informed of this practice; (d) how was the information communicated for each instance in (c); and (e) what is the total number of Canadians whose metadata has been stored by CSIS in each year since 2006?

***Julie McAteer***

Senior Advisor, Parliamentary Affairs / Conseillère principale, affaires parlementaires

Public Safety Canada / Sécurité publique Canada

Tel/Tél: (613) 949-9737

Fax:(613) 948-8870

Email/Courriel: [julie.mcateer@canada.ca](mailto:julie.mcateer@canada.ca) (new/nouveau)

**Pages 23 to / à 28  
are not relevant  
sont non pertinentes**

## McAteer, Julie (PS/SP)

---

**From:** McAteer, Julie (PS/SP)  
**Sent:** Tuesday, November 08, 2016 2:52 PM  
**To:** Leclair, Natalie (PS/SP)  
**Subject:** FW: QPN required this am  
**Attachments:** QP Note- Bilingual\_Warrant conditions\_2016 11 07\_ADP Approved\_FINAL.doc

This is the QPN for small distribution list  
Please add something along these lines in the message:

Note on the ATI release set to be released in the near future. Please note that a release date has yet to be established.

---

**From:** [REDACTED]  
**Sent:** Tuesday, November 08, 2016 2:48 PM  
**To:** McAteer, Julie (PS/SP)  
**Cc:** [REDACTED] parl-affairs [REDACTED]  
**Subject:** RE: QPN required this am

Hello Julie,

Attached is the QP Note relevant to the request below.

Thank you,

---

**From:** McAteer, Julie (PS/SP) [mailto:[julie.mcateer@canada.ca](mailto:julie.mcateer@canada.ca)]  
**Sent:** 7-Nov-16 7:27 AM  
**To:** [REDACTED] parl-affairs [REDACTED]  
**Cc:** Leclair, Natalie (PS/SP); McAteer, Julie (PS/SP); Cintrat, Jean (PS/SP); [REDACTED] (PS/SP); Champoux, Elizabeth (PS/SP); De Santis, Heather (PS/SP)  
**Subject:** QPN required this am

Good morning!

The MO has requested a QPN on the attached ATI, which will be released later today. Please provide the English version of your approved QPN by 10:30 followed by the French by 12:30.

Thank you

Julie

### *Julie McAteer*

Senior Advisor, Parliamentary Affairs / Conseillère principale, affaires parlementaires

Public Safety Canada / Sécurité publique Canada

Tel/Tél: (613) 949-9737

Fax:(613) 948-8870

Email/Courriel: [julie.mcateer@canada.ca](mailto:julie.mcateer@canada.ca) (new/nouveau)

QUESTION PERIOD NOTE

Date: DATE THE DOCUMENT IS SENT  
Classification: UNCLASSIFIED  
Branch / Agency: ORGANIZATION NAME

**Question Period Note / Note pour la Période des questions**

**CSIS WARRANTED COLLECTION**

**ISSUE:** A May 2016 memorandum to the Minister advises that materials and communications lawfully collected under warrant were retained for a period in excess of that permitted by the warrant conditions. This issue is distinct from the recent decision issued by the Federal Court. The redacted memo was released through an Access to Information Request.

**PROPOSED RESPONSE:**

- **CSIS relies on people, policies and information technology to ensure that information lawfully collected under warrant is managed in accordance with all relevant requirements, including conditions imposed by the Federal Court.**
- **Last spring, CSIS advised that there had been a breakdown in this complex system, the result being that information lawfully collected under warrant had, in certain instances, been retained for periods longer than permitted by warrant conditions.**
- **On learning of the issue, CSIS undertook immediate corrective measures. I have also been advised that CSIS launched a full scale review to identify and implement necessary enhancements to the overall system.**
- **I understand that CSIS also advised the Security Intelligence Review Committee and the Federal Court of this matter.**

**IF PRESSED ON RECENT FEDERAL COURT DECISION**

- **The recent Federal Court decision takes issue with the Service's decision to retain metadata associated with communications collected under warrant,** [REDACTED]
- **The CSIS Director and I have both issued public statements regarding the Federal Court's decision. I would refer you to those statements for further information on this issue.**
- **We take these matters very seriously. Our Government is committed to keeping Canadians safe in a manner that safeguards our rights and freedoms in a democratic society.**

## CSIS WARRANTED COLLECTION

### BACKGROUND:

A May 2016 memorandum to the Minister advises that materials and communications lawfully collected under warrant were retained for a period in excess of that permitted by the warrant conditions. The CSIS Executive was advised of the issue April 2016 and, having undertaken preliminary steps to review the matter, issued a Memorandum to the Minister on May 25, 2016. The redacted memo was released through an Access to Information Request.

The memo advises the Minister of issues related to information technology systems relied upon to manage information lawfully collected pursuant to warrants.

This matter is distinct from the recent decision issued by the Federal Court. In its decision, the Court determined that CSIS' decision to retain associated data linked to third party communications found to be unrelated to threats or of no use to an investigation, prosecution, national defence or international affairs was not compliant with the *CSIS Act*. It is important to note that CSIS collected this associated data legally, through warrants issued by the Federal Court.

The Service accepted this ruling and took immediate actions to halt all access to and analysis of associated data as it worked to assess and address the Court's findings. On November 3<sup>rd</sup>, the CSIS Director issued a public statement regarding the decision. On November 6<sup>th</sup>, the CSIS Director issued a second public statement on the matter, particularly as it pertains to CSIS' data retention program undertaken within the Operational Data Analysis Centre (ODAC).

### CONTACTS:

Prepared by

Tel. no.

Approved by

ASSISTANT  
DIRECTOR, POLICY AND  
STRATEGIC PARTNERSHIPS

Tel. no.

**Pages 32 to / à 34  
are not relevant  
sont non pertinentes**

## McAteer, Julie (PS/SP)

---

**From:** McAteer, Julie (PS/SP)  
**Sent:** Friday, November 04, 2016 8:59 AM  
**To:** [REDACTED]  
**Subject:** RE: potential QP tomorrow

No – MO has confirmed that this note stands.

---

**From:** [REDACTED] @pco-bcp.gc.ca]  
**Sent:** Friday, November 04, 2016 8:47 AM  
**To:** McAteer, Julie (PS/SP)  
**Subject:** Re: potential QP tomorrow

Hi Julie, so the request is in, but the focus is on the ODAC. Anything you want to add?

---

**De :** McAteer, Julie (PS/SP) [mailto:julie.mcateer@canada.ca]  
**Envoyé :** Thursday, November 03, 2016 02:58 PM  
**À :** [REDACTED]  
**Objet :** RE: potential QP tomorrow

Here is the note with the correct dates indicated.  
Thx.

[http://cas-cdc-www02.cas-sati.gc.ca/rss/DES%20\(warrant\)%20nov-3-2016%20Media%20Summary%20FINAL%20\(ENG\).pdf](http://cas-cdc-www02.cas-sati.gc.ca/rss/DES%20(warrant)%20nov-3-2016%20Media%20Summary%20FINAL%20(ENG).pdf)

---

**From:** [REDACTED] @pco-bcp.gc.ca]  
**Sent:** Thursday, November 03, 2016 12:47 PM  
**To:** McAteer, Julie (PS/SP)  
**Subject:** RE: potential QP tomorrow

Thanks. There was a typo "when if it is" maybe just when it is would work better.

[REDACTED]  
Secrétariat de la sécurité et du renseignement | Security and Intelligence Secretariat  
Bureau du Conseil privé | Privy Council Office  
Téléphone | Telephone [REDACTED]

---

**From:** McAteer, Julie (PS/SP) [mailto:julie.mcateer@canada.ca]  
**Sent:** November 3, 2016 12:43 PM  
**To:** [REDACTED]  
**Subject:** RE: potential QP tomorrow

With new French bullet

---

**From:** [REDACTED] @pco-bcp.gc.ca]  
**Sent:** Thursday, November 03, 2016 11:11 AM

**To:** McAteer, Julie (PS/SP)  
**Subject:** RE: potential QP tomorrow

Yes, that would be great. Thank you.

[REDACTED]  
Secrétariat de la sécurité et du renseignement | Security and Intelligence Secretariat  
Bureau du Conseil privé | Privy Council Office  
Téléphone | Telephone [REDACTED]

---

**From:** McAteer, Julie (PS/SP) [mailto:julie.mcateer@canada.ca]  
**Sent:** November 3, 2016 11:10 AM  
**To:** [REDACTED]  
**Subject:** Re: potential QP tomorrow

We have a note on this - under embargo until the release. Would you like a copy this am?

---

**From:** [REDACTED]  
**Sent:** Thursday, November 3, 2016 11:04 AM  
**To:** McAteer, Julie (PS/SP)  
**Subject:** RE: potential QP tomorrow

Yes.

[REDACTED]  
Secrétariat de la sécurité et du renseignement | Security and Intelligence Secretariat  
Bureau du Conseil privé | Privy Council Office  
Téléphone | Telephone [REDACTED]

---

**From:** McAteer, Julie (PS/SP) [mailto:julie.mcateer@canada.ca]  
**Sent:** November 3, 2016 10:53 AM  
**To:** [REDACTED]  
**Subject:** RE: potential QP tomorrow

Do you mean on Associated Data?

---

**From:** [REDACTED] [mailto:[REDACTED]@pco-bcp.gc.ca]  
**Sent:** Thursday, November 03, 2016 10:47 AM  
**To:** McAteer, Julie (PS/SP)  
**Subject:** potential QP tomorrow

Hi Julie,

We're anticipating that there will be a request for a QOP card on the *en banc* decision (regarding CSIS). I have seen statements and background material before, but still haven't seen a QP card. DO you have anything ready?

Thank you,

[REDACTED]  
Analyste principale des politiques | Senior Policy Analyst  
Secrétariat de la sécurité et du renseignement | Security and Intelligence Secretariat  
Bureau du Conseil privé | Privy Council Office  
[REDACTED] Succursale postale B | Postal Station Building

59 Rue Sparks | 59 Sparks Street Ottawa ON K1A 0A3

 [@pc0-bcp.gc.ca](mailto:pc0-bcp.gc.ca)

Téléphone | Telephone 

Gouvernement du Canada | Government of Canada

## McAteer, Julie (PS/SP)

---

**From:** McAteer, Julie (PS/SP)  
**Sent:** Friday, November 04, 2016 8:39 AM  
**To:** 'GAIL.DELAFUENTE@forces.gc.ca'  
**Subject:** RE: QP Note- CSIS  
**Attachments:** QPN NCSB 2016-Nov-03 Associated Data.docx

As requested. Have a wonderful weekend!

---

**From:** [GAIL.DELAFUENTE@forces.gc.ca](mailto:GAIL.DELAFUENTE@forces.gc.ca) [<mailto:GAIL.DELAFUENTE@forces.gc.ca>]  
**Sent:** Friday, November 04, 2016 8:36 AM  
**To:** McAteer, Julie (PS/SP)  
**Subject:** QP Note- CSIS

Good morning Julie,  
As discussed, could I please have a copy of your QP Note on the current CSIS issue?  
Thank you,  
Gail

Gail de la Fuente

Policy Officer / Directorate of Parliamentary Affairs / ADM (Policy)  
Department of National Defence / Government of Canada  
[gail.delafuente@forces.gc.ca](mailto:gail.delafuente@forces.gc.ca) / Tel: 613-992-1022

Agente de politiques / Direction des affaires parlementaires / SMA (Politiques)  
Ministère de la Défense nationale / Gouvernement du Canada  
[gail.delafuente@forces.gc.ca](mailto:gail.delafuente@forces.gc.ca) / Tél. : 613-992-1022

**Pages 39 to / à 42  
are duplicates  
sont des duplicatas**

**McAteer, Julie (PS/SP)**

---

**From:** McAteer, Julie (PS/SP)  
**Sent:** Friday, November 04, 2016 6:59 AM  
**To:** Khouri, Lisa (PS/SP); Leclair, Natalie (PS/SP); Richer, Jean-Marc (PS/SP)  
**Subject:** Re: Associated data

Thx. Had made that change before sending out yesterday aft once the date was released. Thx

---

**From:** Khouri, Lisa (PS/SP)  
**Sent:** Thursday, November 3, 2016 5:40 PM  
**To:** Leclair, Natalie (PS/SP); McAteer, Julie (PS/SP); Richer, Jean-Marc (PS/SP)  
**Subject:** FW: Associated data

---

**From:** [REDACTED] (PS/SP)  
**Sent:** Thursday, November 03, 2016 5:38 PM  
**To:** Richer, Jean-Marc (PS/SP)  
**Cc:** Khouri, Lisa (PS/SP); [REDACTED] (PS/SP)  
**Subject:** RE: Associated data

Just wanted to advise that the En Banc QPN has now been updated to reflect the date that the Federal Court decision was made public (today, November 3, 2016). This information had previously been square bracketed in the QPN.

---

**From:** [REDACTED] (PS/SP)  
**Sent:** Thursday, November 03, 2016 12:39 PM  
**To:** Richer, Jean-Marc (PS/SP)  
**Cc:** Khouri, Lisa (PS/SP); Beecher, Sophie (PS/SP); [REDACTED] (PS/SP)  
**Subject:** RE: Associated data

No concerns re the change. We have translated the bullet into French and I have updated the RDIMS version of the document.

Sophie B has also reviewed the change.

---

**From:** Richer, Jean-Marc (PS/SP)  
**Sent:** Thursday, November 03, 2016 12:37 PM  
**To:** [REDACTED] (PS/SP)  
**Subject:** RE: Associated data

Any comeback from [REDACTED] is this ok to go  
jm

---

**From:** [REDACTED] (PS/SP)  
**Sent:** Thursday, November 03, 2016 11:43 AM

**To:** Khouri, Lisa (PS/SP); [REDACTED] (PS/SP)  
**Cc:** Richer, Jean-Marc (PS/SP)  
**Subject:** RE: Associated data

[REDACTED] - this refers to the QP Note that was prepared re the En Banc decision.

I have no concerns with the addition of this bullet, subject to any views from [REDACTED]

---

**From:** Khouri, Lisa (PS/SP)  
**Sent:** Thursday, November 03, 2016 11:41 AM  
**To:** [REDACTED] (PS/SP); [REDACTED] (PS/SP)  
**Cc:** Richer, Jean-Marc (PS/SP)  
**Subject:** FW: Associated data

[REDACTED]

Any concern with the addition of this bullet?

If no concern, please provide translation by 12:30

Lisa

---

**From:** McAteer, Julie (PS/SP)  
**Sent:** Thursday, November 03, 2016 11:18 AM  
**To:** Khouri, Lisa (PS/SP)  
**Subject:** Re: Associated data

MO would like to add the following bullet. Pls confirm and provide translation before 12:30.

- I have asked the Security and Intelligence Review Committee (SIRC) to monitor this process and they have agreed.

---

**From:** Khouri, Lisa (PS/SP)  
**Sent:** Monday, October 24, 2016 10:56 AM  
**To:** McAteer, Julie (PS/SP)  
**Subject:** FW: Associated data

Here you go!

---

**From:** Richer, Jean-Marc (PS/SP)  
**Sent:** Monday, October 24, 2016 10:54 AM  
**To:** Leclair, Natalie (PS/SP)  
**Cc:** Khouri, Lisa (PS/SP); Lacroix-Menard, Gabriel (PS/SP); Robert, Philippe (PS/SP)  
**Subject:** RE: Associated data

Nathalie, this is for you  
English and French,

Jean-Marc Richer

---

**From:** Leclair, Natalie (PS/SP)  
**Sent:** Friday, October 21, 2016 4:42 PM

**To:** Khouri, Lisa (PS/SP); McAteer, Julie (PS/SP); Richer, Jean-Marc (PS/SP)

**Subject:** RE: Associated data

Translation en route?

---

**From:** Khouri, Lisa (PS/SP)

**Sent:** Friday, October 21, 2016 4:36 PM

**To:** McAteer, Julie (PS/SP); Leclair, Natalie (PS/SP); Richer, Jean-Marc (PS/SP)

**Subject:** RE: Associated data

---

**From:** McAteer, Julie (PS/SP)

**Sent:** Friday, October 21, 2016 4:33 PM

**To:** Khouri, Lisa (PS/SP); Leclair, Natalie (PS/SP); Richer, Jean-Marc (PS/SP)

**Subject:** RE: Associated data

No attachment ☺

---

**From:** Khouri, Lisa (PS/SP)

**Sent:** Friday, October 21, 2016 4:26 PM

**To:** Leclair, Natalie (PS/SP); Richer, Jean-Marc (PS/SP)

**Cc:** McAteer, Julie (PS/SP)

**Subject:** RE: Associated data

Here you go

lisa

---

**From:** Leclair, Natalie (PS/SP)

**Sent:** Friday, October 21, 2016 2:59 PM

**To:** Khouri, Lisa (PS/SP); Richer, Jean-Marc (PS/SP)

**Cc:** McAteer, Julie (PS/SP)

**Subject:** RE: Associated data

Good afternoon,

Thx for the note. Could you please have it reformatted/adjusted to the attached QPN template? I believe the drafter used a hot issues template which is for Committee appearances.

Thank you!

Natalie

---

**From:** Khouri, Lisa (PS/SP)

**Sent:** Friday, October 21, 2016 1:39 PM

**To:** Leclair, Natalie (PS/SP); McAteer, Julie (PS/SP); Richer, Jean-Marc (PS/SP)

**Subject:** Associated data

Hi Julie,

Here you go

Lisa

---

**From:** [REDACTED] (PS/SP)  
**Sent:** Friday, October 21, 2016 1:11 PM  
**To:** Khouri, Lisa (PS/SP)  
**Subject:** RE: QP Note

Here is the RDIMS link to the QP Note. I will bring up a paper copy shortly.

---

**From:** Khouri, Lisa (PS/SP)  
**Sent:** Friday, October 21, 2016 12:29 PM  
**To:** [REDACTED] (PS/SP)  
**Subject:** RE: QP Note

Hi [REDACTED]

Parl Aff just called and MO wants the QP – can you please bring it up as soon as you are ready?

Lisa

---

**From:** [REDACTED] (PS/SP)  
**Sent:** Friday, October 21, 2016 10:14 AM  
**To:** Khouri, Lisa (PS/SP)  
**Subject:** RE: QP Note

Not for a tasking – it is related to the issue that everyone is concerned about today.

---

**From:** Khouri, Lisa (PS/SP)  
**Sent:** Friday, October 21, 2016 10:14 AM  
**To:** [REDACTED] (PS/SP); Richer, Jean-Marc (PS/SP)  
**Subject:** Re: QP Note

Thanks [REDACTED] I am in meeting till 11am.

Is this for the tasking or a separate issue?

Lisa

---

**From:** [REDACTED] (PS/SP)  
**Sent:** Friday, October 21, 2016 10:09 AM  
**To:** Khouri, Lisa (PS/SP); Richer, Jean-Marc (PS/SP)  
**Subject:** QP Note

You will soon receive a QP Note from us – it has been approved by John D. If Monique approves the English version, then we will go ahead and have it translated.

Apologies for the cryptic email – feel free to call if you have questions. Note that I will be in a mtg from 10:30 to 11:30.

[REDACTED]  
Policy Analyst | Analyste des politiques  
National Security Policy Directorate | Direction générale des politiques de la sécurité nationale  
Public Safety Canada | Sécurité publique Canada  
269 Laurier Ave. West | 269 ave. Laurier ouest  
Ottawa, ON K1A0P8

 @canada.ca

Telephone | Téléphone : 

Facsimile | Télécopieur : 613-991-9284

Government of Canada | Gouvernement du Canada

## **REPORT ON SENATE COMMITTEE MEETING**

**Name of Committee:** NATIONAL SECURITY AND DEFENCE (SECD)  
**Report prepared by:** Susan Nadon, Public Safety Canada, 613-991-3311  
**Date and time:** Monday, February 22, 2016, 2:00 p.m. to 4:00 p.m.  
**Location:** Room 2, Victoria Building  
**Subject:** **Panel One: SIRC Annual Report**  
**Panel Two: Report 2 of the Fall 2015 AG Report re: CBSA exports**

### **Witnesses:**

#### **Panel One :**

The Honourable Pierre Blais, Chair, Security Intelligence Review Committee  
The Honourable Jean-Pierre Plouffe, Commissioner, Office of the Communications Security Establishment Commissioner

### **HIGHLIGHTS OF HEARING:**

The panels were one hour in duration each.

Although the first panel also contained testimony from the Security Establishment Commissioner (who monitors National Defence) and the second covered Report 5 – *Canadian Armed Forces Housing* – this summary only covers SIRC (affecting CSIS) in panel one and Chapter 2 of the AG's report (affecting CBSA) in panel two.

There were no surprises for CSIS or for CBSA in either presentation, although it came to light in the SIRC question and answer session that the next SIRC annual report will likely cover CSIS' activities around radicalization and the effects of Bill C-44 on CSIS authority in foreign lands.

### **PANEL ONE – ANNUAL REPORT OF THE SECURITY INTELLIGENCE REVIEW COMMITTEE**

**The Honourable Pierre Blais** provided an outline of the 2014-2015 Annual Report of the Security Intelligence Review Committee (SIRC), which was tabled on January 28, 2016. A brief outline of the SIRC annual report follows.

The first report stemmed from SIRC's examination of CSIS's efforts at countering the "insider threat." SIRC's in-depth look at CSIS's own internal investigations revealed a number of deficiencies with respect to training, policy and procedures, investigative thresholds and recording of decision making. In one situation in particular, the Committee found that CSIS had failed to give a case the appropriate level of attention and scrutiny, and to take follow-up action. As a result, the Committee made a number of strong recommendations, several of which that, unfortunately, were not heeded by the Service.

The second report focused on SIRC's review of CSIS's relationship with the Department of Foreign Affairs, Trade and Development (DFATD). The Committee raised a potential legal concern with respect to CSIS's activities and Canada's obligations under international agreements. SIRC found that CSIS lacked procedures to systematically verify whether human source operations were in possible contravention of Canadian regulations implementing United

Nations Security Council resolutions, namely, the *United Nations Al Qaeda and Taliban Regulations*.

The Committee decided to invoke a rarely used clause in the *CSIS Act* to direct CSIS to conduct a review to gather information required for SIRC to take any follow-up action deemed necessary.

In other reviews, SIRC found issues that it felt required corrective action; in those instances, the Committee made recommendations that it will closely monitor going forward. SIRC also made note of several CSIS activities that it will need to re-examine in future reviews.

### **PANEL ONE – QUESTIONS AND ANSWERS**

**Senator Kenny** questioned SIRC's capacity to conduct reviews/audits on such a large and complex organization such as CSIS. He wondered why the organization only reviews for conformance to legislation, and not for effectiveness and value for money.

**Senator White** asked whether SIRC also reviewed warrants that were refused by the court.

**Senator Dagenais** asked about the incident involving a CSIS Intelligence Officer who obtained taxpayer information from the Canada Revenue Agency (CRA) without a Federal Court warrant. **Senator Carignan** asked why the Canadian public was not made aware of the incident before 2016.

**Senator Bayek** asked Mr. Blais to speak about radicalized Canadians who go overseas to fight – has it been mentioned in the SIRC report? Mr. Blais replied that the next report will have more to say about this.

In regards to SIRC's recommendations about CSIS' collection and retention of metadata, **Senator Mitchell** stated that CSIS "thumbed its nose" at SIRC by rejecting these recommendations. (SIRC had recommended that CSIS make the Court aware of the particulars of its retention and use of metadata collected under warrant. It also recommended that CSIS further enhance feedback on the utility of these surveillance operations. Based on these findings, it recommended that CSIS produce an updated internal assessment to help guide the future direction of this program). He asked whether the government should move legislation to address the situation.

**Senator Mitchell** also stated that Bill C-44 gave CSIS authority to break the law in foreign lands – he asked if SIRC was monitoring this situation. Mr. Blais replied that this would be a good question to ask when their next report comes out.

### **PANEL TWO – REPORT 2 OF THE FALL 2015 AUDITOR GENERAL'S REPORT – CONTROLLING EXPORTS AT THE BORDER - CBSA**

#### **PANEL TWO – OFFICE OF THE AUDITOR GENERAL OF CANADA**

Nancy Cheng, Assistant Auditor General  
Gordon Stock, Principal  
Nicholas Swales, Principal

**Nancy Cheng** delivered opening remarks, providing detail on Chapter 2 of the Fall 2015 Auditor General report entitled: *Controlling Exports at the Border*. She described the OAG's findings, including that the Canada Border Services Agency could not review all export declarations; that not all high-risk shipments were examined; that CBSA's ability to examine non-reported shipments was limited; and that some shipments were delayed longer than necessary (although this did not impact upon legitimate trade).

Ms. Cheng made it clear that CBSA had agreed with all recommendations made by the Auditor General in this report and that action plans were being prepared to address them.

## **PANEL TWO – QUESTIONS AND ANSWERS**

**Senator Kenny** was concerned about the limited amount of review time permitted for aircraft and ships. He asked whether CBSA reviewed train shipments as well. (They do not).

**Senator Day** asked why the Auditor General did not recommend that regulations be changed so that review timelines could be extended.

**Senator Dagenais** asked how many border service agents deal with border exports and whether CBSA had enough resources, information and authority to prevent illegal exports.

**Senator Mitchell** stated that better oversight is required (i.e., more than just an auditor general report every few years) and asked whether recommendations were made regarding CBSA oversight.

**Senator Bayek** asked how many shipments get through without examination.

**Senator Carignan** asked, given the gaps, had CBSA referred anyone to the RCMP to be investigated for criminal activity? (Ms. Cheng replied that this was not a forensic audit).

**Senator White** asked whether a recommendation had been made to change legislation so that CBSA is authorized to search. He asked whether Canada could link with other countries who would examine shipments before leaving foreign ports. Ms. Cheng replied that this happens for importing, not for exporting.

## **FOLLOW UP ITEMS**

Nil.

**McAteer, Julie (PS/SP)**

---

**From:** McAteer, Julie (PS/SP)  
**Sent:** Thursday, November 03, 2016 2:58 PM  
**To:** [REDACTED]  
**Subject:** RE: potential QP tomorrow  
**Attachments:** QPN NCSB 2016-Nov-03 Associated Data.docx

Here is the note with the correct dates indicated.

Thx.

[http://cas-cdc-www02.cas-satj.gc.ca/rss/DES%20\(warrant\)%20nov-3-2016%20Media%20Summary%20FINAL%20\(ENG\).pdf](http://cas-cdc-www02.cas-satj.gc.ca/rss/DES%20(warrant)%20nov-3-2016%20Media%20Summary%20FINAL%20(ENG).pdf)

---

**From:** [REDACTED] @pco-bcp.gc.ca]  
**Sent:** Thursday, November 03, 2016 12:47 PM  
**To:** McAteer, Julie (PS/SP)  
**Subject:** RE: potential QP tomorrow

Thanks. There was a typo "when if it is" maybe just when it is would work better.

[REDACTED]  
Secrétariat de la sécurité et du renseignement | Security and Intelligence Secretariat  
Bureau du Conseil privé | Privy Council Office  
Téléphone | Telephone [REDACTED]

---

**From:** McAteer, Julie (PS/SP) [mailto:julie.mcateer@canada.ca]  
**Sent:** November 3, 2016 12:43 PM  
**To:** [REDACTED]  
**Subject:** RE: potential QP tomorrow

With new French bullet

---

**From:** [REDACTED] @pco-bcp.gc.ca]  
**Sent:** Thursday, November 03, 2016 11:11 AM  
**To:** McAteer, Julie (PS/SP)  
**Subject:** RE: potential QP tomorrow

Yes, that would be great. Thank you.

[REDACTED]  
Secrétariat de la sécurité et du renseignement | Security and Intelligence Secretariat  
Bureau du Conseil privé | Privy Council Office  
Téléphone | Telephone [REDACTED]

---

**From:** McAteer, Julie (PS/SP) [mailto:julie.mcateer@canada.ca]  
**Sent:** November 3, 2016 11:10 AM  
**To:** [REDACTED]  
**Subject:** Re: potential QP tomorrow

We have a note on this - under embargo until the release. Would you like a copy this am?

---

**From:** [REDACTED]  
**Sent:** Thursday, November 3, 2016 11:04 AM  
**To:** McAteer, Julie (PS/SP)  
**Subject:** RE: potential QP tomorrow

Yes.

[REDACTED]  
Secrétariat de la sécurité et du renseignement | Security and Intelligence Secretariat  
Bureau du Conseil privé | Privy Council Office  
Téléphone | Telephone [REDACTED]

---

**From:** McAteer, Julie (PS/SP) [<mailto:julie.mcateer@canada.ca>]  
**Sent:** November 3, 2016 10:53 AM  
**To:** [REDACTED]  
**Subject:** RE: potential QP tomorrow

Do you mean on Associated Data?

---

**From:** [REDACTED] [[@pco-bcp.gc.ca](mailto:[REDACTED]@pco-bcp.gc.ca)]  
**Sent:** Thursday, November 03, 2016 10:47 AM  
**To:** McAteer, Julie (PS/SP)  
**Subject:** potential QP tomorrow

Hi Julie,

We're anticipating that there will be a request for a QOP card on the *en banc* decision (regarding CSIS). I have seen statements and background material before, but still haven't seen a QP card. DO you have anything ready?

Thank you,

[REDACTED]  
Analyste principale des politiques | Senior Policy Analyst  
Secrétariat de la sécurité et du renseignement | Security and Intelligence Secretariat  
Bureau du Conseil privé | Privy Council Office  
[REDACTED] Succursale postale B | Postal Station Building  
59 Rue Sparks | 59 Sparks Street Ottawa ON K1A 0A3  
[REDACTED] [[@pco-bcp.gc.ca](mailto:[REDACTED]@pco-bcp.gc.ca)]  
Téléphone | Telephone [REDACTED]  
Gouvernement du Canada | Government of Canada

## McAteer, Julie (PS/SP)

---

**From:** McAteer, Julie (PS/SP)  
**Sent:** Thursday, November 03, 2016 2:58 PM  
**To:** Baker3, Ryan (PS/SP); Bardsley, Scott (PS/SP); Beahen, Megan (PS/SP); Besner, David (PS/SP); Brien, Dan (PS/SP); Butera, Eloge (PS/SP); Champoux, Elizabeth (PS/SP); Cintrat, Jean (PS/SP); De Santis, Heather (PS/SP); Elchamaa, Mona (PS/SP); Gobeil, Renée (PS/SP); Hurl, David (PS/SP); 'Issues Management'; Khouri, Lisa (PS/SP); Lwow, Brooke (PS/SP); Milech, Michael (PS/SP); Miller, Kevin (PS/SP); Pike, Cory (PS/SP); PS.F Speeches / Discours F.SP; PS.O Cabinet Affairs Division / Unité des Affaires du Cabinet O.SP; PS.O CMB ADMO / SGM BSMA O.SP; PS.O Communications Public Affairs Division / Communications Division des affaires publiques O.SP; PS.O Parliamentary Affairs Division / Unité des Affaires parlementaires O.SP; PS.O.EMPB.ADMO Users / Utilisateurs BSMA.SGUP.O.SP; PS.O.PACB.ADMO Users / Utilisateurs BSMA.SAPC.O.SP; [REDACTED] (PS/SP); Richer, Jean-Marc (PS/SP)  
**Subject:** Associated Data QPN  
**Attachments:** QPN NCSB 2016-Nov-03 Associated Data.docx

Hello

In light of the court decision released a short time ago, please find attached the relevant QPN. For ease of reference, the court decision is accessible at the following website: [http://cas-cdc-www02.cas-sati.gc.ca/rss/DES%20\(warrant\)%20nov-3-2016%20Media%20Summary%20FINAL%20\(ENG\).pdf](http://cas-cdc-www02.cas-sati.gc.ca/rss/DES%20(warrant)%20nov-3-2016%20Media%20Summary%20FINAL%20(ENG).pdf)

Should you have any additional questions or concerns, please do not hesitate to contact me.

Thank you

Julie

### ***Julie McAteer***

Senior Advisor, Parliamentary Affairs / Conseillère principale, affaires parlementaires

Public Safety Canada / Sécurité publique Canada

Tel/Tél: (613) 949-9737

Fax:(613) 948-8870

Email/Courriel: [julie.mcateer@canada.ca](mailto:julie.mcateer@canada.ca) (*new/nouveau*)

## Question Period Note / Note pour la Période des questions

**FEDERAL COURT DECISION: CSIS' AUTHORITY TO RETAIN "ASSOCIATED DATA"**

**ISSUE:** On November 3, 2016, the Federal Court released a decision in which, among other matters, the Court ruled that CSIS' retention of certain metadata ("associated data") that is not related to a threat to the security of Canada is illegal.

**PROPOSED RESPONSE:**

- **The Government accepts the Federal Court's findings related to CSIS' retention of "associated data". The decision will not be appealed.**
- **It is important to note that the associated data was collected legally through warrants. The Federal Court's concern relates to CSIS' retention of this data when it is determined not to be related to a threat to the security of Canada.**
- **CSIS is taking immediate action to address the Federal Court's findings; it has halted all access to and analysis of associated data as it works to assess and address the Federal Court's findings.**
- **I have asked the Security and Intelligence Review Committee (SIRC) to monitor this process and they have agreed.**
- **The Government also accepts the Federal Court's findings regarding CSIS' duty of candour to the Federal Court. CSIS will work with the Department of Justice and the Federal Court to ensure that it is fully transparent with the Court.**
- **It is also important to note that the Federal Court agreed with most of the terms and conditions proposed by CSIS in the warrant application that was presented to the Court.**
- **Our Government is committed to hearing from Canadians on how we can best meet our dual objectives of keeping Canadians safe, while safeguarding our freedoms, rights, and values.**
- **Through Bill C-22, *the National Security and Intelligence Committee of Parliamentarians Act*, we are also moving forward to strengthen national security accountability.**

# FEDERAL COURT DECISION: CSIS' AUTHORITY TO RETAIN "ASSOCIATED DATA"

## BACKGROUND:

### *Federal Court En Banc Hearings*

The En Banc hearings began as a result of a December 2015 CSIS application for section 12 warrants in which CSIS proposed certain amendments to CSIS warrants. At the same time, following the tabling of the Security Intelligence Review Committee's (SIRC) 2014-2015 Annual Report, the Federal Court indicated that it also wanted to explore issues related to CSIS retention and use of "associated data". In particular, the Federal Court wanted to address SIRC's finding that "SIRC was given no indication that [CSIS] was fully transparent with the Federal Court about the nature and scope of its activities with respect to metadata in the context of [a particular hearing before the Federal Court]".

The En Banc hearings were held over four days in February, March, and April 2016. The Director of CSIS and the Deputy Minister of Justice also appeared before an En Banc hearing on June 10, 2016 to address concerns raised by the Court regarding CSIS' duty of candour in these matters. On October 4, 2016, Justice Simon Noel, the designated judge selected to lead the En Banc proceedings issued a classified, 136 page decision addressing the matters that were before the Court. An unclassified version was released to the public on [October 24, 2016].

### *CSIS' Retention and Use of Associated Data*

"Associated data" is metadata collected incidentally through the execution of telecommunications and other communications intercepts conducted by CSIS pursuant to *CSIS Act* warrants. It consists of, for example, information about the date, time, and phone numbers related to a phone call, or the email addresses, dates, and times of an email. It does not include content.

CSIS uses associated data to support investigations into threats to the security of Canada. It is used to, among other things, help identify links between subjects of investigation and identify where they were located at particular points in time.

Up to this point, CSIS' practice has been to: (1) assess the contents of all communications intercepts conducted and retain the contents of communications intercepts that are relevant to a threat to the security of Canada; (2) delete content deemed not to be related to a threat, within one year after collection; and (3) retain all associated data related to these communications regardless of whether it is threat-related or not.

### *Key Findings of the Federal Court*

The key aspects of the decision are:

- (1) CSIS' retention of non-threat related "associated data" is illegal;
- (2) CSIS breached its duty of candour in not informing the Court that it was retaining this data and had been doing so since 2006;
- (3) The Federal Court was critical of CSIS' views regarding the Federal Court's role in overseeing CSIS activities, particularly CSIS' contention that "Section 21 of the CSIS Act does not confer any general supervisory authority to the Federal Court"; and,
- (4) The Federal Court largely accepted CSIS' proposals regarding technical amendments to CSIS Act warrant templates.

### *The Government's Response to the Federal Court's Decision*

The Government accepts the Federal Court's ruling that CSIS' retention of non-threat related associated data is not authorized by the *CSIS Act* and further accepts the Court's finding that CSIS breached its duty of candour. The decision will not be appealed.

CSIS has taken immediate action to address the Federal Court's findings and has halted all access to and analysis of associated data until CSIS can further assess the decision and put in place measures to comply with the Federal Court's ruling. CSIS is also working with Justice Canada to ensure that it is fully transparent with the Court.

<b>CONTACTS:</b>			
Prepared by [Redacted]	Tel. no. [Redacted]	Approved by (ADM level only) Monik Beauregard, Senior Assistant Deputy Minister, National and Cyber Security Branch	Tel. no. 613-990-4976
A/Director, Intelligence Policy	[Redacted]		

**Pages 56 to / à 57  
are not relevant  
sont non pertinentes**

**McAteer, Julie (PS/SP)**

---

**From:** McAteer, Julie (PS/SP)  
**Sent:** Thursday, November 03, 2016 2:45 PM  
**To:** [REDACTED]  
**Subject:** RE: potential QP tomorrow

Thank you!

---

**From:** [REDACTED] [@pco-bcp.gc.ca](mailto:[REDACTED]@pco-bcp.gc.ca)  
**Sent:** Thursday, November 03, 2016 2:44 PM  
**To:** McAteer, Julie (PS/SP)  
**Subject:** RE: potential QP tomorrow

FYI, the decision is out.

[REDACTED]  
Secrétariat de la sécurité et du renseignement | Security and Intelligence Secretariat  
Bureau du Conseil privé | Privy Council Office  
Téléphone | Telephone [REDACTED]

---

**From:** McAteer, Julie (PS/SP) [\[mailto:julie.mcateer@canada.ca\]](mailto:julie.mcateer@canada.ca)  
**Sent:** November 3, 2016 12:43 PM  
**To:** [REDACTED]  
**Subject:** RE: potential QP tomorrow

With new French bullet

---

**From:** [REDACTED] [@pco-bcp.gc.ca](mailto:[REDACTED]@pco-bcp.gc.ca)  
**Sent:** Thursday, November 03, 2016 11:11 AM  
**To:** McAteer, Julie (PS/SP)  
**Subject:** RE: potential QP tomorrow

Yes, that would be great. Thank you.

[REDACTED]  
Secrétariat de la sécurité et du renseignement | Security and Intelligence Secretariat  
Bureau du Conseil privé | Privy Council Office  
Téléphone | Telephone [REDACTED]

---

**From:** McAteer, Julie (PS/SP) [\[mailto:julie.mcateer@canada.ca\]](mailto:julie.mcateer@canada.ca)  
**Sent:** November 3, 2016 11:10 AM  
**To:** [REDACTED]  
**Subject:** Re: potential QP tomorrow

We have a note on this - under embargo until the release. Would you like a copy this am?

---

**From:** [REDACTED]  
**Sent:** Thursday, November 3, 2016 11:04 AM

To: McAteer, Julie (PS/SP)

Subject: RE: potential QP tomorrow

Yes.

Secrétariat de la sécurité et du renseignement | Security and Intelligence Secretariat  
Bureau du Conseil privé | Privy Council Office  
Téléphone | Telephone

From: McAteer, Julie (PS/SP) [mailto:julie.mcateer@canada.ca]

Sent: November 3, 2016 10:53 AM

To:

Subject: RE: potential QP tomorrow

Do you mean on Associated Data?

From: @pco-bcp.gc.ca]

Sent: Thursday, November 03, 2016 10:47 AM

To: McAteer, Julie (PS/SP)

Subject: potential QP tomorrow

Hi Julie,

We're anticipating that there will be a request for a QOP card on the *en banc* decision (regarding CSIS). I have seen statements and background material before, but still haven't seen a QP card. DO you have anything ready?

Thank you,

Analyste principale des politiques | Senior Policy Analyst  
Secrétariat de la sécurité et du renseignement | Security and Intelligence Secretariat  
Bureau du Conseil privé | Privy Council Office  
Succursale postale B | Postal Station Building  
59 Rue Sparks | 59 Sparks Street Ottawa ON K1A 0A3  
@pco-bcp.gc.ca  
Téléphone | Telephone  
Gouvernement du Canada | Government of Canada

## McAteer, Julie (PS/SP)

---

**From:** McAteer, Julie (PS/SP)  
**Sent:** Thursday, November 03, 2016 12:44 PM  
**To:** Hurl, David (PS/SP); Milech, Michael (PS/SP)  
**Subject:** RE: Associated Data  
**Attachments:** QPN NCSB 2016-Oct 21 Associated Data1.docx

With new bullet in both official languages

---

**From:** Hurl, David (PS/SP)  
**Sent:** Thursday, November 03, 2016 11:14 AM  
**To:** McAteer, Julie (PS/SP); Milech, Michael (PS/SP)  
**Subject:** RE: Associated Data

Forth bullet. If this makes it too long we can drop the C-22 bullet.

- The Government accepts the Federal Court's findings related to CSIS' retention of "associated data". The decision will not be appealed.
- It is important to note that the associated data was collected legally through warrants. The Federal Court's concern relates to CSIS' retention of this data when it was not determined to be related to a threat to the security of Canada.
- CSIS is taking immediate action to address the Federal Court's findings; it has halted all access to and analysis of associated data as it works to assess and address the Federal Court's findings.
- I have asked the Security and Intelligence Review Committee (SIRC) to monitor this process and they have agreed.
- The Government also accepts the Federal Court's findings regarding CSIS' duty of candour to the Federal Court. CSIS will work with the Department of Justice and the Federal Court to ensure that it is fully transparent with the Court.
- It is also important to note that the Federal Court agreed with most of the terms and conditions proposed by CSIS in the warrant application that was presented to the Court.
- Our Government is committed to hearing from Canadians on how we can best meet our dual objectives of keeping Canadians safe, while safeguarding our freedoms, rights, and values.
- Through Bill C-22, the National Security and Intelligence Committee of Parliamentarians Act, we are also moving forward to strengthen national security accountability.

---

**From:** Hurl, David (PS/SP)  
**Sent:** Thursday, November 03, 2016 11:12 AM  
**To:** McAteer, Julie (PS/SP); Milech, Michael (PS/SP)  
**Subject:** RE: Associated Data

We have one line to add. Will send shortly

---

**From:** McAteer, Julie (PS/SP)  
**Sent:** Thursday, November 03, 2016 11:12 AM  
**To:** Hurl, David (PS/SP); Milech, Michael (PS/SP)  
**Subject:** Associated Data

Pco has asked for the QPN. Pls confirm I can share

Question Period Note / Note pour la Période des questions

**FEDERAL COURT DECISION: CSIS' AUTHORITY TO RETAIN "ASSOCIATED DATA"**

**ISSUE:** On [October 24, 2016], the Federal Court released a decision in which, among other matters, the Court ruled that CSIS' retention of certain metadata ("associated data") that is not related to a threat to the security of Canada is illegal.

**PROPOSED RESPONSE:**

- **The Government accepts the Federal Court's findings related to CSIS' retention of "associated data". The decision will not be appealed.**
- **It is important to note that the associated data was collected legally through warrants. The Federal Court's concern relates to CSIS' retention of this data when if it is determined not to be related to a threat to the security of Canada.**
- **CSIS is taking immediate action to address the Federal Court's findings; it has halted all access to and analysis of associated data as it works to assess and address the Federal Court's findings.**
- **I have asked the Security and Intelligence Review Committee (SIRC) to monitor this process and they have agreed.**
- **The Government also accepts the Federal Court's findings regarding CSIS' duty of candour to the Federal Court. CSIS will work with the Department of Justice and the Federal Court to ensure that it is fully transparent with the Court.**
- **It is also important to note that the Federal Court agreed with most of the terms and conditions proposed by CSIS in the warrant application that was presented to the Court.**
- **Our Government is committed to hearing from Canadians on how we can best meet our dual objectives of keeping Canadians safe, while safeguarding our freedoms, rights, and values.**
- **Through Bill C-22, *the National Security and Intelligence Committee of Parliamentarians Act*, we are also moving forward to strengthen national security accountability.**

# FEDERAL COURT DECISION: CSIS' AUTHORITY TO RETAIN "ASSOCIATED DATA"

## BACKGROUND:

### *Federal Court En Banc Hearings*

The En Banc hearings began as a result of a December 2015 CSIS application for section 12 warrants in which CSIS proposed certain amendments to CSIS warrants. At the same time, following the tabling of the Security Intelligence Review Committee's (SIRC) 2014-2015 Annual Report, the Federal Court indicated that it also wanted to explore issues related to CSIS retention and use of "associated data". In particular, the Federal Court wanted to address SIRC's finding that "SIRC was given no indication that [CSIS] was fully transparent with the Federal Court about the nature and scope of its activities with respect to metadata in the context of [a particular hearing before the Federal Court]".

The En Banc hearings were held over four days in February, March, and April 2016. The Director of CSIS and the Deputy Minister of Justice also appeared before an En Banc hearing on June 10, 2016 to address concerns raised by the Court regarding CSIS' duty of candour in these matters. On October 4, 2016, Justice Simon Noel, the designated judge selected to lead the En Banc proceedings issued a classified, 136 page decision addressing the matters that were before the Court. An unclassified version was released to the public on [October 24, 2016].

### *CSIS' Retention and Use of Associated Data*

"Associated data" is metadata collected incidentally through the execution of telecommunications and other communications intercepts conducted by CSIS pursuant to CSIS Act warrants. It consists of, for example, information about the date, time, and phone numbers related to a phone call, or the email addresses, dates, and times of an email. It does not include content.

CSIS uses associated data to support investigations into threats to the security of Canada. It is used to, among other things, help identify links between subjects of investigation and identify where they were located at particular points in time.

Up to this point, CSIS' practice has been to: (1) assess the contents of all communications intercepts conducted and retain the contents of communications intercepts that are relevant to a threat to the security of Canada; (2) delete content deemed not to be related to a threat, within one year after collection; and (3) retain all associated data related to these communications regardless of whether it is threat-related or not.

### *Key Findings of the Federal Court*

The key aspects of the decision are:

- (1) CSIS' retention of non-threat related "associated data" is illegal;
- (2) CSIS breached its duty of candour in not informing the Court that it was retaining this data and had been doing so since 2006;
- (3) The Federal Court was critical of CSIS' views regarding the Federal Court's role in overseeing CSIS activities, particularly CSIS' contention that "Section 21 of the CSIS Act does not confer any general supervisory authority to the Federal Court"; and,
- (4) The Federal Court largely accepted CSIS' proposals regarding technical amendments to CSIS Act warrant templates.

### *The Government's Response to the Federal Court's Decision*

The Government accepts the Federal Court's ruling that CSIS' retention of non-threat related associated data is not authorized by the CSIS Act and further accepts the Court's finding that CSIS breached its duty of candour. The decision will not be appealed.

CSIS has taken immediate action to address the Federal Court's findings and has halted all access to and analysis of associated data until CSIS can further assess the decision and put in place measures to comply with the Federal Court's ruling. CSIS is also working with Justice Canada to ensure that it is fully transparent with the Court.

## CONTACTS:

Prepared by

[Redacted]

[Redacted]

A/Director, Intelligence Policy

Tel. no.

[Redacted]

[Redacted]

Approved by (ADM level only)

Monik Beauregard,  
Senior Assistant Deputy Minister,  
National and Cyber Security Branch

Tel. no.

613-990-4976

**Pages 64 to / à 66  
are not relevant  
sont non pertinentes**

## McAteer, Julie (PS/SP)

---

**From:** McAteer, Julie (PS/SP)  
**Sent:** Thursday, November 03, 2016 11:28 AM  
**To:** [REDACTED]  
**Subject:** RE: potential QP tomorrow  
**Attachments:** QPN NCSB 2016-Oct 21 Associated Data1.docx

Voila  
We made one small addition (fourth bullet in the English) that is not yet reflected in the French.  
Will revise and send you as soon as I get the French – in the meantime, here is the full English and the French without that one bullet.

---

**From:** [REDACTED] [mailto:pco-bcp.gc.ca]  
**Sent:** Thursday, November 03, 2016 11:11 AM  
**To:** McAteer, Julie (PS/SP)  
**Subject:** RE: potential QP tomorrow

Yes, that would be great. Thank you.

[REDACTED]  
Secrétariat de la sécurité et du renseignement | Security and Intelligence Secretariat  
Bureau du Conseil privé | Privy Council Office  
Téléphone | Telephone [REDACTED]

---

**From:** McAteer, Julie (PS/SP) [mailto:julie.mcateer@canada.ca]  
**Sent:** November 3, 2016 11:10 AM  
**To:** [REDACTED]  
**Subject:** Re: potential QP tomorrow

We have a note on this - under embargo until the release. Would you like a copy this am?

---

**From:** [REDACTED]  
**Sent:** Thursday, November 3, 2016 11:04 AM  
**To:** McAteer, Julie (PS/SP)  
**Subject:** RE: potential QP tomorrow

Yes.

[REDACTED]  
Secrétariat de la sécurité et du renseignement | Security and Intelligence Secretariat  
Bureau du Conseil privé | Privy Council Office  
Téléphone | Telephone [REDACTED]

---

**From:** McAteer, Julie (PS/SP) [mailto:julie.mcateer@canada.ca]  
**Sent:** November 3, 2016 10:53 AM  
**To:** [REDACTED]  
**Subject:** RE: potential QP tomorrow

Do you mean on Associated Data?

---

**From:** [REDACTED] @pco-bcp.gc.ca]  
**Sent:** Thursday, November 03, 2016 10:47 AM  
**To:** McAteer, Julie (PS/SP)  
**Subject:** potential QP tomorrow

Hi Julie,

We're anticipating that there will be a request for a QOP card on the *en banc* decision (regarding CSIS). I have seen statements and background material before, but still haven't seen a QP card. DO you have anything ready?

Thank you,

[REDACTED]  
Analyste principale des politiques | Senior Policy Analyst  
Secrétariat de la sécurité et du renseignement | Security and Intelligence Secretariat  
Bureau du Conseil privé | Privy Council Office  
[REDACTED] Succursale postale B | Postal Station Building  
59 Rue Sparks | 59 Sparks Street Ottawa ON K1A 0A3  
[REDACTED] @pco-bcp.gc.ca  
Téléphone | Telephone [REDACTED]  
Gouvernement du Canada | Government of Canada

Question Period Note / Note pour la Période des questions

**FEDERAL COURT DECISION: CSIS' AUTHORITY TO RETAIN "ASSOCIATED DATA"**

**ISSUE:** On [October 24, 2016], the Federal Court released a decision in which, among other matters, the Court ruled that CSIS' retention of certain metadata ("associated data") that is not related to a threat to the security of Canada is illegal.

**PROPOSED RESPONSE:**

- **The Government accepts the Federal Court's findings related to CSIS' retention of "associated data". The decision will not be appealed.**
- **It is important to note that the associated data was collected legally through warrants. The Federal Court's concern relates to CSIS' retention of this data when if it is determined not to be related to a threat to the security of Canada.**
- **CSIS is taking immediate action to address the Federal Court's findings; it has halted all access to and analysis of associated data as it works to assess and address the Federal Court's findings.**
- **I have asked the Security and Intelligence Review Committee (SIRC) to monitor this process and they have agreed.**
- **The Government also accepts the Federal Court's findings regarding CSIS' duty of candour to the Federal Court. CSIS will work with the Department of Justice and the Federal Court to ensure that it is fully transparent with the Court.**
- **It is also important to note that the Federal Court agreed with most of the terms and conditions proposed by CSIS in the warrant application that was presented to the Court.**
- **Our Government is committed to hearing from Canadians on how we can best meet our dual objectives of keeping Canadians safe, while safeguarding our freedoms, rights, and values.**
- **Through Bill C-22, *the National Security and Intelligence Committee of Parliamentarians Act*, we are also moving forward to strengthen national security accountability.**

# FEDERAL COURT DECISION: CSIS' AUTHORITY TO RETAIN "ASSOCIATED DATA"

## BACKGROUND:

### *Federal Court En Banc Hearings*

The En Banc hearings began as a result of a December 2015 CSIS application for section 12 warrants in which CSIS proposed certain amendments to CSIS warrants. At the same time, following the tabling of the Security Intelligence Review Committee's (SIRC) 2014-2015 Annual Report, the Federal Court indicated that it also wanted to explore issues related to CSIS retention and use of "associated data". In particular, the Federal Court wanted to address SIRC's finding that "SIRC was given no indication that [CSIS] was fully transparent with the Federal Court about the nature and scope of its activities with respect to metadata in the context of [a particular hearing before the Federal Court]".

The En Banc hearings were held over four days in February, March, and April 2016. The Director of CSIS and the Deputy Minister of Justice also appeared before an En Banc hearing on June 10, 2016 to address concerns raised by the Court regarding CSIS' duty of candour in these matters. On October 4, 2016, Justice Simon Noel, the designated judge selected to lead the En Banc proceedings issued a classified, 136 page decision addressing the matters that were before the Court. An unclassified version was released to the public on [October 24, 2016].

### *CSIS' Retention and Use of Associated Data*

"Associated data" is metadata collected incidentally through the execution of telecommunications and other communications intercepts conducted by CSIS pursuant to *CSIS Act* warrants. It consists of, for example, information about the date, time, and phone numbers related to a phone call, or the email addresses, dates, and times of an email. It does not include content.

CSIS uses associated data to support investigations into threats to the security of Canada. It is used to, among other things, help identify links between subjects of investigation and identify where they were located at particular points in time.

Up to this point, CSIS' practice has been to: (1) assess the contents of all communications intercepts conducted and retain the contents of communications intercepts that are relevant to a threat to the security of Canada; (2) delete content deemed not to be related to a threat, within one year after collection; and (3) retain all associated data related to these communications regardless of whether it is threat-related or not.

### *Key Findings of the Federal Court*

The key aspects of the decision are:

- (1) CSIS' retention of non-threat related "associated data" is illegal;
- (2) CSIS breached its duty of candour in not informing the Court that it was retaining this data and had been doing so since 2006;
- (3) The Federal Court was critical of CSIS' views regarding the Federal Court's role in overseeing CSIS activities, particularly CSIS' contention that "Section 21 of the CSIS Act does not confer any general supervisory authority to the Federal Court"; and,
- (4) The Federal Court largely accepted CSIS' proposals regarding technical amendments to CSIS Act warrant templates.

### *The Government's Response to the Federal Court's Decision*

The Government accepts the Federal Court's ruling that CSIS' retention of non-threat related associated data is not authorized by the *CSIS Act* and further accepts the Court's finding that CSIS breached its duty of candour. The decision will not be appealed.

CSIS has taken immediate action to address the Federal Court's findings and has halted all access to and analysis of associated data until CSIS can further assess the decision and put in place measures to comply with the Federal Court's ruling. CSIS is also working with Justice Canada to ensure that it is fully transparent with the Court.

<b>CONTACTS:</b>			
Prepared by	Tel. no.	Approved by (ADM level only)	Tel. no.
[Redacted]	[Redacted]	Monik Beauregard,	613-990-4976
[Redacted]	[Redacted]	Senior Assistant Deputy Minister,	
[Redacted]	[Redacted]	National and Cyber Security Branch	
A/Director, Intelligence Policy			

**Pages 71 to / à 73  
are not relevant  
sont non pertinentes**

**McAteer, Julie (PS/SP)**

---

**From:** McAteer, Julie (PS/SP)  
**Sent:** Saturday, October 22, 2016 2:50 PM  
**To:** Champoux, Elizabeth (PS/SP); Leclair, Natalie (PS/SP)  
**Subject:** Re: QPN - NCSB - 2016-Oct 21 - Associated Data

We are aware that it was not released which is why it was only sent to the small list. We have an eye on the website to know when it's released.

Thx for info on binder - will advise Susan.

Thx

---

**From:** Champoux, Elizabeth (PS/SP)  
**Sent:** Saturday, October 22, 2016 2:39 PM  
**To:** Leclair, Natalie (PS/SP); McAteer, Julie (PS/SP)  
**Subject:** Re: QPN - NCSB - 2016-Oct 21 - Associated Data

The decision wasn't released on Friday. We are still awaiting a date. Please ensure that it doesn't go to the broader list. On a separate note, we may need to add a few related Q+As to the C-22 Secu binder.

Tx! B

Sent from my BlackBerry 10 smartphone on the Rogers network.

---

**From:** Leclair, Natalie (PS/SP)  
**Sent:** Friday, October 21, 2016 4:42 PM  
**To:** Milech, Michael (PS/SP); Hurl, David (PS/SP)  
**Cc:** McAteer, Julie (PS/SP); Champoux, Elizabeth (PS/SP); De Santis, Heather (PS/SP); Cintrat, Jean (PS/SP)  
**Subject:** QPN - NCSB - 2016-Oct 21 - Associated Data

Please find attached a QP note prepared by the department in anticipation of the court decision on CSIS' authority to retain associated data.

Thank you

Natalie

**Analyst/Analyste**  
**Parliamentary Affairs/Affaires parlementaires**  
**Public Safety Canada/Sécurité publique Canada**  
**Tel/Tél: (613) 990-2718**

## McAteer, Julie (PS/SP)

---

**From:** Khouri, Lisa (PS/SP)  
**Sent:** Friday, October 21, 2016 4:49 PM  
**To:** Leclair, Natalie (PS/SP); McAteer, Julie (PS/SP); Richer, Jean-Marc (PS/SP)  
**Subject:** RE: Associated data

Yes it was sent

Lisa

---

**From:** Leclair, Natalie (PS/SP)  
**Sent:** Friday, October 21, 2016 4:42 PM  
**To:** Khouri, Lisa (PS/SP); McAteer, Julie (PS/SP); Richer, Jean-Marc (PS/SP)  
**Subject:** RE: Associated data

Translation en route?

---

**From:** Khouri, Lisa (PS/SP)  
**Sent:** Friday, October 21, 2016 4:36 PM  
**To:** McAteer, Julie (PS/SP); Leclair, Natalie (PS/SP); Richer, Jean-Marc (PS/SP)  
**Subject:** RE: Associated data

---

**From:** McAteer, Julie (PS/SP)  
**Sent:** Friday, October 21, 2016 4:33 PM  
**To:** Khouri, Lisa (PS/SP); Leclair, Natalie (PS/SP); Richer, Jean-Marc (PS/SP)  
**Subject:** RE: Associated data

No attachment ☺

---

**From:** Khouri, Lisa (PS/SP)  
**Sent:** Friday, October 21, 2016 4:26 PM  
**To:** Leclair, Natalie (PS/SP); Richer, Jean-Marc (PS/SP)  
**Cc:** McAteer, Julie (PS/SP)  
**Subject:** RE: Associated data

Here you go

lisa

---

**From:** Leclair, Natalie (PS/SP)  
**Sent:** Friday, October 21, 2016 2:59 PM  
**To:** Khouri, Lisa (PS/SP); Richer, Jean-Marc (PS/SP)  
**Cc:** McAteer, Julie (PS/SP)  
**Subject:** RE: Associated data

Good afternoon,

Thx for the note. Could you please have it reformatted/adjusted to the attached QPN template? I believe the drafter used a hot issues template which is for Committee appearances.

Thank you!  
Natalie

---

**From:** Khouri, Lisa (PS/SP)  
**Sent:** Friday, October 21, 2016 1:39 PM  
**To:** Leclair, Natalie (PS/SP); McAteer, Julie (PS/SP); Richer, Jean-Marc (PS/SP)  
**Subject:** Associated data

Hi Julie,

Here you go

Lisa

---

**From:** [REDACTED] (PS/SP)  
**Sent:** Friday, October 21, 2016 1:11 PM  
**To:** Khouri, Lisa (PS/SP)  
**Subject:** RE: QP Note

Here is the RDIMS link to the QP Note. I will bring up a paper copy shortly.

---

**From:** Khouri, Lisa (PS/SP)  
**Sent:** Friday, October 21, 2016 12:29 PM  
**To:** [REDACTED] (PS/SP)  
**Subject:** RE: QP Note

Hi [REDACTED]

Parl Aff just called and MO wants the QP – can you please bring it up as soon as you are ready?

Lisa

---

**From:** [REDACTED] (PS/SP)  
**Sent:** Friday, October 21, 2016 10:14 AM  
**To:** Khouri, Lisa (PS/SP)  
**Subject:** RE: QP Note

Not for a tasking – it is related to the issue that everyone is concerned about today.

---

**From:** Khouri, Lisa (PS/SP)  
**Sent:** Friday, October 21, 2016 10:14 AM  
**To:** [REDACTED] (PS/SP); Richer, Jean-Marc (PS/SP)  
**Subject:** Re: QP Note

Thanks [REDACTED] I am in meeting till 11am.

Is this for the tasking or a separate issue?

Lisa

---

**From:** [REDACTED] (PS/SP)  
**Sent:** Friday, October 21, 2016 10:09 AM

---

To: Khouri Lisa (PS/SP), Richer Jean-Marc (PS/SP)  
Subject: QP Note

You will soon receive a QP Note from us – it has been approved by John D. If Monique approves the English version, then we will go ahead and have it translated.

Apologies for the cryptic email – feel free to call if you have questions. Note that I will be in a mtg from 10:30 to 11:30.

██████████  
Policy Analyst | Analyste des politiques  
National Security Policy Directorate | Direction générale des politiques de la sécurité nationale  
Public Safety Canada | Sécurité publique Canada  
269 Laurier Ave. West | 269 ave. Laurier ouest  
Ottawa, ON K1A0P8  
██████████@canada.ca  
Telephone | Téléphone : ██████████  
Facsimile | Télécopieur : 613-991-9284  
Government of Canada | Gouvernement du Canada

**McAteer, Julie (PS/SP)**

---

**From:** McAteer, Julie (PS/SP)  
**Sent:** Tuesday, October 18, 2016 8:14 AM  
**To:** Khouri, Lisa (PS/SP)  
**Cc:** Leclair, Natalie (PS/SP); Richer, Jean-Marc (PS/SP)  
**Subject:** associated data crt decision

Good morning Lisa!

Head's up - for your information, we will need a QPN on this issue the day the crt decision is rendered public.

Thank you!

Julie

***Julie McAteer***

Senior Advisor, Parliamentary Affairs / Conseillère principale, affaires parlementaires

Public Safety Canada / Sécurité publique Canada

Tel/Tél: (613) 949-9737

Fax:(613) 948-8870

Email/Courriel: [julie.mcateer@canada.ca](mailto:julie.mcateer@canada.ca) (*new/nouveau*)

**McAteer, Julie (PS/SP)**

---

**From:** McAteer, Julie (PS/SP)  
**Sent:** Friday, October 21, 2016 2:05 PM  
**To:** Leclair, Natalie (PS/SP)  
**Subject:** FW: Associated data  
**Attachments:** PS-SP-#1998092-R-2016-10-21\_-\_QP\_Note\_-\_En\_Banc\_Decision.DOCX

Please process and send to limited list.  
We can call it Associated Data.  
Thx.

---

**From:** Khouri, Lisa (PS/SP)  
**Sent:** Friday, October 21, 2016 1:39 PM  
**To:** Leclair, Natalie (PS/SP); McAteer, Julie (PS/SP); Richer, Jean-Marc (PS/SP)  
**Subject:** Associated data

Hi Julie,

Here you go

Lisa

---

**From:** [REDACTED] (PS/SP)  
**Sent:** Friday, October 21, 2016 1:11 PM  
**To:** Khouri, Lisa (PS/SP)  
**Subject:** RE: QP Note

Here is the RDIMS link to the QP Note. I will bring up a paper copy shortly.

---

**From:** Khouri, Lisa (PS/SP)  
**Sent:** Friday, October 21, 2016 12:29 PM  
**To:** [REDACTED] (PS/SP)  
**Subject:** RE: QP Note

Hi [REDACTED]

Parl Aff just called and MO wants the QP – can you please bring it up as soon as you are ready?

Lisa

---

**From:** [REDACTED] (PS/SP)  
**Sent:** Friday, October 21, 2016 10:14 AM  
**To:** Khouri, Lisa (PS/SP)  
**Subject:** RE: QP Note

Not for a tasking – it is related to the issue that everyone is concerned about today.

---

**From:** Khouri, Lisa (PS/SP)  
**Sent:** Friday, October 21, 2016 10:14 AM

**To:** [REDACTED] (PS/SP); Richer, Jean-Marc (PS/SP)  
**Subject:** Re: QP Note

Thanks [REDACTED] I am in meeting till 11am.

Is this for the tasking or a separate issue?

Lisa

---

**From:** [REDACTED] PS/SP  
**Sent:** Friday, October 21, 2016 10:09 AM  
**To:** Khouri, Lisa (PS/SP); Richer, Jean-Marc (PS/SP)  
**Subject:** QP Note

You will soon receive a QP Note from us – it has been approved by John D. If Monique approves the English version, then we will go ahead and have it translated.

Apologies for the cryptic email – feel free to call if you have questions. Note that I will be in a mtg from 10:30 to 11:30.

[REDACTED]  
Policy Analyst | Analyste des politiques  
National Security Policy Directorate | Direction générale des politiques de la sécurité nationale  
Public Safety Canada | Sécurité publique Canada  
269 Laurier Ave. West | 269 ave. Laurier ouest  
Ottawa, ON K1A0P8

[REDACTED]@canada.ca  
Telephone | Téléphone : [REDACTED]  
Facsimile | Télécopieur : 613-991-9284  
Government of Canada | Gouvernement du Canada

**Question Period Note / Note pour la Période des questions**

**Federal Court Decision: CSIS' Authority to Retain "Associated Data"**

**ISSUE:** On [October 21, 2016], the Federal Court released a decision in which, among other matters, the Court ruled that CSIS' retention of certain metadata ("associated data") that is not related to a threat to the security of Canada is illegal.

**PROPOSED RESPONSE:**

- **The Government accepts the Federal Court's findings related to CSIS' retention of "associated data". The decision will not be appealed.**
- **It is important to note that the associated data was collected legally through warrants. The Federal Court's concern relates to CSIS' retention of this data when if it is determined not to be related to a threat to the security of Canada.**
- **CSIS is taking immediate action to address the Federal Court's findings; it has halted all access to and analysis of associated data as it works to assess and address the Federal Court's findings.**
- **The Government also accepts the Federal Court's findings regarding CSIS' duty of candour to the Federal Court. CSIS will work with the Department of Justice and the Federal Court to ensure that it is fully transparent with the Court.**
- **It is also important to note that the Federal Court agreed with most of the terms and conditions proposed by CSIS in the warrant application that was presented to the Court.**
- **Our Government is committed to hearing from Canadians on how we can best meet our dual objectives of keeping Canadians safe, while safeguarding our freedoms, rights, and values.**
- **Through Bill C-22, the National Security and Intelligence Committee of Parliamentarians Act, we are also moving forward to strengthen national security accountability.**

## Federal Court Decision: CSIS' Authority to Retain "Associated Data"

### BACKGROUND:

#### Q1: What are the "en banc" hearings? Why did the Federal Court become concerned about CSIS' retention and use of "associated data"?

The En Banc hearings began as a result of a December 2015 CSIS application for section 12 warrants in which CSIS proposed certain amendments to CSIS warrants. At the same time, following the tabling of the Security Intelligence Review Committee's (SIRC) 2014-2015 Annual Report, the Federal Court indicated that it also wanted to explore issues related to CSIS retention and use of "associated data". In particular, the Federal Court wanted to address SIRC's finding that "SIRC was given no indication that [CSIS] was fully transparent with the Federal Court about the nature and scope of its activities with respect to metadata in the context of [a particular hearing before the Federal Court]".

The En Banc hearings were held over four days in February, March, and April 2016. The Director of CSIS and the Deputy Minister of Justice also appeared before an En Banc hearing on June 10, 2016 to address concerns raised by the Court regarding CSIS' duty of candour in these matters. On October 4, 2016, Justice Simon Noel, the designated judge selected to lead the En Banc proceedings issued a classified, 136 page decision addressing the matters that were before the Court. An unclassified version was released to the public on [October 21, 2016].

#### Q2: What is "associated data" and how is it used by CSIS?

"Associated data" is metadata collected incidentally through the execution of telecommunications and other communications intercepts conducted by CSIS pursuant to *CSIS Act* warrants. It consists of, for example, information about the date, time, and phone numbers related to a phone call, or the email addresses, dates, and times of an email. It does not include content.

CSIS uses associated data to support investigations into threats to the security of Canada. It is used to, among other things, help identify links between subjects of investigation and identify where they were located at particular points in time.

Up to this point, CSIS' practice has been to: (1) assess the contents of all communications intercepts conducted and retain the contents of communications intercepts that are relevant to a threat to the security of Canada; (2) delete content deemed not to be related to a threat, within one year after collection; and (3) retain all associated data related to these communications regardless of whether it is threat-related or not.

#### Q3: What were the Federal Court's findings?

The key aspects of the decision are:

- (1) CSIS' retention of non-threat related "associated data" is illegal;
- (2) CSIS breached its duty of candour in not informing the Court that it was retaining this data and had been doing so since 2006;
- (3) The Federal Court was critical of CSIS' views regarding the Federal Court's role in overseeing CSIS activities, particularly CSIS' contention that "Section 21 of the CSIS Act does not confer any general supervisory authority to the Federal Court"; and,
- (4) The Federal Court largely accepted CSIS' proposals regarding technical amendments to CSIS Act warrant templates.

#### Q4: How has the Government responded?

The Government accepts the Federal Court's ruling that CSIS' retention of non-threat related associated data is not authorized by the *CSIS Act* and further accepts the Court's finding that CSIS breached its duty of candour. The decision will not be appealed.

CSIS has taken immediate action to address the Federal Court's findings and has halted all access to and analysis of associated data until CSIS can further assess the decision and put in place measures to comply with the Federal Court's ruling. CSIS is also working with Justice Canada to ensure that it is fully transparent with the Court.

### CONTACTS:

Prepared by

[Redacted]

[Redacted]

A/Director, Intelligence Policy

Tel. no.

[Redacted]

[Redacted]

Approved by (ADM level only)

Monik Beauregard,  
Senior Assistant Deputy Minister,  
National and Cyber Security Branch

Tel. no.

613-990-4976

**Coates, Liza-Ann (PS/SP)**

---

**From:** Brien, Dan (PS/SP)  
**Sent:** Thursday, November 10, 2016 8:28 AM  
**To:** Tomlinson, Jamie (PS/SP)  
**Subject:** FW: Message to CSIS Management (3)  
**Attachments:** Message to CSIS Management (3).docx

FYI

**From:** Brien, Dan (PS/SP)  
**Sent:** Thursday, November 10, 2016 8:26 AM  
**To:** [REDACTED]  
**Subject:** Message to CSIS Management (3)



We also have to come to ground on how it's distributed – I'd welcome your recommendations on that too.

Thanks

Dan

Dan Brien  
Director, Communications / Directeur des communications  
Office of the Minister of Public Safety and Emergency Preparedness / Bureau du Ministre de la Sécurité publique et de la Protection civile  
Tel.:613.949.6473  
Mobile:613.698.2270

**Draft**

Message to CSIS [REDACTED]

Formatted: Font: Bold

Formatted: Centered

Last week's Federal Court decision on the Service's retention and analysis of "associated date" data

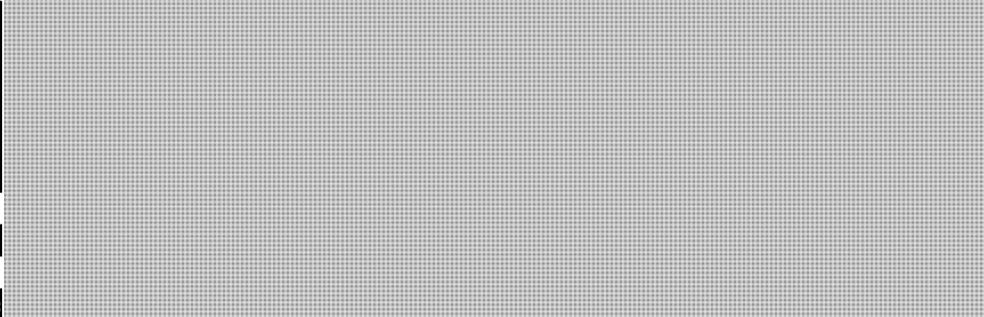
The Government of Canada is committed to keeping Canadians safe while at the same time safeguarding our freedoms, rights and values in an open and democratic society. Public confidence in our institutions, including your work, relies on both parts of this commitment. Effective scrutiny and oversight are central to it.

The unprecedented public communications efforts by the Director, and the immediate steps the Service took to address the court's decision will ultimately help bolster confidence, as will the Security Intelligence Review Committee's monitoring of implementation. Trust will be further bolstered by Bill C-22, the National Security and Intelligence Committee of Parliamentarians Act, which will strengthen accountability for national security across government.

Formatted: Font: Italic

On October 24th, in my remarks to the annual CSIS management conference, I spoke about the consultations currently underway on our national security framework and the opportunity this presents for us to update our legislation, policies and practices for a digital age. I also spoke of the professionalism and outstanding dedication that the men and women of CSIS demonstrate every day as they carry out the difficult work of keeping Canada safe.

Formatted: Superscript



Ralph Goodale  
Minister of Public Safety and Emergency Preparedness

**Coates, Liza-Ann (PS/SP)**

---

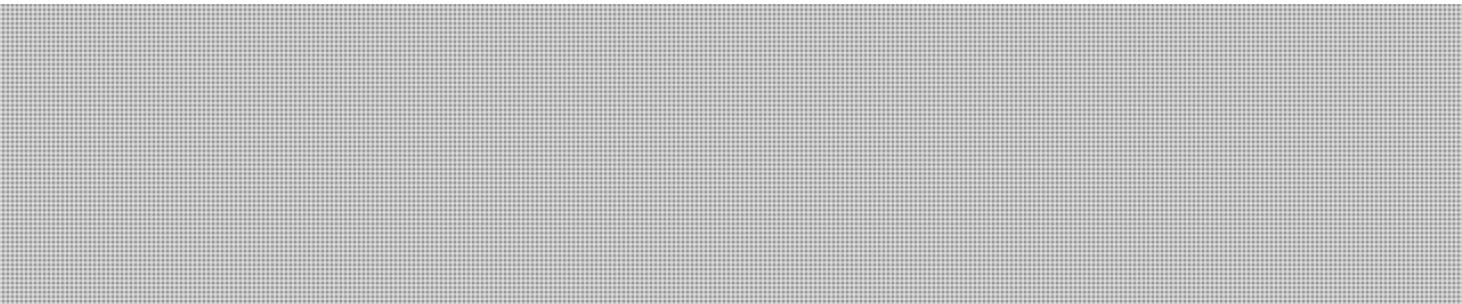
**From:** Brien, Dan (PS/SP)  
**Sent:** Tuesday, November 08, 2016 4:46 PM  
**To:** [REDACTED]  
**Cc:** Tomlinson, Jamie (PS/SP)  
**Subject:** Re: Further edits - comments?

Good point. I'll talk to him tonight.

db mobile  
613.698.2270

**From:** [REDACTED]  
**Sent:** Tuesday, November 8, 2016 4:41 PM  
**To:** Brien, Dan (PS/SP)  
**Cc:** Tomlinson, Jamie (PS/SP)  
**Subject:** RE: Further edits - comments?

Thanks Jamie, and Dan for offering and putting together this message.

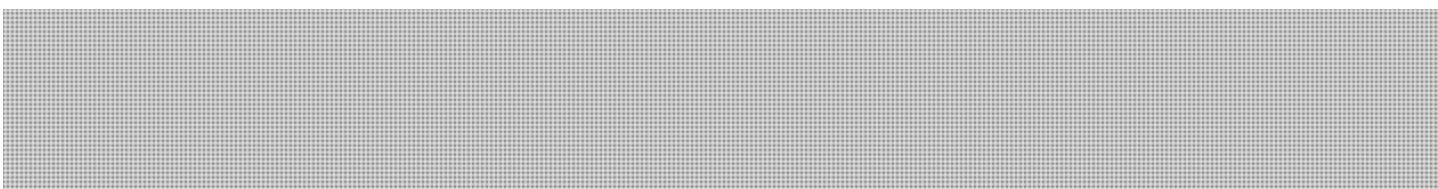


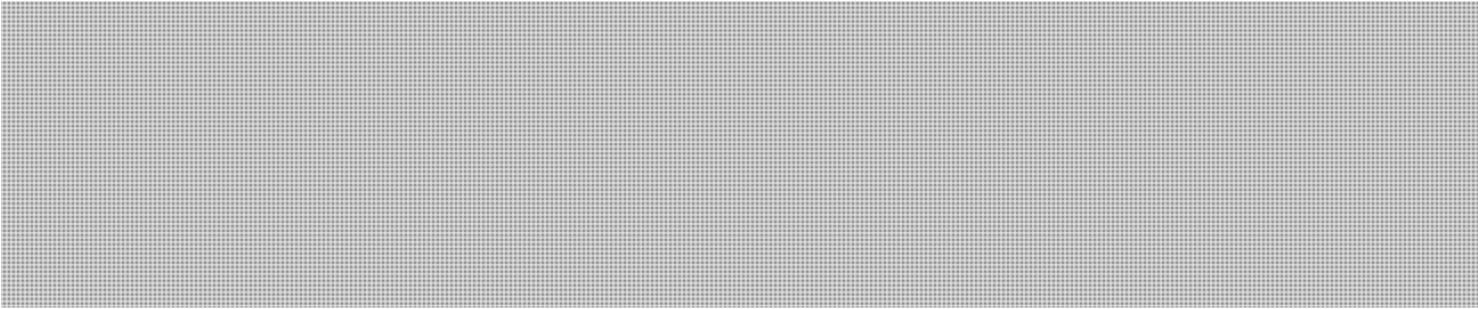
**From:** Brien, Dan (PS/SP) [<mailto:dan.brien@canada.ca>]  
**Sent:** 8-Nov-16 3:57 PM  
**To:** Tomlinson, Jamie (PS/SP); [REDACTED]  
**Subject:** RE: Further edits - comments?

Thanks!

**From:** Tomlinson, Jamie (PS/SP)  
**Sent:** Tuesday, November 08, 2016 3:45 PM  
**To:** Brien, Dan (PS/SP); [REDACTED]  
**Subject:** RE: Further edits - comments?

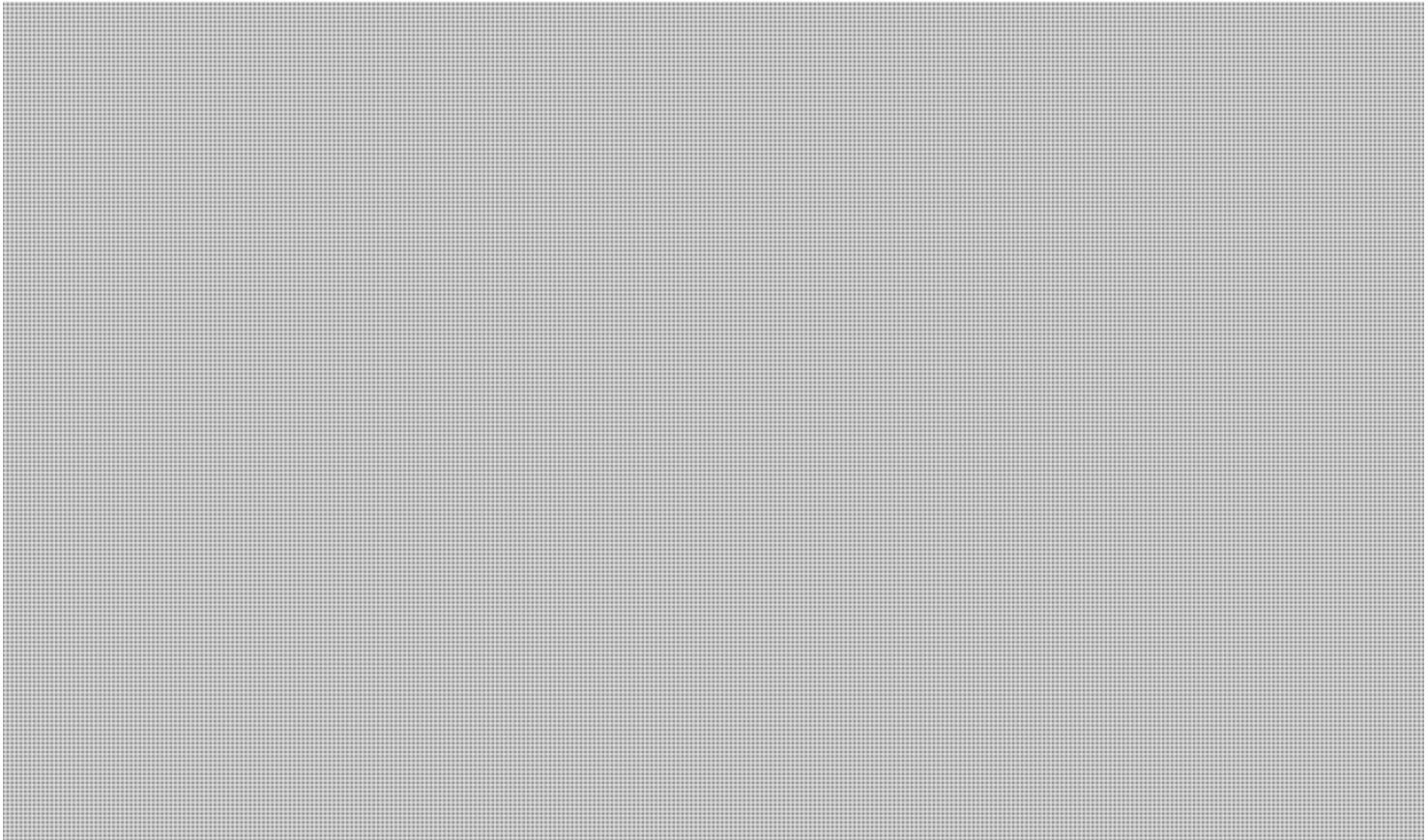
IMHO...





**From:** Brien, Dan (PS/SP)  
**Sent:** November-08-16 3:20 PM  
**To:** [REDACTED] Tomlinson, Jamie (PS/SP)  
**Subject:** Further edits - comments?

Draft



Ralph Goodale  
Minister of Public Safety and Emergency Preparedness

Thanks

Dan Brien  
Director, Communications / Directeur des communications  
Office of the Minister of Public Safety and Emergency Preparedness / Bureau du Ministre de la Sécurité publique et de la Protection civile

**Tel.:613.949.6473**  
**Mobile:613.698.2270**

**Coates, Liza-Ann (PS/SP)**

---

**From:** [REDACTED]  
**Sent:** Sunday, November 06, 2016 9:52 AM  
**To:** COMDO / COMDO (PS/SP); Baker3, Ryan (PS/SP); Tomlinson, Jamie (PS/SP)  
**Subject:** Re: Follow-up: ST by CSIS Director re. Operational Data Analysis Centre

Thanks again for everyone's help.

I think/hope we will be done for urgent statements for the next little while (touch wood).

[REDACTED]  
DG, Communications  
[REDACTED]

@csiscanada / @scrscanada

**From:** COMDO / COMDO (PS/SP)  
**Sent:** Sunday, November 6, 2016 9:39 AM  
**To:** [REDACTED] Baker3, Ryan (PS/SP); Tomlinson, Jamie (PS/SP)  
**Cc:** PS.F Media Monitoring / surveillance des médias F.SP; Ministerial Liaison / Liaison ministerielle (PS/SP)  
**Subject:** Follow-up: ST by CSIS Director re. Operational Data Analysis Centre

Good morning,

The STATEMENT has been posted to the wire and emailed to the press gallery.

**Wire:**

<http://www.newswire.ca/en/releases/archive/November2016/06/c1028.html>  
<http://www.newswire.ca/fr/releases/archive/November2016/06/c8528.html>

**Mo Hashash**

Communications Duty Officer/ Agent de service des communications  
Public Safety Canada / Sécurité publique Canada  
Tel.: (613) 991-7010  
Email/courriel: [ps.comdo-comdo.sp@canada.ca](mailto:ps.comdo-comdo.sp@canada.ca)

**Coates, Liza-Ann (PS/SP)**

---

**From:** Public Safety / Sécurité Publique (PS/SP)  
**Sent:** Sunday, November 06, 2016 9:33 AM  
**To:** Public Safety / Sécurité Publique (PS/SP)  
**Subject:** Statement / Déclaration : CSIS Director statement regarding the Operational Data Analysis Centre / Déclaration du directeur du SCRS au sujet du Centre d'analyse de données opérationnelles

From the Canadian Security Intelligence Service:

## **Statement - CSIS Director statement regarding the Operational Data Analysis Centre**

OTTAWA, Nov. 6, 2016 /CNW/ - The Director of the Canadian Security Intelligence Service, Michel Coulombe, issued the following statement today regarding the recent Federal Court decision and the Service's Operational Data Analysis Centre (ODAC):

"Given recent media coverage, as I indicated in my previous statement and in the news conference when the Federal Court's ruling was issued, I would like to reiterate that all associated data was legally collected under warrants. CSIS, in consultation with the Department of Justice, interpreted the *CSIS Act* to allow for the retention of non-threat related associated data linked with third party communications that were collected while under warrant. The Federal Court has disagreed with this interpretation and we accept their decision. I would like to make it clear that the Service was not knowingly exceeding the scope of the *CSIS Act*.

I would like to address the apparent perception that the Service created and operated ODAC without the knowledge of key government stakeholders.

ODAC was created in 2006 to derive more value from the data already being collected under warrant using data exploitation techniques. The creation of ODAC and this core operational capability was presented to the Minister of Public Safety in July 2006 explaining the requirement for advanced data analytics and the ability of ODAC to retain data, including metadata, for extended periods of time. The Minister was also briefed on the program in March 2010. Information was also shared over the years with various government stakeholders, including the Security Intelligence Review Committee (SIRC), the Privacy Commissioner, including a Privacy Impact Assessment, and the Inspector General of CSIS.

The CSIS 2007-08 Public Report also refers to ODAC, noting the support being provided to its operational branches through the performance of advanced analysis of data, and the program was described over the years in the Directors' Annual Reports to the Minister.

Given the Service and Department of Justice interpretation that the activity in question was within the scope of the *CSIS Act*, these briefings may not have specifically addressed the retention of the sub-set of associated data on which the Court has now ruled. The intent of the Service, however, was to ensure key stakeholders were aware of ODAC, its capabilities, and intentions around retention.

SIRC reviewed CSIS' use of associated data and published its findings on the issue in its 2014-15 annual report. SIRC did not conclude that the retention of associated data was illegal, but did suggest that the Federal Court be made aware.

As I noted in my previous statement, CSIS agrees that the Court should have been informed earlier of the existence of ODAC and the approach to data retention, and acknowledges this was a significant omission. At no point did CSIS deliberately seek to withhold this information from the Court, and the Court acknowledged that there is no evidence to suggest CSIS did.

CSIS recognizes the importance of maintaining public trust and confidence in its activities. CSIS takes very seriously the privacy considerations related to its work, and it is committed to ensuring that its activities are in compliance with all legislation and Ministerial Direction."

SOURCE Canadian Security Intelligence Service (CSIS)

For further information: CSIS Media Relations, [media-medias@smtp.gc.ca](mailto:media-medias@smtp.gc.ca), 613-231-0100

---

Envoi du Service canadien du renseignement de sécurité :

## **Déclaration - Déclaration du directeur du SCRS au sujet du Centre d'analyse de données opérationnelles**

OTTAWA, le 6 nov. 2016 /CNW/ - Le directeur du Service canadien du renseignement de sécurité (SCRS), Michel Coulombe, a fait la déclaration suivante au sujet de la décision récente de la Cour fédérale et du Centre d'analyse de données opérationnelles (CADO) du Service :

« Étant donné la couverture médiatique récente, tel que je l'ai indiqué dans mon énoncé antérieur et au moment de la conférence de presse lorsque la décision de la Cour fédérale a été rendue, je souhaite répéter que toutes les données connexes ont été recueillies légalement en vertu d'un mandat. Selon l'interprétation du SCRS, en consultation avec le ministère de la Justice, la *Loi sur le SCRS* autorisait la conservation de données connexes liées à des communications de tiers et non-relées à une menace qui ont été recueillies en vertu d'un mandat. La Cour fédérale n'a pas souscrit à cette interprétation et nous acceptons sa décision. Je souhaite préciser que le Service n'a pas sciemment excédé la portée de la *Loi sur le SCRS*.

Je souhaite aborder la perception apparente selon laquelle le Service a créé et exploité le CADO à l'insu des principaux intervenants du gouvernement.

Le CADO a été créé en 2006 afin de tirer une plus grande valeur des données déjà recueillies en vertu d'un mandat au moyen de techniques d'exploitation de données. La création du CADO et de ses principales capacités opérationnelles a été présentée au ministre de la Sécurité publique en juillet 2006, expliquant l'exigence d'analyses avancées et de la capacité du SCRS de conserver des données, y compris les métadonnées, pendant de longues périodes. Le ministre a également été informé au sujet du programme en mars 2010. Les renseignements ont également été communiqués, aux cours des années, à divers intervenants du gouvernement,

y compris le Comité de surveillance des activités de renseignement de sécurité (CSARS), le Commissaire à la protection de la vie privée, y compris une évaluation des facteurs relatifs à la vie privée, et l'inspecteur général du SCRS.

Le Rapport public 2007-2008 du SCRS renvoie également au CADO, notant le soutien fourni à ses secteurs opérationnels dans le cadre de l'exécution d'analyses avancées des données et le programme a été décrit au cours des années dans les rapports annuels du directeur à présenter au ministre.

Étant donné l'interprétation du Service et du ministère de la Justice selon laquelle l'activité en question relevait de la portée de la *Loi sur le SCRS*, il se peut que ces séances d'information n'aient pas abordé particulièrement la conservation du sous-ensemble de données connexes visées par la décision de la Cour. Toutefois, l'intention du Service était de s'assurer que les principaux intervenants étaient au courant du CADO, de ses capacités et de ses intentions en ce qui concerne la conservation.

Le CSARS a examiné l'utilisation par le SCRS de données connexes et a publié ses conclusions sur cette question dans son rapport annuel de 2014-2015. Le CSARS n'a pas conclu que la conservation de données connexes était illégale, mais il a suggéré que la Cour fédérale en soit informée.

Tel que je l'ai indiqué dans mon énoncé antérieur, le SCRS convient que la Cour aurait dû être informée plus tôt de l'existence du CADO et de l'approche en matière de conservation de données, et reconnaît qu'il s'agissait d'une omission importante. Jamais le SCRS n'a cherché intentionnellement à cacher cette information à la Cour et cette dernière reconnaît que rien dans la preuve ne porte à le croire.

Le SCRS reconnaît qu'il est important de maintenir la confiance du public et celle à l'égard de ses activités. Le SCRS prend très au sérieux les facteurs liés à la vie privée relativement à son travail et il s'est engagé à s'assurer que ses activités sont conformes à toutes les dispositions législatives et à l'orientation ministérielle. »

SOURCE Service canadien du renseignement de sécurité (SCRS)

Renseignements : Relations avec les médias du SCRS, [media-medias@smtp.gc.ca](mailto:media-medias@smtp.gc.ca), 613-231-0100

## Coates, Liza-Ann (PS/SP)

---

**From:** MacKinnon, Paul (PS/SP)  
**Sent:** Sunday, November 06, 2016 9:46 AM  
**To:** Tomlinson, Jamie (PS/SP); Cintrat, Jean (PS/SP)  
**Cc:** Nguyen, Linda (PS/SP)  
**Subject:** Re: Timeline

Hi folks

Agree Second services would be the best place (if indeed it came through there). We do though need to pause for a moment and not just hand over advice prepared for a previous government and Minister. So, anything during past year, great. Previously, needs discussion.

Sent from my BlackBerry 10 smartphone on the Rogers network.

**From:** Tomlinson, Jamie (PS/SP)  
**Sent:** Sunday, November 6, 2016 8:07 AM  
**To:** Cintrat, Jean (PS/SP); MacKinnon, Paul (PS/SP)  
**Subject:** Fw: Timeline

Paul, Jean,

Last night CSIS provided the timeline below to the MO. Dan came back and said the Minister would like to see the previous briefing notes (I'm not sure if any have been redacted and released via ATIP or whether they are all still classified). CSIS is of a view that this request is best handled through Secretariat Services.

Thoughts?

Sent from my BlackBerry 10 smartphone on the Rogers network.

**From:** Tomlinson, Jamie (PS/SP) <[jamie.tomlinson@canada.ca](mailto:jamie.tomlinson@canada.ca)>  
**Sent:** Saturday, November 5, 2016 6:35 PM  
**To:** Brown, Malcolm (PS/SP); Wilson, Gina (PS/SP); Beauregard, Monik (PS/SP)  
**Cc:** MacKinnon, Paul (PS/SP); De Santis, Heather (PS/SP)  
**Subject:** Timeline

CSIS has also developed a timeline - not to be issued but to provide information on sequencing. They have also provided this to the Minister's Office.

Timeline – Draft

**Page 94**

**is withheld pursuant to sections  
est retenue en vertu des articles**

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

**Coates, Liza-Ann (PS/SP)**

---

**From:** Brien, Dan (PS/SP)  
**Sent:** Sunday, November 06, 2016 9:18 AM  
**To:** Tomlinson, Jamie (PS/SP); [REDACTED] Baker3, Ryan (PS/SP); COMDO / COMDO (PS/SP)  
**Subject:** Re: FINAL statement (Eng and Fr)

Thank you all.

db mobile  
613.698.2270

**From:** Tomlinson, Jamie (PS/SP)  
**Sent:** Sunday, November 6, 2016 9:02 AM  
**To:** [REDACTED] Baker3, Ryan (PS/SP); COMDO / COMDO (PS/SP)  
**Cc:** Brien, Dan (PS/SP)  
**Subject:** Re: FINAL statement (Eng and Fr)

We'll get it out.

Sent from my BlackBerry 10 smartphone on the Rogers network.

**From:** [REDACTED]  
**Sent:** Sunday, November 6, 2016 8:53 AM  
**To:** Baker3, Ryan (PS/SP); Tomlinson, Jamie (PS/SP); COMDO / COMDO (PS/SP)  
**Cc:** Brien, Dan (PS/SP)  
**Subject:** FINAL statement (Eng and Fr)

Jamie,

Attached is the final statement, approved by the Director.

Dan, only change to English since last night was formatting.

French tweaked by the DIR this a.m.

Ready to be issued to the wire and press gallery as soon as is possible.

Many thanks again for your assistance.



DG, Communications

[REDACTED]  
@csiscanada / @scrsCanada

**Coates, Liza-Ann (PS/SP)**

---

**From:** Brien, Dan (PS/SP)  
**Sent:** Sunday, November 06, 2016 7:47 AM  
**To:** [REDACTED] Baker3, Ryan (PS/SP); Tomlinson, Jamie (PS/SP)  
**Subject:** Re: Director Statement - tonight

Thanks.

db mobile  
613.698.2270

**From:** [REDACTED]  
**Sent:** Sunday, November 6, 2016 6:56 AM  
**To:** Brien, Dan (PS/SP); Baker3, Ryan (PS/SP); Tomlinson, Jamie (PS/SP)  
**Subject:** Re: Director Statement - tonight

Thanks Dan.

I've sent Eng and Fr to the DIR this morning and will confirm issuing it at 9:00 am hopefully shortly.

I have sent your request re. previous BNs internally. Will let you know the timeline, documents, etc. as soon as I have details.

[REDACTED]

---

**From:** Brien, Dan (PS/SP)  
**Sent:** Sunday, November 6, 2016 2:01 AM  
**To:** [REDACTED] Baker3, Ryan (PS/SP); Tomlinson, Jamie (PS/SP)  
**Subject:** Re: Director Statement - tonight

Minister is back from the Lieutenant-Governor's gala with CDS Vance.

He has approved the statement.

He'd like to see the previous briefing notes - have they all been redacted for imminent release, or just the most recent ones?

I can relay whatever is unclassified. If some of the older ones (even last year's) pose a concern, we can arrange to have them sent safely via the regional office. None of the above should delay the issuance of the statement, however.

Please let me know when the text is confirmed final.

Thanks.

db mobile  
613.698.2270

---

**From:** [REDACTED]  
**Sent:** Saturday, November 5, 2016 9:47 PM  
**To:** Brien, Dan (PS/SP); Baker3, Ryan (PS/SP); Tomlinson, Jamie (PS/SP)  
**Subject:** Re: Director Statement - tonight

Great, thanks.

[REDACTED]  
DG, Communications

[REDACTED]  
@csiscanada / @scrscanada

**From:** Brien, Dan (PS/SP)  
**Sent:** Saturday, November 5, 2016 9:46 PM  
**To:** [REDACTED] Baker3, Ryan (PS/SP); Tomlinson, Jamie (PS/SP)  
**Subject:** Re: Director Statement - tonight

If the plan is morning, i'll stand by for minister's green light and relay asap

db mobile  
613.698.2270

---

**From:** Brien, Dan (PS/SP)  
**Sent:** Saturday, November 5, 2016 9:31 PM  
**To:** [REDACTED] Baker3, Ryan (PS/SP); Tomlinson, Jamie (PS/SP)  
**Subject:** Re: Director Statement - tonight

Staff is fine. But minister is at the lieutenant-Governor's ball and may be off the berry for a bit.

db mobile  
613.698.2270

---

**From:** [REDACTED]  
**Sent:** Saturday, November 5, 2016 9:07 PM  
**To:** Baker3, Ryan (PS/SP); Brien, Dan (PS/SP); Tomlinson, Jamie (PS/SP)  
**Subject:** Re: Director Statement - tonight

Dan,  
Let me know what your office thinks. DIR wants to be sure before we issue.

[REDACTED]

---

**From:** [REDACTED]  
**Sent:** Saturday, November 5, 2016 9:02 PM  
**To:** Baker3, Ryan (PS/SP); Brien, Dan (PS/SP); Tomlinson, Jamie (PS/SP)  
**Subject:** Re: Director Statement - tonight

Looking like first thing tomorrow is more likely. 9:00 a.m. preferably.

[REDACTED]  
DG, Communications

[REDACTED]  
@csiscanada / @scrscanada

**From:** Baker3, Ryan (PS/SP)  
**Sent:** Saturday, November 5, 2016 9:01 PM  
**To:** [REDACTED] Brien, Dan (PS/SP); Tomlinson, Jamie (PS/SP)  
**Subject:** Re: Director Statement - tonight

Getting the French updated.

Do you still want to issue tonight or wait until morning?

Ryan

Ryan Baker  
Public Safety Canada/ Sécurité publique Canada  
613-796-9750

**From:** [REDACTED]  
**Sent:** Saturday, November 5, 2016 8:52 PM  
**To:** Baker3, Ryan (PS/SP); Brien, Dan (PS/SP); Tomlinson, Jamie (PS/SP)  
**Subject:** Re: Director Statement - tonight

Here is the version that incorporates almost all of PCO's suggested changes.

[REDACTED]  
DG, Communications

[REDACTED]  
@csiscanada / @scrscanada

**From:** Baker3, Ryan (PS/SP)  
**Sent:** Saturday, November 5, 2016 8:46 PM  
**To:** [REDACTED] Brien, Dan (PS/SP); Tomlinson, Jamie (PS/SP)  
**Subject:** Re: Director Statement - tonight

Standing by.

Ryan Baker  
Public Safety Canada/ Sécurité publique Canada  
613-796-9750

**From:** [REDACTED]  
**Sent:** Saturday, November 5, 2016 8:35 PM  
**To:** Brien, Dan (PS/SP); Tomlinson, Jamie (PS/SP)  
**Cc:** Baker3, Ryan (PS/SP)  
**Subject:** Re: Director Statement - tonight

Thanks. Pco has provided some editing to tighten it up but all elements are still conveyed.

Ryan, will have a tracked changes version for you shortly.

[REDACTED]  
DG, Communications

[REDACTED]  
@csiscanada / @scrscanada

**From:** Brien, Dan (PS/SP)  
**Sent:** Saturday, November 5, 2016 8:31 PM  
**To:** [REDACTED] Tomlinson, Jamie (PS/SP)  
**Cc:** Baker3, Ryan (PS/SP)  
**Subject:** Re: Director Statement - tonight

Won't be much trouble - pmo likes it.

db mobile  
613.698.2270

**From:** [REDACTED]  
**Sent:** Saturday, November 5, 2016 6:50 PM  
**To:** Brien, Dan (PS/SP); Tomlinson, Jamie (PS/SP)  
**Cc:** Baker3, Ryan (PS/SP)  
**Subject:** Re: Director Statement - tonight

Ok, thanks. Just sent.

**From:** Brien, Dan (PS/SP)  
**Sent:** Saturday, November 5, 2016 6:46 PM  
**To:** [REDACTED] Tomlinson, Jamie (PS/SP)  
**Cc:** Baker3, Ryan (PS/SP)  
**Subject:** Re: Director Statement - tonight

I think a pco check now is probably a good idea.

db mobile  
613.698.2270

**From:** [REDACTED]  
**Sent:** Saturday, November 5, 2016 5:51 PM  
**To:** Tomlinson, Jamie (PS/SP); Brien, Dan (PS/SP)  
**Cc:** Baker3, Ryan (PS/SP)  
**Subject:** Director Statement - tonight

Jamie, Dan,

As discussed, we would like to issue the attached statement tonight. Please advise of any concerns. The attached timeline would not be issued tonight but may be helpful in briefing on the sequence.

Jamie, can your team start the urgent translation on the statement?

Dan, do you want me to wait before sending to PCO?



DG, Communications



@csiscanada / @scrscanada

**Coates, Liza-Ann (PS/SP)**

---

**From:** MacKinnon, Paul (PS/SP)  
**Sent:** Saturday, November 05, 2016 8:07 PM  
**To:** Tomlinson, Jamie (PS/SP)  
**Subject:** Re: Revised statement

Thanks for this Jamie.

Sent from my BlackBerry 10 smartphone on the Rogers network.

**From:** Tomlinson, Jamie (PS/SP)  
**Sent:** Saturday, November 5, 2016 6:32 PM  
**To:** Brown, Malcolm (PS/SP); Wilson, Gina (PS/SP); Beauregard, Monik (PS/SP)  
**Cc:** MacKinnon, Paul (PS/SP); De Santis, Heather (PS/SP)  
**Subject:** Revised statement

CSIS advises they have done a bit of wordsmithing. Updated version below:

STATEMENT

Ottawa, [REDACTED]

The Director of the Canadian Security Intelligence Service, Michel Coulombe, issued the following statement today regarding the recent Federal Court decision and the Service's Operational Data Analysis Centre (ODAC):

"As I indicated in my previous statement ([hyperlink](#)), and in the news conference when the Federal Court's ruling was issued, all associated data was legally collected under warrants. CSIS, in consultation with the Department of Justice, interpreted the *CSIS Act* to allow for the retention of non-threat related associated data linked with third party communications that were collected while under warrant. The Federal Court has disagreed with this interpretation and we accept their decision. I would like to reiterate that the Service was not knowingly exceeding the scope of the *CSIS Act*.

As for ODAC, it was created in 2006 to derive more value from the data already being collected under warrant using data exploitation techniques.

I would like to address the apparent perception that the Service created and operated ODAC without the knowledge of key government stakeholders.

The creation of ODAC and this core operational capability was presented to the Minister of Public Safety in July 2006, explaining the requirement for advanced data analytics and the ability of ODAC to retain data, including metadata, for extended periods of time.

[REDACTED] The CSIS 2007-08 Public Report ([hyperlink](#)) also refers to ODAC, the support being provided to its operational branches through the performance of advanced analysis of data.

In March 2010, [REDACTED] Minister of Public Safety was briefed [REDACTED]

Given the Service and Department of Justice interpretation that the activity in question was within the scope of the *CSIS Act*, these briefings may not have specifically addressed the retention of the sub-set of associated data on which the Court has now ruled. The intent of the Service, however, was to ensure key stakeholders were aware of ODAC, its capabilities, and intentions around retention.

SIRC reviewed CSIS' use of associated data and published its findings on the issue in its 2014-15 annual report. SIRC did not conclude that the retention of associated data was illegal, but did suggest that the Federal Court be made aware.

CSIS agrees that the Court should have been informed earlier of the existence of ODAC and the approach to data retention, and acknowledges this was a significant omission. At no point did CSIS deliberately seek to withhold this information from the Court, and the Court acknowledged that there is no evidence to suggest we did.

CSIS recognizes the importance of maintaining public trust and confidence in its activities. CSIS takes very seriously the privacy considerations related to its work, and it is committed to ensuring that its activities are in compliance with all legislation and Ministerial Direction.”

**Contact:**

CSIS Media Relations

[media-medias@smtp.gc.ca](mailto:media-medias@smtp.gc.ca)

[613-231-0100](tel:613-231-0100)

## Arbeau, Kristy (PS/SP)

---

**From:** Brien, Dan (PS/SP)  
**Sent:** Friday, November 04, 2016 5:43 PM  
**To:** Ministerial Liaison / Liaison ministerielle (PS/SP); Bardsley, Scott (PS/SP); Peirce, Hilary (PS/SP)  
**Cc:** Tomlinson, Jamie (PS/SP); Nichols, Megan (PS/SP); Baker3, Ryan (PS/SP); Magee, Heather (PS/SP); Wilson, Ashleigh (PS/SP); Grenier, Julie (PS/SP); Miller, Kevin (PS/SP); Duval, Jean Paul (PS/SP); MacLean, Megan (PS/SP); O'Connell, Heather (PS/SP); Cibula, Colette (PS/SP); Crépeault, David (PS/SP); Wilcox, Brent (PS/SP); PS.F Speeches / Discours F.SP  
**Subject:** RE: E-binder: Federal Court / CSIS associated data - November 3 - Ottawa

Thanks!

Have a good weekend!

---

**From:** Ministerial Liaison / Liaison ministerielle (PS/SP)  
**Sent:** Friday, November 04, 2016 5:36 PM  
**To:** Brien, Dan (PS/SP); Bardsley, Scott (PS/SP); Peirce, Hilary (PS/SP)  
**Cc:** Tomlinson, Jamie (PS/SP); Nichols, Megan (PS/SP); Baker3, Ryan (PS/SP); Magee, Heather (PS/SP); Wilson, Ashleigh (PS/SP); Grenier, Julie (PS/SP); Miller, Kevin (PS/SP); Duval, Jean Paul (PS/SP); MacLean, Megan (PS/SP); O'Connell, Heather (PS/SP); Cibula, Colette (PS/SP); Crépeault, David (PS/SP); Wilcox, Brent (PS/SP); PS.F Speeches / Discours F.SP; Ministerial Liaison / Liaison ministerielle (PS/SP)  
**Subject:** E-binder: Federal Court / CSIS associated data - November 3 - Ottawa

Dan, Scott, Hilary,

Please find attached, the final MO and PCO approved communications products for the Federal Court's decision regarding CSIS's retention of associated data.

### PS Products:

- Media Advisory (English and French)
- Ministerial Statement (English and French)
- Speech for Minister Goodale (English and French)
- Key Messages (English and French)
- Questions and Answers (English only)

### CSIS Products

- Statement for Director (English and French)
- Backgrounder (English and French)

Regards,  
Lucie

**Lucie Taillefer**  
**Ministerial Services | Services ministériels**  
Public Safety Canada | Sécurité publique Canada  
E-mail | Courriel : [Lucie.taillefer@canada.ca](mailto:Lucie.taillefer@canada.ca)  
Telephone | Téléphone : 613-991-9492

## Arbeau, Kristy (PS/SP)

---

**From:** Ministerial Liaison / Liaison ministerielle (PS/SP)  
**Sent:** Friday, November 04, 2016 5:36 PM  
**To:** Brien, Dan (PS/SP); Bardsley, Scott (PS/SP); Peirce, Hilary (PS/SP)  
**Cc:** Tomlinson, Jamie (PS/SP); Nichols, Megan (PS/SP); Baker3, Ryan (PS/SP); Magee, Heather (PS/SP); Wilson, Ashleigh (PS/SP); Grenier, Julie (PS/SP); Miller, Kevin (PS/SP); Duval, Jean Paul (PS/SP); MacLean, Megan (PS/SP); O'Connell, Heather (PS/SP); Cibula, Colette (PS/SP); Crépeault, David (PS/SP); Wilcox, Brent (PS/SP); PS.F Speeches / Discours F.SP; Ministerial Liaison / Liaison ministerielle (PS/SP)  
**Subject:** E-binder: Federal Court / CSIS associated data - November 3 - Ottawa  
**Attachments:** PS-SP-#1995114-v1G-Key\_Messages\_-\_FCC\_Associated\_Data REV-PCO.DOC; PS-SP-#1995114-v1G-Key\_Messages\_-\_FCC\_Associated\_Data REV-PCO-tef.doc; PS-SP-#1997111-1-Speaking Notes - FCC Associated Data.docx; PS-SP-#1999749-v1-Speaking\_Notes\_-\_FCC\_Associated\_Data\_FRENCH.DOCX; PS-SP-#1995596-v2-Qs&As\_-\_FCC\_Associated\_Data.doc; PS-SP-#1997213-v1C-Statement - FCC Associated Data.doc; PS-SP-#1998418-v1B-Statement\_FCC\_Associated\_Data\_FRENCH.DOC; Director Statement - French (November 3 with new paragraph tm.docx; Director Statement English (November 3) with new paragraph tm.docx; Backgrounder - Formatted French (November 4).docx; Backgrounder English Formatted (November 4).docx; PS-SP-#2014527-1-MA re CSIS Media Avial and Tech Breifing November 3 201....docx

Dan, Scott, Hilary,

Please find attached, the final MO and PCO approved communications products for the Federal Court's decision regarding CSIS's retention of associated data.

### PS Products:

- Media Advisory (English and French)
- Ministerial Statement (English and French)
- Speech for Minister Goodale (English and French)
- Key Messages (English and French)
- Questions and Answers (English only)

### CSIS Products

- Statement for Director (English and French)
- Backgrounder (English and French)

Regards,  
Lucie

**Lucie Taillefer**

**Ministerial Services | Services ministériels**

Public Safety Canada | Sécurité publique Canada

E-mail | Courriel : [Lucie.taillefer@canada.ca](mailto:Lucie.taillefer@canada.ca)

Telephone | Téléphone : 613-991-9492

Mobile | Cellulaire : 613-219-5435

Government of Canada | Gouvernement du Canada

[www.publicsafety.gc.ca](http://www.publicsafety.gc.ca) | [www.securitepublique.gc.ca](http://www.securitepublique.gc.ca)

# *Media Advisory / Avis aux médias*

## **For Immediate Release**

Thursday, November 3, 2016

## **Canadian Security Intelligence Service and Justice Canada to hold media availability, followed by technical briefing**

Michel Coulombe, Director of the Canadian Security Intelligence Service (CSIS), and Robert Frater, Chief General Counsel for Justice Canada, will hold a media availability on a recent Federal Court decision.

Following the media availability, CSIS and Justice Canada officials will conduct a background technical briefing for the media via teleconference. The briefing is for background information only and not for attribution.

### **Date**

Thursday, November 3, 2016

### **Media Availability**

#### **Time**

5:00 p.m. EDT

#### **Location**

National Press Theatre  
150 Wellington Street  
Ottawa, ON

Media who wish to listen-in live to the event can use the numbers below. This is a listen-only line. Participating media can call in as early as 4:45 p.m. EDT - local time.

Journalists who are not members of the National Press Gallery will require accreditation from the gallery in advance. For more information, contact Collin Lafrance at [collin.lafrance@parl.gc.ca](mailto:collin.lafrance@parl.gc.ca).

#### **Teleconference: LISTEN-ONLY**

**Access numbers / Toll free (Canada and U.S.):** 613-960-7527 / 877-413-4815

**Access Code:** 4974802

### **Media Technical Briefing (Teleconference Only)**

#### **Time**

6:15 p.m. EDT



# *Media Advisory / Avis aux médias*

Participating media can call in as early as 6:00 p.m. EDT - local time.

## **Media Technical Briefing**

### **Participant dial-in numbers:**

**Access numbers / Toll free (Canada and U.S.):** 613-960-7526 / 877-413-4814

**Access Code:** 7556997

## **Information :**

Media Relations

Canadian Security Intelligence Service

613-231-0100

[media-medias@smtp.gc.ca](mailto:media-medias@smtp.gc.ca)

**Pages 107 to / à 108  
are not relevant  
sont non pertinentes**



Canadian  
Security  
Intelligence  
Service

Service  
canadien du  
renseignement  
de sécurité

## BACKGROUND

*Federal Court ruling on the retention of associated data linked to third party information.*

- CSIS takes seriously the concerns expressed by the Court with respect to meeting our duty of candour, and recognizes the importance of openness and transparency with the Federal Court.
- CSIS is working closely with the Department of Justice to develop measures aimed at ensuring that we meet our obligations to the Court in matters of transparency and duty of candour.
- The Canadian Security Intelligence Service is mandated to investigate activities which may, on reasonable grounds, be suspected of posing a threat to the security of Canada. In order to investigate these threats, CSIS may apply to the Federal Court for a warrant when the response to the threat requires more intrusive measures.
- Through the proceedings of the Court, over time, the provisions of warrants have changed to take into account the evolution of technology, legal developments, and investigative measures.
- This ensures that the powers granted by the warrants are clearly defined and that their conditions take into account the impact that the execution of the warrant has on the collection and the retention of information.
- The decision relates to the retention of certain information that has been legally collected via the execution of warrants, issued by the Court, which authorized the interception of communications.
- CSIS had sought to fully analyze all of the information - both the content and the associated data - for example, email addresses and telephone numbers.
- As is the case for many of our international partners, CSIS has developed data analytic capabilities and expertise to significantly enhance the identification and assessment of threats to the security of Canada over time and space. This includes identifying patterns of movement, communications, behaviours, broad trends, and links that are otherwise unidentifiable.



Canadian  
Security  
Intelligence  
Service | Service  
canadien du  
renseignement  
de sécurité

- When it comes to understanding and predicting the actions of the subjects of our investigations, data analytics has proven to be an effective tool.
- In the ruling released today, the Federal Court recognized the intelligence value of the data analytic programme and did not question the authority of collecting telecommunications associated data pursuant to warrants.
- On the very specific issue of associated data linked to third-party communications, the Court found that it can only be retained if it is related to threats or of use to an investigation, prosecution, national defence or international affairs.
- CSIS, in consultation with the Department of Justice, had interpreted the *CSIS Act* as enabling the retention of this sub-set of associated data to allow for that important analytic work. At no time did the Service believe this to be inconsistent with the *CSIS Act*.
- It is now clear that the Federal Court, on the issue of the retention of certain data, interprets the *Act* differently.
- We accept this decision and have taken immediate actions to respond.
- In response to the decision, CSIS halted all access to, and analysis of, associated data while we undertake a thorough review of the decision in order to assess potential operational and legal impacts, and determine our way forward.

**Pages 111 to / à 112  
are not relevant  
sont non pertinentes**



Canadian  
Security  
Intelligence  
Service

Service  
canadien du  
renseignement  
de sécurité

# STATEMENT

## *CSIS Director statement regarding decision of the Federal Court*

Ottawa, Thursday, November 3, 2016 - The Director of the Canadian Security Intelligence Service (CSIS), Michel Coulombe, issued the following statement regarding the decision issued today by the Honourable Justice Noël of the Federal Court:

“The Federal Court has recently ruled on the retention of associated data linked to third party information. CSIS fully accepts the Court’s decision, and has taken immediate actions to respond. Given the Court’s decision with respect to third-party data, CSIS has halted all access to, and analysis of, associated data while we undertake a thorough review of the decision in order to assess potential operational and legal impacts, and determine our way forward.

I regret that we did not meet our duty of candour to the Court, and I commit to continuing my efforts, with the Deputy Minister of Justice, to address the Court’s concerns. Let me be clear: all associated data collected under warrant was done so legally. The Court’s key concern related to our retention of non-threat related associated data linked with third party communications, after it was collected.

CSIS, in consultation with the Department of Justice, had interpreted the *CSIS Act* to allow for the retention of this sub-set of associated data. It is now clear that the Federal Court disagrees with this interpretation; a decision which we fully accept.

As is the case for many of our international partners, CSIS has developed data analytic capabilities and expertise to analyze associated data and enhance its capacity to identify and assess threats to the security of Canada over time. When it comes to understanding and predicting the actions of the subjects of our investigations, data analytics has proven to be an effective tool. In the ruling released today, the Federal Court recognized the intelligence value of the data analytic programme and did not question the authority of collecting telecommunications associated data pursuant to warrants. The Court also rightly acknowledged the age of the *CSIS Act* and that it may not be keeping pace with changing technology and the current threat environment.

The ongoing national security consultations represent an important opportunity to ensure that CSIS is meeting the dual objectives of security and privacy, and has the tools and authorities, with appropriate oversight, to meet both.



Canadian  
Security  
Intelligence  
Service

Service  
canadien du  
renseignement  
de sécurité

Because the nature of our business is principally secret, Canadians are largely unaware of the professionalism and outstanding dedication the men and women of CSIS show every day as they carry out intelligence work. As the Director of CSIS, I am extremely proud of the people with whom I work. Canadians, too, should be proud of those who work tirelessly to keep this great country safe.

In addition, with respect to the ongoing situation in Quebec regarding the surveillance of journalists, I would like to state that I agree fully with the Prime Minister's statement on this matter. Such a situation is not occurring at the federal level given the strong safeguards and protections we have in place to protect the freedom of the press in the course of our business.

We appreciate the confidence the government has in CSIS, and it remains for us a privilege to protect Canadians and Canada's interests at home and abroad."

-30-

**Information:**

Media Relations

Canadian Security Intelligence Service

media-medias@smtp.gc.ca

613-231-0100

**Pages 115 to / à 118  
are not relevant  
sont non pertinentes**



---

# Statement

---

## **STATEMENT BY PUBLIC SAFETY MINISTER RALPH GOODALE ON THE RULING OF THE FEDERAL COURT OF CANADA, PUBLISHED NOVEMBER 3, 2016, WITH RESPECT TO THE CANADIAN SECURITY INTELLIGENCE SERVICE (CSIS) AND THE HANDLING OF "ASSOCIATED DATA"**

November 3, 2016 – “I welcome the decision in this matter rendered by Mr. Justice Noel on behalf of the Federal Court, which the Government will not appeal.

The court's insight and guidance are timely, coming in the midst of the public consultations we now have underway about Canada's national security framework.

CSIS plays a critical role in keeping Canadians safe. As it investigates threats to our national security, the Service collects a considerable amount of information, with full legal authorization pursuant to the CSIS Act and warrants issued by the Federal Court. When the information is intercepted communications, it can often include "associated data" of third-parties such as phone numbers and email addresses.

The court has ruled that while legally collected, such "associated data" cannot be retained and utilized by CSIS unless it relates to a specific threat to the security of Canada or is of use to an investigation, prosecution, national defence or foreign affairs.

The Service has confirmed that it is taking immediate steps to address the court's decision. It has blocked all access to and analysis of any associated data, while it considers its next steps. As Minister of Public Safety, I am asking the Security Intelligence Review Committee (SIRC) to monitor the situation carefully to ensure compliance.

I also take very seriously the explicit finding by Justice Noel that CSIS had failed in its duty to be candid with the court. I will be pursuing this criticism with the executive management of the Service. In matters of security and intelligence, Canadians need to have confidence that all the departments and agencies of the Government of Canada are being effective at keeping Canadians safe, and equally, that they are safeguarding our rights and freedoms.

I also take note of the court's observation that the CSIS Act is now more than 30 years old and showing its age as global affairs, threat profiles, technology and public expectations have rapidly evolved. In his judgement, Justice Noel did not dispute the potential value of "associated data" to the important work CSIS does in this challenging world, but he could not find existing legislative authority permitting its retention and use.”

-30-

Follow Public Safety Canada ([@Safety\\_Canada](https://twitter.com/Safety_Canada)) on Twitter.

For more information, please visit the website [www.publicsafety.gc.ca](http://www.publicsafety.gc.ca).

### **Information:**



- 2 -

**Scott Bardsley**  
**Office of the Minister of Public Safety and Emergency Preparedness**  
**613-998-5681**

**Media Relations**  
**Public Safety Canada**  
**(613) 991-0657**



---

# *Questions and Answers*

---

## **FEDERAL COURT DECISION CSIS' Authority to Retain Associated Data Collected Through Warrants**

### **1. Would the National Security and Intelligence Committee of Parliamentarians have been able to detect the issue raised by the Federal Court?**

While it is speculative to say whether the proposed committee would have explored this issue or not, its mandate and scope would have enabled access to the information pertinent to this case.

The proposed committee would have the authority to review any department or agency of the Government of Canada that performs national security or intelligence activities, including their ongoing operations.

### **2. [For Minister] Does the Minister still have confidence in CSIS?**

CSIS plays a vital role in keeping Canadians safe by investigating threats, and collecting and analyzing information to protect our national security. I continue to have confidence in their ability to deliver on that mandate.

### **3. Will this decision impact or influence the issue of Basic Subscriber Information / Lawful Access?**

The Federal Court's concern does not extend to the issue of the provision of Basic Subscriber Information to law enforcement and intelligence agencies.

Basic Subscriber Information is one of the 10 topics the Government has selected for its public consultation on national security. The input the Government receives from Canadians, including experts, stakeholders, and Parliamentarians, will help inform the development of national security law and policies.

The security and privacy of Canadians are both crucial considerations for BSI.

All Canadians are welcome to participate in the online consultation at: [Canada.ca/national-security-consultation](http://Canada.ca/national-security-consultation)

### **4. Does this decision represent a failure from SIRC in its oversight role?**

SIRC reviewed CSIS' use of associated data and published its findings on the issue in its 2014-15 annual report. SIRC did not conclude that the retention of associated data was illegal. The Federal Court arrived at a different conclusion. Upon review, the Government accepts the Federal Court's findings.



- 2 -

SIRC continues to play a very critical role in keeping CSIS accountable through in-depth reviews of its activities. The Minister of Public Safety has asked SIRC to monitor CSIS's compliance with the Federal Court decision.

**5. Can you expand on what the Minister is asking SIRC to do in relation to reviewing CSIS's compliance with the decision?**

SIRC has a unique mandate in keeping CSIS accountable through in-depth reviews of its activities. The findings of its reviews are made available to all Canadians through SIRC's annual reports. These reports are extremely valuable in ensuring that CSIS is operating consistently with Canadian law and values.

Section 54 (2) of the *CSIS Act* provides the Minister of Public Safety with the authority to request a special report from SIRC concerning any matter that relates to the performance of its duties and functions. These special reports are only requested in exceptional circumstances, and do not form part of SIRC's regular review plans for a given year.

The Minister of Public Safety is using this authority to request that the SIRC monitor CSIS' compliance with the Federal Court decision in the matter of "associated data" retention.

SIRC will report its findings directly to the Minister through a classified document. A summary of the findings will be included in SIRC's Annual Report to Parliament, which is available to all Canadians.

**Pages 123 to / à 126  
are not relevant  
sont non pertinentes**

## **Minister's Speaking Notes on the Federal Court's "En banc" Decision**

**Speaking Notes**

**For the**

**Honourable Ralph Goodale**  
**Minister of Public Safety and Emergency Preparedness**

**On the**

**Federal Court's "En banc" Decision**

**Ottawa, ON**

**November 3, 2016**

*Check Against Delivery*

I welcome the decision in this matter rendered by Mr. Justice Noel on behalf of the Federal Court.

The court's insight and guidance are timely, coming in the midst of the public consultations on Canada's national security framework.

CSIS plays a critical role in keeping Canadians safe. As it investigates threats to our national security, the Service collects a considerable amount of information, with full legal authorization pursuant to the CSIS Act and warrants issued by the Federal Court. When the information is intercepted communications, it can often include "associated data" of third-parties such as phone numbers and email addresses.

The court has ruled that while legally collected, such "associated data" cannot be retained and utilized by CSIS unless it relates to a specific threat to the security of Canada or is of use to an investigation, prosecution, national defence or foreign affairs.

The Service has confirmed that it is taking immediate steps to address the court's decision. It has blocked all access to and analysis of any associated data, while it considers its next steps. I am asking the Security Intelligence Review Committee (SIRC) to monitor the situation carefully to ensure compliance.

I also take very seriously the explicit finding by Justice Noel that CSIS had failed in its duty to be candid with the court. I will be pursuing this criticism with the executive management of the Service. In matters of security and intelligence, Canadians need to have confidence that all the departments and agencies of the Government of Canada are being effective at keeping Canadians safe, and equally, that they are safeguarding our rights and freedoms.

**Pages 131 to / à 132  
are not relevant  
sont non pertinentes**



---

# *Media Lines*

---

## **FEDERAL COURT “EN BANC” DECISION CSIS’ Authority to Retain Associated Data Collected Through Warrants**

**Issue:** The Federal Court is anticipated to release its decision regarding the CSIS Act and CSIS’ authority to retain associated data collected through Federal Court issued warrants in the near future. The Federal Court found that CSIS’ retention of associated data linked to third party communications found to be unrelated to threats to the security of Canada is illegal. The Federal Court also found that CSIS breached its duty of candour by failing to fully and transparently inform the Court of its retention program and the establishment of the Operational Data Analysis Centre (ODAC).

### **Key Messages:**

- The Government accepts the Federal Court’s findings on this matter.
- It is important to underline that the associated data was collected legally through warrants, and CSIS acted pursuant to Court authorized warrants. The Federal Court’s key concern relates to CSIS’ retention of such data (e.g., date, time, and phone numbers related to a call) when it is not related to a threat to the security of Canada.
- CSIS is taking immediate action to address the Federal Court’s findings. CSIS halted all access to, and analysis of, the associated data as it actively works to assess and address the Federal Court’s decision.
- The Government accepts the Federal Court’s findings regarding its duty of candour. In fact, the Government conceded to the Court that it had failed to meet its duty of candour in this case. CSIS has committed to working with the Federal Court to ensure that it is fully transparent with the Court.
- The Federal Court agreed with CSIS’ proposal to update warrants, and generally accepted the changes proposed by CSIS.
- In its decision, the Federal Court noted that the CSIS Act is now more than 30 years old and changes may need to be made to ensure that it keeps pace with changes in technology and the privacy expectations of Canadians. This is something that we will review as part of our public consultation on Canada's national security framework.
- We are also taking measures to strengthen national security accountability. In June, we put forward legislation to create a National Security and Intelligence Committee of Parliamentarians which would have a broad mandate to scrutinize the activities of any federal department or agency with national security responsibilities, including operational matters.
- The Government is committed to keeping Canadians safe while at the same time safeguarding our freedoms, rights and values in an open and democratic society.



- In September we launched a broad public consultation on national security. We want to hear from Canadians on how we can best meet our dual objectives of security and rights. We invite all Canadians to provide us with their views and ideas on our national security framework through our online consultation, which is open until December 15. ([www.canada.ca/national-security-consultation](http://www.canada.ca/national-security-consultation))

**Ministerial Talking Point:**

CSIS plays a vital role in keeping Canadians safe by investigating threats, and collecting and analyzing information to protect our national security. I continue to have confidence in their ability to deliver on that mandate.

## **Sayarh, Omar (PS/SP)**

---

**From:** Baker3, Ryan (PS/SP)  
**Sent:** Friday, November 04, 2016 9:55 AM  
**To:** Brien, Dan (PS/SP); Bardsley, Scott (PS/SP); Peirce, Hilary (PS/SP)  
**Cc:** Tomlinson, Jamie (PS/SP); Magee, Heather (PS/SP); De Curtis, Laura (PS/SP); Wilson, Ashleigh (PS/SP); Slack, Jessica (PS/SP); Miller, Kevin (PS/SP)  
**Subject:** FYI - NDP newser on court decision at 10 a.m.

Hi Dan,

Just a heads up to flag this media availability happening in foyer at 10 a.m. We wouldn't be able to get a transcript in time for the Minister's availability, so you may want to consider sending someone to listen in.

### **OTTAWA, ON**

NDP House Leader and Justice Critic Murray Rankin, joined by NDP Public Safety Critic Matthew Dubé, reacts to the Federal Court ruling on CSIS bulk data collection.

Foyer  
House of Commons  
10 a.m.

Thanks,  
Ryan

Ryan Baker  
Director, Public Affairs / Directeur, Affaires publiques  
Public Safety Canada / Sécurité publique Canada  
Tel: (613) 991-3549  
Mobile: (613) 796-9750  
[Ryan.Baker3@canada.ca](mailto:Ryan.Baker3@canada.ca)

## Sayarh, Omar (PS/SP)

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Friday, November 04, 2016 8:34 AM  
**To:** [REDACTED] (PS/SP); [REDACTED] (PS/SP); Beecher, Sophie (PS/SP)  
**Subject:** Fw: Transcript: Technical Briefing on Federal Court decision re: CSIS data retention - 2016-11-03 - 18:15 ET

FYI

---

**From:** PSPMediaCentre / CentredesmediasPSP (PS/SP) <ps.pspmediacentre-centredesmediaspsp.sp@canada.ca>  
**Sent:** Friday, November 4, 2016 8:31 AM  
**To:** Today's News / Actualités (PS/SP)  
**Subject:** Transcript: Technical Briefing on Federal Court decision re: CSIS data retention - 2016-11-03 - 18:15 ET

**DATE/DATE:**  
November 3, 2016, 6:15 p.m. (EDT)

**LOCATION/ENDROIT:**  
Teleconference, OTTAWA, ON

**PRINCIPAL(S)/PRINCIPAUX:**  
Senior Government Officials

**SUBJECT/SUJET:**  
CSIS and Justice Canada officials conduct a **not for attribution**, background technical briefing on a recent Federal Court decision.

**Operator:** Good evening ladies and gentlemen.

Bonjour mesdames et messieurs.

Welcome to the CSIS medial technical briefing conference call.

Bienvenue à l'appel conférence séance d'information du SCRS.

I would now like to turn the meeting over to Senior Government Official.

J'aimerais maintenant céder la parole à haut fonctionnaire.

Please go ahead.

La parole est à vous.

**Senior Government Official:** Thank you very much. Good day everyone.

Bonjour mesdames et messieurs.

Again, my name is Senior Government Official from the Canadian Security Intelligence Service. We have convened this conference call in order to provide a background briefing related to the decision released today by Justice Noël of the Federal Court. The objective of the briefing is to highlight key elements of the decision, what the decision means to CSIS and what has CSIS done to respond?

Je m'appelle haut fonctionnaire, je suis du Service canadien du renseignement de sécurité. Nous avons convoqué cette téléconférence afin de fournir des renseignements généraux au sujet de la décision communiquée aujourd'hui par le juge Noël de la Cour fédérale. L'objet de cette séance d'information est de mettre en évidence les éléments principaux de la décision, ce qu'elle signifie pour le SCRS et ce qui a été fait par le SCRS pour y répondre.

I am joined today by representatives from the Canadian Security Intelligence Service and Justice Canada. As you may know, the identities of CSIS employees are not made public, therefore we will not be able to provide the last name of the CSIS speaker on the line today. We will however identify them by their first name. They will also identify themselves before they start speaking in order to make it easier for you to follow along.

Les représentants du Service canadien du renseignement de sécurité m'accompagnent aujourd'hui. Comme vous le savez peut-être, les identités des employés du SCRS ne sont pas rendues publiques. Nous ne pourrions donc pas fournir les noms de famille des participants. Nous les désignerons cependant par leurs prénoms. Ils s'identifieront par le prénom avant de commencer à parler afin que vous puissiez suivre plus facilement.

On the line today, I am accompanied by Senior Government Official at CSIS and will provide some opening remarks before we open the phone line to questions. Senior Government Official is supported by technical experts who may help to provide further details should they be required.

As I previously indicated, they identify themselves by name should they help respond to a question. Senior Government Official will be accompanied by Senior Government Official from the Department of Justice. I would like to underscore that this briefing is for background information and is not for attribution. While it can be recorded for your personal use, it should not be rebroadcast in any form.

Pour cet appel aujourd'hui, je suis accompagné de haut fonctionnaire, au SCRS. Il présentera ses observations préliminaires avant que nous commencions à recevoir des questions. Haut fonctionnaire aura le soutien d'experts techniques qui fourniront des précisions au besoin. Comme je l'ai déjà indiqué, ils s'identifieront par leurs prénoms avant de prendre la parole.

Haut fonctionnaire est aussi accompagné par haut fonctionnaire du ministère de la Justice. J'aimerais souligner que cette séance d'information est fournie à des fins d'information et sans attribution. Bien qu'il soit possible de l'enregistrer à des fins personnelles, il ne devrait pas être rediffusé sous quelque forme que soit.

I will now invite Senior Government Official to provide an overview of the key elements of the decision, what this decision means and what CSIS has done to respond.

J'inviterais maintenant haut fonctionnaire à fournir un aperçu des principaux éléments de la décision, ce qu'elle signifie et ce qui a été fait par le SCRS pour y répondre.

**Senior Government Official:** Bonjour. Je m'appelle haut fonctionnaire. Je suis au Service canadien du renseignement de sécurité. Je suis ici aujourd'hui pour vous fournir des informations contextuelles au sujet de certains aspects de la décision récente de la Cour fédérale du Canada. Je ferai des remarques préliminaires et je répondrai à autant de questions que possible.

Il faut noter cependant qu'il y a des questions auxquelles je ne pourrai pas répondre pour des raisons opérationnelles et de sécurité nationale.

Good evening, I'm Senior Government Official at Canadian Security Intelligence Service. I'm here today to provide a background briefing about certain aspects of the Federal Court of Canada's recent decision. I'll make an initial statement and then, I'll try to answer as many questions as possible, keeping in mind that there are some questions that I will not be able to answer for both operational and national security reasons. As Senior Government Official has just stated, this meeting is not for attribution but you can identify me as a Senior CSIS Official.

The Federal Court has issued a judgement in relation to the issue of the legal authority for CSIS to retain associated data of lawfully intercepted third-party communications. This background brief is focused solely on this issue and my team and I will not be commenting on other aspects of the ruling.

La Cour fédérale a rendu une décision concernant la question de l'autorisation légale du SCRS de conserver des données connexes reliées aux communications de tiers interceptées légalement. Cette séance d'information est axée uniquement sur cette question, et mon équipe et moi ne feront pas de commentaire quant à d'autres aspects de cette décision.

In the context of a lawfully intercepted communication, at this point, I would like to clarify what is meant by both associated data and third-party communications. I will then discuss how this information has been lawfully collected, but as per the

Court's decision, that it may only be retained if it is threat-related or of use to an investigation, prosecution, national defence or international affairs.

I'll start with associated data. Associated data is also known as metadata. It consists of information about the lawfully intercepted communication, such as the date, time, telephone numbers and duration of the communication. It does not refer to, include, nor reveal the content of a communication.

I would like to emphasize at this point that any representation or suggestion that CSIS's collection of associated data or metadata is analogous to both data acquisition would be factually incorrect. The very use of the term associated in associated data denotes that it is associated to the communication. It is separate and distinct from the content. In fact, it is used by computer system to identify, describe, manage or route the communication across a network. For the sake of simplicity, I will use the term associated data from this point on as it is the term used in the legal decision.

Les données connexes sont aussi appelées métadonnées. Il s'agit de renseignements au sujet de communications interceptées légalement tels que la date, l'heure, les numéros de téléphone et la durée de la communication. Elle ne renvoie pas au contenu d'une communication, ni ne l'inclut, ni n'en révèle le contenu.

J'aimerais maintenant insister sur le fait que toute représentation ou suggestion selon laquelle l'ensemble des données connexes ou métadonnées du SCRS serait analogue à l'acquisition de données en masse est une erreur factuelle. L'utilisation même du terme connexe dans données connexes dénote que ces données sont associées à la communication. Or, elles sont séparées et distinctes du contenu. En fait, elles sont utilisées par les systèmes informatiques pour identifier, décrire, gérer ou acheminer la communication dans l'ensemble d'un réseau. Par souci de simplicité, je vais utiliser l'expression données connexes à partir de maintenant car c'est celui qui est utilisé par la Cour fédérale.

Next, I would like to define third-party communications. The simplest way to describe third-party communications is by exclusion. They are any lawfully intercepted communications which does not involve the target. Typical third-party communications lawfully intercepted by CSIS include those of the target's family members, or anyone using a target's communication device.

La façon la plus simple de décrire les communications de tiers consiste à procéder par exclusion. Ils sont toutes les communications interceptées légalement qui n'impliquent pas la cible. Parmi les communications de tiers typiques interceptées légalement par le SCRS, il y a celle des membres de la famille de la cible ou de toute personne qui utilise l'appareil de communication de la cible.

Having provided these definitions, I will now describe how this information is lawfully collected by CSIS. In order to investigate threats to the security of Canada, CSIS may apply to the Federal Court for a warrant when the response to a threat requires more intrusive measures. Through these warrants, the Federal Court may authorize CSIS to, for example, intercept a target's communications.

As I stated in the definitions, when these communications are intercepted, CSIS obtains both the content and the associated data. Through the execution of these warrants, CSIS may also incidentally collect third-party communications. The warrants account for this reality and impose specific conditions concerning the retention of third-party communications, namely third-party communications can only be retained if they are found to be related to threats or of use to an investigation, prosecution, national defence or international affairs.

Afin d'enquêter sur des menaces à la sécurité du Canada, le SCRS peut demander à la Cour fédérale l'émission d'un mandat lorsque la réponse à la menace exige des mesures plus inclusives. Au moyen de ces mandats, la Cour fédérale peut autoriser le SCRS à intercepter les communications d'une cible. Comme je l'ai indiqué dans les définitions, lorsque ces communications sont interceptées, le SCRS en obtient, on obtient le contenu et les données connexes.

Par l'exécution de ces mandats, le SCRS peut par ailleurs recueillir aussi des communications de tiers. Les mandats tiennent compte de cette réalité et imposent des conditions précises quant à la conservation de communications de tiers, c'est-à-dire que les communications de tiers peuvent seulement être conservées s'ils s'avèrent être liées à des menaces ou utiles pour une enquête, une poursuite, la défense nationale ou les affaires internationales.

So why are we here? The Court has ruled that we are not authorized to retain the associated data of third-party communications when it does not meet these specific conditions. The Court's ruling effectively means that the warrant conditions apply equally to both the content and the associated data of third-party communications. In the context of lawfully intercepted third-party communications, prior to the Federal Court's decision, CSIS practice was to delete content deemed to be of no intelligence value but it kept the associated data for the purpose of data analytics.

Data analytics employs computers to analyse data and discover linkages, trends and patterns. These techniques enable CSIS to make sense of volumes of information that could not be processed without a computer's assistance. Determining whether these communications are threat related is complex, and may only become apparent as an investigation progresses. Through data analytics, lawfully intercepted communications initially assessed to have no intelligence value were later revealed to contain key threat related information.

En raison de la décision de la Cour, le SCRS a suspendu tout accès aux données connexes ainsi que leur analyse pendant que nous entreprenons l'examen approfondi de la décision afin d'en évaluer les effets opérationnels et juridiques potentiels et de déterminer les prochaines étapes. L'analytique de données est un outil précieux pour l'exercice du mandat du SCRS, mais elle doit être entreprise de façon responsable et en accord avec les pouvoirs qui nous sont conférés. La décision de la Cour fédérale fournit une nouvelle orientation à cet égard.

Given the Court's decision, CSIS has halted all access to an analysis of associated data while we undertake a thorough review of the decision in order to assess potential operational and legal impacts and determine our way forward. Data analytics is invaluable in relation to the exercise of CSIS' mandate, but it must be undertaken responsibly and in accordance with our authorities. The Federal Court decision provides new direction in this regard and we will adjust our practices accordingly.

In closing, it is important to note that the Federal Court's decision concerning third-party associated data pertains exclusively to its retention, not its collection. Warrants granted by the Federal Court are narrowly focused on targets whose activities have been demonstrated to represent unreasonable grounds to believe threats to the security of Canada.

Pour conclure, il est important de noter que la décision de la Cour fédérale au sujet des données connexes de tiers ne concerne que sa conservation et non pas sa collecte. Les mandats accordés par la Cour fédérale sont étroitement centrés sur les cibles dont on a démontré que les activités représentent avec des motifs sérieux de le croire des menaces pour la sécurité du Canada.

I will now turn it back to our moderator.

**Senior Government Official:** Thank you, Senior Government Official.

Sans plus tarder, nous allons commencer la séance d'information.

Operator, please instruct the participants on how to proceed with their questions.

**Operator:** Thank you. Merci.

We will now take questions from the telephone line.

Nous allons maintenant passer à la période de questions.

If you have a question and you are using a speaker phone, please lift your handset before making your selection.

Si vous utilisez un téléphone mains libres, s'il vous plaît soulevez le combiné avant d'effectuer votre sélection.

If you have a question, please press \*1 on your telephone keypad.

Si vous désirez poser une question, veuillez s'il vous plaît appuyer sur les touches \*1 sur votre téléphone à clavier.

If at any time, you wish to cancel your question, please press the pound sign.

Vous pouvez çà tout moment annuler votre question en appuyant sur le dièse.

Please press \*1 at this time if you have a question.

S'il vous plaît appuyez sur \*1 maintenant pour poser une question.

There will be a brief pause while the participants register for questions.

Il y aura un court délai vous permettant de vous enregistrer dans la file d'attente pour la période de questions.

Thank you for your patience.

Merci de patienter.

The first question is from (inaudible) McGraw from Wall Street Journal.

La première question nous vient de (inaudible) McGraw de Wall Street Journal.

Please go ahead, your line is open.

**Question:** Hi, thanks for taking my question. My question is that I'm hoping you can help me understand how this ruling from the judge (inaudible) out. So is it correct that this was a question of a warrant application, a federal warrant application brought to the Federal Court along with a request to amend warrant templates going forward and that the judge subsequently learned of those, the program and issued this ruling? Is that correct? And if not, can you explain?

**Senior Government Official:** Well, parts – Senior Government Official from the Department of Justice – parts of what you say are correct. Yes, it was a warrant application and it was an application in which we sought to set the terms and conditions for warrants going forward.

**Question:** Okay. So what parts of what I said were incorrect?

**Senior Government Official:** Well, the, I can't remember exactly the last part. Can you repeat the last part again? The first parts were certainly correct.

**Question:** Okay, so if I understand correctly based on what you just said, that it was, this is an application for a warrant and for amendment of future warrant templates, including the ones that you were signing for, or that you were applying for at the time. And this ruling was issued in response to those requests?

**Senior Government Official:** Yes, that's correct.

**Question:** Okay. Thank you.

**Operator:** Thank you. The next question is from Justin Ling from Vice News. Please go ahead, your line is open.

La parole est à vous.

**Question:** Hi there. Yeah, thanks for doing this. I was hoping you could walk me through a little bit about, you know, how you would analyse and treat this data going forward? Obviously, I don't expect you to get into specifics of each investigation, but could you form a hypothetical about how you might, in the course of an investigation, go back to this database, go back to, you know, the data centre and treat that data to obtain new, or reassess the previous intelligence?

**Senior Government Official:** So, so this is Senior Government Official again back on the line. I'm not prepared to provide any specific examples because that would put me into a place where I would be probably revealing operational trade craft and I'm not prepared or authorized to do so. What I can say is that the data analytics program has demonstrated its usefulness in being able to identify trends, find patterns in the data and help in investigative situations. So – follow on.

**Operator:** The next question is from Cathy Simpson from CBC News. Please go ahead.

La parole est à vous.

**Question:** Hi, I have a question about the timelines involved in holding onto this data. Under the CSIS Act, it says that investigators have a year to determine whether they can hold onto this information. I don't understand why that wouldn't apply to the data in this case.

**Senior Government Official:** Well, the short answer is there is no specific statement like that in the CSIS act. The, the ability to hang onto things is set by the Court when we're making warrant applications.

**Question:** So does it not, does it not say, according to the ruling, a warrant, 60 days where the warrant is issued, and then you've got one year in any other case to determine whether or not you can keep that information. Is that not the case or what is the case?

**Senior Government Official:** I think you're referring to the, the terms and conditions that were set by the Court as a result of this judgement. And yes, that's what this application was about, setting those terms and conditions, and the Court set them down. So those are what CSIS will comply with, going forward.

**Question:** So previously, there were no, previously there was no set in stone rules about how long you could hold onto this data?

**Senior Government Official:** Well, it's difficult because some of this information about, about what can or can't be done is subject to editing in the judgement, so I think I've gone as far as I can go on, on that question.

**Operator:** Thank you. The next question is from Jim Bronskill, from The Canadian Press. Please go ahead.

La parole est à vous.

**Question:** The Court ruling is pretty clear. But you mentioned that you are analysing the ruling and Senior Government Official said that. The Minister of Public Safety says the government will not appeal the ruling, and given its clarity. What exactly are you analysing to figure out what to do next? Isn't it obvious?

**Senior Government Official:** So it's Senior Government Official again. What we're analyzing is the operational and legal impact of the, this decision. From a technical perspective, we're exploring options on how we're going to go about making the necessary changes to meet the clarified conditions for us. I would say as well that what we've done in the interim is that we've halted access to and all use of associated data until we can come up with these options to fully meet the new requirements as laid out by the Court.

**Question:** Is this a matter of technically looking through the data and question to determine whether it meets the narrow criteria of the CSIS Act?

**Senior Government Official:** No. It's not necessarily looking at the data, it's looking at the systems themselves as to how we will go about implementing these new changes. Prior to the clarification provided by the Federal Court, the service's practice, as I mentioned earlier, was to keep all associated data. Given that we now have a clarification in that regard and we are only authorized to keep a certain amount of that associated data, we have to adjust the systems to basically allow for those distinctions.

**Question:** So it is a technical matter?

**Senior Government Official:** Correct.

**Question:** Okay.

**Operator:** Thank you. The next question is from David Ljunggren from Reuters Canada. Please go ahead, your line is open.

La parole est à vous.

**Question:** Yeah, thank you. Good evening. First question, is it my understanding, and I'm not an expert so please do feel free to correct me, is it my understanding that your reason for keeping this data for so long is that you might be able to evolve techniques in the future that would enable you to discern something interesting that you couldn't do now with current techniques?

**Senior Government Official:** No. That's probably not completely accurate. What we are looking to do is to use associated data to assist with ongoing current investigations. And I would remind folks that, you know, what we're talking about here is information that was collected under lawful authority and within that lawful authority, we get both content and associated data. And within the judgment of the federal court, the only impact this has is on a subset of associated data, ie., associated data of a third party communication which doesn't meet the thresholds set out in the warrant.

**Question:** Then, does that imply that an investigation being carried out now could somehow benefit from associated data you retain from 2007, say?

**Senior Government Official:** Yes. That's what our, that is correct, sir.

**Question:** And finally, how much of a blow would you say this Court ruling is?

**Senior Government Official:** So, you know, the Service has many investigative steps, so when the Service is investing threats to the security of Canada, it doesn't immediately start with applying for a warrant. There is a very sequential step in which an investigation proceeds. What we have to remember with this ruling is it's affecting only a very small subset of the information that we're lawfully authorized to collect.

**Question:** Okay. Thank you.

**Senior Government Official:** You're welcome.

**Operator:** Thank you. The next question is from Tonda MacCharles, from Toronto Star. Please go ahead, your line is open.

La parole est à vous.

**Question:** Hi, thanks for taking the question. Could you help me understand a little bit more? I know there's lots of folks that understand metadata better than some of us do. But I'd like to understand a little bit of the scope of, you say it's a small set, subset of the data, but, but what's the scope of the number of third-party communications that you would have scoped out or scooped up in this collection and retention exercise? Are we talking thousands of Canadians, tens of thousands of Canadians, millions of Canadians would be incidentally caught up in this?

**Senior Government Official:** So I'm not prepared or capable, to be honest, to provide you with an exact number. What I'm, I understand the question of people trying to understand the scope of the issue, and I guess if I go back to my previous answer, maybe if I expand a little bit farther on that, you know, recognizing that as we investigate threats to the security of Canada, and follow through on several investigative steps, we would only get to the application of a warrant when the threat dictated, the urgency dictated that that was what we were going to do.

I can tell you that that represents not the majority of our investigations, and as we then go farther in, if we did get into a situation where we would apply for a warrant again, when we're talking about collection, lawfully authorized collection under warrant, we collect both content and associated data. The context which has been deemed not threat related was destroyed, has always been destroyed. This ruling basically clarifies that our previous practice of maintaining associated data, all associated data is problematic.

But again, inside of associated data, this judgement is really around a very specific subset of that associated data, which is sub, associated data of third-party communications not related to the threat. So again, when we're talking about scope, if you look at it from, you know, the overall breadth of service investigations all the way down to how much this affects, you could see that as we go farther and farther down, it becomes a rather small subset.

**Question:** Right. But bear with me, cause, again, I'm just a layman trying to understand here, but you know, when I am on Twitter or Facebook or LinkedIn, all the algorithms prompt all kinds of connections and patterns and people I might know and people I might like to connect with, whether or not I do or don't want to.

So I assume you guys have similar kinds of algorithms to detect patterns in the kinds of things you're doing, but I mean, I can scroll through these kinds of connections by the hundreds. You must be, you must be establishing, through the associated data of third-parties, some, some big number of Canadians. Otherwise, it's not a concern for anyone. So, so can you not give us some kind of analogy or comparison to what it is you're doing with that stuff?

**Senior Government Official:** I'm not prepared to get into comparison, analogies or examples for the same reason I mentioned earlier, that it draws me into operational trade craft and revealing methodologies used by the Service, which could compromise our investigations. I will say that, you know, you have to remember that what the service does is surgically focused under warrant when we have reasonable grounds to believe that a warrant is required. So to suggest that this is a wide swap I think would be erroneous.

**Operator:** Thank you. The next question is from Dominique Cambron-Goulet from TC Media. Please go ahead.

La parole est à vous.

**Question:** Oui, bonsoir. Je voulais savoir en fait, vous avez parlé de données connexes comme la date, l'heure, les numéros de téléphone. Est-ce que c'est des données connexes qui sont reliées aux communications électroniques, comme des adresses IP ou les lieux où sont utilisés des appareils électroniques comme des téléphones intelligents ou des ordinateurs?

**Haut fonctionnaire:** Oui. En effet, des données connexes sont générées lorsqu'on fait une interception sous mandat d'une cible qui utilise un appareil pour faire des communications. Les données connexes peuvent varier, dépendant de, du type de communication, le type d'équipement que la personne ciblée utilise.

**Question:** Okay. Donc, ce que j'ai nommé, est-ce que c'est inclus dans les, dans les données connexes?

**Haut fonctionnaire:** Vous avez nommé date, heure, j'ai manqué les deux autres que vous avez nommés.

**Question:** J'ai parlé d'adresse IP puis de lieu d'utilisation là des appareils électroniques, comme une géolocalisation, par exemple.

**Haut fonctionnaire:** Les adresses IP, oui, la deuxième, géo, ça c'est, ça dépend. C'est pas, c'est pas tout le temps.

**Question:** C'est pas systématique? Ça dépend de l'appareil?

**Haut fonctionnaire:** Ça dépend de l'appareil, à dépend des, des —

**Question:** Des mandats?

**Haut fonctionnaire:**— comment ce que le, comment ce qui est configuré.

**Question:** Okay. Parfait. Merci.

**Operator:** Thank you. The next question is from Collin Freeze from The Globe and Mail. Please go ahead.

La parole est à vous.

**Question:** Hi. Thanks for taking these questions. Earlier this year, the SIRC reported that CSIS was ingesting bulk data sets and I'm just wondering if you could explain what that is in relation to the operational data analysis centre, whether it's populated both by the, what you're skimming off a warranted collection and the, the ingested bulk data sets? What, what were we talking about there, relative to what we're talking about here?

**Senior Government Official:** I'm sorry, but I'm not going to be able to answer that question because that is outside of the scope of what this technical briefing is focused. I really want to stay focused on the Court ruling and around associated data of third-party. So I'm not prepared to discuss other operational programs of the Service.

**Question:** Okay. The question I want to ask you too is the judges did take pains to point out that you are collecting records from the Canada Revenue Agency under Bill C-51 SCISA records you had previously needed a warrant to obtain and which you had been faulted before for not getting warrants for. I'm just wondering if you could give me an idea of the scale of information you're getting from places like the Canada Revenue Agency, places like the Immigration Canada? Given that you, you do have the state analysis centre and you do have relatively unimpeded access to other federal departments.

**Senior Government Official:** This is Senior Government Official from CSIS again. I think, again, I'm not sure, your reference to SCISA is part of the decision of the Court today and —

**Question:** No, no. It is directly referenced, I can give you a paragraph reference, it's, the judges basically point out that CSIS do not need warrants for stuff from the Canada Revenue Agency and leave it at that. I'm just wondering if your, your guests could expand on that. Given, given the context of what we're describing, that could be considered alarming.

**Senior Government Official:** Colin, we can't answer your question right now, we can look into this and follow up with you after the call. Just we want to be sure that we're, we're making the right reference.

**Question:** Okay.

**Senior Government Official:** We can, but we can follow up with you after.

**Question:** Yeah. Just as a point of information, the reference is paragraph 46.

**Senior Government Official:** Thank you very much.

**Operator:** Thank you. The next question is from Rebecca Lindell from Global News. Please go ahead, your line is open.

**Question:** Hello. Sorry, I missed the top of the technical briefing cause we were going live to air. This may have already been covered, but I just wanted to clarify this ruling is only referenced to third-party associated data. Is that correct? And can you provide an example of what this type of data is? Is this, you know, phone numbers of friends of people you're investigating or what does it actually look like?

**Senior Government Official:** So yes, that is correct. This is, the ruling basically addresses the question of retention of third party associated data. If you're looking for a specific example in my earlier text, what I gave as an example was typical third-party communication occurs when, if we have a, a lawful authorization to intercept a target, the family members of that target placing a call would be a, you know, a typical example where third-party communications would come into play.

**Question:** Oh okay. So if I'm another person using the same phone line as the target, then my data would be intercepted or the same IP address, for example?

**Senior Government Official:** Correct.

**Question:** Okay. Thank you.

**Operator:** Thank you. Once again, please press \*1 at this time if you have a question.

De nouveau, n'hésitez pas à appuyer sur \*1 pour toutes questions.

**Senior Government Official:** Operator, we have time for about two more questions at most.

**Operator:** Thank you. The other question is from Colin Freeze from Globe and Mail. Please go ahead.

La parole est à vous.

**Question:** Yeah. Sorry, I'm just wondering if you could tell us, you know, why we have an operational data analysis centre in the first place? You know, for people not initiated with, with such a place, I'm just wondering, you know, does it have any value in keeping Canada safe, fundamentally?

**Senior Government Official:** So the operational data analysis centre was created in 2006 with the recognition that the Service needed to ensure that we could keep up with the volumes of information, as our investigations proceeded. We view advanced analytics and the usefulness of advanced analytics as very important to our investigations. As I mentioned earlier, determining leads, identifying trends in the data that we've lawfully collected is very important. So yes, ODAC plays a key role in the intelligence mission.

**Question:** And do you ever imagine, I mean, **Minister Goodale said the laws for CSIS, at least in this front, strictly necessary collection are very, very old.** That to me, suggests he may be amenable to changing legislation on some date. But could CSIS provide a granular example to the Minister or to us right now about how this place has value because big data sometimes sounds like, you know, a crystal ball that's being created. It doesn't, it's hard to judge its value from the outside looking in.

**Senior Government Official:** I am not able to provide an example for this briefing today. But I would indicate that, you know, I think the, there's a general acceptance that advanced analytics and, you know, utilizing and exploiting data is advantageous operationally. It's even listed in the federal ruling where they recognize the value of advanced analytics. As far as the specific example, I have not been able to come up with one that keeps me in the unclassified space. Will I be asked to provide one to the Minister, I strongly suspect at some point we will be able to do so.

**Question:** Thank you.

**Senior Government Official:** You're welcome.

**Operator:** Thank you. The last question is from Justin Ling from Vice News. Please go ahead, your line is open.

La parole est à vous.

**Question:** Hi there. I'm actually just following up on what Colin was just asking about. Can you give us anymore information about the operational data analysis centre? And by that, I mean, you know, where is it? You know, what exactly is it? Can you give us any sort of insight into, you know, staffing, into mandate? Is this literally just a server farm, is this a team of people that are doing the analysis?

Is this, you know, how big is this? Can you give us a general ballpark budget? This place was literally secret up until today. And of course, you were rapped by the Court for being so secretive about this centre. So can you, you know, take a step towards transparency here and tell us a little bit about what the centre is and then what it actually does?

**Senior Government Official:** Well, I'll give it y best. So in 2006, the operational data analysis centre was created. So what that means is it's a group of people, it is an organizational entity who provide analytic capability to the organization. It's located here in Ottawa but data analytics is not limited to simply a group of people in Ottawa any longer because time has evolved and analytics is occurring around us pretty much as we speak.

What we look is exploiting lawfully authorized information and reaping the maximum intelligence benefit.

**Question:** Now, would ODAC be used by potentially the RCMP, law enforcement services? Is this strictly CSIS information? Would there be any mandate there for them to treat information collected by a different agency or from them to partner in any way with CSE? Is there any sort of MOU or understanding there that would allow them to, to kind of cross pollinate with other agencies?

**Senior Government Official:** I don't want to get into the operational elements of how ODAC operates. I think I'm just going to leave it at what I've provided to date.

**Question:** Okay. I guess finally, you know, is there, can you envision a sort of legislative change that would empower ODAC or just a general analytics programming in CSIS to operate in a realm that's a little bit more free, that would not get you in trouble like, like you got in trouble this month? Can you envision a legislative change that would encompass analytics on previously collected data?

**Senior Government Official:** That's not – I'm not prepared to discuss that at this moment.

**Senior Government Official:** Thank you very much Operator. That is all the time we have to today, and so we would like to thank everyone for taking part in this background briefing. If you have further questions, I would encourage you to contact CSIS Media Relations.

C'est tout le temps que nous aujourd'hui, alors nous aimerions remercier tous ceux et celles qui ont participé à cette séance d'information. Si vous avez d'autres questions, je vous encourage à communiquer avec les relations avec les médias du SCRS. Merci beaucoup.

**Operator:** Thank you. Merci.

The conference has now ended.

La conférence est maintenant terminée.

Please disconnect your lines at this time.

Veuillez s'il vous plaît raccrocher votre ligne .

Thank you for your participation.

Merci à tous les participants qui se sont joints.

**NOTE: TRANSCRIPTS CANNOT BE SHARED OR TRANSFERRED OUTSIDE OF YOUR DEPARTMENT WITHOUT  
THE CONSENT OF MEDIA Q INC.**

Questions? Please contact us at [ps.pspmediacentre-centredesmediaspsp.sp@canada.ca](mailto:ps.pspmediacentre-centredesmediaspsp.sp@canada.ca)

Questions? Veuillez communiquer avec nous au [ps.pspmediacentre-centredesmediaspsp.sp@canada.ca](mailto:ps.pspmediacentre-centredesmediaspsp.sp@canada.ca)

Sent to: !INTERNAL; !INTERNAL 2; CBSA Breaking News; RCMP Breaking News

## Sayarh, Omar (PS/SP)

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Thursday, November 03, 2016 6:10 PM  
**To:** [REDACTED]  
**Subject:** FW: Follow-up: ST by CSIS Director re. metadata court decision

FYI

Julie G  
Tel : 613-993-4415 | BB : 613-410-6059

---

**From:** COMDO / COMDO (PS/SP)  
**Sent:** Thursday, November 03, 2016 6:08 PM  
**To:** Tomlinson, Jamie (PS/SP); Nichols, Megan (PS/SP); Baker3, Ryan (PS/SP); Magee, Heather (PS/SP); Wilson, Ashleigh (PS/SP); Grenier, Julie (PS/SP); Miller, Kevin (PS/SP); Duval, Jean Paul (PS/SP); MacLean, Megan (PS/SP); O'Connell, Heather (PS/SP); Cibula, Colette (PS/SP); Crépeault, David (PS/SP); Wilcox, Brent (PS/SP); PS.F Speeches / Discours F.SP; Ministerial Liaison / Liaison ministerielle (PS/SP)  
**Cc:** PS.F Media Monitoring / surveillance des médias F.SP  
**Subject:** Follow-up: ST by CSIS Director re. metadata court decision

Good evening,

The STATEMENT has been posted to the wire and emailed to the press gallery.

**Wire:**  
<http://www.newswire.ca/en/releases/archive/November2016/03/c7880.html>  
<http://www.newswire.ca/fr/releases/archive/November2016/03/c7313.html>

**Mo Hashash**  
Communications Duty Officer/ Agent de service des communications  
Public Safety Canada / Sécurité publique Canada  
Tel.: (613) 991-7010  
Email/courriel: [ps.comdo-comdo.sp@canada.ca](mailto:ps.comdo-comdo.sp@canada.ca)

## Sayarh, Omar (PS/SP)

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Thursday, November 03, 2016 10:57 AM  
**To:** Wilson, Ashleigh (PS/SP)  
**Cc:** Ministerial Liaison / Liaison ministerielle (PS/SP)  
**Subject:** RE: For approval: CSIS En banc products

I don't have the final French of the Key Messages. Ryan was coordinating with COMDO. Do you have it?

Julie G  
Tel : 613-993-4415 | BB : 613-410-6059

-----Original Message-----

**From:** Wilson, Ashleigh (PS/SP)  
**Sent:** Thursday, November 03, 2016 10:56 AM  
**To:** Grenier, Julie (PS/SP)  
**Cc:** Ministerial Liaison / Liaison ministerielle (PS/SP)  
**Subject:** FW: For approval: CSIS En banc products

Would you mind sending an email to Min Liaison with all the final PS products so we can prepare an E-binder? I will be reaching out to CSIS with the same request.

-----Original Message-----

**From:** Baker3, Ryan (PS/SP)  
**Sent:** Wednesday, November 02, 2016 9:38 PM  
**To:** COMDO / COMDO (PS/SP)  
**Cc:** Wilson, Ashleigh (PS/SP)  
**Subject:** Fw: For approval: CSIS En banc products

James,

Please get the French updated for these key messages. I've attached the old version in French. Back by 9 am is fine - it's not a big job.

Thanks,  
Ryan

Ryan Baker  
Public Safety Canada/ Sécurité publique Canada  
613-796-9750

Original Message

**From:** Grenier, Julie (PS/SP) <julie.grenier@canada.ca>  
**Sent:** Wednesday, November 2, 2016 9:04 PM  
**To:** Baker3, Ryan (PS/SP); Magee, Heather (PS/SP)  
**Subject:** Re: For approval: CSIS En banc products

Hi Ryan,

As there are no changes to Statement and Speaking Notes, the only product that required updates was the Key Messages. The attached version of the Key Messages (clean) reflects PCO comments. If you would like me to send up to PCO through Min Liaison I can definitely do that - just let me know. Thanks!

Julie

Tel: 613-993-4415, BB: 613-410-6059

Original Message

From: Baker3, Ryan (PS/SP)

Sent: Wednesday, November 2, 2016 8:28 PM

To: Grenier, Julie (PS/SP); Magee, Heather (PS/SP)

Subject: Re: For approval: CSIS En banc products

Go ahead and update the date now.

Thanks,  
Ryan

Ryan Baker

Public Safety Canada/ Sécurité publique Canada

613-796-9750

Original Message

From: Grenier, Julie (PS/SP)

Sent: Wednesday, November 2, 2016 8:25 PM

To: Baker3, Ryan (PS/SP); Magee, Heather (PS/SP)

Subject: Re: For approval: CSIS En banc products

Thx Ryan! Looks like I'll be fine to make changes by BlackBerry and I saw Dan answered our question re: SIRC.

Last lingering issue: are we ok to update end date of consultation in the key messages? Or do keep it Dec 1 until approach to publicize extension is confirmed?

Julie

Tel: 613-993-4415, BB: 613-410-6059

Original Message

From: Baker3, Ryan (PS/SP)

Sent: Wednesday, November 2, 2016 8:16 PM

To: Grenier, Julie (PS/SP); Magee, Heather (PS/SP)

Subject: Re: For approval: CSIS En banc products

Don't go back to the office! Do what you can. We'll get the language translated and format it in the morning.

Ryan Baker

Public Safety Canada/ Sécurité publique Canada

613-796-9750

Original Message

From: Grenier, Julie (PS/SP)

Sent: Wednesday, November 2, 2016 8:14 PM

To: Baker3, Ryan (PS/SP); Magee, Heather (PS/SP)

Subject: Re: For approval: CSIS En banc products

Hi Ryan,

[REDACTED] I will try to edit by Blackberry but if that fails I will return to the office to finalize.

Tel: 613-993-4415, BB: 613-410-6059

Original Message

From: Baker3, Ryan (PS/SP)

Sent: Wednesday, November 2, 2016 7:56 PM

To: Grenier, Julie (PS/SP); Magee, Heather (PS/SP)

Subject: Re: For approval: CSIS En banc products

Hi Julie,

Given the timing is uncertain for tomorrow, I'd rather we finalize the products tonight and the French updated for morning. COMDO is on stand-by to coordinate the translation.

Could I ask you to please update the messages and remarks? I'll send them back to PCO and to COMDO for translation.

I'll check with Dan now on the SIRC question and get right back to you.

The Minister is not part of the media availability, but Dan is interested in having notes for him in case he needs them.

Thanks,

Ryan

Ryan Baker

Public Safety Canada/ Sécurité publique Canada

613-796-9750

Original Message

From: Grenier, Julie (PS/SP)

Sent: Wednesday, November 2, 2016 7:48 PM

To: Magee, Heather (PS/SP); Baker3, Ryan (PS/SP)

Subject: Re: For approval: CSIS En banc products

Hi Heather and Ryan,

With no change to Min statement and only minor updates to Key Messages and Speaking Remarks I'm proposing to send finals back to MO and PCO first thing tomorrow.

Will one of you check with Dan to confirm that Min has already asked SIRC to review?

Also, is the Min confirmed for a media avail? Sorry if I'm not clear on that. It is pertinent to how we communicate the consultation deadline. If he is talking to media and mentions the consultation he could mention the extension. (end date is not currently stated in the statement so nothing to update there) If no media avail, we could announce in Twitter Chat.

Thx,

Julie

Tel: 613-993-4415, BB: 613-410-6059

Original Message

From: Tomlinson, Jamie (PS/SP) <jamie.tomlinson@canada.ca>  
Sent: Wednesday, November 2, 2016 7:11 PM  
To: Baker3, Ryan (PS/SP); Magee, Heather (PS/SP); Grenier, Julie (PS/SP)  
Subject: Fw: For approval: CSIS En banc products

Fyi

Sent from my BlackBerry 10 smartphone on the Rogers network.

Original Message

From: Brien, Dan (PS/SP) <dan.brien@canada.ca>  
Sent: Wednesday, November 2, 2016 6:57 PM  
To: Surkes, Marci (PS/SP); Hurl, David (PS/SP); Tomlinson, Jamie (PS/SP); [REDACTED] Bardsley, Scott (PS/SP)  
Subject: FW: For approval: CSIS En banc products

-----Original Message-----

From: [REDACTED] [mailto:[REDACTED]]  
Sent: Wednesday, November 02, 2016 6:55 PM  
To: Brien, Dan (PS/SP)  
Subject: FW: For approval: CSIS En banc products

-----Original Message-----

From: [REDACTED]  
Sent: November 2, 2016 6:46 PM  
To: O'Nions, Christine; [REDACTED]  
Cc: Fox, Christiane; Noftle, Tracie; Lindblad, Anabel  
Subject: RE: For approval: CSIS En banc products

Thank you for your patience --

On the Key Messages --

It is the only document which conflates metadata and associated data in the top. Can we remain consistent in all our products?

Isn't the consultation extended until Dec 15, or is that a different one?

We should have a link that the review will include issues like the ones identified in the court ruling. Now it's just stated as fact that the review is happening, when in fact it's an important on how we're addressing this (IE it's reflected in the Minister's remarks in the second sentence).

Committee of Parliamentarians should be bumped up higher.

Speaking remarks for the Minister -- Has the Minister already asked SIRC to monitor compliance? Otherwise OK.

Minister's Statement -- OK

CSIS Statement- OK (just noticed that he references the DOJ Deputy, who won't be attending the presser)

Going through QA now.

-----Original Message-----

From: O'Nions, Christine

Sent: October 24, 2016 4:31 PM

To: [REDACTED]

Cc: Fox, Christiane; Noftle, Tracie; Lindblad, Anabel

Subject: For approval: CSIS En banc products

For approval: Pls find attached the final products for the CSIS en banc decision. [REDACTED]

Since the court is still translating the decision and plans to provide 48 hours notice, we have more time than anticipated for approvals.

Products are;

-CSIS backgrounder

-Director's statement

-CSIS and Justice Q&A to be posted on the Web -Director opening remarks -PS key messages -PS responsive Qs&As -PS minister's speaking notes -PS statement

## **Sayarh, Omar (PS/SP)**

---

**From:** Baker3, Ryan (PS/SP)  
**Sent:** Thursday, November 03, 2016 10:45 AM  
**To:** Magee, Heather (PS/SP); Grenier, Julie (PS/SP); Miller, Kevin (PS/SP); Wilson, Ashleigh (PS/SP); Duval, Jean Paul (PS/SP); Ministerial Liaison / Liaison ministerielle (PS/SP); De Curtis, Laura (PS/SP); Van Crieking, Jane (PS/SP)  
**Subject:** Court Decision

Update:

The media availability is off. We will still host the technical briefing. We're updating the media advisory now.

Thanks,  
Ryan

Ryan Baker  
Director, Public Affairs / Directeur, Affaires publiques  
Public Safety Canada / Sécurité publique Canada  
Tel: (613) 991-3549  
Mobile: (613) 796-9750  
[Ryan.Baker3@canada.ca](mailto:Ryan.Baker3@canada.ca)

## Sayarh, Omar (PS/SP)

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Wednesday, November 02, 2016 9:25 PM  
**To:** Baker3, Ryan (PS/SP); Magee, Heather (PS/SP)  
**Subject:** Re: For approval: CSIS En banc products  
**Attachments:** FRENCH - PS-SP-#1999745-v1A-Key\_Messages\_-\_FCC\_Associated\_Data\_FRENCH.DOCX

Thanks! I was in process of highlighting but that's more effective! I'm learning the BlackBerry editing tools (and limitations) in real time tonight!

Attached is the original French translation for reference, if that helps.

Julie

Tel: 613-993-4415, BB: 613-410-6059

Original Message

**From:** Baker3, Ryan (PS/SP)  
**Sent:** Wednesday, November 2, 2016 9:22 PM  
**To:** Grenier, Julie (PS/SP); Magee, Heather (PS/SP)  
**Subject:** Re: For approval: CSIS En banc products

Hi Julie,

I'll ask COMDO to do a document compare before sending to translation. No need to track changes.

Thanks,  
Ryan

Ryan Baker  
Public Safety Canada/ Sécurité publique Canada  
613-796-9750

Original Message

**From:** Baker3, Ryan (PS/SP)  
**Sent:** Wednesday, November 2, 2016 9:08 PM  
**To:** Grenier, Julie (PS/SP); Magee, Heather (PS/SP)  
**Subject:** Re: For approval: CSIS En banc products

Thanks Julie.

We'll send to PCO in the morning. We'll update the translation this evening. Are you able to send a version with tracked changes?

Ryan

Ryan Baker  
Public Safety Canada/ Sécurité publique Canada  
613-796-9750

Original Message

From: Grenier, Julie (PS/SP)  
Sent: Wednesday, November 2, 2016 9:04 PM  
To: Baker3, Ryan (PS/SP); Magee, Heather (PS/SP)  
Subject: Re: For approval: CSIS En banc products

Hi Ryan,  
As there are no changes to Statement and Speaking Notes, the only product that required updates was the Key Messages. The attached version of the Key Messages (clean) reflects PCO comments.

If you would like me to send up to PCO through Min Liaison I can definitely do that - just let me know. Thanks!

Julie  
Tel: 613-993-4415, BB: 613-410-6059  
Original Message  
From: Baker3, Ryan (PS/SP)  
Sent: Wednesday, November 2, 2016 8:28 PM  
To: Grenier, Julie (PS/SP); Magee, Heather (PS/SP)  
Subject: Re: For approval: CSIS En banc products

Go ahead and update the date now.

Thanks,  
Ryan

Ryan Baker  
Public Safety Canada/ Sécurité publique Canada  
613-796-9750  
Original Message  
From: Grenier, Julie (PS/SP)  
Sent: Wednesday, November 2, 2016 8:25 PM  
To: Baker3, Ryan (PS/SP); Magee, Heather (PS/SP)  
Subject: Re: For approval: CSIS En banc products

Thx Ryan! Looks like I'll be fine to make changes by BlackBerry and I saw Dan answered our question re: SIRC.

Last lingering issue: are we ok to update end date of consultation in the key messages? Or do keep it Dec 1 until approach to publicize extension is confirmed?

Julie  
Tel: 613-993-4415, BB: 613-410-6059  
Original Message  
From: Baker3, Ryan (PS/SP)  
Sent: Wednesday, November 2, 2016 8:16 PM  
To: Grenier, Julie (PS/SP); Magee, Heather (PS/SP)  
Subject: Re: For approval: CSIS En banc products

Don't go back to the office! Do what you can. We'll get the language translated and format it in the morning.

Ryan Baker

Public Safety Canada/ Sécurité publique Canada

613-796-9750

Original Message

From: Grenier, Julie (PS/SP)

Sent: Wednesday, November 2, 2016 8:14 PM

To: Baker3, Ryan (PS/SP); Magee, Heather (PS/SP)

Subject: Re: For approval: CSIS En banc products

Hi Ryan,

[REDACTED] I will try to edit by Blackberry but if that fails I will return to the office to finalize.

Tel: 613-993-4415, BB: 613-410-6059

Original Message

From: Baker3, Ryan (PS/SP)

Sent: Wednesday, November 2, 2016 7:56 PM

To: Grenier, Julie (PS/SP); Magee, Heather (PS/SP)

Subject: Re: For approval: CSIS En banc products

Hi Julie,

Given the timing is uncertain for tomorrow, I'd rather we finalize the products tonight and the French updated for morning. COMDO is on stand-by to coordinate the translation.

Could I ask you to please update the messages and remarks? I'll send them back to PCO and to COMDO for translation.

I'll check with Dan now on the SIRC question and get right back to you.

The Minister is not part of the media availability, but Dan is interested in having notes for him in case he needs them.

Thanks,

Ryan

Ryan Baker

Public Safety Canada/ Sécurité publique Canada

613-796-9750

Original Message

From: Grenier, Julie (PS/SP)

Sent: Wednesday, November 2, 2016 7:48 PM

To: Magee, Heather (PS/SP); Baker3, Ryan (PS/SP)

Subject: Re: For approval: CSIS En banc products

Hi Heather and Ryan,

With no change to Min statement and only minor updates to Key Messages and Speaking Remarks I'm proposing to send finals back to MO and PCO first thing tomorrow.

Will one of you check with Dan to confirm that Min has already asked SIRC to review?

Also, is the Min confirmed for a media avail? Sorry if I'm not clear on that. It is pertinent to how we communicate the consultation deadline. If he is talking to media and mentions the consultation he could mention the extension. (end date is not currently stated in the statement so nothing to update there) If no media avail, we could announce in Twitter Chat.

Thx,  
Julie

Tel: 613-993-4415, BB: 613-410-6059

Original Message

From: Tomlinson, Jamie (PS/SP) <jamie.tomlinson@canada.ca>

Sent: Wednesday, November 2, 2016 7:11 PM

To: Baker3, Ryan (PS/SP); Magee, Heather (PS/SP); Grenier, Julie (PS/SP)

Subject: Fw: For approval: CSIS En banc products

Fyi

Sent from my BlackBerry 10 smartphone on the Rogers network.

Original Message

From: Brien, Dan (PS/SP) <dan.brien@canada.ca>

Sent: Wednesday, November 2, 2016 6:57 PM

To: Surkes, Marci (PS/SP); Hurl, David (PS/SP); Tomlinson, Jamie (PS/SP); Andrew Swift; Bardsley, Scott (PS/SP)

Subject: FW: For approval: CSIS En banc products

-----Original Message-----

From: [REDACTED] [mailto:[REDACTED]]

Sent: Wednesday, November 02, 2016 6:55 PM

To: Brien, Dan (PS/SP)

Subject: FW: For approval: CSIS En banc products

-----Original Message-----

From: [REDACTED]

Sent: November 2, 2016 6:46 PM

To: O'Nions, Christine; [REDACTED]

Cc: Fox, Christiane; Noftle, Tracie; Lindblad, Anabel

Subject: RE: For approval: CSIS En banc products

Thank you for your patience --

On the Key Messages --

It is the only document which conflates metadata and associated data in the top. Can we remain consistent in all our products?

Isn't the consultation extended until Dec 15, or is that a different one?

We should have a link that the review will include issues like the ones identified in the court ruling. Now it's just stated as fact that the review is happening, when in fact it's an important on how we're addressing this (IE it's reflected in the Minister's remarks in the second sentence).

Committee of Parliamentarians should be bumped up higher.

Speaking remarks for the Minister -- Has the Minister already asked SIRC to monitor compliance? Otherwise OK.

Minister's Statement -- OK

CSIS Statement- OK (just noticed that he references the DOJ Deputy, who won't be attending the presser)

Going through QA now.

-----Original Message-----

From: O'Nions, Christine

Sent: October 24, 2016 4:31 PM

To: [REDACTED]  
[REDACTED]

Cc: Fox, Christiane; Nofle, Tracie; Lindblad, Anabel

Subject: For approval: CSIS En banc products

For approval: Pls find attached the final products for the CSIS en banc decision. [REDACTED]  
[REDACTED]

Since the court is still translating the decision and plans to provide 48 hours notice, we have more time than anticipated for approvals.

Products are;

-CSIS backgrounder

-Director's statement

-CSIS and Justice Q&A to be posted on the Web -Director opening remarks -PS key messages -PS responsive Qs&As -PS minister's speaking notes -PS statement

**Pages 159 to / à 160  
are not relevant  
sont non pertinentes**

## Sayarh, Omar (PS/SP)

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Wednesday, November 02, 2016 9:31 PM  
**To:** Beecher, Sophie (PS/SP); Davies, John (PS/SP)  
**Cc:** [REDACTED] (PS/SP); [REDACTED] (PS/SP)  
**Subject:** Re: PCO comments on CSIS associated data products

Thanks Sophie. Spoke to John by phone and he's good with the updates as well. Enjoy the rest of your evening. [REDACTED]  
[REDACTED]

Julie  
Tel: 613-993-4415, BB: 613-410-6059  
Original Message  
From: Beecher, Sophie (PS/SP)  
Sent: Wednesday, November 2, 2016 9:29 PM  
To: Grenier, Julie (PS/SP); Davies, John (PS/SP)  
Cc: [REDACTED] PS/SP; [REDACTED] PS/SP  
Subject: Re: PCO comments on CSIS associated data products

I'm ok with the paragraph as modified and the other minor changes.

Sent from my BlackBerry 10 smartphone on the Rogers network.

Original Message  
From: Grenier, Julie (PS/SP)  
Sent: Wednesday, November 2, 2016 8:54 PM  
To: Davies, John (PS/SP); Beecher, Sophie (PS/SP)  
Cc: [REDACTED] (PS/SP); [REDACTED] (PS/SP)  
Subject: PCO comments on CSIS associated data products

Hi Sophie and John,

We received comments from PCO tonight on the comms products for the Fed Court decision re associated data. (see comments in email chain below)

We are looking to finalize everything tonight.

We are updating key messages to reflect the new end date of the consultation.

For the key messages they also want us to clarify the context for reviewing CSIS Act.

To the paragraph below I have added specificity in the last line that this would be done through the NS Consultation. I understand this to be the case through a previous discussion with John. If you have any concerns with this, request to flag immediately.

Update to key message:

In its decision, the Federal Court noted that the CSIS Act is now more than 30 years old and changes may need to be made to ensure that it keeps pace with changes in technology and the privacy expectations of Canadians. This is something that we will review \*as part of our consultation on national security.\*

Julie

Tel: 613-993-4415, BB: 613-410-6059

Original Message

From: Tomlinson, Jamie (PS/SP) <[jamie.tomlinson@canada.ca](mailto:jamie.tomlinson@canada.ca)>

Sent: Wednesday, November 2, 2016 7:11 PM

To: Baker3, Ryan (PS/SP); Magee, Heather (PS/SP); Grenier, Julie (PS/SP)

Subject: Fw: For approval: CSIS En banc products

Fyi

Sent from my BlackBerry 10 smartphone on the Rogers network.

Original Message

From: Brien, Dan (PS/SP) <[dan.brien@canada.ca](mailto:dan.brien@canada.ca)>

Sent: Wednesday, November 2, 2016 6:57 PM

To: Surkes, Marci (PS/SP); Hurl, David (PS/SP); Tomlinson, Jamie (PS/SP); [REDACTED] Bardsley, Scott (PS/SP)

Subject: FW: For approval: CSIS En banc products

-----Original Message-----

From: [REDACTED] [[mailto:\[REDACTED\]](mailto:[REDACTED])]

Sent: Wednesday, November 02, 2016 6:55 PM

To: Brien, Dan (PS/SP)

Subject: FW: For approval: CSIS En banc products

-----Original Message-----

From: [REDACTED]

Sent: November 2, 2016 6:46 PM

To: O'Nions, Christine; [REDACTED]

Cc: Fox, Christiane; Noftle, Tracie; Lindblad, Anabel

Subject: RE: For approval: CSIS En banc products

Thank you for your patience --

On the Key Messages --

It is the only document which conflates metadata and associated data in the top. Can we remain consistent in all our products?

Isn't the consultation extended until Dec 15, or is that a different one?

We should have a link that the review will include issues like the ones identified in the court ruling. Now it's just stated as fact that the review is happening, when in fact it's an important on how we're addressing this (IE it's reflected in the Minister's remarks in the second sentence).

Committee of Parliamentarians should be bumped up higher.

Speaking remarks for the Minister -- Has the Minister already asked SIRC to monitor compliance? Otherwise OK.

Minister's Statement -- OK

CSIS Statement- OK (just noticed that he references the DOJ Deputy, who won't be attending the presser)

Going through QA now.

-----Original Message-----

From: O'Nions, Christine

Sent: October 24, 2016 4:31 PM

To: [REDACTED]

Cc: Fox, Christiane; Noftle, Tracie; Lindblad, Anabel

Subject: For approval: CSIS En banc products

For approval: Pls find attached the final products for the CSIS en banc decision. [REDACTED]

Since the court is still translating the decision and plans to provide 48 hours notice, we have more time than anticipated for approvals.

Products are;

-CSIS backgrounder

-Director's statement

-CSIS and Justice Q&A to be posted on the Web -Director opening remarks -PS key messages -PS responsive Qs&As -PS minister's speaking notes -PS statement

**Pages 164 to / à 165  
are duplicates  
sont des duplicatas**

## Arbeau, Kristy (PS/SP)

---

**From:** Tomlinson, Jamie (PS/SP)  
**Sent:** Wednesday, November 02, 2016 4:33 PM  
**To:** Bearegard, Monik (PS/SP); Davies, John (PS/SP)  
**Cc:** Baker3, Ryan (PS/SP); Magee, Heather (PS/SP); Nichols, Megan (PS/SP); MacKinnon, Paul (PS/SP)  
**Subject:** Federal Court

We just convened a communications coordination call with PCO, CSIS and Justice. So, to update you from the communications side.....

It is the desire of the centre to hold the media availability and technical briefing on the same day that the court ruling is made public.

Approximately 90 minutes after the ruling is public, the media availability will take place. There is still discussion about who from DoJ will be alongside the Director (either the DM or Senior General Counsel).

At the time of the media availability, we will issue the statement from the Minister and CSIS will issue the statement from the Director.

The technical briefing (by CSIS and Justice officials) will take place one hour after the media avail. We will host the tech briefing here.

---

**Jamie Tomlinson**  
Director General, Communications | Directeur général, communications  
Public Safety Canada | Sécurité publique Canada  
Telephone | Téléphone: 613-990-2642  
**New** E-mail | Courriel: [jamie.tomlinson@canada.ca](mailto:jamie.tomlinson@canada.ca)

## Arbeau, Kristy (PS/SP)

---

**From:** Tomlinson, Jamie (PS/SP)  
**Sent:** Thursday, November 03, 2016 3:19 PM  
**To:** Nichols, Megan (PS/SP); Baker3, Ryan (PS/SP); Magee, Heather (PS/SP); Grenier, Julie (PS/SP)  
**Subject:** FW: CSIS Federal Court decision - update - decision posted

fyi

---

**From:** Tomlinson, Jamie (PS/SP)  
**Sent:** November-03-16 3:18 PM  
**To:** Davies, John (PS/SP); Beaugard, Monik (PS/SP); [REDACTED] (PS/SP); [REDACTED] (PS/SP); Beecher, Sophie (PS/SP); Khouri, Lisa (PS/SP); De Santis, Heather (PS/SP); Brown, Malcolm (PS/SP); Wilson, Gina (PS/SP)  
**Cc:** Sousa, Michael (PS/SP); MacKinnon, Paul (PS/SP)  
**Subject:** RE: CSIS Federal Court decision - update - decision posted

Following discussion with PCO:

One media advisory.

Media avail at the National Press Theatre with CSIS Director and Robert Frater at 4:30pm.

Technical briefing via teleconference with CSIS and Justice officials at 6:00pm.

---

**From:** Davies, John (PS/SP)  
**Sent:** November-03-16 3:13 PM  
**To:** Beaugard, Monik (PS/SP); [REDACTED] (PS/SP); [REDACTED] (PS/SP); Beecher, Sophie (PS/SP); Khouri, Lisa (PS/SP); De Santis, Heather (PS/SP)  
**Cc:** Sousa, Michael (PS/SP); Tomlinson, Jamie (PS/SP)  
**Subject:** FW: CSIS Federal Court decision - update - decision posted

---

**From:** Bouzigon, Mylène [<mailto:Mylene.Bouzigon@justice.gc.ca>]  
**Sent:** Thursday, November 03, 2016 2:55 PM  
**To:** [REDACTED] (CSIS); Matte, Daniel; 'Vigneault, David'; [REDACTED]; [REDACTED] 'Noftle, Tracie'; 'O'Nions, Christine'; Off, Shirley Anne; Ghiz, Joanne; Webber, Grégoire; Tomlinson, Jamie (PS/SP); Hurl, David (PS/SP); Davies, John (PS/SP); Brien, Dan (PS/SP); [REDACTED]; Gowing, Andrew; [REDACTED] (PS/SP); Brender, James (PS/SP); Allen, Kristine; [REDACTED]; Leclerc, Caroline; Sousa, Michael (PS/SP)  
**Cc:** [REDACTED] Farkas, Jennifer; Benoit, Nathalie; Frater, Robert  
**Subject:** RE: CSIS Federal Court decision - update - decision posted

En Banc decision posted now.

It is now live:

[http://cas-cdc-www02.cas-sati.gc.ca/rss/DES%20\(warrant\)%20nov-3-2016%20Media%20Summary%20FINAL%20\(ENG\).pdf](http://cas-cdc-www02.cas-sati.gc.ca/rss/DES%20(warrant)%20nov-3-2016%20Media%20Summary%20FINAL%20(ENG).pdf)

MB

## Arbeau, Kristy (PS/SP)

---

**From:** Tomlinson, Jamie (PS/SP)  
**Sent:** Wednesday, November 02, 2016 12:26 PM  
**To:** Baker3, Ryan (PS/SP); Magee, Heather (PS/SP); Grenier, Julie (PS/SP); Nichols, Megan (PS/SP)  
**Subject:** Fw: CSIS Federal Court decision - update

Fyi

Sent from my BlackBerry 10 smartphone on the Rogers network.

Original Message

**From:** De Mora, Joe <Joe.DeMora@justice.gc.ca>  
**Sent:** Wednesday, November 2, 2016 12:21 PM  
**To:** Fox, Christiane; [REDACTED] Off, Shirley Anne; Noftle, Tracie; O'Nions, Christine  
**Cc:** Tomlinson, Jamie (PS/SP); [REDACTED]  
**Subject:** Re: CSIS Federal Court decision - update

Latest I have is that it will be Rob Frater from our side that will accompany the Director for the presser. He will not offer opening remarks but will be there if questions are directed to Justice.

Joe

Original Message

**From:** Fox, Christiane  
**Sent:** Wednesday, November 2, 2016 7:05 AM  
**To:** [REDACTED] Off, Shirley Anne; Noftle, Tracie; O'Nions, Christine  
**Cc:** Jamie Tomlinson; De Mora, Joe; [REDACTED]  
**Subject:** Re: CSIS Federal Court decision - update

That is accurate although I understand DoJ had reconsidered but we remain of the view that it should be the DM. Chris

Sent from my BlackBerry 10 smartphone on the Rogers network.

**From:** [REDACTED]  
**Sent:** Wednesday, November 2, 2016 6:54 AM  
**To:** Off, Shirley Anne; Fox, Christiane; Noftle, Tracie; O'Nions, Christine  
**Cc:** Jamie Tomlinson; De Mora, Joe; [REDACTED]  
**Subject:** Re: CSIS Federal Court decision - update

My understanding is that it was confirmed mid-week last week to the Director by Assistant secretary David V at PCO;

**From:** Off, Shirley Anne  
**Sent:** Tuesday, November 1, 2016 10:01 PM  
**To:** [REDACTED] Fox, Christiane; Noftle, Tracie; O'Nions, Christine  
**Cc:** Jamie Tomlinson; De Mora, Joe; [REDACTED]

Subject: Re: CSIS Federal Court decision - update

To clarify - we have Geoff confirmed. Discussions still underway re DM. Will try to get more info tomorrow.

Sent from my BlackBerry 10 smartphone on the Rogers network.

From: [REDACTED]  
Sent: Tuesday, November 1, 2016 9:52 PM  
To: Fox, Christiane; Noftle, Tracie; O'Nions, Christine  
Cc: Jamie Tomlinson; Off, Shirley Anne; De Mora, Joe; [REDACTED]  
Subject: Re: CSIS Federal Court decision - update

That would be great.

Yes, Shirley Ann can jump in, but last confirmation we had heard was that the DM would participate in the media avail and Geoff Bickert in the background brief.

From: Fox, Christiane  
Sent: Tuesday, November 1, 2016 9:01 PM  
To: [REDACTED] Noftle, Tracie; O'Nions, Christine  
Cc: Jamie Tomlinson; Shirley Anne Off; Joe De Mora; [REDACTED]  
Subject: RE: CSIS Federal Court decision - update

Hi.

I am told we will get them first thing tomorrow – there is also ongoing discussions to have someone from DOJ at the presser – have we nailed that down on our end?

From: [REDACTED] [mailto:[REDACTED]]  
Sent: November-01-16 18:46  
To: Fox, Christiane; Noftle, Tracie; O'Nions, Christine  
Cc: Jamie Tomlinson; Shirley Anne Off; Joe De Mora; [REDACTED]  
Subject: Fw: CSIS Federal Court decision - update

Chris, Tracie, Christine,

[REDACTED]

Shirley Anne/Joe, I will send you tomorrow a.m. the scripts for the media avail and bkgd brief sessions for your quick review.

Could PCO reconvene the group via teleconference tomorrow, perhaps early afternoon?

[REDACTED]

[REDACTED]  
DG, Communications  
[REDACTED]

From: Bouzigon, Mylène <Mylene.Bouzigon@justice.gc.ca>

Sent: Tuesday, November 1, 2016 5:16 PM

To: [REDACTED] Matte, Daniel; Vigneault, David; [REDACTED]

[REDACTED]; Nofle, Tracie; O'Nions, Christine; Off, Shirley Anne; Ghiz, Joanne; Webber, Grégoire;

'jamie.tomlinson@canada.ca'; 'david.hurl@canada.ca'; john.davies@canada.ca; 'dan.brien@canada.ca'; [REDACTED]

[REDACTED]; Gowing, Andrew; [REDACTED] (PS/SP); 'Brender, James (PS/SP)'; Allen, Kristine; [REDACTED] Leclerc,

Caroline; Sousa, Michael (PS)

Cc [REDACTED] Farkas, Jennifer; Benoit, Nathalie; Frater, Robert

Subject: CSIS Federal Court decision - update

Good afternoon,

[REDACTED]

Mylène

Me Mylène Bouzigon

Senior General Counsel | Avocate générale principale

(613) 842-1197 / (613) 231-0027 | bouzigon.mylene@justice.gc.ca<mailto:bouzigon.mylene@justice.gc.ca> | Facsimile  
- télécopieur: (613) 842-1345

This communication contains information that may be confidential, exempt from disclosure, subject to litigation privilege or protected by the privilege that exists between lawyers and their clients. If you are not the intended recipient, you should not read, rely on, retain, or distribute it. Please delete or otherwise destroy this communication and all copies of it immediately, and contact the sender.

Ce message contient des renseignements qui pourraient être confidentiels, soustraits à la communication, ou protégés par le privilège relatif au litige ou par le secret professionnel liant l'avocat à son client. S'il ne vous est pas destiné, vous êtes priés de ne pas le lire, l'utiliser, le conserver ou le diffuser. Veuillez sans tarder le supprimer et en détruire toute copie, et communiquer avec l'expéditeur.

## Arbeau, Kristy (PS/SP)

---

**From:** Tomlinson, Jamie (PS/SP)  
**Sent:** Wednesday, November 02, 2016 10:28 AM  
**To:** Baker3, Ryan (PS/SP); Magee, Heather (PS/SP); Nichols, Megan (PS/SP)  
**Subject:** Fw: CSIS Federal Court decision - update

Fyi

Sent from my BlackBerry 10 smartphone on the Rogers network.

---

**From:** Bustros, Katia <[Katia.Bustros@justice.gc.ca](mailto:Katia.Bustros@justice.gc.ca)>  
**Sent:** Wednesday, November 2, 2016 10:11 AM  
**To:** Bouzigon, Mylène; [REDACTED] (CSIS); Matte, Daniel; Vigneault, David; [REDACTED] Noftle, Tracie; O'Nions, Christine; Off, Shirley Anne; Ghiz, Joanne; Webber, Grégoire; Tomlinson, Jamie (PS/SP); Hurl, David (PS/SP); Davies, John (PS/SP); Brien, Dan (PS/SP); [REDACTED] Gowing, Andrew; [REDACTED] (PS/SP); Brender, James (PS/SP); Allen, Kristine; [REDACTED]; Leclerc, Caroline; Sousa, Michael (PS/SP)  
**Cc:** Farkas, Jennifer; Benoit, Nathalie; Frater, Robert  
**Subject:** RE: CSIS Federal Court decision - update

Good morning,

[REDACTED]

Thank you.

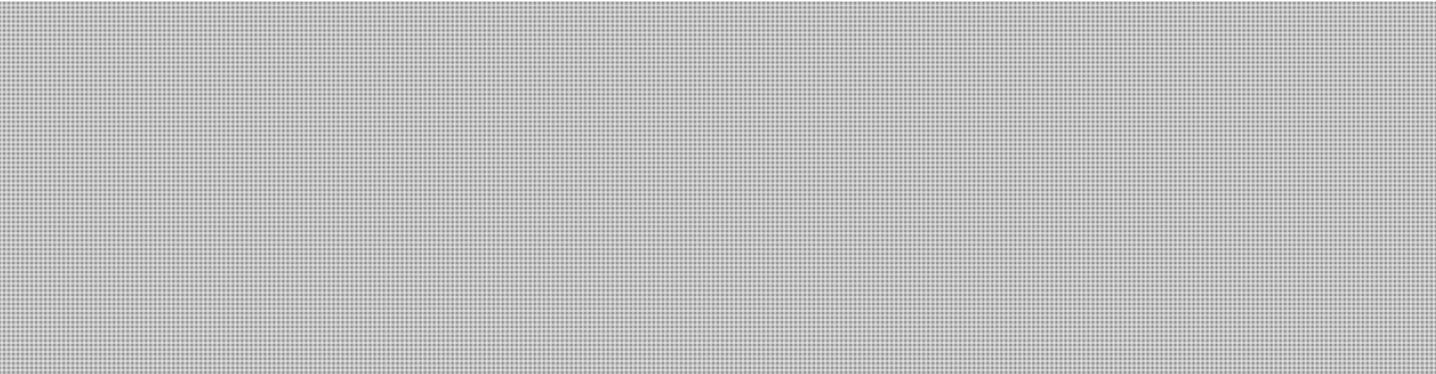
Katia

Katia Bustros  
Avocate-conseil | Senior Counsel  
Ministère de la Justice Canada | Department of Justice Canada  
Groupe Litiges et conseils | National Security Litigation  
en sécurité nationale & Advisory Group  
Tél. | Tel.: 613 231-0009  
Télé. | Fax: 613 842-1345  
Courriel | e-mail: [katia.bustros@justice.gc.ca](mailto:katia.bustros@justice.gc.ca)  
Gouvernement du Canada | Government of Canada

**From:** Bouzigon, Mylène  
**Sent:** Tuesday, November 01, 2016 5:03 PM

To: [redacted]; Matte, Daniel <Daniel.Matte@justice.gc.ca>; Vigneault, David <David.Vigneault@pco-bcp.gc.ca>; [redacted]@pco-bcp.gc.ca>; [redacted]  
[redacted] Noftle, Tracie <Tracie.Noftle@pco-bcp.gc.ca>; O'Nions, Christine <Christine.O'Nions@pco-bcp.gc.ca>; Off, Shirley Anne <ShirleyAnne.Off@justice.gc.ca>; Ghiz, Joanne <Joanne.Ghiz@justice.gc.ca>; Webber, Grégoire <Gregoire.Webber@justice.gc.ca>; 'jamie.tomlinson@canada.ca' <jamie.tomlinson@canada.ca>; 'david.hurl@canada.ca' <david.hurl@canada.ca>; john.davies@canada.ca; 'dan.brien@canada.ca' <dan.brien@canada.ca>; [redacted]  
[redacted]; Gowing, Andrew <Andrew.Gowing@justice.gc.ca>; [redacted] (PS/SP) @canada.ca>; 'Brender, James (PS/SP)' <james.brender@canada.ca>; Allen, Kristine <Kristine.Allen@justice.gc.ca>; [redacted]@smtp.gc.ca>; Leclerc, Caroline <Caroline.Leclerc@justice.gc.ca>; Sousa, Michael (PS) <Michael.Sousa@canada.ca>  
Cc: Bustros, Katia <Katia.Bustros@justice.gc.ca>; Farkas, Jennifer <Jennifer.Farkas@justice.gc.ca>; Benoit, Nathalie <Nathalie.Benoit@justice.gc.ca>; Frater, Robert <Robert.Frater@justice.gc.ca>  
Subject: CSIS Federal Court decision - update

Good afternoon,



Mylène

**Me Mylène Bouzigon**

Senior General Counsel | Avocate générale principale

(613) 842-1197 / (613) 231-0027 | [bouzigon.mylene@justice.gc.ca](mailto:bouzigon.mylene@justice.gc.ca) | Facsimile - télécopieur: (613) 842-1345

*This communication contains information that may be confidential, exempt from disclosure, subject to litigation privilege or protected by the privilege that exists between lawyers and their clients. If you are not the intended recipient, you should not read, rely on, retain, or distribute it. Please delete or otherwise destroy this communication and all copies of it immediately, and contact the sender.*

*Ce message contient des renseignements qui pourraient être confidentiels, soustraits à la communication, ou protégés par le privilège relatif au litige ou par le secret professionnel liant l'avocat à son client. S'il ne vous est pas destiné, vous êtes priés de ne pas le lire, l'utiliser, le conserver ou le diffuser. Veuillez sans tarder le supprimer et en détruire toute copie, et communiquer avec l'expéditeur.*

## **Arbeau, Kristy (PS/SP)**

---

**From:** Tomlinson, Jamie (PS/SP)  
**Sent:** Wednesday, November 02, 2016 8:33 AM  
**To:** Nichols, Megan (PS/SP)  
**Subject:** RE: CSIS Federal Court decision - update

Thanks!

Btw... as I was thinking about it, I wasn't clear as to who will draft the note to staff about the staff meeting. Was it me or you?

-----Original Message-----

**From:** Nichols, Megan (PS/SP)  
**Sent:** November-02-16 8:32 AM  
**To:** Tomlinson, Jamie (PS/SP)  
**Subject:** Re: CSIS Federal Court decision - update

Thanks! Enjoy the session this morning.

Sent from my BlackBerry 10 smartphone on the Rogers network.

Original Message  
**From:** Tomlinson, Jamie (PS/SP)  
**Sent:** Wednesday, November 2, 2016 8:27 AM  
**To:** Nichols, Megan (PS/SP)  
**Subject:** RE: CSIS Federal Court decision - update

Yes - the sequencing will be as soon as we know court decision is public, statements from CSIS Director and Minister get posted.

A short time later (we would issue the media advisory soon after posting the statements) the media availability with the Director and Justice DM takes places. About an hour after that, the tech briefing with CSIS and Justice officials happens. It will be a teleconference.

Depending on timing (ie whether it is Thursday or Friday), the Minister may scrum with media before or after QP.

-----Original Message-----

**From:** Nichols, Megan (PS/SP)  
**Sent:** November-02-16 8:20 AM  
**To:** Tomlinson, Jamie (PS/SP)  
**Subject:** Re: CSIS Federal Court decision - update

Jamie, I guess the EXCOM update on this is that we are on standby to host the tech brief, release statements, etc, as soon as the release happens?

Sent from my BlackBerry 10 smartphone on the Rogers network.

Original Message

From: Tomlinson, Jamie (PS/SP)  
Sent: Tuesday, November 1, 2016 6:58 PM  
To: Baker3, Ryan (PS/SP); Magee, Heather (PS/SP); Grenier, Julie (PS/SP)  
Cc: Nichols, Megan (PS/SP)  
Subject: Fw: CSIS Federal Court decision - update

Fyi

Sent from my BlackBerry 10 smartphone on the Rogers network.

Original Message

From: O'Nions, Christine <Christine.O'Nions@pco-bcp.gc.ca>  
Sent: Tuesday, November 1, 2016 6:52 PM  
To: [REDACTED] Fox, Christiane; Noftle, Tracie  
Cc: Tomlinson, Jamie (PS/SP); Shirley Anne Off; Joe De Mora; [REDACTED]  
Subject: Re: CSIS Federal Court decision - update

I will prompt first thing in the morning.

Sent from my BlackBerry 10 smartphone on the Rogers network.

From: [REDACTED]  
Sent: Tuesday, November 1, 2016 6:45 PM  
To: Fox, Christiane; Noftle, Tracie; O'Nions, Christine  
Cc: Jamie Tomlinson; Shirley Anne Off; Joe De Mora; [REDACTED] Anam ALVI  
Subject: Fw: CSIS Federal Court decision - update

Chris, Tracie, Christine,

[REDACTED]

Shirley Anne/Joe, I will send you tomorrow a.m. the scripts for the media avail and bkgd brief sessions for your quick review.

Could PCO reconvene the group via teleconference tomorrow, perhaps early afternoon?

[REDACTED]

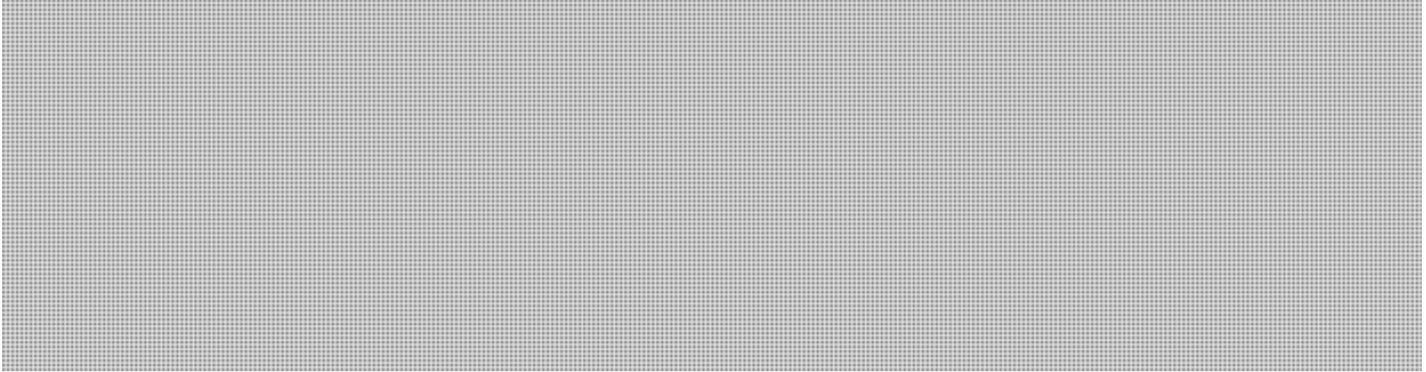
DG, Communications

[REDACTED]

From: Bouzigon, Mylène <Mylene.Bouzigon@justice.gc.ca>  
Sent: Tuesday, November 1, 2016 5:16 PM  
To: [REDACTED] Matte, Daniel; Vigneault, David; [REDACTED]  
[REDACTED] Noftle, Tracie; O'Nions, Christine; Off, Shirley Anne; Ghiz, Joanne; Webber, Grégoire;

'jamie.tomlinson@canada.ca'; 'david.hurl@canada.ca'; john.davies@canada.ca; 'dan.brien@canada.ca'; [REDACTED]  
[REDACTED] Gowing, Andrew; [REDACTED] (PS/SP); 'Brender, James (PS/SP)'; Allen, Kristine; [REDACTED] Leclerc,  
Caroline; Sousa, Michael (PS)  
Cc: Bustros, Katia; Farkas, Jennifer; Benoit, Nathalie; Frater, Robert  
Subject: CSIS Federal Court decision - update

Good afternoon,



Mylène

Me Mylène Bouzigon  
Senior General Counsel | Avocate générale principale

(613) 842-1197 / (613) 231-0027 | bouzigon.mylene@justice.gc.ca<mailto:bouzigon.mylene@justice.gc.ca> | Facsimile  
- télécopieur: (613) 842-1345

This communication contains information that may be confidential, exempt from disclosure, subject to litigation privilege or protected by the privilege that exists between lawyers and their clients. If you are not the intended recipient, you should not read, rely on, retain, or distribute it. Please delete or otherwise destroy this communication and all copies of it immediately, and contact the sender.

Ce message contient des renseignements qui pourraient être confidentiels, soustraits à la communication, ou protégés par le privilège relatif au litige ou par le secret professionnel liant l'avocat à son client. S'il ne vous est pas destiné, vous êtes priés de ne pas le lire, l'utiliser, le conserver ou le diffuser. Veuillez sans tarder le supprimer et en détruire toute copie, et communiquer avec l'expéditeur.

## **Arbeau, Kristy (PS/SP)**

---

**From:** Baker3, Ryan (PS/SP)  
**Sent:** Tuesday, November 01, 2016 6:51 PM  
**To:** Magee, Heather (PS/SP); Tomlinson, Jamie (PS/SP); Nichols, Megan (PS/SP); Grenier, Julie (PS/SP)  
**Subject:** Re: CSIS Federal Court decision - update

Hi Heather,

Yes, will make arrangements for tech brief. Will also follow up on products.

Enjoy your training!

Ryan

Ryan Baker  
Public Safety Canada/ Sécurité publique Canada  
613-796-9750

---

**From:** Magee, Heather (PS/SP)  
**Sent:** Tuesday, November 1, 2016 6:18 PM  
**To:** Tomlinson, Jamie (PS/SP); Nichols, Megan (PS/SP); Baker3, Ryan (PS/SP); Grenier, Julie (PS/SP)  
**Subject:** Re: CSIS Federal Court decision - update

One thing to flag, if this happens Thursday we are also doing our Twitter chat. We already have a mitigation plan in place and are developing tweets that would direct to the statements and CSIS has been engaged. I recommend we still proceed but would like to know what others think.

That said, we were using the triple C for our Twitter chat so if there is also a CSIS tech briefing call we may need to look at room options just in case there is a conflict re: timing (hopefully not).

Ryan: As I am out of the office tomorrow could you look into a plan B for the room. Thanks!

Heather Magee  
Public Safety Canada / Sécurité publique Canada  
T: 613-949-6191 M: 613-302-3752  
[Heather.Magee@canada.ca](mailto:Heather.Magee@canada.ca)

---

**From:** Tomlinson, Jamie (PS/SP)  
**Sent:** Tuesday, November 1, 2016 5:14 PM  
**To:** Nichols, Megan (PS/SP); Magee, Heather (PS/SP); Baker3, Ryan (PS/SP); Grenier, Julie (PS/SP)  
**Cc:** MacKinnon, Paul (PS/SP); Nguyen, Linda (PS/SP)  
**Subject:** FW: CSIS Federal Court decision - update

fyi

**From:** Brien, Dan (PS/SP)  
**Sent:** November-01-16 5:08 PM  
**To:** Surkes, Marci (PS/SP); Tomlinson, Jamie (PS/SP); Hurl, David (PS/SP); Pike, Cory (PS/SP); Baker3, Ryan (PS/SP)  
**Subject:** Fw: CSIS Federal Court decision - update  
**Importance:** High

Heads up - Here we go.

db mobile  
613.698.2270

---

**From:** Bouzigon, Mylène <[Mylene.Bouzigon@justice.gc.ca](mailto:Mylene.Bouzigon@justice.gc.ca)>  
**Sent:** Tuesday, November 1, 2016 5:03 PM  
**To:** [REDACTED] (CSIS); Matte, Daniel; Vigneault, David; Rogers, Daniel; [REDACTED]  
[REDACTED] Michael; Nofle, Tracie; O'Nions, Christine; Off, Shirley Anne; Ghiz, Joanne; Webber, Grégoire;  
Tomlinson, Jamie (PS/SP); Hurl, David (PS/SP); Davies, John (PS/SP); Brien, Dan (PS/SP);  
Gowing, Andrew; [REDACTED] (PS/SP); Brender, James (PS/SP); Allen, Kristine; [REDACTED]; Leclerc, Caroline; Sousa,  
Michael (PS/SP)  
**Cc:** Bustros, Katia; Farkas, Jennifer; Benoit, Nathalie; Frater, Robert  
**Subject:** CSIS Federal Court decision - update

Good afternoon,

Mylène

**Me Mylène Bouzigon**  
Senior General Counsel | Avocate générale principale

(613) 842-1197 / (613) 231-0027 | [bouzigon.mylene@justice.gc.ca](mailto:bouzigon.mylene@justice.gc.ca) | Facsimile - télécopieur: (613) 842-1345

*This communication contains information that may be confidential, exempt from disclosure, subject to litigation privilege or protected by the privilege that exists between lawyers and their clients. If you are not the intended recipient, you should not read, rely on, retain, or distribute it. Please delete or otherwise destroy this communication and all copies of it immediately, and contact the sender.*

*Ce message contient des renseignements qui pourraient être confidentiels, soustraits à la communication, ou protégés par le privilège relatif au litige ou par le secret professionnel liant l'avocat à son client. S'il ne vous est pas destiné, vous êtes priés de ne pas le lire, l'utiliser, le conserver ou le diffuser. Veuillez sans tarder le supprimer et en détruire toute copie, et communiquer avec l'expéditeur.*

## **Arbeau, Kristy (PS/SP)**

---

**From:** Tomlinson, Jamie (PS/SP)  
**Sent:** Tuesday, November 01, 2016 6:22 PM  
**To:** Magee, Heather (PS/SP); Nichols, Megan (PS/SP); Baker3, Ryan (PS/SP); Grenier, Julie (PS/SP)  
**Subject:** Re: CSIS Federal Court decision - update

The Twitter chat proceeds. If anything it is timely - you have views on CSIS oversight? we want to hear those views as part of our national security consultations.

Sent from my BlackBerry 10 smartphone on the Rogers network.

---

**From:** Magee, Heather (PS/SP)  
**Sent:** Tuesday, November 1, 2016 6:18 PM  
**To:** Tomlinson, Jamie (PS/SP); Nichols, Megan (PS/SP); Baker3, Ryan (PS/SP); Grenier, Julie (PS/SP)  
**Subject:** Re: CSIS Federal Court decision - update

One thing to flag, if this happens Thursday we are also doing our Twitter chat. We already have a mitigation plan in place and are developing tweets that would direct to the statements and CSIS has been engaged. I recommend we still proceed but would like to know what others think.

That said, we were using the triple C for our Twitter chat so if there is also a CSIS tech briefing call we may need to look at room options just in case there is a conflict re: timing (hopefully not).

Ryan: As I am out of the office tomorrow could you look into a plan B for the room. Thanks!

Heather Magee  
Public Safety Canada / Sécurité publique Canada  
T: 613-949-6191 M: 613-302-3752  
[Heather.Magee@canada.ca](mailto:Heather.Magee@canada.ca)

---

**From:** Tomlinson, Jamie (PS/SP)  
**Sent:** Tuesday, November 1, 2016 5:14 PM  
**To:** Nichols, Megan (PS/SP); Magee, Heather (PS/SP); Baker3, Ryan (PS/SP); Grenier, Julie (PS/SP)  
**Cc:** MacKinnon, Paul (PS/SP); Nguyen, Linda (PS/SP)  
**Subject:** FW: CSIS Federal Court decision - update

fyi

---

**From:** Brien, Dan (PS/SP)  
**Sent:** November-01-16 5:08 PM  
**To:** Surkes, Marci (PS/SP); Tomlinson, Jamie (PS/SP); Hurl, David (PS/SP); Pike, Cory (PS/SP); Baker3, Ryan (PS/SP)  
**Subject:** Fw: CSIS Federal Court decision - update  
**Importance:** High

Heads up - Here we go.

db mobile  
613.698.2270

**From:** Bouzigon, Mylène <Mylene.Bouzigon@justice.gc.ca>

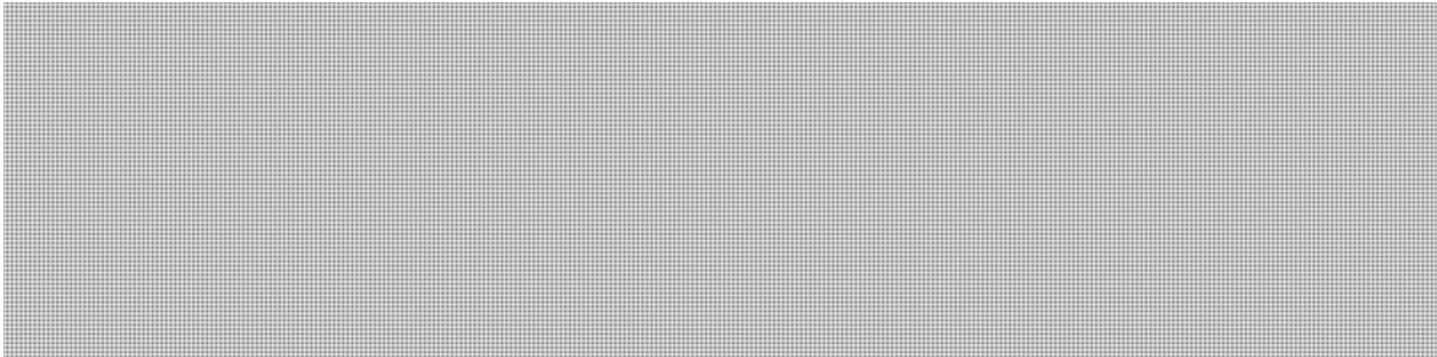
**Sent:** Tuesday, November 1, 2016 5:03 PM

**To:** [REDACTED] (CSIS); Matte, Daniel; Vigneault, David; Rogers, Daniel; [REDACTED] Michael; Nofle, Tracie; O'Nions, Christine; Off, Shirley Anne; Ghiz, Joanne; Webber, Grégoire; Tomlinson, Jamie (PS/SP); Hurl, David (PS/SP); Davies, John (PS/SP); Brien, Dan (PS/SP); [REDACTED] Gowing, Andrew; [REDACTED] (PS/SP); Brender, James (PS/SP); Allen, Kristine; [REDACTED] Leclerc, Caroline; Sousa, Michael (PS/SP)

**Cc:** Bustros, Katia; Farkas, Jennifer; Benoit, Nathalie; Frater, Robert

**Subject:** CSIS Federal Court decision - update

Good afternoon,



Mylène

**Me Mylène Bouzigon**

Senior General Counsel | Avocate générale principale

(613) 842-1197 / (613) 231-0027 | [bouzigon.mylene@justice.gc.ca](mailto:bouzigon.mylene@justice.gc.ca) | Facsimile - télécopieur: (613) 842-1345

*This communication contains information that may be confidential, exempt from disclosure, subject to litigation privilege or protected by the privilege that exists between lawyers and their clients. If you are not the intended recipient, you should not read, rely on, retain, or distribute it. Please delete or otherwise destroy this communication and all copies of it immediately, and contact the sender.*

*Ce message contient des renseignements qui pourraient être confidentiels, soustraits à la communication, ou protégés par le privilège relatif au litige ou par le secret professionnel liant l'avocat à son client. S'il ne vous est pas destiné, vous êtes priés de ne pas le lire, l'utiliser, le conserver ou le diffuser. Veuillez sans tarder le supprimer et en détruire toute copie, et communiquer avec l'expéditeur.*

## Arbeau, Kristy (PS/SP)

---

**From:** Tomlinson, Jamie (PS/SP)  
**Sent:** Tuesday, November 01, 2016 5:36 PM  
**To:** Brien, Dan (PS/SP); Baker3, Ryan (PS/SP); Nichols, Megan (PS/SP); Magee, Heather (PS/SP)  
**Subject:** RE: CSIS Federal Court decision - update

We will send you the latest set. We are following up with PCO – the products had not been PMO approved.

We will advise if we get word on another dry run.

---

**From:** Brien, Dan (PS/SP)  
**Sent:** November-01-16 5:28 PM  
**To:** Tomlinson, Jamie (PS/SP); Baker3, Ryan (PS/SP); Nichols, Megan (PS/SP); Magee, Heather (PS/SP)  
**Subject:** Fw: CSIS Federal Court decision - update

Have the products changed much? Do you know if another meet/dry run is being contemplated?

Either way, would appreciate a set of current products to refresh my memory - whether or not they're deemed final.

Thanks

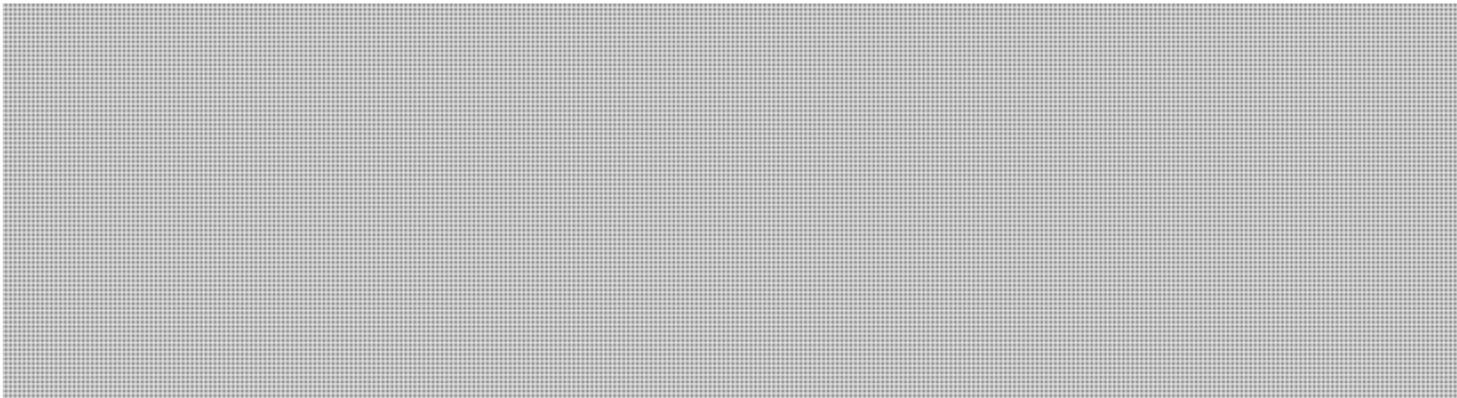
Dan

db mobile  
613.698.2270

---

**From:** Bouzigon, Mylène <Mylene.Bouzigon@justice.gc.ca>  
**Sent:** Tuesday, November 1, 2016 5:03 PM  
**To:** [REDACTED] (CSIS); Matte, Daniel; Vigneault, David; Rogers, Daniel; [REDACTED]; [REDACTED], Michael; Nofle, Tracie; O'Nions, Christine; Off, Shirley Anne; Ghiz, Joanne; Webber, Grégoire; Tomlinson, Jamie (PS/SP); Hurl, David (PS/SP); Davies, John (PS/SP); Brien, Dan (PS/SP); Gowing, Andrew; [REDACTED] (PS/SP); Brender, James (PS/SP); Allen, Kristine; [REDACTED]; Leclerc, Caroline; Sousa, Michael (PS/SP)  
**Cc:** Bustros, Katia; Farkas, Jennifer; Benoit, Nathalie; Frater, Robert  
**Subject:** CSIS Federal Court decision - update

Good afternoon,



Mylène

**Me Mylène Bouzigon**

Senior General Counsel | Avocate générale principale

(613) 842-1197 / (613) 231-0027 | [bouzigon.mylene@justice.gc.ca](mailto:bouzigon.mylene@justice.gc.ca) | Facsimile - télécopieur: (613) 842-1345

*This communication contains information that may be confidential, exempt from disclosure, subject to litigation privilege or protected by the privilege that exists between lawyers and their clients. If you are not the intended recipient, you should not read, rely on, retain, or distribute it. Please delete or otherwise destroy this communication and all copies of it immediately, and contact the sender.*

*Ce message contient des renseignements qui pourraient être confidentiels, soustraits à la communication, ou protégés par le privilège relatif au litige ou par le secret professionnel liant l'avocat à son client. S'il ne vous est pas destiné, vous êtes priés de ne pas le lire, l'utiliser, le conserver ou le diffuser. Veuillez sans tarder le supprimer et en détruire toute copie, et communiquer avec l'expéditeur.*

## Sayarh, Omar (PS/SP)

---

**From:** Tomlinson, Jamie (PS/SP)  
**Sent:** Wednesday, October 26, 2016 5:23 PM  
**To:** Magee, Heather (PS/SP); Grenier, Julie (PS/SP)  
**Subject:** FW: Q & A: What is Metadata?

fyi

---

**From:** [redacted] [mailto:[redacted]@pco-bcp.gc.ca]  
**Sent:** October-26-16 5:23 PM  
**To:** [redacted] Millar, Scott D.; Davies, John (PS/SP); Matz, Mark (PS/SP); Merchant, Colleen (PS/SP); Alison Whelan (Alison.Whelan@rcmp-grc.gc.ca)  
**Cc:** Tomlinson, Jamie (PS/SP); Beecher, Sophie (PS/SP); [redacted] (PS/SP); [redacted] (PS/SP)  
**Subject:** RE: Q & A: What is Metadata?

No concerns on my end.

---

**From:** [redacted]  
**Sent:** October-26-16 2:43 PM  
**To:** Millar, Scott D.; Davies, John (PS/SP); [redacted] Matz, Mark (PS/SP); Merchant, Colleen (PS/SP); Alison Whelan (Alison.Whelan@rcmp-grc.gc.ca)  
**Cc:** Tomlinson, Jamie (PS/SP); Beecher, Sophie (PS/SP); [redacted] (PS/SP); [redacted] (PS/SP)  
**Subject:** Re: Q & A: What is Metadata?

It's accurate from our perspective. There is a nuance to it that our adm of tech wants to discuss with theirs, but for this purpose, it's accurate. Thanks guys, T

---

**From:** Millar, Scott D.  
**Sent:** Wednesday, October 26, 2016 12:07 PM  
**To:** Davies, John (PS/SP); [redacted] Matz, Mark (PS/SP); Merchant, Colleen (PS/SP); Alison Whelan (Alison.Whelan@rcmp-grc.gc.ca)  
**Cc:** Tomlinson, Jamie (PS/SP); Beecher, Sophie (PS/SP); [redacted] (PS/SP); [redacted] (PS/SP)  
**Subject:** Re: Q & A: What is Metadata?

I'm biased, but I love it.

---

**From:** Davies, John (PS/SP)  
**Sent:** Wednesday, October 26, 2016 10:32 AM  
**To:** [redacted] Millar, Scott D.; [redacted] Matz, Mark (PS/SP); Merchant, Colleen (PS/SP); Alison Whelan (Alison.Whelan@rcmp-grc.gc.ca)  
**Cc:** Tomlinson, Jamie (PS/SP); Beecher, Sophie (PS/SP); [redacted] (PS/SP); [redacted] (PS/SP)  
**Subject:** Q & A: What is Metadata?

Can everyone confirm they are OK with the answer below? This was asked for in context of upcoming MIN Committee appearances (and possibly other media issues). Our DM has suggested it would be good to have one definition we all are working from. The core of the definition is taken from CSE website. Thanks. John

<https://www.cse-cst.gc.ca/en/inside-interieur/metadata-metadonnees>

Q: What is metadata?

A:

- Metadata is the context, not the content of a communication.
- It is information used to identify, describe, manage or route communications across networks. For example, metadata can refer to an internet protocol address or a phone number or the time of a transmission or the location of a device.

**Sayarh, Omar (PS/SP)**

---

**From:** [REDACTED] (PS/SP)  
**Sent:** Wednesday, October 26, 2016 1:23 PM  
**To:** Grenier, Julie (PS/SP)  
**Subject:** Backgrounder on Metadata  
**Attachments:** PS-SP-#2001277-1-Metadata Overview.DOCX

**Importance:** Low

FYI – Attached is a useful backgrounder re metadata that you may wish to read. [REDACTED]

[REDACTED]

[REDACTED]

**Page 186**

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

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

## Sayarh, Omar (PS/SP)

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Wednesday, October 26, 2016 10:50 AM  
**To:** [REDACTED] (PS/SP)  
**Subject:** RE: Q & A: What is Metadata?  
**Attachments:** MRLs\_2014-2015\_OCSEC\_Annual\_Report.doc

Thanks for letting me know!

CSE used very similar messaging in their Media Lines for the last OCSEC report (which you may recall focused on an issue related to metadata) Attached for reference.

They also added this bullet, which I feel could be useful to communicate for public audiences – but I recognize that it may be too late to amend:

- Metadata is not the content of a communication. Metadata does not include the content of e-mails, text messages, phone calls, photos or any other electronic communication.

Julie G

Tel : 613-993-4415 | BB : 613-410-6059

---

**From:** [REDACTED] (PS/SP)  
**Sent:** Wednesday, October 26, 2016 10:43 AM  
**To:** Grenier, Julie (PS/SP)  
**Subject:** FW: Q & A: What is Metadata?

FYI – this Q & A has been sent for consult to CSIS and CSE.

---

**From:** Davies, John (PS/SP)  
**Sent:** Wednesday, October 26, 2016 10:33 AM  
**To:** [REDACTED]; Millar, Scott D.; [REDACTED] Matz, Mark (PS/SP); Merchant, Colleen (PS/SP); Alison Whelan ([Alison.Whelan@rcmp-grc.gc.ca](mailto:Alison.Whelan@rcmp-grc.gc.ca))  
**Cc:** Tomlinson, Jamie (PS/SP); Beecher, Sophie (PS/SP); [REDACTED] (PS/SP); [REDACTED] (PS/SP)  
**Subject:** Q & A: What is Metadata?

Can everyone confirm they are OK with the answer below? This was asked for in context of upcoming MIN Committee appearances (and possibly other media issues). Our DM has suggested it would be good to have one definition we all are working from. The core of the definition is taken from CSE website. Thanks. John

<https://www.cse-cst.gc.ca/en/inside-interieur/metadata-metadonnees>

Q: What is metadata?

A:

- Metadata is the context, not the content of a communication.

- It is information used to identify, describe, manage or route communications across networks. For example, metadata can refer to an internet protocol address or a phone number or the time of a transmission or the location of a device.

UNCLASSIFIED

CERRID# 25603023

## **MEDIA RESPONSE LINES**

**ISSUE:** Tabling of 2014-2015 CSE Commissioner Annual Report, and release of findings related to a review of certain metadata activities.

**Media Query:** In anticipation of inquiries

**Date:** 15 January 2016

## **OVERVIEW**

The CSE Commissioner has submitted his 2014-2015 annual report to the Minister of National Defence. The report summarizes the results of nine classified reports that the Commissioner submitted to the Minister in 2014-2015:

- Review of metadata activities related to CSE's foreign signals intelligences activities.
- Review of CSE's information technology security activities conducted under Ministerial Authorization.
- Review of the Canadian Armed Forces Cyber Support Detachments.
- Review of CSE assistance to the Canadian Security Intelligence Service under Part C of CSE's mandate and section 16 of the CSIS Act. Three annual combined reviews: Foreign signals intelligence ministerial authorizations, and two spot check reviews of intercepted private communications.
- Annual review of disclosures of Canadian identity information, 2013-2014.
- Annual review of CSE's Privacy Incidents File and Minor Procedural Errors Record, 2014.

The Commissioner's report is expected to be tabled in parliament in January 2016.

- The Minister will also confirm that he has received the findings of a completed review related to a review of certain metadata activities. The review was flagged in the annual report, and has been completed in the time since the annual report was finalized.

## **KEY MESSAGES**

### **Annual Report**

- The independent CSE Commissioner has submitted his annual report to the Minister of National Defence, who has tabled the report in Parliament.
- In the 2014-2015 annual report, the CSE Commissioner made eight recommendations to promote compliance with the law and to strengthen privacy protections.

*UNCLASSIFIED*

CERRID# 25603023

- Over the course of the year, the Commissioner submitted nine classified reports to the Minister of National Defence, containing these eight recommendations. All eight of the recommendations have been accepted by CSE and by the Minister.
- With the exception of one review related to metadata, the Commissioner found that all of the CSE activities reviewed in 2014-2015 complied with the law.
- The Commissioner noted that CSE dealt with his office in a forthright manner, and remarked that CSE's transparency with his office is a testament to the seriousness and confidence with which CSE approaches its legislated mandate.

### **Metadata Review**

- During the course of a review of certain CSE metadata activities, CSE discovered on its own that certain metadata was not being properly minimized prior to being shared with allies, due to technical deficiencies.
- CSE proactively informed the Minister of National Defence and the Commissioner about these matters.
- CSE proactively suspended the sharing of certain types of metadata. The suspension of these activities will be in place until the Chief of CSE and, subsequently, The Minister of National Defence are satisfied that proper systems are in place to ensure that all Canadian identity information is properly minimized according to the 2011 Ministerial Directive on metadata.
- The CSE Commissioner stated that he believes this error was unintentional and that there was no intention of the part of CSE to act in a way that did not conform to ministerial direction or operational policy.

### **The Office of the CSE Commissioner**

- The CSE Commissioner is a fully independent review body. The CSE Commissioner reviews activities undertaken by CSE, and must review all activities carried out under a Ministerial Authorization.
- The Commissioner and his expert staff have complete access to CSE facilities, information holdings and employees at all stages of their review activities.
- The Commissioner independently determines which activities his staff will review in any given year.
- Since 1997, the Commissioner has submitted 90 classified reports to the Minister. In total, the reports have made 156 recommendations.

UNCLASSIFIED

CERRID# 25603023

- The Commissioner states that CSE has accepted and implemented and/or is working to address 93% (145 of 156) of these recommendations. All eight recommendations from this year have been accepted by the Minister and CSE.
- This year, CSE advised the Commissioner that work had been completed in response to six past recommendations.
- The Commissioner has confirmed that the scope of his powers and the size of his office are sufficient to fully review CSE.

### **Outstanding Recommendations**

- Those few recommendations not implemented are typically no longer relevant as a result of events or circumstances. They may also have been determined by CSE to have minimal risk or have not been feasible, or there are already appropriate safeguards in place.
- In an instance where CSE does not implement a recommendation, the Commissioner reviews the reasons provided by CSE, then assesses whether to accept these reasons or to pursue the issue further.

### **About CSE**

- The Communications Security Establishment (CSE) is mandated to collect foreign signals and provide intelligence in response to the Government of Canada's intelligence priorities. CSE also helps Government of Canada departments and agencies effectively secure their electronic information and networks. In addition, CSE provides assistance to federal law enforcement and security agencies.
- The Chief of CSE Reports to the Minister of National Defence. CSE is subject to all federal legislation governing finance, human resources, privacy and access to information, including the *Charter of Rights and Freedoms*, the *Privacy Act*, and the *Criminal Code of Canada*.

### **Metadata**

- Metadata is information about communications used by computer systems to identify, describe, manage or route communications over global communications networks. The *National Defence Act* lawfully authorizes CSE to collect and use metadata.
- Metadata is not the content of a communication. Metadata does not include the content of e-mails, text messages, phone calls, photos or any other electronic communication.
- CSE collects metadata to better understand complex global communications networks, assess cyber threats, and to ensure that our foreign intelligence activities are directed only at legitimate foreign targets, and not at Canadians or at anyone in Canada.

UNCLASSIFIED

CERRID# 25603023

- Metadata is essential in determining the location of a communication and helps CSE avoid directing its activities at a Canadian or any person in Canada.

## 2014-2015 Report

### Review of metadata activities related to CSE's foreign signals intelligences activities

- This review examined metadata activities related to CSE's foreign intelligence activities, and is the first in an ongoing comprehensive review of CSE's metadata activities.
- The Commissioner confirmed that metadata remains critical to all aspects of CSE's foreign intelligence mission.
- The Commissioner noted that metadata is essential in helping CSE to avoid directing its activities at a Canadian or any person in Canada.
- While this review was being conducted, CSE discovered on its own that certain types of metadata were not being properly minimized due to technical deficiencies. The Commissioner found that CSE took corrective actions and proactively suspended the sharing of certain types of metadata in order to protect the privacy of Canadians. CSE proactively informed the Minister of National Defence and the Commissioner about these matters.
- The Commissioner stated that he believes this failure to minimize information was unintentional: there was no intention of the part of CSE to act in a way that did not conform to ministerial direction or operational policy.
- The Commissioner has recommended that CSE seek an updated Ministerial Directive to obtain clear guidance related to the collection, use and disclosure of metadata in a foreign intelligence context.
- The Commissioner has recommended that CSE use its existing centralized records system to record decisions and actions taken regarding new and updated collection systems, as well as decisions and actions taken regarding the minimization of Canadian identity information.
- While conducting this review, the Commissioner also reviewed in greater depth the CSE activity that was reported in the media following the unauthorized disclosure of a presentation called *IP Profiling Analytics and Mission Impacts*. The Commissioner confirmed that these activities were authorized under the *National Defence Act* and that CSE took measures to protect the privacy of Canadians.

### Review of CSE's information technology security activities conducted under Ministerial Authorization

UNCLASSIFIED

CERRID# 25603023

- This review examined two types of information technology security activities conducted by CSE under Ministerial Authorizations.
- The Commissioner found that CSE's IT Security activities were appropriately authorized and conducted in accordance with the law and in accordance with ministerial authorizations and ministerial direction.
- The Commissioner determined that CSE has sufficient policies in place to satisfy the legal requirements to not direct its IT security activities at Canadians or any person in Canada, and to protect the privacy of Canadians in the use and retention of communications used to protect Government of Canada computer systems and networks.
- The Commissioner noted that the majority of private communications intercepted and examined consisted of unsolicited e-mails sent from cyber threat actors to the Government of Canada, which contained nothing more than malicious code. The Commissioner believes that these communications whose sole purpose is to compromise a government network should not be treated as private communications. Treating these communications as private communications distorts the privacy risks of CSE's IT security activities.
- The Commissioner has recommended that CSE reporting to the Minister on private communications unintentionally intercepted under Ministerial Authorization should highlight the difference between one-end-in-Canada e-mails intercepted under cyber defence operations and under foreign signals intelligence activities; and should note the lower expectation of privacy attached to communications intercepted under cyber defence operations.
- The Commissioner has also recommended that subsection 276.65(3) of the *National Defence Act* should be amended to remove any ambiguities respecting CSE's authority to conduct IT Security activities that risk the interception of private communications.

#### **Review of the Canadian Armed Forces Cyber Support Detachments.**

- The Canadian Armed Forces Information Operations Group (CFIOG) may, on behalf of CSE and in accordance with CSE's foreign intelligence mandate, respond to military-related requests to CSE from the Canadian Armed Forces (CAF). CFIOG support detachments provide CSE reports on foreign intelligence matters to clients within the CAF.
- The Commissioner found that considerable care was taken by the CFIOG to ensure that cyber support detachments complied with the law and all legal and policy conditions imposed on CSE, and that appropriate policies and procedures were in place to guide activities.

UNCLASSIFIED

CERRID# 25603023

- The Commissioner confirmed that only authorized CFIOG personnel are granted a foreign signals intelligence qualification after passing an annual CSE test on how to protect privacy and ensure legal compliance in the conduct of CSE activities. This is the same standard that applies to CSE employees.
- The Commissioner concluded that the Cyber Support Detachment activities reviewed complied with the law and that the activities carried out by the Cyber Support Detachments do not affect the privacy of Canadians.

#### **CSE assistance to the Canadian Security Intelligence Service under Part C of CSE's mandate and section 16 of the CSIS Act.**

- Section 16 of the *CSIS Act* allows CSIS to assist the Ministers of Foreign Affairs and National Defence in foreign intelligence collection activities.
- CSE may provide CSIS with technical and operational assistance for section 16 activities under part C of CSE's mandate.
- The Commissioner examined all cases where CSE provided assistance to CSIS under section 16 warrants issued to CSIS by the Federal Court.
- The Commissioner found that CSE's assistance to CSIS complied with the law and ministerial direction, and included measures to protect the privacy of Canadians.
- The Commissioner made four recommendations related to CSE's assistance to CSIS under part C of the CSE mandate. Two recommendations related to updating or creating governing process documentation; one on the updating or creation of interdepartmental memoranda of understanding between CSE and CSIS where applicable; and one recommendation that CSE should develop caveats to attach to specific operational information that may be shared with Second Party Partners in order to ensure that material would not be used without the express authorization of CSE.
- CSE has accepted the Commissioner's recommendations that interdepartmental agreements and internal CSE policies be updated to reflect current procedures and practices.

#### **Annual combined review of foreign signals intelligence ministerial authorizations and private communications, 2013-2014**

- This year the Commissioner reviewed three foreign signals intelligence ministerial authorizations in effect from December 1, 2013 to November 30, 2014 and conducted spot checks of private communications that were used and retained.
- The Commissioner found that the activities conducted under the 2013-2014 foreign signals intelligence ministerial authorization were authorized as required by the *National Defence Act*.

UNCLASSIFIED

CERRID# 25603023

- Through spot checks, the Commissioner determined that the private communications that were retained in the review period were essential to international affairs, defence or security, and related to foreign intelligence as required by law.
- The Commissioner found no cases of CSE retaining a private communication any longer than strictly necessary.
- Although the Commissioner did not make any recommendations related to this item, he noted spot checks will continue.

#### **Annual review of disclosures of Canadian identity information, 2013-2014**

- CSE is required to take measures to protect the privacy of Canadians, and their personal information. Canadian identity information may be included in CSE reports if the information is essential to understanding the intelligence reports.
- With minimal exceptions, any information that identifies a Canadian must be suppressed in reports, replaced with a generic term such as "a named Canadian".
- When CSE receives a request to disclose suppressed Canadian identity information, CSE must verify that the requesting Government of Canada agency or Second Party partner has both the authority and the operational justification for obtaining the Canadian identity information.
- The Commissioner found CSE to be rigorous and thorough in its handling of such requests and that CSE's disclosures of Canadian identity information complied with the law and ministerial direction, and that CSE took appropriate measures to protect the privacy of Canadians.
- The Commissioner confirmed that requests not supported by adequate authority or operational justification were denied.
- The Commissioner also examined assessments completed by CSE under the Ministerial Directive on Addressing Risks in Sharing Information with Foreign Entities. There were six such assessments in the review period.
- The Commissioner's annual review of disclosures of Canadian identity information determined that these activities were conducted in compliance with the law, ministerial direction and internal CSE policies and procedures. This review did not result in any recommendations for CSE.

#### **Review of CSE's *Privacy Incidents File* and *Minor Procedural Errors Record*, 2014**

- CSE must record privacy incidents where the privacy of a Canadian is put at risk. These incidents are recorded in CSE's *Privacy Incidents File* and CSE's *Minor Procedural Error Record*.

*UNCLASSIFIED*

CERRID# 25603023

- The Commissioner found that CSE took appropriate corrective actions in response to the privacy incidents and minor procedural errors identified in 2014.
- None of these suggest any systemic deficiencies or issues that require follow up.

**Referral of item to the Security Intelligence Review Committee (SIRC)**

- Questions on this matter should be referred to the Security Intelligence Review Committee (SIRC).

UNCLASSIFIED

CERRID# 25603023

## **Metadata Review**

### **Questions and Answers**

#### **Q1. Please explain in more detail what exactly happened.**

**A1.** This error was the result of deficiencies within certain CSE automated systems. Following a systems upgrade, CSE discovered on its own that certain metadata was not being properly minimized prior to being shared with allies, due to technical deficiencies. Minimization is the process by which Canadian identity information is rendered unidentifiable before being shared with allies. CSE proactively informed the Minister of National Defence and the Commissioner about these matters.

CSE proactively suspended the sharing of certain types of metadata. The suspension of these activities will be in place until the Chief of CSE is satisfied that proper systems are in place to ensure that all Canadian identity information is properly minimized.

#### **Q2. Does this mean that CSE has broken the law?**

**A2.** The CSE Commissioner has found that CSE was non-compliant with certain sections of the NDA, and as a result, Section 8 of the Privacy Act. The Commissioner also stated that he believes this error was unintentional and that there was no intention of the part of CSE to act in a way that did not conform to ministerial direction or operational policy.

#### **Q3. What happens now?**

**A3.** CSE took corrective actions and proactively suspended the sharing of certain types of metadata in order to protect the privacy of Canadians. CSE proactively informed the Minister of National Defence and the Commissioner about these matters. CSE has accepted the Commissioner's recommendations related to this metadata activity, including revising the Ministerial Directive to obtain clear guidance related to the collection, use and disclosure of metadata in a foreign intelligence context.

#### **Q4. How did this happen?**

**A4.** CSE uses many automated systems in the collection and processing of data. In this case, some changes in communications technology were not captured by certain CSE automated systems. This deficiency left some metadata un-minimized when it was shared with CSE's Five Eyes partners. This error only affected a subset of CSE's shared metadata. Other metadata minimization processes were not affected.

The Commissioner stated that he believes this failure to minimize information was unintentional and that there was no intention of the part of CSE to act in a way that did not conform to ministerial direction or operational policy.

UNCLASSIFIED

CERRID# 25603023

**Q5: How much information was shared? How many Canadians were affected? Can CSE quantify this or put the numbers in perspective?**

**A5.** The metadata that was shared does not contain enough information on its own or contextual details to identify individuals associated with this metadata. As such, the privacy impact is assessed as low.

The possible impact on any Canadian is further reduced through other safeguards and privacy protections in place, applied by both CSE and its Five Eyes partners.

Other safeguards include the fact that CSE:

- focuses collection of metadata to areas of the global network that are most likely to provide foreign intelligence, and avoids collection in areas that are not expected to be predominantly foreign in nature;
- limits the length of time that metadata can be retained;
- restricts access to metadata stores to only trained CSE operational and policy officials, and only for authorized analytic activities;
- administers regular legal briefings, as well as annual privacy policy testing for CSE operational and policy officials (revoking access to data until successful results are achieved);
- prohibits searches for information about Canadians anywhere or individuals in Canada;
- respects the privacy rights of Canadians when sharing information, including suppressing any identifying information about Canadians in foreign intelligence reporting;
- audits and reports on compliance with these activities; and
- cooperates with the CSE Commissioner in the review of metadata activities.

**Q6. What kind of information was shared?**

**A6.** This incident involved the sharing of certain types of metadata. Metadata is information about communications used by computer systems to identify, manage or route communications over global communications networks. Metadata does not include the content of a communication. For example, metadata does not include the content of e-mails, text messages, or phone calls.

Metadata is essential to allow CSE to better understand complex communications networks, discover foreign intelligence targets, and assess cyber threats. It is also used to ensure that CSE's foreign intelligence activities are directed only at legitimate foreign targets, and not at Canadians or anyone in Canada.

UNCLASSIFIED

CERRID# 25603023

**Q7. Who was this information shared with?**

**A7.** This information was shared with CSE's Five Eyes partners. The sharing of intelligence information with CSE's partners is critical to ensuring the security of Canada and protecting Canadians at home and around the world. It is also important to note that CSE and ant its Five Eyes partners have arrangements in place to respect each other's privacy.

**Q8. How will this affect the privacy interests of Canadians? What is the impact on the individual Canadians whose information was affected?**

**A8.** The unminimized metadata that was shared with CSE's Five Eyes partners does not contain names or other contextual details related to individuals associated with this metadata. As such, the privacy impact is assessed as low.

**Q9. Have you informed or will you inform the Canadians whose information was inadvertently shared?**

**A9. No.** The unminimized metadata that was shared with CSE's Five Eyes partners does not contain names or other contextual details related to individuals associated with this metadata. Consequently, any impact on privacy is considered to be low.

**Q10. What is metadata?**

**A10.** As the Commissioner notes in his report: "Metadata is information associated with a communication that is used to identify, describe, manage or route that communication. It includes, but is not limited to, a telephone number, an e-mail or an IP (Internet protocol) address, and network and location information. Metadata excludes the content of a communication. CSEC is allowed to use metadata only to understand the global information infrastructure, to provide foreign intelligence on foreign entities located outside Canada or to protect computer systems of importance to the Government of Canada."

Metadata is essential to allow CSE to deliver its mandate to help protect Canadians. CSE uses metadata to understand complex communications networks, discover foreign intelligence targets, and assess foreign cyber threats. It is also used to ensure that CSE's foreign intelligence activities are directed only at legitimate foreign targets, and not at Canadians or anyone in Canada.

In addition to supporting CSE's foreign intelligence mission, CSE cyber defence analysts use metadata to discover cyber threats from foreign states, criminals and other threat actors who are trying to extract information from Canada's systems, or are attempting to disrupt service on Canada's critical electronic networks with malicious software or malware.

**Q11. Is CSE allowed to collect metadata?**

**A11.** Yes. The *National Defence Act* legally authorizes CSE to acquire and use information to support its foreign intelligence program. The Ministerial Directive on the collection and use of

UNCLASSIFIED

CERRID# 25603023

metadata provides CSE with further direction and restrictions on how metadata can be collected, used and shared.

**Q12. Why does CSE collect metadata?**

**A12.** CSE is mandated to collect foreign signals intelligence based on the Government of Canada's intelligence priorities; to protect information and information systems of importance to the Government of Canada; and to assist federal law enforcement and security agencies, under their lawful authorities.

To deliver on its foreign intelligence and cyber defence mandates, CSE must understand complex and constantly changing communications networks. Metadata helps CSE understand these constantly changing networks and direct our foreign intelligence activities at foreign entities, outside of Canada.

Metadata also helps CSE protect the Government of Canada's most vital computer and information systems. Metadata helps CSE discover cyber threats from foreign states, criminals and other threat actors who are constantly trying to extract critical and private information from the Government of Canada's computer networks. Metadata analysis enables CSE to detect and disrupt malicious attempts by threat actors to infect Canada's critical electronic networks with malware. This ensures that CSE can identify malicious cyber threat actors, alert system operators to threats, and take appropriate defensive actions to mitigate these persistent cyber threats.

**Q13. Is CSE allowed to share metadata? With who?**

**A13.** Yes, the *National Defence Act* legally authorizes CSE to acquire and use information to support its foreign intelligence program. The Ministerial Directive on the collection and use of metadata provides CSE with further direction and restrictions on how metadata can be collected, used and shared.

**Q14. How many of the Commissioners eight new recommendations have been actioned? Are any outstanding? Why?**

**A14.** CSE has accepted all eight of the Commissioners recommendations this year and is currently working to implement them.

**Q 15: How much metadata does CSE collect? Does this include Canadian metadata? Is it shared/when? Is it kept/for how long?**

**A15.** CSE is selective, collecting subsets of metadata required to understand complex networks, discover foreign intelligence targets and assess cyber threats.

The Ministerial Directive on Metadata describes the activities that CSE can undertake under the authority of the *National Defence Act*, and establishes privacy protections that must be applied to these activities, including sharing of metadata collected by CSE. This directive serves to

UNCLASSIFIED

CERRID# 25603023

constrain CSE's activities and does not provide authority for activities that CSE is unable to undertake under the *National Defence Act*.

**Q16. In this case, how much unminimized metadata was shared?**

**A16.** Given the complexity of CSE's collection systems and the limited retention period of collected and shared metadata, CSE was not able to assess the number of records inadvertently shared.

**Q17. Who was the unminimized metadata shared with?**

**A17.** This information was shared with CSE's Five Eyes partners. The sharing of intelligence information with CSE's partners is critical to ensuring the security of Canada and protecting Canadians at home and around the world.

**Q18. What types of unminimized Canadian metadata was shared?**

**A18.** The unminimized metadata that was shared with CSE's Five Eyes partners does not contain names or other contextual details related to individuals associated with this metadata.

**Q19. Why didn't CSE inform the Privacy Commissioner?**

**A19.** The OCSEC has the statutory mandate to review CSE on all privacy matters. CSE proactively notified the Minister and the CSE Commissioner of this issue and provided each with regular updates on this issue. CSE also documented this error in its Privacy Incidents File, which is reviewed annually by the CSE Commissioner.

**Q20. Why haven't you resumed sharing metadata?**

**A20.** The activities will remain suspended until the Chief of CSE is satisfied that effective measures for sharing metadata are in place.

**Q21. Were employees reprimanded for these errors?**

**A21.** No. All errors were unintentional, resulting from technical deficiencies in automated systems.

**Q22. Why didn't you ask your FIVE Eyes partners to minimize the data in question once you determined the error?**

**A22.** The metadata that was shared does not contain enough information or contextual details to identify individuals associated with this metadata. Significant further analysis would be required in order to link this information with any specific Canadian or person in Canada.

**Q23. How long was this going on? When did CSE first identify the problem?**

**A.23.** CSE discovered on its own that certain metadata was not being properly minimized prior to being shared with allies, due to technical deficiencies. CSE proactively informed the Minister

*UNCLASSIFIED*

CERRID# 25603023

of National Defence and the Commissioner about these matters. CSE proactively suspended the sharing of certain types of metadata. The suspension of these activities will be in place until the Chief of CSE is satisfied that effective measures for sharing metadata are in place.

## Arbeau, Kristy (PS/SP)

---

**From:** Wilson, Ashleigh (PS/SP)  
**Sent:** Tuesday, October 25, 2016 10:47 AM  
**To:** Brien, Dan (PS/SP); Bardsley, Scott (PS/SP); Peirce, Hilary (PS/SP)  
**Cc:** Tomlinson, Jamie (PS/SP); Magee, Heather (PS/SP); Nichols, Megan (PS/SP); Cibula, Colette (PS/SP)  
**Subject:** Latest CSIS Products  
**Attachments:** Director Opening Remarks ADP bilingual with French DoJ edits (Oct.24 aft....docx; Backgrounder ADP Approved-French (Oct.24 clean).docx; Backgrounder ADP Approved (Oct.24 clean english).docx; Director Statement ADP approved-French (Oct.24 afternoon clean).docx; Director Statement ADP approved English (Oct.24 afternoon clean).docx; QA ADP approved - French (Oct.24 afternoon clean).docx; QA ADP approved DoJ edits - English (Oct.24 afternoon clean).docx; PS-SP-#1997111-1-Speaking Notes - FCC Associated Data.docx; PS-SP-#1997213-v1C-Statement - FCC Associated Data.doc; PS-SP-#1998418-v1B-Statement\_FCC\_Associated\_Data\_FRENCH.DOC; PS-SP-#1999749-v1-Speaking\_Notes\_-\_FCC\_Associated\_Data\_FRENCH.DOCX; PS-SP-#1995596-v2-Qs&As\_-\_FCC\_Associated\_Data.doc; PS-SP-#1995114-v1G-Key\_Messages\_-\_FCC\_Associated\_Data.doc; PS-SP-#1999745-v1A-Key\_Messages\_-\_FCC\_Associated\_Data\_FRENCH.DOCX

Hi Dan, Scott and Hilary,

Here are the CSIS and PS products currently with PCO. We'll keep you posted as they are finalized.

### PS Products

- Statement (English and French)
- Speaking Notes (English and French)
- Key Messages (English and French)
- Qs&As (English only)

### CSIS Products

- Director Statement (English and French)
- Backgrounder (English and French)
- Director Opening Remarks (Bilingual)
- Q and A (English and French)

### Ashleigh Wilson

Communications Manager | Gestionnaire de communications  
Ministerial Services | Services ministériels  
Public Safety Canada | Sécurité publique Canada  
Telephone | Téléphone : 613-990-2603  
Mobile | Cellulaire : 343-998-3994  
E-mail | Courriel: [ashleigh.wilson@canada.ca](mailto:ashleigh.wilson@canada.ca)

UNCLASSIFIED  
NON CLASSIFIÉ

## **Opening Remarks on Justice Noel's Decision**

### **National Press Gallery**

#### **Mot d'ouverture sur la décision rendue par le juge Noël**

#### **Tribune de la presse nationale**

- **Thank you Andrew. Bonjour Mesdames et Messieurs. Today (or TBD), Justice Noel of the Federal Court issued an *En Banc* a decision related to CSIS warrant applications. I am here to explain what this decision means.**
- **I would like to start off by saying, first and foremost, that the Canadian Security Intelligence Service accepts in full the Court's decision, and have taken immediate actions to respond.**
- **I deeply regret the Court's serious concerns with respect to our duty of candour and I commit to continuing my efforts, with the Deputy Minister of Justice, to fully address this concern.**
- **CSIS recognizes the importance of openness and transparency with the Federal Court, and we are working closely with the Department of Justice to develop measures aimed at ensuring that**

UNCLASSIFIED  
NON CLASSIFIÉ

**we meet our obligations to the Court in matters of transparency and duty of candour.**

- **Given the Court's decision with respect to third-party data, CSIS has halted all access to, and analysis of, associated data while we undertake a thorough review of the decision in order to assess potential operational and legal impacts, and determine our way forward.**
- **Let me be clear: all associated data collected under warrant was done so legally. The Court's key concern related to our retention of non-threat related associated data linked with third party communications, after it was collected.**
- **CSIS, in consultation with the Department of Justice, interpreted the CSIS Act to allow for the retention of this sub-set of associated data.**
- **It is now clear that the Federal Court disagrees with this interpretation; a decision which we fully accept.**

UNCLASSIFIED  
NON CLASSIFIÉ

- **The Court rightly acknowledged the age of the *CSIS Act* and that it may not be keeping pace with changing technology and the current threat environment, contributing to this challenge.**
- **That said, again, we fully accept the decision of the Court.**
- **As Canada's national intelligence agency, CSIS investigates activities which may, on reasonable grounds, be suspected of posing a threat to the security of Canada.**
- **One of the ways we investigate these threats is through warrants issued by the Federal Court which authorize the interception of communications. This includes analysis of all of the information - both the content and the associated data.**
- **Associated data includes information such as: email addresses and telephone numbers but never the content.**
- **It is useful in identifying patterns of movement, communications, behaviours, significant trends, and links that are otherwise unidentifiable.**
- **As is the case for many of our international partners, CSIS has developed data analytic capabilities and expertise to analyze**

UNCLASSIFIED  
NON CLASSIFIÉ

**associated data and enhance its capacity to identify and assess threats to the security of Canada over time.**

- **When it comes to understanding and predicting the actions of the subjects of our investigations, data analytics has proven to be an effective tool.**
- **In the ruling released today the Federal Court recognized the value of the data analytic programme and confirmed the legality of collecting telecommunications associated data pursuant to warrants.**
- **I would add that, like the threats we face today, technologies and associated privacy implications have also evolved.**
- **The retention and analysis of information is a significant public policy issue, not just in Canada, but also among our closest allies.**
- **I would like to say, that the trust of Canadians is fundamental to our ability to deliver on our mandate.**
- **Because the nature of our business is principally secret, Canadians are largely unaware of the professionalism and outstanding dedication the men and women of CSIS show every**

UNCLASSIFIED  
NON CLASSIFIÉ

**day as they carry out intelligence work. As the Director of CSIS, I am extremely proud of the people with whom I work. Canadians, too, should be proud of those who work tirelessly to keep this great country safe.**

- **We appreciate the confidence the government invests in CSIS, and it remains for us a privilege to protect Canadians and Canada's interests at home and abroad.**
- **The ongoing national security consultations represent an important opportunity to ensure that CSIS is meeting the dual objectives of security and privacy, and has the tools and authorities, with appropriate oversight, to meet both.**
- **(REPEAT IN FRENCH)**
- **(RÉPÉTER EN FRANÇAIS)**
- **Aujourd'hui (ou à confirmer), le juge Noël de la Cour fédérale a rendu une décision liée aux demandes de mandat du SCRS. Je suis ici pour expliquer ce que signifie cette décision.**

**Pages 209 to / à 216  
are not relevant  
sont non pertinentes**

# Backgrounder

*Federal Court ruling on the retention of associated data linked to third party information.*

## **IMPACT OF THE DECISION ON CSIS:**

- The Canadian Security Intelligence Service is mandated to investigate activities which may, on reasonable grounds, be suspected of posing a threat to the security of Canada. In order to investigate these threats, CSIS may apply to the Federal Court for a warrant when the response to the threat requires more intrusive measures.
- Through the proceedings of the Court, over time, the provisions of warrants have changed to take into account the evolution of technology, legal developments, and investigative measures.
- This ensures that the powers granted by the warrants are clearly defined and that their conditions take into account the impact that the execution of the warrant has on the collection and the retention of information.
- The decision relates to the retention of certain information that has been legally collected via the execution of warrants, issued by the Court, which authorized the interception of communications.
- CSIS had sought to fully analyze all of the information - both the content and the associated data - for example, email addresses and telephone numbers.
- As is the case for many of our international partners, CSIS has developed data analytic capabilities and expertise to significantly enhance the identification and assessment of threats to the security of Canada over time and space. This includes identifying patterns of movement, communications, behaviours, significant trends, and links that are otherwise unidentifiable.

- When it comes to understanding and predicting the actions of the subjects of our investigations, data analytics has proven to be an effective tool.
- In the ruling released today, the Federal Court recognized the value of the data analytic programme and confirmed the legality of collecting telecommunications associated data pursuant to warrants.
- On the very specific issue of associated data linked to third-party communications, the Court found that it can only be retained if it is related to threats or of use to an investigation, prosecution, national defence or international affairs.
- CSIS, in consultation with the Department of Justice, had interpreted the *CSIS Act* as enabling the retention of this sub-set of associated data to allow for that important analytic work. At no time did the Service believe this to be inconsistent with the *CSIS Act*.
- It is now clear that the Federal Court, on the issue of the retention of certain data, interprets the *Act* differently.
- We accept this decision in full, and have taken immediate actions to respond.
- In response to the decision, CSIS halted all access to, and analysis of, associated data while we undertake a thorough review of the decision in order to assess potential operational and legal impacts, and determine our way forward.
- CSIS takes seriously the concerns expressed by the Court with respect to our duty of candour and recognizes the importance of openness and transparency with the Federal Court.
- CSIS is working closely with the Department of Justice to develop measures aimed at ensuring that we meet our obligations to the Court in matters of transparency and duty of candour.

**Pages 219 to / à 220  
are not relevant  
sont non pertinentes**

# STATEMENT

## *CSIS Director statement regarding decision of the Federal Court*

Ottawa, xxxxdays, [REDACTED] - The Director of the Canadian Security Intelligence Service (CSIS), Michel Coulombe, issued the following statement regarding the decision issued today by the Honourable Justice Noël of the Federal Court:

“The Federal Court has recently ruled on the retention of associated data linked to third party information. CSIS accepts in full the Court’s decision, and has taken immediate actions to respond. Given the Court’s decision with respect to third-party data, CSIS has halted all access to, and analysis of, associated data while we undertake a thorough review of the decision in order to assess potential operational and legal impacts, and determine our way forward.

[REDACTED] and I commit to continuing my efforts, with the Deputy Minister of Justice, [REDACTED] address this concern. Let me be clear: all associated data collected under warrant was done so legally. The Court’s key concern related to our retention of non-threat related associated data linked with third party communications, after it was collected.

CSIS, in consultation with the Department of Justice, had interpreted the *CSIS Act* to allow for the retention of this sub-set of associated data. It is now clear that the Federal Court disagrees with this interpretation; a decision which we fully accept.

As is the case for many of our international partners, CSIS has developed data analytic capabilities and expertise to analyze associated data and enhance its capacity to identify and assess threats to the security of Canada over time. When it comes to understanding and predicting the actions of the subjects of our investigations, data analytics has proven to be an effective tool. In the ruling released today, the Federal Court recognized the value of the data analytic programme and [REDACTED] of collecting telecommunications associated data pursuant to warrants. The Court also rightly acknowledged the age of the *CSIS Act* and that it may not be keeping pace with changing technology and the current threat environment.

The ongoing national security consultations represent an important opportunity to ensure that CSIS is meeting the dual objectives of security and privacy, and has the tools and authorities, with appropriate oversight, to meet both.

Because the nature of our business is principally secret, Canadians are largely unaware of the professionalism and outstanding dedication the men and women of CSIS show every day as they carry out intelligence work. As the Director of CSIS, I am extremely proud of the people with whom I work. Canadians, too, should be proud of those who work tirelessly to keep this great country safe.

We appreciate the confidence the government has in CSIS, and it remains for us a privilege to protect Canadians and Canada's interests at home and abroad.”

-30-

**Information:**

Media Relations

Canadian Security Intelligence Service

media-medias@smtp.gc.ca

613-231-0100

**Pages 223 to / à 237  
are not relevant  
sont non pertinentes**

UNCLASSIFIED

Embargoed until decision is published

## Qs & As

### A. THE FEDERAL COURT DECISION

#### 1. Why did you appear before the Federal Court?

- The Canadian Security Intelligence Service is mandated to investigate activities which may, on reasonable grounds, be suspected of posing a threat to the security of Canada. In order to investigate these threats, CSIS may apply to the Federal Court for a warrant when the response to the threat requires more intrusive measures. Late 2015, CSIS applied to renew and obtain new warrants as well as propose amendments to warrant conditions.
- In light of the finding in the Security Intelligence Review Committee's (SIRC) annual report (2014-15), the Court requested that the collection, use, retention and destruction of associated data (referred to by SIRC as metadata) collected under warrants also be addressed.

#### 2. What is the decision?

- The Court agreed with most of the terms and conditions proposed by CSIS on the warrant application that was presented to the Court.
- The Court found that CSIS failed to fully and transparently inform the Court of its retention program and the establishment of the Operational Data Analysis Centre (ODAC), but did not find evidence that this had been done deliberately.
- The Court determined that CSIS' retention of associated data linked to third-party communications found to be unrelated to threats or of no use to an investigation, prosecution, national defence or international affairs, to be illegal.
- That said, it is important to underline that all associated data was collected legally through warrants. The Federal Court's key concern relates to CSIS' retention of non-threat related associated data linked with third party communications, after it was collected.
- Further, the Court rightly acknowledged the age of the *CSIS Act* and that it may not be keeping pace with changing technology and the current threat environment.

UNCLASSIFIED

Embargoed until decision is published

**3. What is the Government's duty of candour?**

- In all instances where only one party is before the Court, without having all of the other interested parties present (known as an "*ex parte*" or "in private" hearing), that the party is under a duty of utmost good faith in the representations it makes to the Court.
- The evidence presented must be complete and thorough and no relevant information adverse to the interests of the party may be withheld. The Federal Court has noted that this duty is heightened when hearings take place behind closed doors, rather than in public, as often occurs in cases related to national security.

**4. So the Government breached its duty of candour in this case?**

- Department of Justice lawyers, who represented CSIS in this matter, strive to uphold the highest standards of the legal profession in their representation of the Government interests in the Courts.
- The Government accepts the Federal Court's findings regarding its duty of candour. In fact, the Government conceded to the Court that it had failed to meet its duty of candour in this case.
- The Attorney General of Canada has taken a number of steps, including receiving advice from external experts, to ensure they are in the best possible position to meet the Government's duty of candour in future hearings.
- CSIS can and will do more to ensure that it is fully transparent with the Federal Court regarding the use it makes or plans to make of the information it collects pursuant to Federal Court issued warrants.

**5. This is not the first incident of CSIS being found to be in breach of Duty of Candour. Why and what is being done to address this?**

- CSIS recognizes the importance of openness and transparency with the Federal Court.
- Over time the provisions of the warrants have changed to take into account the evolution of technology, legal developments and investigate measures.
- The *CSIS Act* defines the Service's relationship with the Court. The means to approach the Court is through a warrant application, which creates a very focused type of interaction.

UNCLASSIFIED

Embargoed until decision is published

- We take these concerns very seriously and are working closely with the Department of Justice to develop measures aimed at ensuring that we meet our obligations to the Court in matters of transparency and duty of candour.
- The Attorney General of Canada has taken a number of steps, including receiving advice from external experts, to ensure they are in the best possible position to meet the Government's duty of candour in future hearings.

**6. Why did CSIS not inform the Court of its new position on the retention of data and the creation of the Operational Data Analysis Centre (ODAC)?**

- At various points, the Government, the Security Intelligence Review Committee and the Office of the Privacy Commissioner were made aware of CSIS' position on the retention of data and the establishment of ODAC.
- In June 2011, CSIS did advise the Federal Court that it amended the wording of warrant conditions in an effort to distinguish the content of communications from the associated data of communications. The Court found that notification to be insufficient.
- CSIS takes notice of the fact that the Court should have been informed earlier of the existence of ODAC and the change in the retention policy and acknowledges this was a significant omission. At no point did CSIS deliberately seek to withhold this information from the Court, and the Court acknowledged that there is no evidence to that fact.
- The development of this new capability evolved over time as has our understanding of our obligations towards the Federal Court in this regard, which CSIS determines in close consultation with the Department of Justice.

**7. SIRC recommended in their 2014-15 Report that the Service advise the Federal Court of activities relating to metadata collected under a warrant. CSIS, however believed that SIRC's recommendation was both inappropriate and unwarranted given that section 21 of the CSIS Act does not confer any general supervisory authority to Federal Court judges. Why did CSIS take this position?**

- It is SIRC that reviews the activities of CSIS and not the Federal Court. This stems from a strict interpretation of the CSIS Act. It is now clear that the Federal Court disagrees with such an interpretation. The Service accepts this finding.

UNCLASSIFIED

Embargoed until decision is published

- The Service was under the impression that the Federal Court had been sufficiently advised of the retention of associated data in 2011. The Court also disagreed with this assessment. The Service accepts this finding.

**8. Has CSIS briefed this Minister on this matter?**

- In the context of an update on the court hearing, the current Minister of Public Safety has been briefed a number of times.
- At various points, previous Ministers, the Security Intelligence Review Committee and the Office of the Privacy Commissioner were made aware of CSIS' position on the retention of data and the establishment of ODAC.

**9. Did CSIS purposely mislead the Court in this case?**

- Government officials did not deliberately mislead the Court. The Court found that CSIS failed to fully and transparently inform the Court of its retention program and the establishment of the Operational Data Analysis Centre (ODAC), but did not find evidence that this had been done deliberately.

**10. Can the Government be held in "contempt of court" for not disclosing this information?**

- Although Justice Noel makes reference to this in his decision, contempt of court proceedings will absolutely not be necessary to ensure that the Government addresses the Court's concerns.
- Both CSIS and the Department of Justice take these matters very seriously and have already taken steps to ensure that no such breach of candour occurs in the future.

**CSIS RESPONSE TO THE DECISION**

**11. What have you done to respond to the judgement?**

- On duty of candour: We take this finding very seriously and recognize the importance of compliance with Ministerial Direction and the CSIS Act, as well as openness and transparency with the Court.
- We can and will do more to ensure that it is fully transparent with the Federal Court regarding the use it makes or plans to make of the information it collects pursuant to Federal Court issued warrants. To that end, it is working closely with the Department of Justice.

UNCLASSIFIED

Embargoed until decision is published

- On the retention of non-threat related associated data linked with third-party communications: CSIS immediately halted access to, and analysis of, associated data until such time as it can successfully distinguish associated data linked to third-party communications from that of subject of investigation communications.

**12. What steps will CSIS take to implement the Court's recommended two-step process of assessment?**

- CSIS will be required to assess, within a short period, communications data to determine its relevance to a subject of investigation or threat to the security of Canada.
- Significant efforts will be required to implement policies, processes and technology that will successfully distinguish between threat related and non-threat related associated data.

**13. Has CSIS destroyed the data deemed illegal by the Court?**

- The Court did not order CSIS to destroy third-party associated data from its databases and recognized that the retention and analysis of associated data has yielded useful intelligence results in the past.
- CSIS immediately halted analysis and use of all associated data until such time as it can successfully distinguish associated data from that linked to a threat.
- We are assessing the application of the Court's finding in this regard.

**IMPACTS OF THE DECISION**

**14. Did CSIS collect this information legally?**

- Any collection activity that requires the use of specific investigative techniques is authorized by warrants issued by the Federal Court. CSIS collected this information legally, as confirmed in the decision.
- The Federal Court's key concern relates to CSIS' retention of non-threat related associated data linked with third-party communications, after it was collected.

UNCLASSIFIED

Embargoed until decision is published

**15. Why was CSIS retaining this third party associated data if it was not authorized by the CSIS Act?**

- CSIS, in consultation with the Department of Justice, interpreted the CSIS Act to allow for the retention of this data.
- It is now clear that the Federal Court disagrees with this interpretation.
- We fully accept the Court's ruling and has taken appropriate steps to respond.

**16. Will this decision affect the admissibility of evidence used in the cases of convicted terrorists?**

- CSIS is mandated to collect, by investigation or otherwise, to the extent that is strictly necessary, and analyze and retain information and intelligence regarding activities that may on reasonable grounds be suspected of constituting threats to the security of Canada.
- CSIS collects intelligence or information for the purpose of advising the Government, providing security advice or security assessments. It does not, however, collect evidence.

**17. Were leads generated by the use of third-party associated data provided to the RCMP or other law enforcement partners for the purposes of counter terrorism investigations?**

- CSIS is assessing the decision in an effort to determine how it impacts operations. CSIS cannot, however, comment on the nature of its operations, and how they are impacted.

**18. Does this decision impact any current terrorism related cases?**

- CSIS is assessing the decision in an effort to determine how it impacts operations. CSIS cannot, however, comment on the nature of its operations, and how they are impacted.

**19. How many Canadians were impacted?**

- It is impossible to quantify the number of individuals linked to the associated data, much less identify personal details such as citizenship.
- The associated data in question is associated with communications lawfully intercepted under warrant in relation to the investigation of threats to the security of Canada.

UNCLASSIFIED

Embargoed until decision is published

- Associated data does not reveal the purpose of the communication, nor any part of the content and, on its own, does not identify individuals who are party to the communication.
- This speaks directly to the nature of associated data, which, on its own, does not readily identify an individual.

## **BROADER IMPLICATIONS OF THE DECISION**

### **20. Are there any privacy implications noted in the decision?**

- The Federal Court did not speak to the privacy considerations of the retention of third-party associated data.
- CSIS recognizes the importance of maintaining public trust and confidence in its activities. CSIS takes very seriously potential privacy considerations related to its work, and it is committed to ensuring that its activities are transparent, accountable and in compliance with privacy legislation, guidelines and best practices.
- Of note, a Privacy Impact Assessment on ODAC was completed in August 2010. Should the Office of the Privacy Commissioner be interested in investigating the privacy implications of the decision, CSIS will cooperate fully.

### **21. Can Canadians have confidence in CSIS?**

- CSIS recognizes the importance of maintaining public trust and confidence, and has a strong record of responsibly exercising its authorities and has matured as an organization over its 32 year history.
- SIRC, and the Inspector General before it, has consistently found that the Service has carried out its duties in accordance with the *CSIS Act* and Ministerial Direction and that the exercise of its activities has been reasonable and necessary.
- CSIS maintains a productive relationship with SIRC. SIRC's findings and recommendations have demonstrably shaped the conduct of CSIS operations and continue to do so.
- And in the context of warrant powers, CSIS must also answer to the Federal Court.
- As CSIS adapts to an ever-changing environment, challenges do emerge, demanding continual improvement to operational policies and procedures, supported by a robust governance framework.

UNCLASSIFIED

Embargoed until decision is published

- CSIS operates in a rigorous system of checks and balances. These layers of accountability are mutually reinforcing, which is certainly highlighted in this instance and will be bolstered by enhanced oversight by the proposed Committee of Parliamentarians.

**22. Will the government consult Canadians on the data exploitation activities of CSIS?**

- The Government is committed to keeping Canadians safe while at the same time safeguarding our freedoms, rights and values in an open and democratic society.
- The ongoing national security consultations represent an important opportunity to ensure that CSIS is meeting the dual objectives of security and privacy and has the tools and authorities, with appropriate oversight, to meet both.

**23. Will the new National Security and Intelligence Committee of Parliamentarians have any role in reviewing CSIS' data exploitation activities?**

- Enhancements to the review system, including the proposed National Security and Intelligence Committee of Parliamentarians, will be properly decided by Parliament.
- As currently drafted, the Bill to establish the Committee would authorize it to review the operational activities of CSIS, including programmes such as its data exploitation activities.
- CSIS will, of course, respect and fully cooperate with this committee, should it be stood up and wish to review this issue, or any other CSIS activity.

**METADATA AND ASSOCIATED DATA**

**24. What kind of communications data does the Service collect?**

- In the course of an investigation, CSIS may obtain warrant powers against individuals or entities to authorize the use of specific investigative techniques. These powers, for example, allow CSIS to intercept communications. Execution of such warrant powers may result in the incidental collection of information from parties other than the target (i.e. third-parties).
- When CSIS intercepts a communication, it obtains the content of the communication, as well as data about the communication. This could include: email addresses and telephone numbers.
- This data does not include any information that could reveal the purpose of the communication, nor any part of its content.

UNCLASSIFIED

Embargoed until decision is published

**25. What is the difference between associated data and metadata?**

- There is no difference. Associated data – or metadata – refers to information associated to a communication intercepted pursuant to a warrant.
- Neither metadata or associated data includes any information that could relate to content.
- Metadata is the context, not the content of a communication. It is information used by computer systems to identify, describe, manage or route communications across a network.

**26. What is associated data as defined by the Federal Court?**

- CSIS had applied the term associated data to all metadata associated to a communication intercepted under warrant.
- The Federal Court, however, diverged from the Service's definition.
- The Federal Court defines associated data as communications data collected under warrant from which the content was assessed as unrelated to threats and of no use to an investigation, prosecution, national defence or international affairs.
- Given the Federal Court's interpretation, the Service will undertake to review the terminology it applies to management of information collected under warrant.

**27. What is the difference between associated data and the dataset collection SIRC reviewed recently?**

- SIRC's 2016 Annual Report reviewed CSIS's non-warranted collection of datasets. This does not include communications content or data collected under Federal Court warrant.
- As an example, some non-warranted datasets are referential and provide contextual information which is publicly available. CSIS has developed a rigorous governance framework for the collection of non-referential datasets. This framework sets out clear requirements and a decision-making process to ensure that our collection in this regard respects *CSIS Act* requirements and the Charter, including privacy considerations.

UNCLASSIFIED

Embargoed until decision is published

- The Federal Court was concerned only with warranted collection, namely retention of third party associated data. That said, the Service is assessing the implications of this ruling for the non-warranted datasets SIRC recently reviewed.

### **CSIS USE OF ASSOCIATED DATA, ODAC**

#### **28. How will CSIS deal with the associated data it currently holds?**

- CSIS immediately halted all access to, and analysis of, all associated data until such time as it can successfully distinguish associated data from that linked to a threat.

#### **29. Has or does CSIS share its associated data holdings with foreign partners?**

- CSIS does not share raw associated data with foreign or domestic partners.
- Associated data that has been analysed and determined to be related to a threat could have been shared with domestic and foreign partners in accordance with our national security mandate.
- Although raw associated data would not have been shared with partners, it is used to inform our investigations as well as intelligence products which may be discussed and shared with partners.
- In this context the associated data would have been deemed threat related and thus is authorized to be retained by the Service.

#### **30. How is this collection different from the bulk collection of signals intelligence (SIGINT) agencies?**

- CSIS collection of communications data is authorized under Federal Court warrants and is specifically focused on an identified target of investigation.

#### **31. How does or did CSIS previously ensure that data exploitation technologies did not unnecessarily target individuals NOT engaged in threat related activity?**

- Data exploitation is used in response to specific operational queries related to mandated investigations.
- Data exploitation is a tool to assist the Service in discovering linkages, trends and patterns to advance investigations.

UNCLASSIFIED

Embargoed until decision is published

- Determining whether or not a communication is threat-related is complex and may only become apparent as an investigation progresses.
- The Service has seen examples where communications originally assessed to have no intelligence value were later revealed to contain key threat-related information.

### **32. What is third party information?**

- Subjects of investigation communicate with a whole range of people for a whole range of purposes, which may or may not be threat-related.
- When these communications are intercepted, it is not immediately known whether or not the communication is related to the threat.
- The Court acknowledged that in executing warrant powers, CSIS will by necessity collect third party information; information that is not directly associated with a subject of investigation.
- Some third party information is threat-related and provides essential investigative leads. Some, however, has no intelligence value
- CSIS policy and practice is to delete the content of communications intercepts collected under warrant assessed to be of no intelligence value.
- Though the content was destroyed, the data about the communication was retained, whether or not it was related to a third party.
- On the very specific issue of non-threat related associated data linked to third-party communications, the Court found that it can only be retained if it is related to threats or of use to an investigation, prosecution, national defence or international affairs.

### **33. What is data exploitation, how does CSIS conduct data exploitation and why?**

- Data exploitation employs computers to analyze data and discover linkages, trends and patterns. These techniques enable humans to make sense of volumes of information that could not be processed without a computer's assistance.
- Data exploitation enables the Service to effectively analyze threats to the security of Canada over time. It can provide insight into subjects of investigation; identify new leads and intelligence gaps and provide context and understanding to operations.

UNCLASSIFIED

Embargoed until decision is published

- The exploitation of data is invaluable in relation to the exercise of CSIS' mandate, but it must be undertaken responsibly and in accordance with our authorities. The Federal Court decision provides new direction in this regard.

#### **34. What is ODAC?**

- To derive more value from the data already being collected under warrant using data exploitation techniques, the Service established the Operational Data Analysis Centre (ODAC) in 2006.
- The necessity of creating this capability was described to the Minister of Public Safety in July 2006, noting that a basic requirement of ODAC would be the ability to retain data for extended periods of time.
- CSIS also informed subsequent ministers, the Inspector General, the Privacy Commissioner and SIRC of the existence of the programme.

#### **35. How long has CSIS had a formal data exploitation program?**

- The necessity of creating this capability was described to the Minister of Public Safety in July 2006 when CSIS developed the Operational Data and Analysis Centre (ODAC). This capability was created with full disclosure to the Government.

#### **36. Was SIRC aware of CSIS' data exploitation activities and collection of associated data?**

- SIRC was aware of CSIS' data exploitation activities from shortly after the establishment of ODAC in 2006. In 2007, CSIS responded to a SIRC query about ODAC and its support to operations.
- The Inspector General was provided a verbal briefing on ODAC and data exploitation in support of operations in 2011.
- SIRC reviewed CSIS' use of associated data and published its findings on the issue in its 2014-15 annual report. SIRC did not conclude that the retention of associated data was illegal.

#### **37. What were the Service's practices with regard to the retention of data collected under warrant prior to the Federal Court's decision?**

- Pursuant to policy, one year after collection, CSIS practice was to delete the content of communications intercepts collected under warrant assessed to be of no intelligence value.

UNCLASSIFIED

Embargoed until decision is published

- Though the content was destroyed, the data about the communication was retained, whether or not it was related to a third-party.

### **FEDERAL COURT HEARINGS**

#### **38. What is an “en banc” hearing, why are they being held in relation to national security issues and what was the Government’s role?**

- These are hearings where all available designated judges of the Federal Court, may attend, participate, and hear evidence. The Federal Court of Canada determines when en banc hearings occur. Very rarely the Court has requested that a warrant application be heard in the presence of most or all designated judges.
- As stated in Justice Noel’s decision, sitting en banc in this case was helpful in reaching a decision as he had the benefit of his colleagues’ perspectives.
- Counsel for the Attorney General attended these hearings to represent CSIS in relation to specific warrant applications.

#### **39. Why were these hearings held in secret?**

- In this case, the hearing was held in private (also known as “in-camera”) pursuant to section 27 of the CSIS Act which outlines how certain applications are heard by the Court.

#### **40. Is it an infringement of someone’s rights not to be represented at a private hearing? How are the other parties’ rights safeguarded?**

- While the *CSIS Act* does require that these hearings be held in private, a “friend of the Court” or “*amicus curiae*” can be appointed by the Court if required.
- In the warrant application at issue, two *amicus curiae* were appointed by the Court. This is to ensure that the matter is fully argued and the Court has the benefit of competing views. The submissions made by the *amicus curiae* are mindful of the rights and interests of the party which is not present at the private hearing.
- The *amicus curiae*, also known as a “friend of the court” is a security-cleared lawyer with expertise in national security matters.

## **Minister's Speaking Notes on the Federal Court's "En banc" Decision**

**Speaking Notes**

**For the**

**Honourable Ralph Goodale**  
**Minister of Public Safety and Emergency Preparedness**

**On the**

**Federal Court's "En banc" Decision**

**Ottawa, ON**

**October 24, 2016**

*Check Against Delivery*

I welcome the decision in this matter rendered by Mr. Justice Noel on behalf of the Federal Court.

The court's insight and guidance are timely, coming in the midst of the public consultations on Canada's national security framework.

CSIS plays a critical role in keeping Canadians safe. As it investigates threats to our national security, the Service collects a considerable amount of information, with full legal authorization pursuant to the CSIS Act and warrants issued by the Federal Court. When the information is intercepted communications, it can often include "associated data" of third-parties such as phone numbers and email addresses.

The court has ruled that while legally collected, such "associated data" cannot be retained and utilized by CSIS unless it relates to a specific threat to the security of Canada or is of use to an investigation, prosecution, national defence or foreign affairs.

The Service has confirmed that it is taking immediate steps to address the court's decision. It has blocked all access to and analysis of any associated data, while it considers its next steps. I am asking the Security Intelligence Review Committee (SIRC) to monitor the situation carefully to ensure compliance.

I also take very seriously the explicit finding by Justice Noel that CSIS had failed in its duty to be candid with the court. I will be pursuing this criticism with the executive management of the Service. In matters of security and intelligence, Canadians need to have confidence that all the departments and agencies of the Government of Canada are being effective at keeping Canadians safe, and equally, that they are safeguarding our rights and freedoms.



---

# Statement

---

## **STATEMENT BY PUBLIC SAFETY MINISTER RALPH GOODALE ON THE RULING OF THE FEDERAL COURT OF CANADA, PUBLISHED OCTOBER XX, 2016, WITH RESPECT TO THE CANADIAN SECURITY INTELLIGENCE SERVICE (CSIS) AND THE HANDLING OF "ASSOCIATED DATA"**

October XX, 2016 – "I welcome the decision in this matter rendered by Mr. Justice Noel on behalf of the Federal Court, which the Government will not appeal.

The court's insight and guidance are timely, coming in the midst of the public consultations we now have underway about Canada's national security framework.

CSIS plays a critical role in keeping Canadians safe. As it investigates threats to our national security, the Service collects a considerable amount of information, with full legal authorization pursuant to the CSIS Act and warrants issued by the Federal Court. When the information is intercepted communications, it can often include "associated data" of third-parties such as phone numbers and email addresses.

The court has ruled that while legally collected, such "associated data" cannot be retained and utilized by CSIS unless it relates to a specific threat to the security of Canada or is of use to an investigation, prosecution, national defence or foreign affairs.

The Service has confirmed that it is taking immediate steps to address the court's decision. It has blocked all access to and analysis of any associated data, while it considers its next steps. As Minister of Public Safety, I am asking the Security Intelligence Review Committee (SIRC) to monitor the situation carefully to ensure compliance.

I also take very seriously the explicit finding by Justice Noel that CSIS had failed in its duty to be candid with the court. I will be pursuing this criticism with the executive management of the Service. In matters of security and intelligence, Canadians need to have confidence that all the departments and agencies of the Government of Canada are being effective at keeping Canadians safe, and equally, that they are safeguarding our rights and freedoms.

I also take note of the court's observation that the CSIS Act is now more than 30 years old and showing its age as global affairs, threat profiles, technology and public expectations have rapidly evolved. In his judgement, Justice Noel did not dispute the potential value of "associated data" to the important work CSIS does in this challenging world, but he could not find existing legislative authority permitting its retention and use."

-30-

Follow Public Safety Canada ([@Safety\\_Canada](https://twitter.com/Safety_Canada)) on Twitter.

For more information, please visit the website [www.publicsafety.gc.ca](http://www.publicsafety.gc.ca).

### **Information:**



- 2 -

Scott Bardsley  
Office of the Minister of Public Safety and Emergency Preparedness  
613-998-5681

Media Relations  
Public Safety Canada  
(613) 991-0657

**Pages 257 to / à 262  
are not relevant  
sont non pertinentes**



---

# *Questions and Answers*

---

## **FEDERAL COURT DECISION CSIS' Authority to Retain Metadata Collected Through Warrants**

### **1. Would the National Security and Intelligence Committee of Parliamentarians have been able to detect the issue raised by the Federal Court?**

While it is speculative to say whether the proposed committee would have explored this issue or not, its mandate and scope would have enabled access to the information pertinent to this case.

The proposed committee would have the authority to review any department or agency of the Government of Canada that performs national security or intelligence activities, including their ongoing operations.

### **2. [For Minister] Does the Minister still have confidence in CSIS?**

CSIS plays a vital role in keeping Canadians safe by investigating threats, and collecting and analyzing information to protect our national security. I continue to have confidence in their ability to deliver on that mandate.

### **3. Will this decision impact or influence the issue of Basic Subscriber Information / Lawful Access?**

The Federal Court's concern does not extend to the issue of the provision of Basic Subscriber Information to law enforcement and intelligence agencies.

Basic Subscriber Information is one of the 10 topics the Government has selected for its public consultation on national security. The input the Government receives from Canadians, including experts, stakeholders, and Parliamentarians, will help inform the development of national security law and policies.

The security and privacy of Canadians are both crucial considerations for BSI.

All Canadians are welcome to participate in the online consultation from now until December 1st, 2016, at: [Canada.ca/national-security-consultation](http://Canada.ca/national-security-consultation)

### **4. Does this decision represent a failure from SIRC in its oversight role?**

SIRC reviewed CSIS' use of associated data and published its findings on the issue in its 2014-15 annual report. SIRC did not conclude that the retention of associated data was illegal. The Federal Court arrived at a different conclusion. Upon review, the Government accepts the Federal Court's findings.



- 2 -

SIRC continues to play a very critical role in keeping CSIS accountable through in-depth reviews of its activities. The Minister of Public Safety has asked SIRC to monitor CSIS's compliance with the Federal Court decision.

**5. Can you expand on what the Minister is asking SIRC to do in relation to reviewing CSIS's compliance with the decision?**

SIRC has a unique mandate in keeping CSIS accountable through in-depth reviews of its activities. The findings of its reviews are made available to all Canadians through SIRC's annual reports. These reports are extremely valuable in ensuring that CSIS is operating consistently with Canadian law and values.

Section 54 (2) of the *CSIS Act* provides the Minister of Public Safety with the authority to request a special report from SIRC concerning any matter that relates to the performance of its duties and functions. These special reports are only requested in exceptional circumstances, and do not form part of SIRC's regular review plans for a given year.

The Minister of Public Safety is using this authority to request that the SIRC monitor CSIS' compliance with the Federal Court decision in the matter of "associated data" retention.

SIRC will report its findings directly to the Minister through a classified document. A summary of the findings will be included in SIRC's Annual Report to Parliament, which is available to all Canadians.

**Prepared by:** Julie Grenier

**Consulted:**

NS Intelligence  
CSIS Comms (FYI)  
DoJ Comms (FYI)

**Approved by:**

John Davies, DG, NS Policy (approved)  
Monik Beaugard, ADM, NCSB (approved)  
Heather Magee, Director, Communications (approved)  
MO (pending)  
PCO (pending)



---

# *Media Lines*

---

## **FEDERAL COURT "EN BANC" DECISION CSIS' Authority to Retain Associated Data Collected Through Warrants**

**Issue:** The Federal Court is anticipated to release its decision regarding the CSIS Act and CSIS' authority to retain certain metadata ("associated data") collected through Federal Court issued warrants in the near future. The Federal Court found that CSIS' retention of associated data linked to third party communications found to be unrelated to threats to the security of Canada is illegal. The Federal Court also found that CSIS breached its duty of candour by failing to fully and transparently inform the Court of its retention program and the establishment of the Operational Data Analysis Centre (ODAC).

### **Key Messages:**

- The Government accepts the Federal Court's findings on this matter.
- It is important to underline that the associated data was collected legally through warrants, and CSIS acted pursuant to Court authorized warrants. The Federal Court's key concern relates to CSIS' retention of such data (e.g., date, time, and phone numbers related to a call) when it is not related to a threat to the security of Canada.
- CSIS is taking immediate action to address the Federal Court's findings. CSIS halted all access to, and analysis of, the associated data as it actively works to assess and address the Federal Court's decision.
- The Government accepts the Federal Court's findings regarding its duty of candour. In fact, the Government conceded to the Court that it had failed to meet its duty of candour in this case. CSIS has committed to working with the Federal Court to ensure that it is fully transparent with the Court.
- The Federal Court agreed with CSIS' proposal to update warrants, and generally accepted the changes proposed by CSIS.
- In its decision, the Federal Court noted that the CSIS Act is now more than 30 years old and changes may need to be made to ensure that it keeps pace with changes in technology and the privacy expectations of Canadians. This is something that we will review.
- The Government is committed to keeping Canadians safe while at the same time safeguarding our freedoms, rights and values in an open and democratic society.
- In September we launched a broad public consultation on national security. We want to hear from Canadians on how we can best meet our dual objectives of security and rights. We invite all Canadians to provide us with their views and ideas on our national security framework through our online consultation, which is open until December 1<sup>st</sup>. ([www.canada.ca/national-security-consultation](http://www.canada.ca/national-security-consultation))



- Concurrently, we are taking measures to strengthen national security accountability. In June, we put forward legislation to create a National Security and Intelligence Committee of Parliamentarians which would have a broad mandate to scrutinize the activities of any federal department or agency with national security responsibilities, including operational matters.

**Ministerial Talking Point:**

CSIS plays a vital role in keeping Canadians safe by investigating threats, and collecting and analyzing information to protect our national security. I continue to have confidence in their ability to deliver on that mandate.

**Prepared by:** Julie Grenier

**Consulted:** NS Intelligence, Legal, CSIS Policy, Justice

**Approved by:**

John Davies, DG, NS Policy (approved)  
Monik Beauregard, ADM, NCSB (approved)  
Heather Magee, Director, Communications (approved)  
Jamie Tomlinson, DG, Communications (approved)  
MO (pending)  
PCO (pending)

**Pages 267 to / à 268  
are not relevant  
sont non pertinentes**

**Coates, Liza-Ann (PS/SP)**

---

**From:** Brien, Dan (PS/SP)  
**Sent:** Monday, October 24, 2016 5:15 PM  
**To:** Tomlinson, Jamie (PS/SP)  
**Cc:** Magee, Heather (PS/SP); Wilson, Ashleigh (PS/SP)  
**Subject:** Re: federal court update

Has the Deputy AG role been nailed down and confirmed? It keeps swinging back and forth.

db mobile  
613.698.2270

**From:** Tomlinson, Jamie (PS/SP)  
**Sent:** Monday, October 24, 2016 4:27 PM  
**To:** Brien, Dan (PS/SP)  
**Cc:** Magee, Heather (PS/SP); Wilson, Ashleigh (PS/SP)  
**Subject:** RE: federal court update

There have been tweaks (mostly from various Legal folks) to some of the DOJ and CSIS products. We are in the process of pulling together all of the pieces and will send you a set in the morning. PCO has advised that PMO may yet have comments.

**From:** Brien, Dan (PS/SP)  
**Sent:** October-24-16 4:02 PM  
**To:** Tomlinson, Jamie (PS/SP)  
**Subject:** RE: federal court update

I saw that – good news!

Have the products changed a lot today?

**From:** Tomlinson, Jamie (PS/SP)  
**Sent:** Monday, October 24, 2016 4:00 PM  
**To:** Brien, Dan (PS/SP)  
**Subject:** federal court update

- barring additional comments that may be provided by the amici, the Court has accepted the proposed redactions as submitted by the Service
- the decision will be released in both official languages. The translation is still ongoing.
- the Court does not have a release date for the decision **but intends to give the applicant a 48 h notice.**

## Coates, Liza-Ann (PS/SP)

---

**From:** O'Nions, Christine <Christine.O'Nions@pco-bcp.gc.ca>  
**Sent:** Monday, October 24, 2016 4:52 PM  
**To:** Magee, Heather (PS/SP)  
**Cc:** Tomlinson, Jamie (PS/SP); Nichols, Megan (PS/SP); Wilson, Ashleigh (PS/SP)  
**Subject:** Re: Public Safety Products - Federal Court Decision

Thx!

---

**From:** Magee, Heather (PS/SP) [<mailto:heather.magee@canada.ca>]  
**Sent:** Monday, October 24, 2016 04:09 PM  
**To:** O'Nions, Christine  
**Cc:** Tomlinson, Jamie (PS/SP) <[Jamie.Tomlinson@canada.ca](mailto:Jamie.Tomlinson@canada.ca)>; Nichols, Megan (PS/SP) <[megan.nichols@canada.ca](mailto:megan.nichols@canada.ca)>;  
Wilson, Ashleigh (PS/SP) <[ashleigh.wilson@canada.ca](mailto:ashleigh.wilson@canada.ca)>  
**Subject:** Public Safety Products - Federal Court Decision

Hi Christine,

As requested, resending you our products for the Federal Court's decision regarding CSIS. Please let us know when these are PMO approved. Products are:

- Minister's Statement
- Speaking Notes
- Key Messages
- Qs&As

Thanks,

Heather

Telephone | Téléphone : 613-949-6191  
Mobile | Cellulaire : 613-302-3752

## Arbeau, Kristy (PS/SP)

---

**From:** Tomlinson, Jamie (PS/SP)  
**Sent:** Monday, October 24, 2016 3:26 PM  
**To:** Magee, Heather (PS/SP); Wilson, Ashleigh (PS/SP); Nichols, Megan (PS/SP)  
**Subject:** FW: CSIS Federal Court decision - update

More info....

**From:** [REDACTED]  
**Sent:** October-24-16 3:12 PM  
**To:** Bouzigon, Mylène; Matte, Daniel; Vigneault, David; [REDACTED]  
[REDACTED] Noftle, Tracie; O'Nions, Christine; Off, Shirley Anne; Ghiz, Joanne; Webber, Grégoire; Tomlinson, Jamie (PS/SP); Hurl, David (PS/SP); Davies, John (PS/SP); Brien, Dan (PS/SP); [REDACTED]; Gowing, Andrew; [REDACTED] (PS/SP); Brender, James (PS/SP); Allen, Kristine; Frater, Robert; [REDACTED] Leclerc, Caroline  
**Cc:** Bustros, Katia; Farkas, Jennifer; Benoit, Nathalie  
**Subject:** Re: CSIS Federal Court decision - update

Bonjour à tous,

[REDACTED]

Thank you.

[REDACTED]

Envoyé de mon smartphone BlackBerry 10 sur le réseau Rogers.

**De:** Bouzigon, Mylène  
**Envoyé:** vendredi 21 octobre 2016 1:32 PM  
**À:** Matte, Daniel; Vigneault, David; [REDACTED]  
Noftle, Tracie; O'Nions, Christine; Off, Shirley Anne; Ghiz, Joanne; Webber, Grégoire; 'jamie.tomlinson@canada.ca'; 'david.hurl@canada.ca'; 'john.davies@canada.ca'; 'dan.brien@canada.ca'; [REDACTED] Gowing, Andrew; [REDACTED] (PS/SP); 'Brender, James (PS/SP)'; Allen, Kristine; Frater, Robert; [REDACTED]; Leclerc, Caroline  
**Cc:** Bustros, Katia; Farkas, Jennifer; Benoit, Nathalie  
**Objet:** CSIS Federal Court decision - update

Good afternoon,

[REDACTED]

Thank you.

MB

**Me Mylène Bouzigon**

Senior General Counsel | Avocate générale principale

(613) 842-1197 / (613) 231-0027 | [bouzigon.mylene@justice.gc.ca](mailto:bouzigon.mylene@justice.gc.ca) | Facsimile - télécopieur: (613) 842-1345

*This communication contains information that may be confidential, exempt from disclosure, subject to litigation privilege or protected by the privilege that exists between lawyers and their clients. If you are not the intended recipient, you should not read, rely on, retain, or distribute it. Please delete or otherwise destroy this communication and all copies of it immediately, and contact the sender.*

*Ce message contient des renseignements qui pourraient être confidentiels, soustraits à la communication, ou protégés par le privilège relatif au litige ou par le secret professionnel liant l'avocat à son client. S'il ne vous est pas destiné, vous êtes priés de ne pas le lire, l'utiliser, le conserver ou le diffuser. Veuillez sans tarder le supprimer et en détruire toute copie, et communiquer avec l'expéditeur.*

**De :** Benoit, Nathalie

**Envoyé :** 20 octobre 2016 15:52

**À :** Matte, Daniel <[Daniel.Matte@justice.gc.ca](mailto:Daniel.Matte@justice.gc.ca)>; Benoit, Nathalie <[Nathalie.Benoit@justice.gc.ca](mailto:Nathalie.Benoit@justice.gc.ca)>; Vigneault, David <[David.Vigneault@pco-bcp.gc.ca](mailto:David.Vigneault@pco-bcp.gc.ca)>; [redacted] <[redacted]@pco-bcp.gc.ca>;

[redacted] <[redacted]@pco-bcp.gc.ca>; Noftle, Tracie <[Tracie.Noftle@pco-bcp.gc.ca](mailto:Tracie.Noftle@pco-bcp.gc.ca)>; O'Nions, Christine <[Christine.O'Nions@pco-bcp.gc.ca](mailto:Christine.O'Nions@pco-bcp.gc.ca)>; Off, Shirley Anne <[ShirleyAnne.Off@justice.gc.ca](mailto:ShirleyAnne.Off@justice.gc.ca)>; Ghiz, Joanne <[Joanne.Ghiz@justice.gc.ca](mailto:Joanne.Ghiz@justice.gc.ca)>; Webber, Grégoire <[Gregoire.Webber@justice.gc.ca](mailto:Gregoire.Webber@justice.gc.ca)>; 'jamie.tomlinson@canada.ca' <[jamie.tomlinson@canada.ca](mailto:jamie.tomlinson@canada.ca)>; 'david.hurl@canada.ca' <[david.hurl@canada.ca](mailto:david.hurl@canada.ca)>; [john.davies@canada.ca](mailto:john.davies@canada.ca); 'dan.brien@canada.ca' <[dan.brien@canada.ca](mailto:dan.brien@canada.ca)>; [redacted]; [redacted]; [redacted]; Gowing, Andrew <[Andrew.Gowing@justice.gc.ca](mailto:Andrew.Gowing@justice.gc.ca)>; [redacted] (PS/SP) <[redacted]@canada.ca>; 'Brender, James (PS/SP)' <[james.brender@canada.ca](mailto:james.brender@canada.ca)>; Allen, Kristine <[Kristine.Allen@justice.gc.ca](mailto:Kristine.Allen@justice.gc.ca)>; Frater, Robert <[Robert.Frater@justice.gc.ca](mailto:Robert.Frater@justice.gc.ca)>; [redacted]; Leclerc, Caroline <[Caroline.Leclerc@justice.gc.ca](mailto:Caroline.Leclerc@justice.gc.ca)>

**Cc :** Bouzigon, Mylène <[Mylene.Bouzigon@justice.gc.ca](mailto:Mylene.Bouzigon@justice.gc.ca)>; Bustros, Katia <[Katia.Bustros@justice.gc.ca](mailto:Katia.Bustros@justice.gc.ca)>

**Objet :** CSIS Federal Court decision - update

Good afternoon,

Salutations,

**Nathalie Benoit**  
**General Counsel, NLSAG**  
**613-369-2499.**

**AVIS DE CONFIDENTIALITÉ**

Le contenu de ce courrier électronique est confidentiel et strictement réservé à l'usage des personnes auxquelles il s'adresse. Ce message peut contenir de l'information privilégiée protégée par le secret professionnel avocat-client. Si vous avez reçu ce message par erreur, contactez immédiatement l'expéditeur afin de confirmer que vous avez détruit le message original et toute copie. Veuillez noter qu'il est strictement interdit de divulguer, reproduire ou diffuser le contenu de ce message ou de prendre des mesures en conséquence. Tout nouvel envoi, reproduction ou usage de ce message par une personne autre que le destinataire est strictement interdit. Merci.

**CONFIDENTIALITY NOTICE**

The contents of this electronic mail message are confidential and strictly reserved for the sole use of its intended recipients. This message may contain information protected by the solicitor-client privilege. If you receive this message in error, please notify the sender immediately in order to confirm that the original message as well as all copies have been deleted. Any disclosure, copying, distribution or reliance on the contents of the information is strictly prohibited. Thank you.

## Sayarh, Omar (PS/SP)

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Monday, October 24, 2016 10:45 AM  
**To:** Magee, Heather (PS/SP)  
**Subject:** Duty of Candour - Min Statement and CSIS Q&A  
**Attachments:** PS-SP-#1997213-v1C-Minister\_-\_Statement\_on\_En\_Banc\_Decision.doc; QA ADP approved DoJedits Oct 23.docx

Hi Heather,

On the matter of Duty of Candour:

The Minister's Statement states:

- **I also take very seriously the explicit finding by Justice Noel that CSIS had failed in its duty to be candid with the court.**

- **The Government accepts the Federal Court's findings regarding its duty of candour. In fact, the Government conceded to the Court that it had failed to meet its duty of candour in this case.**
- **The Court found that CSIS failed to fully and transparently inform the Court of its retention program and the establishment of the Operational Data Analysis Centre (ODAC), but did not find evidence that this had been done deliberately.**

Suggest we keep the current wording in the Statement, but I'll update our Key Messages to mirror CSIS Q&A.

Hope this helps,  
Julie



---

# Statement

---

## **STATEMENT BY PUBLIC SAFETY MINISTER RALPH GOODALE ON THE RULING OF THE FEDERAL COURT OF CANADA, PUBLISHED OCTOBER XX, 2016, WITH RESPECT TO THE CANADIAN SECURITY INTELLIGENCE SERVICE (CSIS) AND THE HANDLING OF "ASSOCIATED DATA"**

October XX, 2016 – “I welcome the decision in this matter rendered by Mr. Justice Noel on behalf of the Federal Court, which the Government will not appeal.

The court's insight and guidance are timely, coming in the midst of the public consultations we now have underway about Canada's national security framework.

CSIS plays a critical role in keeping Canadians safe. As it investigates threats to our national security, the Service collects a considerable amount of information, with full legal authorization pursuant to the CSIS Act and warrants issued by the Federal Court. When the information is intercepted communications, it can often include "associated data" of third-parties such as phone numbers and email addresses.

The court has ruled that while legally collected, such "associated data" cannot be retained and utilized by CSIS unless it relates to a specific threat to the security of Canada or is of use to an investigation, prosecution, national defence or foreign affairs.

The Service has confirmed that it is taking immediate steps to address the court's decision. It has blocked all access to and analysis of any associated data, while it considers its next steps. As Minister of Public Safety, I am asking the Security Intelligence Review Committee (SIRC) to monitor the situation carefully to ensure compliance.

I also take very seriously the explicit finding by Justice Noel that CSIS had failed in its duty to be candid with the court. I will be pursuing this criticism with the executive management of the Service. In matters of security and intelligence, Canadians need to have confidence that all the departments and agencies of the Government of Canada are being effective at keeping Canadians safe, and equally, that they are safeguarding our rights and freedoms.

I also take note of the court's observation that the CSIS Act is now more than 30 years old and showing its age as global affairs, threat profiles, technology and public expectations have rapidly evolved. In his judgment, Justice Noel did not dispute the potential value of "associated data" to the important work CSIS does in this challenging world, but he could not find existing legislative authority permitting its retention and use.”

-30-

Follow Public Safety Canada ([@Safety\\_Canada](#)) on Twitter.

For more information, please visit the website [www.publicsafety.gc.ca](http://www.publicsafety.gc.ca).

### Information:



- 2 -

Scott Bardsley  
Office of the Minister of Public Safety and Emergency Preparedness  
613-998-5681

Media Relations  
Public Safety Canada  
(613) 991-0657

**Pages 277 to / à 289  
are withheld pursuant to section  
sont retenues en vertu de l'article**

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

## Arbeau, Kristy (PS/SP)

---

**From:** Magee, Heather (PS/SP)  
**Sent:** Monday, October 24, 2016 10:19 AM  
**To:** Wilson, Ashleigh (PS/SP); Nichols, Megan (PS/SP)  
**Subject:** Fw: DOJ DM TPs - Federal Court CSIS decision  
**Attachments:** CSIS Noel Decision Speaking Notes E - October 21, 2016v3 DM version.docx; CSIS Noel Decision Statement E - October 21, 2016v2.docx

Heather Magee  
Public Safety Canada / Sécurité publique Canada  
T: 613-949-6191 M: 613-302-3752  
[Heather.Magee@canada.ca](mailto:Heather.Magee@canada.ca)

**From:** Tomlinson, Jamie (PS/SP) <[jamie.tomlinson@canada.ca](mailto:jamie.tomlinson@canada.ca)>  
**Sent:** Monday, October 24, 2016 6:39 AM  
**To:** Magee, Heather (PS/SP); Grenier, Julie (PS/SP)  
**Subject:** FW: DOJ DM TPs - Federal Court CSIS decision

Fyi.... DOJ products

**From:** De Mora, Joe [<mailto:Joe.DeMora@justice.gc.ca>]  
**Sent:** October-23-16 8:29 PM  
**To:** Noftle, Tracie; Fox, Christiane; [REDACTED] O'Nions, Christine  
**Cc:** Off, Shirley Anne; [REDACTED] Lindblad, Anabel; Tomlinson, Jamie (PS/SP); Magee, Heather (PS/SP)  
**Subject:** Fw: DOJ DM TPs - Federal Court CSIS decision

Pls find attached talking points for our DM for the presser and, shd it be needed, a draft statement as well.

Best

Joe

**Pages 291 to / à 294  
are withheld pursuant to section  
sont retenues en vertu de l'article**

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

**Sayarh, Omar (PS/SP)**

---

**From:** Tomlinson, Jamie (PS/SP)  
**Sent:** Monday, October 24, 2016 6:39 AM  
**To:** Grenier, Julie (PS/SP); Magee, Heather (PS/SP)  
**Subject:** FW: Updated CSIS products  
**Attachments:** QA ADP approved DoJedits Oct 23 (redacted edit clean).docx

Latest CSIS Qs & As

---

**From:** (redacted)  
**Sent:** October-23-16 9:35 PM  
**To:** (redacted) De Mora, Joe; Christiane Fox; Noftle, Tracie; Off, Shirley Anne; Tomlinson, Jamie (PS/SP); O'Nions, Christine  
**Cc:** (redacted)  
**Subject:** Re: Updated CSIS products

Here is the updated Q&A product with the adjustment to questions 4 and 5.

Thx  
Tahera

---

**From:** (redacted)  
**Sent:** Sunday, October 23, 2016 9:02 PM  
**To:** De Mora, Joe; Christiane Fox; Noftle, Tracie; Off, Shirley Anne; Tomlinson, Jamie (PS/SP); O'Nions, Christine  
**Cc:** (redacted)  
**Subject:** Re: Updated CSIS products

Thanks Joe.

(redacted) can you please make that change, flag to translation and please re-send the clean products to this email?

(redacted)  
DG, Communications

(redacted)  
@csiscanada / @scrscanada

---

**From:** De Mora, Joe  
**Sent:** Sunday, October 23, 2016 9:00 PM  
**To:** (redacted) Christiane Fox; Noftle, Tracie; Off, Shirley Anne; Tomlinson, Jamie (PS/SP); O'Nions, Christine  
**Cc:** (redacted)  
**Subject:** Re: Updated CSIS products

(redacted) one word change to the Q and A that affects questions 4 and 5. I have cited it in CAPS below.

Tks

Joe

The Attorney General of Canada has taken a number of steps, including SEEKING advice from external experts, to ensure they are in the best possible position to meet the Government's duty of candour in future hearings.

---

**From:** [REDACTED]  
**Sent:** Sunday, October 23, 2016 8:30 PM  
**To:** Christiane Fox; Noftle, Tracie; Off, Shirley Anne; Tomlinson, Jamie (PS/SP); O'Nions, Christine; De Mora, Joe  
**Cc:** [REDACTED]  
**Subject:** Updated CSIS products

As discussed, please find the updated products (Q/A, DIR opening remarks, DIR statement, and CSIS backgrounder) following our conference call this afternoon. [REDACTED]

[REDACTED]

DG, Communications

[REDACTED]

@csiscanada / @scrscanada

**Pages 297 to / à 308  
are withheld pursuant to section  
sont retenues en vertu de l'article**

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

## Sayarh, Omar (PS/SP)

---

**From:** Davies, John (PS/SP)  
**Sent:** Monday, October 24, 2016 8:24 AM  
**To:** Grenier, Julie (PS/SP); Tomlinson, Jamie (PS/SP); Magee, Heather (PS/SP)  
**Cc:** [REDACTED] (PS/SP); [REDACTED] (PS/SP)  
**Subject:** FW: Updated Products  
**Attachments:** Backgrounder ADP Approved.docx; Backgrounder ADP Approved-French.docx; Director Opening Remarks ADP approved French.docx; Director Statement ADP approved.docx; Director Statement ADP approved-French.docx; Q&A ADP approved..docx; Q&A ADP approved.-TEF.DOCX

I assume you have these already, but just in case.

Can you let us know where things are at from your perspective? Do we owe you any comments etc? Does MO have all they need?

Thanks.

John

---

**From:** [REDACTED]  
**Sent:** Sunday, October 23, 2016 8:25 AM  
**To:** Davies, John (PS/SP); [REDACTED]  
**Cc:** Vigneault, David; [REDACTED]  
**Subject:** Fw: Updated Products

Hi guys,

John and Nada, your comms folks have these and for version control and coordination, probably easiest for you to feed specific comments or any suggested changes directly to them (that said, we are at disaster check stage) and you may even want to wait for whatever pmo or mo consulted version they want to send you, first. Still may see some dm level edits as well. That said, if after reading these you have questions or comments more generally, please let me know. Happy to do by email or with a call, preferably this afternoon.

---

**From:** [REDACTED]  
**Sent:** Saturday, October 22, 2016 4:45 PM  
**To:** [REDACTED]  
**Cc:** [REDACTED]  
**Subject:** Updated Products

As discussed, please find attached the updated and translated products. I will now send them to DG Comms at Justice, Public Safety and PCO.

I have printed copies for yourself, the ADE, the Director and [REDACTED] and will bring them to the retreat tomorrow.



**Pages 311 to / à 312  
are duplicates  
sont des duplicatas**

**Pages 313 to / à 315  
are not relevant  
sont non pertinentes**

UNCLASSIFIED  
NON CLASSIFIÉ

## **Opening Remarks on Federal Court *En Banc* Decision**

### **National Press Gallery**

### **Mot d'ouverture sur la décision rendue en banc par la Cour fédérale**

### **Tribune de la presse nationale**

- **Thank you Andrew. Bonjour Mesdames et Messieurs. Today (or TBD) the Federal Court issued an *En Banc* Decision. I am here to explain what this decision means.**
- **I would like to start off by saying, first and foremost, that the Canadian Security Intelligence Service accepts in full the Court's decision, and have taken immediate actions to respond.**
- **I deeply regret the Court's serious concerns with respect to our duty of candour and I commit to continuing my efforts, with the Deputy Minister of Justice, to fully address this concern.**
- **CSIS recognizes the importance of openness and transparency with the Federal Court, and we are working closely with the Department of Justice to develop measures aimed at ensuring that**

UNCLASSIFIED  
NON CLASSIFIÉ

**we meet our obligations to the Court in matters of transparency and duty of candour.**

- **Given the Court's decision with respect to third-party data, CSIS has halted all access to, and analysis of, associated data while we undertake a thorough review of the decision in order to assess potential operational and legal impacts, and determine our way forward.**
- **Let me be clear that all associated data collected, under warrant, was done so legally. The Court's key concern related to our retention of non-threat related associated data linked with third party communications, after it was collected.**
- **CSIS, in consultation with the Department of Justice, interpreted the CSIS Act to allow for the retention of this sub-set of associated data.**
- **It is now clear that the Federal Court disagrees with this interpretation; a decision which we fully accept.**

UNCLASSIFIED  
NON CLASSIFIÉ

- **All laws must be interpreted in the circumstances, and when the Act was written, current technologies and the potential for data analytics could not have been anticipated.**
- **The Court rightly acknowledged the age of the *CSIS Act* and that it may not be keeping pace with changing technology and the current threat environment, contributing to this challenge.**
- **That said, again, we fully accept the decision of the Court.**
- **As Canada's national intelligence agency, CSIS investigates activities which may, on reasonable grounds, be suspected of posing a threat to the security of Canada.**
- **One of the ways we investigate these threats is through warrants issued by the Federal Court which authorize the interception of communications. This includes analysis of all of the information - both the content and the associated data.**
- **Associated data includes information such as: email addresses and telephone numbers but never the content.**

UNCLASSIFIED  
NON CLASSIFIÉ

- **It is useful in identifying patterns of movement, communications, behaviours, significant trends, and links that are otherwise unidentifiable.**
- **As is the case for many of our international partners, CSIS has developed data analytic capabilities and expertise to exploit associated data and enhance its capacity to identify and assess threats to the security of Canada over time.**
- **When it comes to understanding and predicting the actions of the subjects of our investigations, data analytics has proven to be an effective tool.**
- **In the ruling released today the Federal Court recognized the value of the data analytic programme and confirmed the legality of collecting telecommunications associated data pursuant to warrants.**
- **I would add that, like the threats we face today, technologies and associated privacy implications have also evolved.**
- **The retention and analysis of information is a significant public policy issue, not just in Canada, but also among our closest allies.**

UNCLASSIFIED  
NON CLASSIFIÉ

- **I would like to say, that the trust of Canadians is fundamental to our ability to deliver on our mandate.**
- **Because the nature of our business is principally secret, Canadians are largely unaware of the professionalism and outstanding dedication the men and women of CSIS show every day as they carry out intelligence work. As the Director of CSIS, I am extremely proud of the people with whom I work. Canadians, too, should be proud of those who work tirelessly to keep this great country safe.**
- **We appreciate the confidence the government invests in CSIS, and it remains for us a privilege to protect Canadians and Canada's interest at home and abroad.**
- **The ongoing national security consultations represent an important opportunity to ensure that CSIS is meeting the dual objectives of security and privacy, and has the tools and authorities, with appropriate oversight, to meet both.**
- **(REPEAT IN FRENCH)**
- **(RÉPÉTER EN FRANÇAIS)**

**Pages 321 to / à 326  
are not relevant  
sont non pertinentes**

**Pages 327 to / à 328**

**are duplicates**

**sont des duplicatas**

**Pages 329 to / à 330  
are not relevant  
sont non pertinentes**

UNCLASSIFIED

Embargoed until decision is published

## Qs & As

### A. THE FEDERAL COURT DECISION

#### **1. Why did you appear before the Federal Court?**

- The Canadian Security Intelligence Service is mandated to investigate activities which may, on reasonable grounds, be suspected of posing a threat to the security of Canada. In order to investigate these threats, CSIS may apply to the Federal Court for a warrant when the response to the threat requires more intrusive measures. Late 2015, CSIS applied to renew and obtain new warrants as well as propose amendments to warrant conditions.
- In light of the finding in the Security Intelligence Review Committee's (SIRC) annual report (2014-15), the Court requested that the collection, use, retention and destruction of associated data (referred to by SIRC as metadata) collected under warrants also be addressed.
- These issues were heard en banc.

#### **2. What is the decision?**

- The Court agreed with most of the terms and conditions proposed by CSIS on the warrant application that was presented to the Court.
- The Court found that CSIS failed to fully and transparently inform the Court of its retention program and the establishment of the Operational Data Analysis Centre (ODAC), but did not find evidence that this had been done deliberately.
- The Court also determined that CSIS' retention of associated data linked to third-party communications found to be unrelated to threats or of no use to an investigation, prosecution, national defence or international affairs to be illegal.
- That said, it is important to underline that all associated data was collected legally through warrants. The Federal Court's key concern relates to CSIS' retention of non-threat related associated data linked with third party communications, after it was collected.
- Further, the Court rightly acknowledged the age of the *CSIS Act* and that it may not be keeping pace with changing technology and the current threat environment.

#### **3. What is the Government's duty of candour?**

- In all instances where only one party is before the Court, without having all of the other interested parties present (known as an "*ex parte*" or "*in private*" hearing), that the party is under a duty of utmost good faith in the representations it makes to the Court.

UNCLASSIFIED

Embargoed until decision is published

- The evidence presented must be complete and thorough and no relevant information adverse to the interests of the party may be withheld.
- The Federal Court has noted that this duty is heightened when hearings take place behind closed doors, rather than in public, as often occurs in cases related to national security.
- The duty of candour applies to all parties, not just the Government.

**4. So the Government breached its duty of candour in this case?**

- Department of Justice lawyers, who represented CSIS in this matter, strive to uphold the highest standards of the legal profession in their representation of the Government interests in the Courts.
- In this case, the Government accepts the Federal Court's findings that regarding CSIS's duty of candour and is taking immediate action to address those findings.
- CSIS can and will do more to ensure that it is fully transparent with the Federal Court regarding the use it makes or plans to make of the information it collects pursuant to Federal Court issued warrants. To that end, it is working closely with the Department of Justice.

**5. This is not the first incident of CSIS being found to be in breach of Duty of Candour. Why and what is being done to address this?**

- CSIS recognizes the importance of openness and transparency with the Federal Court.
- Overtime the provisions of the warrants have changed to take into account the evolution of technology, legal developments and investigate measures.
- The *CSIS Act* defines the Service's relationship with the Court. The means to approach the Court is through a warrant application, which creates a very focused type of interaction.
- Given the Court's findings, we are seized with these concerns and are working closely with the Department of Justice to develop measures aimed at ensuring that we meet our obligations to the Court in matters of transparency and duty of candour.

**6. What is CSIS doing to address the duty of candour issues and why should they be trusted given that this is a second breach of this nature?**

- CSIS is committed to improve its practices involving the Court to ensure it fully meets its duty of candour

UNCLASSIFIED

Embargoed until decision is published

- In consultation with the Department of Justice, we are working to develop measures aimed at ensuring that we meet our obligations to the Court in matters of transparency and duty of candour.

**7. Why did CSIS not inform the Court of its new position on the retention of data and the creation of the Operational Data Analysis Centre (ODAC)?**

- At various points, the Government, the Security Intelligence Review Committee and the Office of the Privacy Commissioner were made aware of CSIS' position on the retention of data and the establishment of ODAC.
- In June 2011, CSIS did advise the Federal Court that it amended the wording of warrant conditions in an effort to distinguish the content of communications from the associated data of communications. The Court found that notification to be insufficient.
- CSIS takes notice of the fact that the Court should have been informed earlier of the existence of ODAC and the change in the retention policy and acknowledges this was a significant omission. At no point did CSIS deliberately seek to withhold this information from the Court, and the Court acknowledged that there is no evidence to that fact.
- The development of this new capability evolved over time as has our understanding of our obligations towards the Federal Court in this regard, which CSIS determines in close consultation with the Department of Justice.

**8. SIRC recommended in their 2014-15 Report that the Service advise the Federal Court of activities relating to metadata collected under a warrant. CSIS, however believed that SIRC's recommendation was both inappropriate and unwarranted given that section 21 of the CSIS Act does not confer any general supervisory authority to Federal Court judges. Why did CSIS take this position?**

- It is SIRC that reviews the activities of CSIS and not the Federal Court. This stems from a strict interpretation of the CSIS Act. It is now clear that the Federal Court disagrees with such an interpretation. The Service accepts this finding.
- The Service was under the impression that the Federal Court had been sufficiently advised of the retention of associated data in 2011. The Court also disagreed with this assessment. The Service accepts this finding.

**9. Has CSIS briefed this Minister on this matter?**

- In the context of an update on the en banc hearing, the current Minister of Public Safety has been briefed a number of times.
- At various points, previous Ministers, the Security Intelligence Review Committee and the Office of the Privacy Commissioner were made aware of CSIS' position on the retention of data and the establishment of ODAC.

UNCLASSIFIED

Embargoed until decision is published

**10. Did CSIS purposely mislead the Court in this case?**

- The Court found that CSIS failed to fully and transparently inform the Court of its retention program and the establishment of the Operational Data Analysis Centre (ODAC), but did not find evidence that this had been done deliberately.

**11. Can CSIS be held in “contempt of court” for not disclosing this information?**

- (Answer to be provided by DoJ)

**CSIS RESPONSE TO THE DECISION**

**12. What have you done to respond to the judgement?**

- On duty of candour: CSIS takes this finding very seriously and recognizes the importance of compliance with Ministerial Direction and the *CSIS Act*, as well as openness and transparency with the Court.
- CSIS can and will do more to ensure that it is fully transparent with the Federal Court regarding the use it makes or plans to make of the information it collects pursuant to Federal Court issued warrants. To that end, it is working closely with the Department of Justice.
- On the retention of non-threat related associated data linked with third-party communications: CSIS immediately halted access to, and analysis of, associated data until such time as it can successfully distinguish associated data linked to third-party communications from that of subject of investigation communications.

**13. What steps will CSIS take to implement the Court’s recommended two-step process of assessment?**

- CSIS will be required to assess, within a short period, communications data to determine its relevance to a subject of investigation or threat to the security of Canada.
- Significant efforts will be required to implement policies, processes and technology that will successfully distinguish between threat related and non-threat related associated data. ~~associated data (third-party communications) from that of threat-related communications.~~

**14. Has CSIS destroyed the data deemed illegal by the Court?**

- The Court did not order CSIS to destroy third-party associated data from its databases and recognized that the retention and analysis of associated data has yielded useful intelligence results in the past.

UNCLASSIFIED

Embargoed until decision is published

- CSIS immediately halted analysis and use of all associated data until such time as it can successfully distinguish associated data from that linked to a threat.
- We are assessing the application of the Court's finding in this regard.

### **IMPACTS OF THE DECISION**

#### **15. Did CSIS collect this information legally?**

- Any collection activity that requires the use of specific investigative techniques is authorized by warrants issued by the Federal Court. CSIS collected this information legally, as confirmed in the decision.
- The Federal Court's key concern relates to CSIS' retention of non-threat related associated data linked with third-party communications, after it was collected.

#### **16. Why was CSIS retaining this third party associated data if it was not authorized by the CSIS Act?**

- All laws must be interpreted in the circumstances and when the CSIS Act was written, it did not conceive of current technologies and the potential for data analytics.
- CSIS, in consultation with the Department of Justice, interpreted the CSIS Act to allow for the retention of this data.
- It is now clear that the Federal Court disagrees with this interpretation.
- CSIS fully accepts the Court's ruling and has taken appropriate steps to respond.

#### **17. Will this decision affect the admissibility of evidence used in the cases of convicted terrorists?**

- CSIS is mandated to collect, by investigation or otherwise, to the extent that is strictly necessary, and analyze and retain information and intelligence regarding activities that may on reasonable grounds be suspected of constituting threats to the security of Canada.
- CSIS collects intelligence or information for the purpose of advising the Government, providing security advice or security assessments. It does not, however, collect evidence.

#### **18. Were leads generated by the use of third-party associated data provided to the RCMP or other law enforcement partners for the purposes of counter terrorism investigations?**

- CSIS is assessing the decision in an effort to determine how it impacts operations. CSIS cannot, however, comment on the nature of its operations, and how they are impacted.

UNCLASSIFIED

Embargoed until decision is published

**19. Does this decision impact any current terrorism related cases?**

- CSIS is assessing the decision in an effort to determine how it impacts operations. CSIS cannot, however, comment on the nature of its operations, and how they are impacted.

**20. How many Canadians were impacted?**

- It is impossible to quantify the number of individuals linked to the associated data, much less identify personal details such as citizenship.
- The associated data in question is associated with communications lawfully intercepted under warrant in relation to the investigation of threats to the security of Canada.
- Associated data does not reveal the purpose of the communication, nor any part of the content and, on its own, does not identify individuals who are party to the communication.
- This speaks directly to the nature of associated data, which, on its own, does not readily identify an individual.

**BROADER IMPLICATIONS OF THE DECISION**

**21. Are there any privacy implications noted in the decision?**

- The Federal Court did not speak to the privacy considerations of the retention of third-party associated data.
- CSIS recognizes the importance of maintaining public trust and confidence in its activities. CSIS takes very seriously potential privacy considerations related to its work, and it is committed to ensuring that its activities are transparent, accountable and in compliance with privacy legislation, guidelines and best practices.
- Of note, a Privacy Impact Assessment on ODAC was completed in August 2010. Should the Office of the Privacy Commissioner be interested in investigating the privacy implications of the decision, CSIS will cooperate fully.

**22. How can Canadians have confidence in the organization?**

- CSIS recognizes the importance of maintaining public trust and confidence, and has a strong record of responsibly exercising its authorities and has matured as an organization over its 30 year history.
- SIRC, and the Inspector General before it, has consistently found that the Service has carried out its duties in accordance with the CSIS Act and Ministerial Direction and that the exercise of its activities has been reasonable and necessary.
- CSIS maintains a productive relationship with SIRC. SIRC's findings and recommendations have demonstrably shaped the conduct of CSIS operations and continue to do so.
- And in the context of warrant powers, CSIS must also answer to the Federal Court.
- As CSIS adapts to an ever-changing environment, challenges do emerge, demanding continual improvement to operational policies and procedures, supported by a robust governance framework.

UNCLASSIFIED

Embargoed until decision is published

- CSIS operates in a rigorous system of checks and balances. These layers of accountability are mutually reinforcing, which is certainly highlighted in this instance and will be bolstered by enhanced oversight by the proposed Committee of Parliamentarians.

**23. Will the government consult Canadians on the data exploitation activities of CSIS?**

- The Government is committed to keeping Canadians safe while at the same time safeguarding our freedoms, rights and values in an open and democratic society.
- The ongoing national security consultations represent an important opportunity to ensure that CSIS is meeting the dual objectives of security and privacy and has the tools and authorities, with appropriate oversight, to meet both.

**24. Will the new National Security and Intelligence Committee of Parliamentarians have any role in reviewing CSIS' data exploitation activities?**

- Enhancements to the review system, including the proposed National Security and Intelligence Committee of Parliamentarians, will be properly decided by Parliament.
- As currently drafted, the Bill to establish the Committee would authorize it to review the operational activities of CSIS, including programmes such as its data exploitation activities.
- CSIS will, of course, respect and fully cooperate with this committee, should it be stood up and wish to review this issue, or any other CSIS activity.

**ODAC, DATA EXPLOITATION AND ASSOCIATED DATA**

**25. What kind of communications data does the Service collect?**

- In the course of an investigation, CSIS may obtain warrant powers against individuals or entities to authorize the use of specific investigative techniques. These powers, for example, allow CSIS to intercept communications. Execution of such warrant powers may result in the incidental collection of information from parties other than the target (i.e. third-parties).
- When CSIS intercepts a communication, it obtains the content of the communication, as well as data about the communication. This could include: email addresses and telephone numbers.
- This data does not include any information that could reveal the purpose of the communication, nor any part of its content.

**26. What is the difference between associated data and metadata?**

- There is no difference. Associated data – or metadata – refers to information associated to a communication intercepted pursuant to a warrant.

UNCLASSIFIED

Embargoed until decision is published

- Neither metadata or associated data includes any information that could relate to content.
- Metadata is the context, not the content of a communication. It is information used by computer systems to identify, describe, manage or route communications across a network.

**27. What is associated data as defined by the Federal Court?**

- CSIS had applied the term associated data to all metadata associated to a communication intercepted under warrant.
- The Federal Court, however, diverged from the Service's definition.
- The Federal Court defines associated data as communications data collected under warrant from which the content was assessed as unrelated to threats and of no use to an investigation, prosecution, national defence or international affairs.
- Given the Federal Court's interpretation, the Service will undertake to review the terminology it applies to management of information collected under warrant.

**28. What is the difference between associated data and the dataset collection SIRC reviewed recently?**

- SIRC's 2016 Annual Report reviewed CSIS's non-warranted collection of datasets. This does not include communications content or data collected under Federal Court warrant.
- As an example, some non-warranted datasets are referential and provide contextual information which is publicly available. CSIS has developed a rigorous governance framework for the collection of non-referential datasets. This framework sets out clear requirements and a decision-making process to ensure that our collection in this regard respects *CSIS Act* requirements and the Charter, including privacy considerations.
- The Federal Court was concerned only with warranted collection, namely retention of third party associated data. That said, the Service is assessing the implications of this ruling for the non-warranted datasets SIRC recently reviewed.

**CSIS USE OF ASSOCIATED DATA**

**29. How will CSIS deal with the associated data it currently holds?**

- CSIS immediately halted all access to, and analysis of, all associated data until such time as it can successfully distinguish associated data from that linked to a threat.

**30. Has or does CSIS share its associated data holdings with foreign partners?**

- CSIS does not share raw associated data with foreign or domestic partners.
- Associated data that has been analysed and determined to be related to a threat could have been shared with domestic and foreign partners in accordance with our national security mandate.

UNCLASSIFIED

Embargoed until decision is published

- Although raw associated data would not have been shared with partners, it is used to inform our investigations as well as intelligence products which may be discussed and shared with partners.
- In this context the associated data would have been deemed threat related and thus is authorized to be retained by the Service.

**31. How is this collection different from the bulk collection of SIGINT agencies?**

- CSIS collection of communications data is authorized under Federal Court warrants and is specifically focused on an identified target of investigation.

**32. How does or did CSIS previously ensure that data exploitation technologies did not unnecessarily target individuals NOT engaged in threat related activity?**

- Data exploitation is used in response to specific operational queries related to mandated investigations.
- Data exploitation is a tool to assist the Service in discovering linkages, trends and patterns to advance investigations.
- Determining whether or not a communication is threat-related is complex and may only become apparent as an investigation progresses.
- The Service has seen examples where communications originally assessed to have no intelligence value were later revealed to contain key threat-related information.

**33. What is third party information?**

- Subjects of investigation communicate with a whole range of people for a whole range of purposes, which may or may not be threat-related.
- When these communications are intercepted, it is not immediately known whether or not the communication is related to the threat.
- The Court acknowledged that in executing warrant powers, CSIS will by necessity collect third party information; information that is not directly associated with a subject of investigation.
- Some third party information is threat-related and provides essential investigative leads. Some, however, has no intelligence value
- CSIS policy and practice is to delete the content of communications intercepts collected under warrant assessed to be of no intelligence value.
- Though the content was destroyed, the data about the communication was retained, whether or not it was related to a third party.
- On the very specific issue of non-threat related associated data linked to third-party communications, the Court found that it can only be retained if it is related to threats or of use to an investigation, prosecution, national defence or international affairs.

UNCLASSIFIED

Embargoed until decision is published

**34. What is data exploitation, how does CSIS conduct data exploitation and why?**

- Data exploitation employs computers to analyze data and discover linkages, trends and patterns. These techniques enable humans to make sense of volumes of information that could not be processed without a computer's assistance.

Data exploitation enables the Service to effectively analyze threats to the security of Canada over time. It can provide insight into subjects of investigation; identify new leads and intelligence gaps and provide context and understanding to operations.

- The exploitation of data is invaluable in relation to the exercise of CSIS' mandate, but it must be undertaken responsibly and in accordance with our authorities. The Federal Court decision provides new direction in this regard.

**35. What is ODAC? Was anyone advised of its existence?**

- To derive more value from the data already being collected under warrant using data exploitation techniques, the Service established the Operational Data Analysis Centre in 2006.
- The necessity of creating this capability was described to the Minister of Public Safety in July 2006, noting that a basic requirement of ODAC would be the ability to retain data for extended periods of time.
- CSIS also informed subsequent ministers, the Inspector General, the Privacy Commissioner and SIRC.

**36. How long has CSIS had a formal data exploitation program?**

- The necessity of creating this capability was described to the Minister of Public Safety in July 2006 when CSIS developed the Operational Data and Analysis Centre (ODAC). This capability was created with full disclosure to the Government.

**37. Was SIRC aware of CSIS' data exploitation activities and collection of associated data?**

- SIRC was aware of CSIS' data exploitation activities from shortly after the establishment of ODAC in 2006. In 2007, CSIS responded to a SIRC query about ODAC and its support to operations.
- The Inspector General was provided a verbal briefing on ODAC and data exploitation in support of operations in 2011.
- SIRC reviewed CSIS' use of associated data and published its findings on the issue in its 2014-15 annual report. SIRC did not conclude that the retention of associated data was illegal.

**38. What were the Service's practices with regard to the retention of data collected under warrant prior to the Federal Court's decision?**

UNCLASSIFIED

Embargoed until decision is published

- Pursuant to policy, one year after collection, CSIS practice was to delete the content of communications intercepts collected under warrant assessed to be of no intelligence value.
- Though the content was destroyed, the data about the communication was retained, whether or not it was related to a third-party.

### **FEDERAL COURT, "EN BANC" HEARINGS**

#### **39. What is an "en banc" hearing and why are they used?**

- These are hearings where all available judges, in this case designated judges of the Federal Court, attend, participate, and hear evidence. These hearings are a longstanding judicial practice which is utilized in Courts around the world. For example, all Supreme Court of Canada hearings are conducted "en banc".
- Sitting "en banc" is helpful because it avoids the need to repeat evidence in similar applications in the future. In reaching a decision, judges also have the benefit of one another's perspectives.

#### **40. Why are "en banc" hearings being held in relation to national security issues? What was the Governments' role?**

- The Federal Court of Canada, which has requested that some warrant applications be heard in the presence of all designated judges, determines when en banc hearings occur.
- Representatives of CSIS and the Attorney General of Canada attended these hearings in order to fully understand the Court's expectations and to be in the best possible position to meet them in future ex parte proceedings involving warrants requested by CSIS.

#### **41. Why were these hearings held in secret?**

- There are many reasons why court proceedings may be held privately (also known as "in-camera"), including the protection of national security. This is a common practice which applied to all types of hearings, not just "en banc" hearings.
- In this case, the hearing was held in-camera pursuant to section 27 of the *CSIS Act*

**Pages 342 to / à 354  
are not relevant  
sont non pertinentes**

**Arbeau, Kristy (PS/SP)**

---

**From:** Tomlinson, Jamie (PS/SP)  
**Sent:** Sunday, October 23, 2016 8:45 PM  
**To:** Magee, Heather (PS/SP); Grenier, Julie (PS/SP)  
**Cc:** Wilson, Ashleigh (PS/SP); Nichols, Megan (PS/SP)  
**Subject:** Fw: Updated CSIS products  
**Attachments:** Backgrounder ADP Approved (Oct.23 [redacted] edit clean).docx; Director Opening Remarks ADP approved French DoJ edits October 23 [redacted] edit clean - english only).docx; Director Statement ADP approved (Oct.23 [redacted] edit clean).docx; QA ADP approved DoJedits Oct 23 [redacted] edit clean).docx

**Importance:** High

Fyi

Sent from my BlackBerry 10 smartphone on the Rogers network.

**From:** [redacted]  
**Sent:** Sunday, October 23, 2016 8:32 PM  
**To:** Christiane Fox; Nofle. Tracie; Shirlev Anne Off; Tomlinson, Jamie (PS/SP); O'Nions, Christine; Joe De Mora  
**Cc:** [redacted]  
**Subject:** Updated CSIS products

As discussed, please find the updated products (Q/A, DIR opening remarks, DIR statement, and CSIS backgrounder) following our conference call this afternoon. [redacted]

[redacted]

[redacted]

[redacted]

DG, Communications

[redacted]

@csiscanada / @scrscanada

# Backgrounder

*Federal Court ruling on the retention of associated data linked to third party information.*

## **IMPACT OF THE DECISION ON CSIS:**

- The Canadian Security Intelligence Service is mandated to investigate activities which may, on reasonable grounds, be suspected of posing a threat to the security of Canada. In order to investigate these threats, CSIS may apply to the Federal Court for a warrant when the response to the threat requires more intrusive measures.
- Through the proceedings of the Court, over time, the provisions of warrants have changed to take into account the evolution of technology, legal developments, and investigative measures.
- This ensures that the powers granted by the warrants are clearly defined and that their conditions take into account the impact that the execution of the warrant has on the collection and the retention of information.
- The decision relates to the retention of certain information that has been legally collected via the execution of warrants, issued by the Court, which authorized the interception of communications.
- CSIS had sought to fully analyze all of the information - both the content and the associated data - for example, email addresses and telephone numbers.
- As is the case for many of our international partners, CSIS has developed data analytic capabilities and expertise to significantly enhance the identification and assessment of threats to the security of Canada over time and space. This includes identifying patterns of movement, communications, behaviours, significant trends, and links that are otherwise unidentifiable.

- When it comes to understanding and predicting the actions of the subjects of our investigations, data analytics has proven to be an effective tool.
- In the ruling released today, the Federal Court recognized the value of the data analytic programme and confirmed the legality of collecting telecommunications associated data pursuant to warrants.
- On the very specific issue of associated data linked to third-party communications, the Court found that it can only be retained if it is related to threats or of use to an investigation, prosecution, national defence or international affairs.
- CSIS, in consultation with the Department of Justice, had interpreted the *CSIS Act* as enabling the retention of this sub-set of associated data to allow for that important analytic work. At no time did the Service believe this to be inconsistent with the *CSIS Act*.
- It is now clear that the Federal Court, on the issue of the retention of certain data, interprets the *Act* differently.
- We accept this decision in full, and have taken immediate actions to respond.
- In response to the decision, CSIS halted all access to, and analysis of, associated data while we undertake a thorough review of the decision in order to assess potential operational and legal impacts, and determine our way forward.
- CSIS takes seriously the concerns expressed by the Court with respect to our duty of candour and recognizes the importance of openness and transparency with the Federal Court.
- CSIS is working closely with the Department of Justice to develop measures aimed at ensuring that we meet our obligations to the Court in matters of transparency and duty of candour.

UNCLASSIFIED  
NON CLASSIFIÉ

## Opening Remarks on Justice Noel's Decision

Comment [DMJ1]: Justice Noel makes it clear in the decision it is his decision alone

### National Press Gallery

### Mot d'ouverture sur la décision rendue en banc par la Cour fédérale

### Tribune de la presse nationale

- **Thank you Andrew. Bonjour Mesdames et Messieurs. Today (or TBD), Justice Noel of the Federal Court issued a decision related to CSIS warrant applications. I am here to explain what this decision means.**
- **I would like to start off by saying, first and foremost, that the Canadian Security Intelligence Service accepts in full the Court's decision, and have taken immediate actions to respond.**
- **I deeply regret the Court's serious concerns with respect to our duty of candour and I commit to continuing my efforts, with the Deputy Minister of Justice, to fully address this concern.**
- **CSIS recognizes the importance of openness and transparency with the Federal Court, and we are working closely with the Department of Justice to develop measures aimed at ensuring that**

UNCLASSIFIED  
NON CLASSIFIÉ

**we meet our obligations to the Court in matters of transparency and duty of candour.**

- **Given the Court's decision with respect to third-party data, CSIS has halted all access to, and analysis of, associated data while we undertake a thorough review of the decision in order to assess potential operational and legal impacts, and determine our way forward.**
- **Let me be clear: all associated data collected under warrant was done so legally. The Court's key concern related to our retention of non-threat related associated data linked with third party communications, after it was collected.**
- **CSIS, in consultation with the Department of Justice, interpreted the CSIS Act to allow for the retention of this sub-set of associated data.**
- **It is now clear that the Federal Court disagrees with this interpretation; a decision which we fully accept.**

UNCLASSIFIED  
NON CLASSIFIÉ



- **The Court rightly acknowledged the age of the *CSIS Act* and that it may not be keeping pace with changing technology and the current threat environment, contributing to this challenge.**
- **That said, again, we fully accept the decision of the Court.**
- **As Canada's national intelligence agency, CSIS investigates activities which may, on reasonable grounds, be suspected of posing a threat to the security of Canada.**
- **One of the ways we investigate these threats is through warrants issued by the Federal Court which authorize the interception of communications. This includes analysis of all of the information - both the content and the associated data.**
- **Associated data includes information such as: email addresses and telephone numbers but never the content.**

UNCLASSIFIED  
NON CLASSIFIÉ

- **It is useful in identifying patterns of movement, communications, behaviours, significant trends, and links that are otherwise unidentifiable.**
- **As is the case for many of our international partners, CSIS has developed data analytic capabilities and expertise to analyze associated data and enhance its capacity to identify and assess threats to the security of Canada over time.**
- **When it comes to understanding and predicting the actions of the subjects of our investigations, data analytics has proven to be an effective tool.**
- **In the ruling released today the Federal Court recognized the value of the data analytic programme and confirmed the legality of collecting telecommunications associated data pursuant to warrants.**
- **I would add that, like the threats we face today, technologies and associated privacy implications have also evolved.**
- **The retention and analysis of information is a significant public policy issue, not just in Canada, but also among our closest allies.**

UNCLASSIFIED  
NON CLASSIFIÉ

- **I would like to say, that the trust of Canadians is fundamental to our ability to deliver on our mandate.**
- **Because the nature of our business is principally secret, Canadians are largely unaware of the professionalism and outstanding dedication the men and women of CSIS show every day as they carry out intelligence work. As the Director of CSIS, I am extremely proud of the people with whom I work. Canadians, too, should be proud of those who work tirelessly to keep this great country safe.**
- **We appreciate the confidence the government invests in CSIS, and it remains for us a privilege to protect Canadians and Canada's interest at home and abroad.**
- **The ongoing national security consultations represent an important opportunity to ensure that CSIS is meeting the dual objectives of security and privacy, and has the tools and authorities, with appropriate oversight, to meet both.**

# STATEMENT

## *CSIS Director statement regarding decision of the Federal Court*

Ottawa, xxxxday, [REDACTED] - The Director of the Canadian Security Intelligence Service (CSIS), Michel Coulombe, issued the following statement regarding the decision issued today by the Honourable Justice Noël of the Federal Court:

“The Federal Court has recently ruled on the retention of associated data linked to third party information. CSIS accepts in full the Court’s decision, and has taken immediate actions to respond. Given the Court’s decision with respect to third-party data, CSIS has halted all access to, and analysis of, associated data while we undertake a thorough review of the decision in order to assess potential operational and legal impacts, and determine our way forward.

[REDACTED] and I commit to continuing my efforts, with the Deputy Minister of Justice, [REDACTED] address this concern. Let me be clear: all associated data collected under warrant was done so legally. The Court’s key concern related to our retention of non-threat related associated data linked with third party communications, after it was collected.

CSIS, in consultation with the Department of Justice, had interpreted the *CSIS Act* to allow for the retention of this sub-set of associated data. It is now clear that the Federal Court disagrees with this interpretation; a decision which we fully accept. [REDACTED]

As is the case for many of our international partners, CSIS has developed data analytic capabilities and expertise to analyze associated data and enhance its capacity to identify and assess threats to the security of Canada over time. When it comes to understanding and predicting the actions of the subjects of our investigations, data analytics has proven to be an effective tool. In the ruling released today, the Federal Court recognized the value of the data analytic programme and [REDACTED] of collecting telecommunications associated data pursuant to warrants. The Court also rightly acknowledged the age of the *CSIS Act* and that it may not be keeping pace with changing technology and the current threat environment.

The ongoing national security consultations represent an important opportunity to ensure that CSIS is meeting the dual objectives of security and privacy, and has the tools and authorities, with appropriate oversight, to meet both.

Because the nature of our business is principally secret, Canadians are largely unaware of the professionalism and outstanding dedication the men and women of CSIS show every day as they carry out intelligence work. As the Director of CSIS, I am extremely proud of the people with whom I work. Canadians, too, should be proud of those who work tirelessly to keep this great country safe.

We appreciate the confidence the government has in CSIS, and it remains for us a privilege to protect Canadians and Canada's interests at home and abroad.”

-30-

**Information:**  
Media Relations  
Canadian Security Intelligence Service  
[media-medias@smtp.gc.ca](mailto:media-medias@smtp.gc.ca)  
613-231-0100

**Pages 365 to / à 376  
are withheld pursuant to section  
sont retenues en vertu de l'article**

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

**Sayarh, Omar (PS/SP)**

---

**From:** Khouri, Lisa (PS/SP)  
**Sent:** Friday, October 21, 2016 5:19 PM  
**To:** Grenier, Julie (PS/SP); Magee, Heather (PS/SP)  
**Subject:** PS-SP-#1995596-v1-QsAs\_-\_En\_Banc\_Associated\_Data  
**Attachments:** PS-SP-#1995596-v1-QsAs\_-\_En\_Banc\_Associated\_Data.doc

Julie/heather,

Please see slight revision to Q3.

Lisa



---

# Questions and Answers

---

## FEDERAL COURT DECISION CSIS' Authority to Retain Metadata Collected Through Warrants

### 1. Would the National Security and Intelligence Committee of Parliamentarians have been able to detect the issue raised by the Federal Court?

While it is speculative to say whether the proposed committee would have explored this issue or not, its mandate and scope would have enabled access to the information pertinent to this case.

The proposed committee would have the authority to review any department or agency of the Government of Canada that performs national security or intelligence activities, including their ongoing operations.

### 2. [For Minister] Does the Minister still have confidence in CSIS?

CSIS plays a vital role in keeping Canadians safe by investigating threats, and collecting and analyzing information to protect our national security. I continue to have confidence in their ability to deliver on that mandate.

### 3. Will this decision impact or influence the issue of Basic Subscriber Information / Lawful Access?

~~The Federal Court's concern in relation to the retention of associated data by CSIS does not extend to Basic Subscriber Information~~

"The Federal Court's concern does not extend to the issue of the provision of Basic Subscriber Information to law enforcement and intelligence agencies."

Basic Subscriber Information is one of the 10 topics the Government has selected for its public consultation on national security.

The input that the Government receives from Canadians, including experts, stakeholders, and Parliamentarians, will help inform the development of national security law and policies. The security and privacy of Canadians are both crucial considerations for BSI.

All Canadians are welcome to participate in the online consultation from now until December 1st, 2016, at: [Canada.ca/national-security-consultation](http://Canada.ca/national-security-consultation)

### 4. Does this decision represent a failure from SIRC in its oversight role?

SIRC reviewed CSIS' use of associated data and published its findings on the issue in its 2014-15 annual report. SIRC did not conclude that the retention of associated data was illegal. The Federal Court arrived at a different conclusion. Upon review, the Government accepts the Federal Court's findings.



SIRC continues to play a very critical role in keeping CSIS accountable through in-depth reviews of its activities. The Minister of Public Safety has asked SIRC to monitor CSIS's compliance with the Federal Court decision.

**5. Can you expand on what the Minister is asking SIRC to do in relation to reviewing CSIS's compliance with the decision?**

SIRC has a unique mandate in keeping CSIS accountable through in-depth reviews of its activities. The findings of its reviews are made available to all Canadians through SIRC's annual reports. These reports are extremely valuable in ensuring that CSIS is operating consistently with Canadian law and values.

Section 54 (2) of the *CSIS Act* provides the Minister of Public Safety with the authority to request a special report from SIRC concerning any matter that relates to the performance of its duties and functions. These special reports are only requested in exceptional circumstances, and do not form part of SIRC's regular review plans for a given year.

The Minister of Public Safety is using this authority to request that the SIRC monitor CSIS' compliance with the Federal Court decision in the matter of "associated data" retention.

SIRC will report its findings directly to the Minister through a classified document. A summary of the findings will be included in SIRC's Annual Report to Parliament, which is available to all Canadians.

**Prepared by:** Julie Grenier

**Consulted:**

NS Intelligence  
CSIS Comms (FYI)  
DoJ Comms (FYI)

**Approved by:**

John Davies, DG, NS Policy (approved)  
Monik Beauregard, ADM, NCSB (pending)  
Heather Magee, Director, Communications (pending)  
Jamie Tomlinson, DG, Communications (pending)  
MO (pending)  
PCO (pending)

## Sayarh, Omar (PS/SP)

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Thursday, October 20, 2016 5:38 PM  
**To:** Magee, Heather (PS/SP)  
**Subject:** Issue Statement - CSIS Check  
**Attachments:** PS-SP-#1995114-v1F-Key\_Messages\_-\_En\_Banc\_Associated\_Data.doc

**Importance:** High

Hi Heather,

Policy has provided an issue statement to include in the key messages for the En Banc decision.

John D's explicit instructions were to run this by CSIS Comms before going to PCO. Could you run this urgently through [REDACTED]?

**Issue:** The Federal Court is anticipated to release its decision regarding the CSIS Act and CSIS' authority to retain certain metadata ("associated data") collected through Federal Court issued warrants in the near future. The Federal Court found that CSIS' retention of associated data linked to third party communications found to be unrelated to threats to the security of Canada is illegal. The Federal Court also found that CSIS breached its duty of candour by failing to fully and transparently inform the Court of its retention program and the establishment of the Operational Data Analysis Centre (ODAC).

Julie Grenier  
Senior Communications Advisor / Conseillère principale de communications  
Portfolio Affairs and Communications Branch/  
Secteur des affaires du portefeuille et des communications  
Public Safety Canada / Sécurité publique du Canada  
Tel : 613-993-4415 | BB : 613-410-6059

**Pages 381 to / à 382**

**are duplicates**

**sont des duplicatas**

## Sayarh, Omar (PS/SP)

---

**From:** Magee, Heather (PS/SP)  
**Sent:** Friday, October 21, 2016 5:32 PM  
**To:** Ministerial Liaison / Liaison ministérielle (PS/SP); Brien, Dan (PS/SP); Bardsley, Scott (PS/SP); Peirce, Hilary (PS/SP)  
**Cc:** Tomlinson, Jamie (PS/SP); Baker3, Ryan (PS/SP); Grenier, Julie (PS/SP); Wilson, Ashleigh (PS/SP); Miller, Kevin (PS/SP); De Curtis, Laura (PS/SP)  
**Subject:** RE: For MO Approval: "En Banc" Ministerial Statement and Speaking Notes  
**Attachments:** PS-SP-#1995596-2-Qs&As - En Banc Associated Data.DOC

In addition to what was sent earlier, attached are Qs and As to support the Minister. These are in addition to the Qs and As prepared by CSIS.

Have a good weekend!

Heather Magee  
Telephone | Téléphone : 613-949-6191  
Mobile | Cellulaire : 613-302-3752

---

**From:** Ministerial Liaison / Liaison ministérielle (PS/SP)  
**Sent:** Friday, October 21, 2016 4:00 PM  
**To:** Brien, Dan (PS/SP); Bardsley, Scott (PS/SP); Peirce, Hilary (PS/SP)  
**Cc:** Tomlinson, Jamie (PS/SP); Magee, Heather (PS/SP); Baker3, Ryan (PS/SP); Grenier, Julie (PS/SP); Wilson, Ashleigh (PS/SP); Miller, Kevin (PS/SP); De Curtis, Laura (PS/SP); Ministerial Liaison / Liaison ministérielle (PS/SP)  
**Subject:** FW: For MO Approval: "En Banc" Ministerial Statement and Speaking Notes  
**Importance:** High

Dan, Scott, Hilary,

Attached for your approval is an updated Ministerial Statement reflecting your edits, as well as proposed Speaking Notes drawing from the statement that could be used for a scrum.

For the statement, a few very small tweaks were applied after a fact check with DoJ, CSIS and PS Policy. (We have provided these in tracked changes for your reference, as well)

- 1) In the first line, Justice Noel makes it clear in the decision it is his decision alone. As such, "en banc" has been removed.
- 2) In the third paragraph, "and" was replaced with "or".
- 3) "Perusing" was corrected to "pursuing"
- 4) We fixed the grammatical error in the last sentence, reversing "find" and "not"

Please track any changes and reply all.

**Ashleigh Wilson**  
Communications Manager | Gestionnaire de communications  
Ministerial Services | Services ministériels  
Public Safety Canada | Sécurité publique Canada  
Telephone | Téléphone : 613-990-2603  
Mobile | Cellulaire : 343-998-3994  
E-mail | Courriel: [ashleigh.wilson@canada.ca](mailto:ashleigh.wilson@canada.ca)

---

**From:** Ministerial Liaison / Liaison ministerielle (PS/SP)

**Sent:** Thursday, October 20, 2016 10:36 AM

**Cc:** Tomlinson, Jamie (PS/SP); Magee, Heather (PS/SP); Baker3, Ryan (PS/SP); Grenier, Julie (PS/SP); Wilson, Ashleigh (PS/SP); Miller, Kevin (PS/SP); De Curtis, Laura (PS/SP); Ministerial Liaison / Liaison ministerielle (PS/SP)

**Subject:** For Approval: "En Banc" Key Messages and Talking Point

Dan, Scott, Hilary,

CSIS has provided a small but important change to the third bullet in the Key Messages. (Noted below in bold and underlined)

- CSIS is taking immediate action to address the Federal Court's findings. CSIS halted **all access to and** analysis of **the** associated data as it actively works to assess and address the Federal Court's decision.

We have updated in the attached. Please use this version for your approvals.

Please track any changes and reply all.

Thanks,  
Lucie

---

**From:** Baker3, Ryan (PS/SP)

**Sent:** Wednesday, October 19, 2016 6:12 PM

**To:** Brien, Dan (PS/SP); Bardsley, Scott (PS/SP); Peirce, Hilary (PS/SP)

**Cc:** Tomlinson, Jamie (PS/SP); Magee, Heather (PS/SP); Grenier, Julie (PS/SP); Wilson, Ashleigh (PS/SP); Ministerial Liaison / Liaison ministerielle (PS/SP); Miller, Kevin (PS/SP); De Curtis, Laura (PS/SP)

**Subject:** For approval: "En Banc" Key Messages and Talking Point

Dan, Scott, Hilary,

Attached for your approval are the proposed Key Messages and a Talking Point for the "En Banc" Federal Court decision pertaining to CSIS' retention of associated data.



Please track any changes and reply all.

Thanks,

Ryan



---

# *Questions and Answers*

---

## **FEDERAL COURT DECISION CSIS' Authority to Retain Metadata Collected Through Warrants**

### **1. Would the National Security and Intelligence Committee of Parliamentarians have been able to detect the issue raised by the Federal Court?**

While it is speculative to say whether the proposed committee would have explored this issue or not, its mandate and scope would have enabled access to the information pertinent to this case.

The proposed committee would have the authority to review any department or agency of the Government of Canada that performs national security or intelligence activities, including their ongoing operations.

### **2. [For Minister] Does the Minister still have confidence in CSIS?**

CSIS plays a vital role in keeping Canadians safe by investigating threats, and collecting and analyzing information to protect our national security. I continue to have confidence in their ability to deliver on that mandate.

### **3. Will this decision impact or influence the issue of Basic Subscriber Information / Lawful Access?**

The Federal Court's concern does not extend to the issue of the provision of Basic Subscriber Information to law enforcement and intelligence agencies.

Basic Subscriber Information is one of the 10 topics the Government has selected for its public consultation on national security. The input the Government receives from Canadians, including experts, stakeholders, and Parliamentarians, will help inform the development of national security law and policies.

The security and privacy of Canadians are both crucial considerations for BSI.

All Canadians are welcome to participate in the online consultation from now until December 1st, 2016, at: [Canada.ca/national-security-consultation](http://Canada.ca/national-security-consultation)

### **4. Does this decision represent a failure from SIRC in its oversight role?**

SIRC reviewed CSIS' use of associated data and published its findings on the issue in its 2014-15 annual report. SIRC did not conclude that the retention of associated data was illegal. The Federal Court arrived at a different conclusion. Upon review, the Government accepts the Federal Court's findings.



SIRC continues to play a very critical role in keeping CSIS accountable through in-depth reviews of its activities. The Minister of Public Safety has asked SIRC to monitor CSIS's compliance with the Federal Court decision.

**5. Can you expand on what the Minister is asking SIRC to do in relation to reviewing CSIS's compliance with the decision?**

SIRC has a unique mandate in keeping CSIS accountable through in-depth reviews of its activities. The findings of its reviews are made available to all Canadians through SIRC's annual reports. These reports are extremely valuable in ensuring that CSIS is operating consistently with Canadian law and values.

Section 54 (2) of the *CSIS Act* provides the Minister of Public Safety with the authority to request a special report from SIRC concerning any matter that relates to the performance of its duties and functions. These special reports are only requested in exceptional circumstances, and do not form part of SIRC's regular review plans for a given year.

The Minister of Public Safety is using this authority to request that the SIRC monitor CSIS' compliance with the Federal Court decision in the matter of "associated data" retention.

SIRC will report its findings directly to the Minister through a classified document. A summary of the findings will be included in SIRC's Annual Report to Parliament, which is available to all Canadians.

**Prepared by:** Julie Grenier

**Consulted:**

NS Intelligence  
CSIS Comms (FYI)  
DoJ Comms (FYI)

**Approved by:**

John Davies, DG, NS Policy (approved)  
Monik Beauregard, ADM, NCSB (approved)  
Heather Magee, Director, Communications (approved)  
MO (pending)  
PCO (pending)

## Sayarh, Omar (PS/SP)

---

**From:** Brien, Dan (PS/SP)  
**Sent:** Friday, October 21, 2016 4:52 PM  
**To:** Ministerial Liaison / Liaison ministerielle (PS/SP); Bardsley, Scott (PS/SP); Peirce, Hilary (PS/SP)  
**Cc:** Tomlinson, Jamie (PS/SP); Magee, Heather (PS/SP); Baker3, Ryan (PS/SP); Grenier, Julie (PS/SP); Wilson, Ashleigh (PS/SP); Miller, Kevin (PS/SP); De Curtis, Laura (PS/SP)  
**Subject:** RE: For MO Approval: "En Banc" Ministerial Statement and Speaking Notes

Thanks – will review.

---

**From:** Ministerial Liaison / Liaison ministerielle (PS/SP)  
**Sent:** Friday, October 21, 2016 4:00 PM  
**To:** Brien, Dan (PS/SP); Bardsley, Scott (PS/SP); Peirce, Hilary (PS/SP)  
**Cc:** Tomlinson, Jamie (PS/SP); Magee, Heather (PS/SP); Baker3, Ryan (PS/SP); Grenier, Julie (PS/SP); Wilson, Ashleigh (PS/SP); Miller, Kevin (PS/SP); De Curtis, Laura (PS/SP); Ministerial Liaison / Liaison ministerielle (PS/SP)  
**Subject:** FW: For MO Approval: "En Banc" Ministerial Statement and Speaking Notes  
**Importance:** High

Dan, Scott, Hilary,

Attached for your approval is an updated Ministerial Statement reflecting your edits, as well as proposed Speaking Notes drawing from the statement that could be used for a scrum.

For the statement, a few very small tweaks were applied after a fact check with DoJ, CSIS and PS Policy. (We have provided these in tracked changes for your reference, as well)

- 1) In the first line, Justice Noel makes it clear in the decision it is his decision alone. As such, "en banc" has been removed.
- 2) In the third paragraph, "and" was replaced with "or".
- 3) "Perusing" was corrected to "pursuing"
- 4) We fixed the grammatical error in the last sentence, reversing "find" and "not"

Please track any changes and reply all.

### Ashleigh Wilson

Communications Manager | Gestionnaire de communications  
Ministerial Services | Services ministériels  
Public Safety Canada | Sécurité publique Canada  
Telephone | Téléphone : 613-990-2603  
Mobile | Cellulaire : 343-998-3994  
E-mail | Courriel: [ashleigh.wilson@canada.ca](mailto:ashleigh.wilson@canada.ca)

---

**From:** Ministerial Liaison / Liaison ministerielle (PS/SP)  
**Sent:** Thursday, October 20, 2016 10:36 AM  
**Cc:** Tomlinson, Jamie (PS/SP); Magee, Heather (PS/SP); Baker3, Ryan (PS/SP); Grenier, Julie (PS/SP); Wilson, Ashleigh (PS/SP); Miller, Kevin (PS/SP); De Curtis, Laura (PS/SP); Ministerial Liaison / Liaison ministerielle (PS/SP)  
**Subject:** For Approval: "En Banc" Key Messages and Talking Point

Dan, Scott, Hilary,

CSIS has provided a small but important change to the third bullet in the Key Messages. (Noted below in bold and underlined)

- CSIS is taking immediate action to address the Federal Court's findings. CSIS halted **all access to and** analysis of **the** associated data as it actively works to assess and address the Federal Court's decision.

We have updated in the attached. Please use this version for your approvals.

Please track any changes and reply all.

Thanks,  
Lucie

---

**From:** Baker3, Ryan (PS/SP)  
**Sent:** Wednesday, October 19, 2016 6:12 PM  
**To:** Brien, Dan (PS/SP); Bardsley, Scott (PS/SP); Peirce, Hilary (PS/SP)  
**Cc:** Tomlinson, Jamie (PS/SP); Magee, Heather (PS/SP); Grenier, Julie (PS/SP); Wilson, Ashleigh (PS/SP); Ministerial Liaison / Liaison ministerielle (PS/SP); Miller, Kevin (PS/SP); De Curtis, Laura (PS/SP)  
**Subject:** For approval: "En Banc" Key Messages and Talking Point

Dan, Scott, Hilary,

Attached for your approval are the proposed Key Messages and a Talking Point for the "En Banc" Federal Court decision pertaining to CSIS' retention of associated data.



Please track any changes and reply all.

Thanks,

Ryan

## Sayarh, Omar (PS/SP)

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Friday, October 21, 2016 4:45 PM  
**To:** Magee, Heather (PS/SP)  
**Subject:** Products for Federal Court decision re: CSIS "associated data"  
**Attachments:** PS-SP-#1998418-v1A-Minister\_-\_Statement\_-\_En\_Banc\_Decision\_FRENCH.DOC; PS-SP-#1995596-v1-Qs&As\_-\_En\_Banc\_Associated\_Data.doc; PS-SP-#1997213-v1C-Minister\_-\_Statement\_on\_En\_Banc\_Decision.doc; PS-SP-#1995114-v1F-Key\_Messages\_-\_En\_Banc\_Associated\_Data.doc; PS-SP-#1997111-1-Minister - Federal Court Decision - En Banc.docx

Hi Heather,

Attached are the most up-to-date products to support the Federal Court's decision regarding CSIS's retention of "associated data."

- Key Messages (in MO)
- Statement (in MO) *Note: I've attached the latest French version; translation is being updated to reflect the minor tweaks after the disaster check*
- Speaking Notes (in MO)
- Qs&As (currently pending with Monik)

Julie Grenier  
Senior Communications Advisor / Conseillère principale de communications  
Portfolio Affairs and Communications Branch/  
Secteur des affaires du portefeuille et des communications  
Public Safety Canada / Sécurité publique du Canada  
Tel : 613-993-4415 | BB : 613-410-6059

**Pages 390 to / à 391  
are not relevant  
sont non pertinentes**

**Pages 392 to / à 401  
are duplicates  
sont des duplicatas**

## Sayarh, Omar (PS/SP)

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Friday, October 21, 2016 4:26 PM  
**To:** Tahera MUFTI; Andrew Swift; Gowing, Andrew; 'De Mora, Joe'  
**Subject:** Clean Min Statement, and FYI on Qs&As  
**Attachments:** PS-SP-#1995596-v1-Qs&As\_-\_En\_Banc\_Associated\_Data.doc; PS-SP-#1997213-v1C-Minister\_-\_Statement\_on\_En\_Banc\_Decision.doc

Hi all,

Here's a clean of the statement back in our Minister's Office for approval. Appreciate the fact-check and recommendations. We accepted most of them.

I've also attached, for your information, a small set of Qs&As currently in Policy approvals.

Thanks all!

Julie Grenier  
Senior Communications Advisor / Conseillère principale de communications  
Portfolio Affairs and Communications Branch/  
Secteur des affaires du portefeuille et des communications  
Public Safety Canada / Sécurité publique du Canada  
Tel : 613-993-4415 | BB : 613-410-6059

**Pages 403 to / à 406  
are duplicates  
sont des duplicatas**

## Sayarh, Omar (PS/SP)

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Friday, October 21, 2016 4:20 PM  
**To:** Khouri, Lisa (PS/SP)  
**Subject:** RE: For Urgent Approval: Qs&As - CSIS Associated Data  
**Attachments:** PS-SP-#1995596-v1-Qs&As\_-\_En\_Banc\_Associated\_Data.doc

Hi Lisa,  
Meant to copy you! Is there any chance Monik is in a position to look at this urgently?

Julie G  
Tel : 613-993-4415 | BB : 613-410-6059

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Friday, October 21, 2016 4:06 PM  
**To:** Beaugard, Monik (PS/SP)  
**Cc:** Davies, John (PS/SP); Magee, Heather (PS/SP)  
**Subject:** For Urgent Approval: Qs&As - CSIS Associated Data

Hi Monik,

Apologies for another urgent but the Minister's Office has requested a handful of Qs&As to support the release of the Federal Court decision on CSIS's retention of associated data.

CSIS a robust set of Qs&As. These are supplementary.

If you could review and **approve by 5 p.m.** that would be greatly appreciated as MO would like to have the material ASAP today.

John Davies has approved the attached.

Thanks,  
Julie Grenier  
Senior Communications Advisor / Conseillère principale de communications  
Portfolio Affairs and Communications Branch/  
Secteur des affaires du portefeuille et des communications  
Public Safety Canada / Sécurité publique du Canada  
Tel : 613-993-4415 | BB : 613-410-6059

**Pages 408 to / à 409  
are duplicates  
sont des duplicatas**

**Sayarh, Omar (PS/SP)**

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Friday, October 21, 2016 3:05 PM  
**To:** [REDACTED] (PS/SP); [REDACTED] (PS/SP); Davies, John (PS/SP); Sousa, Michael (PS/SP); Brender, James (PS/SP)  
**Cc:** Magee, Heather (PS/SP)  
**Subject:** URGENT Input & Approval: Qs&As  
**Attachments:** PS-SP-#1995596-v1-Qs&As\_-\_En\_Banc\_Metadata.doc  
**Importance:** High

Hi,

Attached are the Qs with proposed As requested by MO.

**Request to urgently review and approve as MO is looking for this material ASAP today.**

If you can provide DG approval by 4 p.m., I will coordinate Monik's approval.

I have highlighted in grey the sentences that I'm particularly unsure about.

Julie Grenier  
Senior Communications Advisor / Conseillère principale de communications  
Portfolio Affairs and Communications Branch/  
Secteur des affaires du portefeuille et des communications  
Public Safety Canada / Sécurité publique du Canada  
Tel : 613-993-4415 | BB : 613-410-6059



---

# Questions and Answers

---

## FEDERAL COURT "EN BANC" DECISION CSIS' Authority to Retain Metadata Collected Through Warrants

### 1. Would the National Security and Intelligence Committee of Parliamentarians have been able to detect the issue raised by the Federal Court?

While it is speculative to say whether the proposed committee would have explored this issue or not, its mandate and scope would have enabled access to the information pertinent to this case.

The proposed committee would have the authority to review any department or agency of the Government of Canada that performs national security or intelligence activities, including their ongoing operations.

### 2. [For Minister] Does the Minister still have confidence in CSIS?

CSIS plays a vital role in keeping Canadians safe by investigating threats, and collecting and analyzing information to protect our national security. I continue to have confidence in their ability to deliver on that mandate.

### 3. Will this decision impact or influence the issue of Basic Subscriber Information / Lawful Access?

~~The Federal Court's concern in relation to the retention of associated data by CSIS does not extend to Basic Subscriber Information.~~

Basic Subscriber Information is one of the 10 topics the Government has selected for its public consultation on national security.

The input that the Government receives from Canadians, including experts, stakeholders, and Parliamentarians, will help inform the development of national security law and policies. The security and privacy of Canadians are both crucial considerations for BSI.

All Canadians are welcome to participate in the online consultation from now until December 1st, 2016, at: [Canada.ca/national-security-consultation](http://Canada.ca/national-security-consultation)

### 4. Does this decision represent a failure from SIRC in its oversight role?

SIRC reviewed CSIS' use of associated data and published its findings on the issue in its 2014-15 annual report. SIRC did not conclude that the retention of associated data was illegal. ~~The Federal Court arrived at a different conclusion. Upon review, the Government accepts the Federal Court's findings.~~



- 2 -

SIRC continues to play a very critical role in keeping CSIS accountable through in-depth reviews of its activities. The Minister of Public Safety has asked SIRC to monitor CSIS's compliance with the Federal Court decision.

**5. Can you expand on what the Minister is asking SIRC to do in relation to reviewing CSIS's compliance with the decision?**

SIRC has a unique mandate in keeping CSIS accountable through in-depth reviews of its activities. The findings of its reviews are made available to all Canadians through SIRC's annual reports. These reports are extremely valuable in ensuring that CSIS is operating consistently with Canadian law and values.

Section 54 (2) of the *CSIS Act* provides the Minister of Public Safety with the authority to request a special report from SIRC concerning any matter that relates to the performance of its duties and functions. These special reports are only requested in exceptional circumstances, and do not form part of SIRC's regular review plans for a given year.

The Minister of Public Safety is using this authority to request that the SIRC monitor CSIS' compliance with the Federal Court decision in the matter of "associated data" retention.

SIRC will report its findings directly to the Minister through a classified document. A summary of the findings will be included in SIRC's Annual Report to Parliament, which is available to all Canadians.

Prepared by: Julie Grenier

Consulted: NS Intelligence

Approved by:

**Sayarh, Omar (PS/SP)**

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Friday, October 21, 2016 8:10 AM  
**To:** Davies, John (PS/SP); [REDACTED] (PS/SP); [REDACTED] (PS/SP); Sousa, Michael (PS/SP); Brender, James (PS/SP)  
**Subject:** Fw: Products for the En banc decision

FYI

As far as I know, no action from us required on these.

Julie  
Tel: 613-993-4415, BB: 613-410-6059

---

**From:** Tomlinson, Jamie (PS/SP) <[jamie.tomlinson@canada.ca](mailto:jamie.tomlinson@canada.ca)>  
**Sent:** Friday, October 21, 2016 6:47 AM  
**To:** Magee, Heather (PS/SP); Grenier, Julie (PS/SP); Wilson, Ashleigh (PS/SP)  
**Cc:** Nichols, Megan (PS/SP)  
**Subject:** FW: Products for the En banc decision

fyi

---

**From:** De Mora, Joe [<mailto:Joe.DeMora@justice.gc.ca>]  
**Sent:** October-20-16 10:49 PM  
**To:** [REDACTED] 'Fox, Christiane'; O'Nions, Christine; Tomlinson, Jamie (PS/SP); Off, Shirley Anne  
**Cc:** Nofle, Tracie  
**Subject:** Re: Products for the En banc decision

[REDACTED]

Joe

---

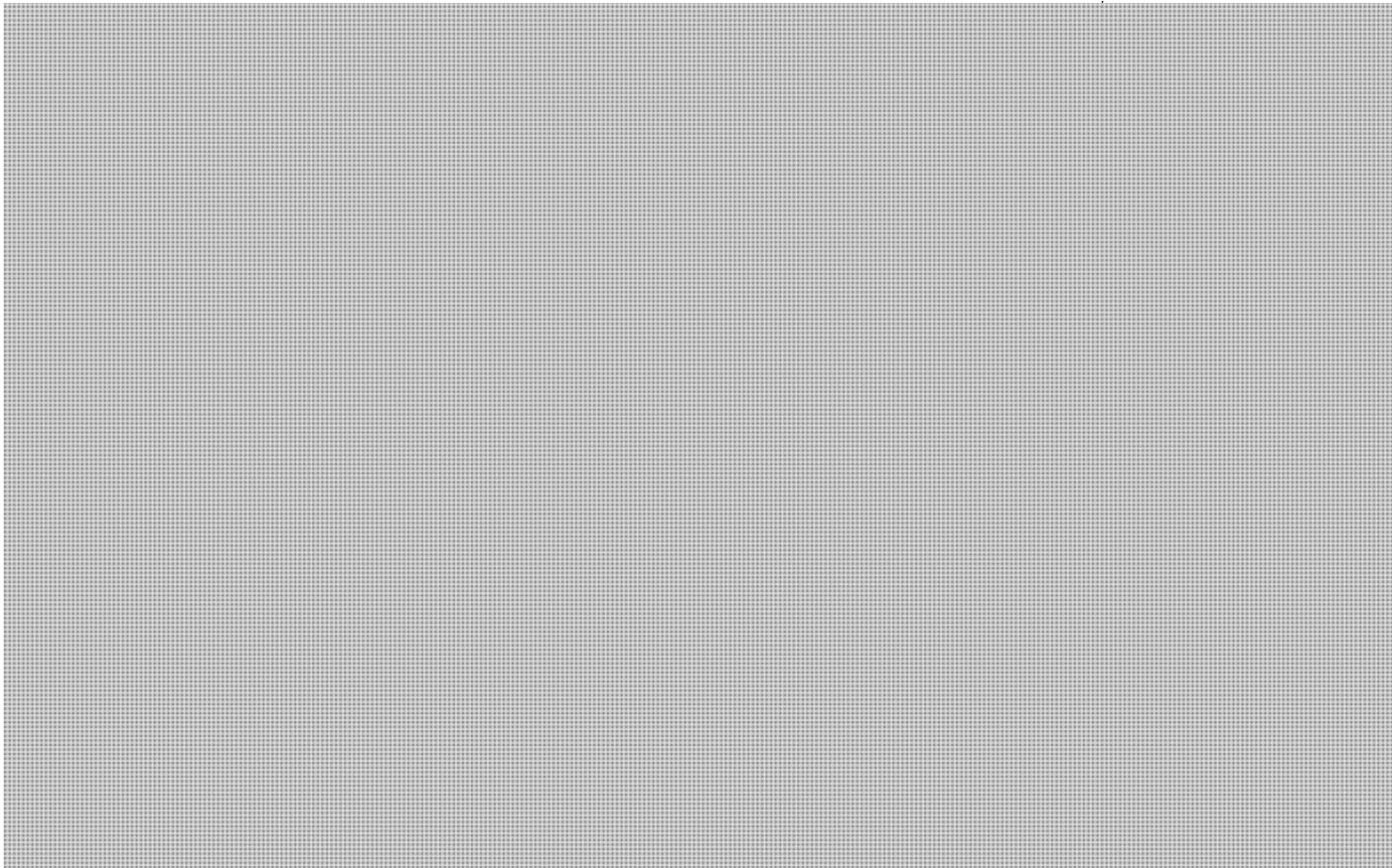
**From:** [REDACTED]  
**Sent:** Thursday, October 20, 2016 10:46 PM  
**To:** 'Fox, Christiane'; O'Nions, Christine; Tomlinson, Jamie (PS/SP); De Mora, Joe; Off, Shirley Anne  
**Cc:** Nofle, Tracie  
**Subject:** RE: Products for the En banc decision

Thanks Chris. [REDACTED]

[REDACTED]

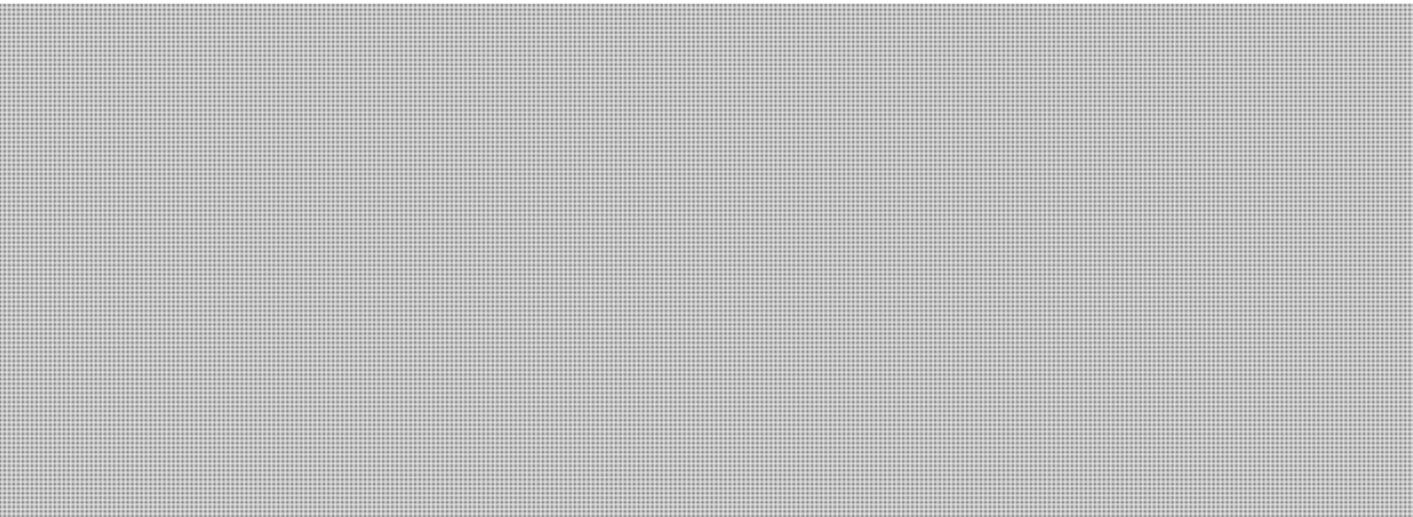
Joe/Shirley Anne, [REDACTED]

[REDACTED]



---

**From:** Fox, Christiane [<mailto:Christiane.Fox@pco-bcp.gc.ca>]  
**Sent:** 20-Oct-16 10:03 PM  
**To:** O'Nions, Christine; [REDACTED] Tomlinson, Jamie (PS/SP); 'De Mora, Joe'; 'ShirleyAnne.Off@justice.gc.ca'  
**Cc:** Nofle, Tracie  
**Subject:** RE: Products for the En banc decision



---

**From:** O'Nions, Christine  
**Sent:** October-20-16 19:06  
**To:** Gwyn, Andrew; Tomlinson, Jamie (PS/SP); 'De Mora, Joe'; 'ShirleyAnne.Off@justice.gc.ca'

**Cc:** Fox, Christiane; Nofle, Tracie

**Subject:** Products for the En banc decision

Here are all the docs for the en banc decision. No changes at this point except to the QA pkg, which is still a work in progress. Pls feel free to call if you have any questions.

Christine  
613 853-1042

## Sayarh, Omar (PS/SP)

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Friday, October 21, 2016 8:07 AM  
**To:** Davies, John (PS/SP); [REDACTED] (PS/SP); [REDACTED] (PS/SP)  
**Cc:** Sousa, Michael (PS/SP); Brender, James (PS/SP)  
**Subject:** Fw: Products for the En banc decision  
**Attachments:** PS-SP-#1995114-v1F-Key\_Messages\_-\_En\_Banc\_Associated\_Data1.doc

**Importance:** High

Good morning.

PCO is asking whether our review of the CSIS Act (in reference to their comment that it may be outdated) is part of the consultation. John D: Can I respond that it's not a specific topic in the Green Paper but as we are examining the whole NS framework, it'll be considered in the consultation?

[REDACTED]

We are still waiting on MO edits to statement.

We've also been advised that DoJ Comms has been tasked with Qs+As. I'll forward the email I received from Joe De Mora.

Julie  
Tel: 613-993-4415, BB: 613-410-6059

---

**From:** Tomlinson, Jamie (PS/SP) <[jamie.tomlinson@canada.ca](mailto:jamie.tomlinson@canada.ca)>  
**Sent:** Friday, October 21, 2016 6:45 AM  
**To:** Magee, Heather (PS/SP); Grenier, Julie (PS/SP); Wilson, Ashleigh (PS/SP)  
**Cc:** Nichols, Megan (PS/SP)  
**Subject:** FW: Products for the En banc decision

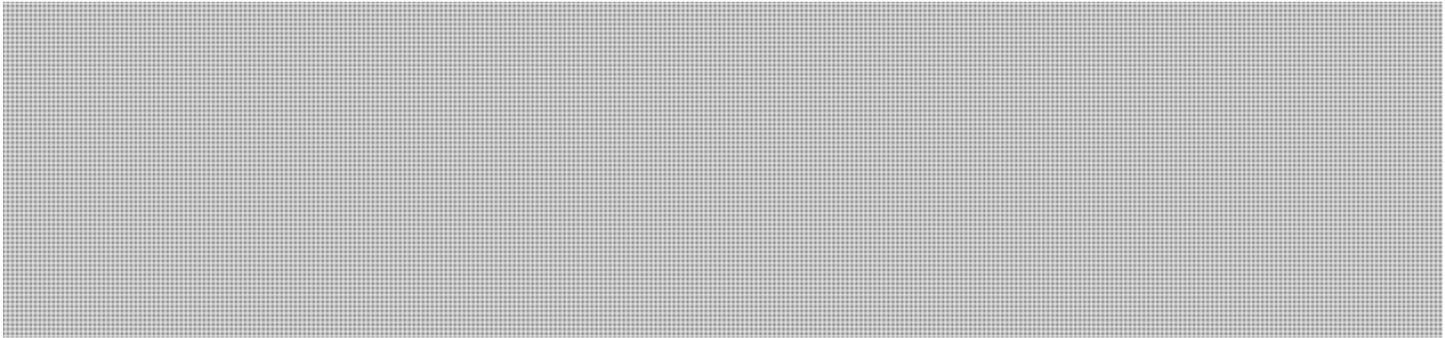
Fyi from PCO.

Please note, in the 6<sup>th</sup> bullet there is a question about the Green Paper.

---

**From:** Fox, Christiane [<mailto:Christiane.Fox@pco-bcp.gc.ca>]  
**Sent:** October-20-16 10:03 PM  
**To:** O'Nions, Christine; [REDACTED] Tomlinson, Jamie (PS/SP); 'De Mora, Joe'; 'ShirleyAnne.Off@justice.gc.ca'  
**Cc:** Noftle, Tracie  
**Subject:** RE: Products for the En banc decision

[REDACTED]



---

**From:** O'Nions, Christine  
**Sent:** October-20-16 19:06  
**To:** Gwyn, Andrew; Tomlinson, Jamie (PS/SP); 'De Mora, Joe'; 'ShirleyAnne.Off@justice.gc.ca'  
**Cc:** Fox, Christiane; Nofle, Tracie  
**Subject:** Products for the En banc decision

Here are all the docs for the en banc decision. No changes at this point except to the QA pkg, which is still a work in progress. Pls feel free to call if you have any questions.

Christine  
613 853-1042



---

# *Media Lines*

---

## **FEDERAL COURT “EN BANC” DECISION CSIS’ Authority to Retain Associated Data Collected Through Warrants**

**Issue:** The Federal Court is anticipated to release, in the near future, its decision regarding the CSIS Act and CSIS’ authority to retain certain metadata [may want to stick w associated data as were court's words] (“associated data”) collected under the authority of Federal Court issued warrants. The Federal Court found that CSIS’ retention of associated data linked to third party communications found to be unrelated to threats to the security of Canada was illegal. While conceded by CSIS, the Federal Court also found that CSIS breached its duty of candour by failing to fully and transparently inform the Court of its retention program and the establishment of the Operational Data Analysis Centre (ODAC).

### **Key Messages:**

- The Government accepts the Federal Court’s findings on this matter.
- It is important to underline that the associated data was collected legally pursuant to court authorized warrants. The Federal Court’s key concern relates to CSIS’ retention of such data (e.g., date, time, and phone numbers related to a call) when the content of the communication is not related to a threat to the security of Canada.
- CSIS is taking immediate action to address the Federal Court’s findings. CSIS halted all access to and analysis of the associated data as it actively works to assess and address the Federal Court’s decision.
- As conceded to, the Government also accepts the Federal Court’s findings regarding CSIS’ duty of candour to the Federal Court. The Government takes this finding very seriously. CSIS has committed to working with the Federal Court to ensure that it is fully transparent with the Court.
- The Federal Court agreed with CSIS’ proposal to update warrants, and generally accepted the changes proposed by CSIS. (need to clarify this process w CSIS ie warrant templates)
- In its decision, the Federal Court noted that the CSIS Act is now more than 30 years old and suggested that changes may need to be made to ensure that it keeps pace with changes in technology and the privacy expectations of Canadians. This is something that we will review: (is this review part of NS review green paper?)
- The Government is committed to keeping Canadians safe while at the same time safeguarding our freedoms, rights and values in an open and democratic society.
- We want to hear from Canadians on how we can best meet our dual objectives of security and rights. We invite all Canadians to provide us with their views and ideas on our national security framework through our online consultation, which is open until December 1<sup>st</sup>. ([www.canada.ca/national-security-consultation](http://www.canada.ca/national-security-consultation)) (mention this has been



ongoing - not triggered by this decision)

- Concurrently, we are taking measures to strengthen national security accountability. In June, we put forward legislation to create a National Security and Intelligence Committee of Parliamentarians which would have a broad mandate to scrutinize the activities of any federal department or agency with national security responsibilities, including operational matters.

**Ministerial Talking Point:**

CSIS plays a vital role in keeping Canadians safe by investigating threats, and collecting and analyzing information to protect our national security. I continue to have confidence in their ability to deliver on that mandate.

**Prepared by:** Julie Grenier

**Consulted:** NS Intelligence, Legal, CSIS Policy, Justice

**Approved by:**

John Davies, DG, NS Policy (approved)  
Monik Beauregard, ADM, NCSB (approved)  
Heather Magee, Director, Communications (approved)  
Jamie Tomlinson, DG, Communications (approved)  
MO (pending)  
PCO (pending)

**Sayarh, Omar (PS/SP)**

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Friday, October 21, 2016 7:11 AM  
**To:** Magee, Heather (PS/SP)  
**Cc:** Wilson, Ashleigh (PS/SP)  
**Subject:** Re: Products for the En banc decision  
**Attachments:** PS-SP-#1995114-v1F-Key\_Messages\_-\_En\_Banc\_Associated\_Data1.doc

Hi Heather,

I'll be in by 845 to make tweaks and respond to Qs.

How are we routing back to PCO? Are we waiting for MO edits and then send back to PCO or responding to PCO while we wait for MO?

Julie

Tel: 613-993-4415, BB: 613-410-6059

---

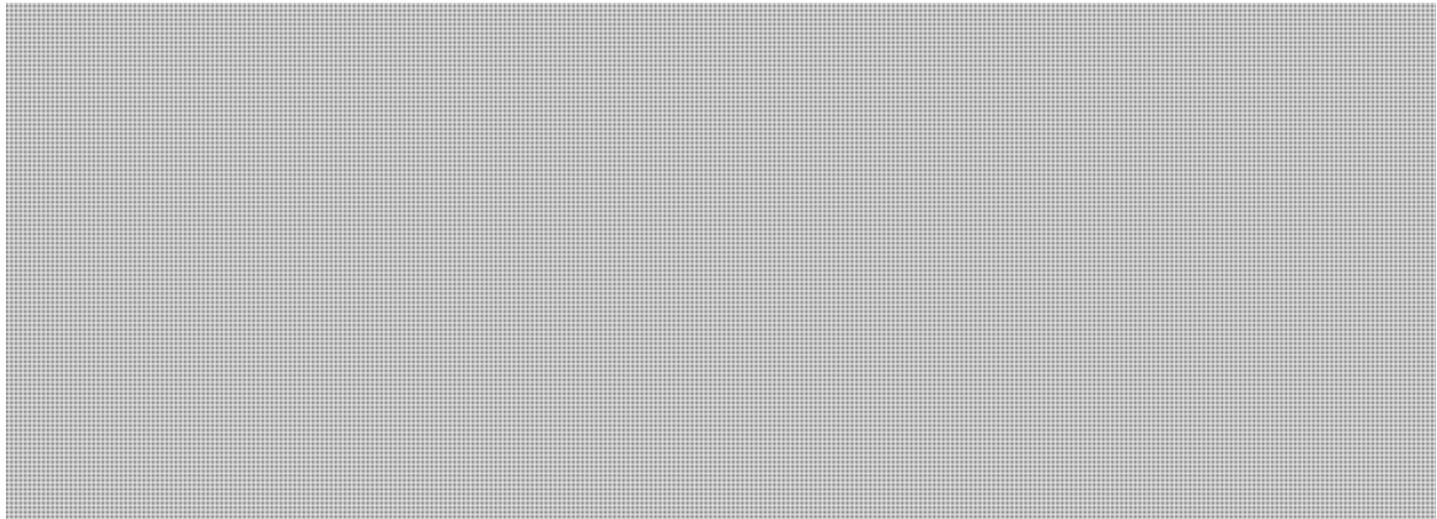
**From:** Tomlinson, Jamie (PS/SP) <[jamie.tomlinson@canada.ca](mailto:jamie.tomlinson@canada.ca)>  
**Sent:** Friday, October 21, 2016 6:45 AM  
**To:** Magee, Heather (PS/SP); Grenier, Julie (PS/SP); Wilson, Ashleigh (PS/SP)  
**Cc:** Nichols, Megan (PS/SP)  
**Subject:** FW: Products for the En banc decision

Fyi from PCO.

Please note, in the 6<sup>th</sup> bullet there is a question about the Green Paper.

---

**From:** Fox, Christiane [<mailto:Christiane.Fox@pco-bcp.gc.ca>]  
**Sent:** October-20-16 10:03 PM  
**To:** O'Nions, Christine; [REDACTED] Tomlinson, Jamie (PS/SP); 'De Mora, Joe'; 'ShirleyAnne.Off@justice.gc.ca'  
**Cc:** Nofle, Tracie  
**Subject:** RE: Products for the En banc decision



---

**From:** O'Nions, Christine  
**Sent:** October-20-16 19:06  
**To:** Gwyn, Andrew; Tomlinson, Jamie (PS/SP); 'De Mora, Joe'; 'ShirleyAnne.Off@justice.gc.ca'  
**Cc:** Fox, Christiane; Noftle, Tracie  
**Subject:** Products for the En banc decision

Here are all the docs for the en banc decision. No changes at this point except to the QA pkg, which is still a work in progress. Pls feel free to call if you have any questions.

Christine  
613 853-1042



---

# Media Lines

---

## FEDERAL COURT “EN BANC” DECISION CSIS’ Authority to Retain Associated Data Collected Through Warrants

**Issue:** The Federal Court is anticipated to release, in the near future, its decision regarding the CSIS Act and CSIS’ authority to retain certain metadata [may want to stick w associated data as were court's words] (“associated data”) collected under the authority of Federal Court issued warrants. The Federal Court found that CSIS’ retention of associated data linked to third party communications found to be unrelated to threats to the security of Canada was illegal. While conceded by CSIS, the Federal Court also found that CSIS breached its duty of candour by failing to fully and transparently inform the Court of its retention program and the establishment of the Operational Data Analysis Centre (ODAC).

### Key Messages:

- The Government accepts the Federal Court’s findings on this matter.
- It is important to underline that the associated data was collected legally pursuant to court authorized warrants. The Federal Court’s key concern relates to CSIS’ retention of such data (e.g., date, time, and phone numbers related to a call) when the content of the communication is not related to a threat to the security of Canada.
- CSIS is taking immediate action to address the Federal Court’s findings. CSIS halted all access to and analysis of the associated data as it actively works to assess and address the Federal Court’s decision.
- As conceded to, the Government also accepts the Federal Court’s findings regarding CSIS’ duty of candour to the Federal Court. The Government takes this finding very seriously. CSIS has committed to working with the Federal Court to ensure that it is fully transparent with the Court.
- The Federal Court agreed with CSIS’ proposal to update warrants, and generally accepted the changes proposed by CSIS. (need to clarify this process w CSIS ie warrant templates)
- In its decision, the Federal Court noted that the CSIS Act is now more than 30 years old and suggested that changes may need to be made to ensure that it keeps pace with changes in technology and the privacy expectations of Canadians. This is something that we will review. (is this review part of NS review green paper?)
- The Government is committed to keeping Canadians safe while at the same time safeguarding our freedoms, rights and values in an open and democratic society.
- We want to hear from Canadians on how we can best meet our dual objectives of security and rights. We invite all Canadians to provide us with their views and ideas on our national security framework through our online consultation, which is open until December 1<sup>st</sup>. ([www.canada.ca/national-security-consultation](http://www.canada.ca/national-security-consultation)) (mention this has been



ongoing - not triggered by this decision)

- Concurrently, we are taking measures to strengthen national security accountability. In June, we put forward legislation to create a National Security and Intelligence Committee of Parliamentarians which would have a broad mandate to scrutinize the activities of any federal department or agency with national security responsibilities, including operational matters.

**Ministerial Talking Point:**

CSIS plays a vital role in keeping Canadians safe by investigating threats, and collecting and analyzing information to protect our national security. I continue to have confidence in their ability to deliver on that mandate.

**Prepared by:** Julie Grenier

**Consulted:** NS Intelligence, Legal, CSIS Policy, Justice

**Approved by:**

John Davies, DG, NS Policy (approved)  
Monik Beauregard, ADM, NCSB (approved)  
Heather Magee, Director, Communications (approved)  
Jamie Tomlinson, DG, Communications (approved)  
MO (pending)  
PCO (pending)

**Sayarh, Omar (PS/SP)**

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Thursday, October 20, 2016 9:37 PM  
**To:** [REDACTED] (PS/SP)  
**Subject:** Re: Qs&As

Ok. Hope "early" isn't too early...  
Could there be a basic or simple answer while we consult on a more elaborate one?  
Appreciate all your work.

Julie  
Tel: 613-993-4415, BB: 613-410-6059

---

**From:** [REDACTED] PS/SP  
**Sent:** Thursday, October 20, 2016 8:57 PM  
**To:** Grenier, Julie (PS/SP); [REDACTED] PS/SP; Davies, John (PS/SP)  
**Cc:** [REDACTED] (PS/SP)  
**Subject:** Re: Qs&As

Julie,

Answering the Lawful Access question will be tricky. We will absolutely need to consult Justice.

I will be in early tomorrow to work on this.

[REDACTED]

Sent from my BlackBerry 10 smartphone on the Rogers network.

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Thursday, October 20, 2016 6:17 PM  
**To:** [REDACTED] PS/SP; [REDACTED] (PS/SP); Davies, John (PS/SP)  
**Subject:** RE: Qs&As

Hi,

My Sr Mgmt was just on a call with PCO and our understanding is that the Court will file their decision at noon tomorrow, and we are preparing to issue our statement shortly after it is made public. We'll update you on the rollout tomorrow as there will be a dry-run at PCO for the CSIS tech brief.

If you could get an answer to us in the morning on the lawful access question, that would be great. At the moment, that's the only one that's not clearly covered in the CSIS Qs&As.

Thanks,  
Julie G  
Tel : 613-993-4415 | BB : 613-410-6059

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Thursday, October 20, 2016 5:53 PM

**To:** [REDACTED] (PS/SP)  
**Cc:** [REDACTED] (PS/SP); Davies, John (PS/SP)  
**Subject:** Qs&As  
**Importance:** High

Hi,

On the matter of Qs&As, as Heather and I cross-reference CSIS' Qs&As against the draft I provided, we feel Questions 3 and 4 are covered, and Question 5 is covered with our Key Messages. I will delete those from the document.

The issue of issue of privacy (our Question 1) is noted in the CSIS Qs&As but not clearly from the perspective of concerns that may arise from Canadians when they learn of this decision. Key question: Would this to be something for us to answer?

If the privacy one is not ours, we're really down to the Q&A around lawful access. Would it be possible to have an answer for that one?

Julie G  
Tel : 613-993-4415 | BB : 613-410-6059

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Thursday, October 20, 2016 5:42 PM  
**To:** [REDACTED] (PS/SP)  
**Cc:** [REDACTED] (PS/SP); Davies, John (PS/SP)  
**Subject:** RE: Help if you can! En Banc

Hi,

Heather will run it past it [REDACTED]

I have also discussed status of Qs&As with her. There is call happening at 5:45 re: Comms. They have asked that we finalize all materials tonight, and there is an expectation that we will have our own Qs&As.

Julie G  
Tel : 613-993-4415 | BB : 613-410-6059

---

**From:** [REDACTED] (PS/SP)  
**Sent:** Thursday, October 20, 2016 5:31 PM  
**To:** Grenier, Julie (PS/SP)  
**Cc:** [REDACTED] (PS/SP); Davies, John (PS/SP)  
**Subject:** RE: Help if you can! En Banc

Julie,

John D's explicit instructions were to run this by CSIS Comms before going to PCO. Are you able to do this?

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Thursday, October 20, 2016 5:29 PM  
**To:** [REDACTED] (PS/SP)  
**Cc:** [REDACTED] (PS/SP)  
**Subject:** RE: Help if you can! En Banc

Thank you [REDACTED]

Understanding that this is drawing from approved material and it's been reviewed by John, just want to confirm that this up to PCO as an "issue statement" at the top of the Key Messages document.

Julie G

Tel : 613-993-4415 | BB : 613-410-6059

---

**From:** [REDACTED] (PS/SP)  
**Sent:** Thursday, October 20, 2016 5:25 PM  
**To:** Grenier, Julie (PS/SP)  
**Cc:** [REDACTED] (PS/SP)  
**Subject:** RE: Help if you can! En Banc

Here you go (see below)

Please run this by CSIS Comms before giving this to PCO.

Of note, the last two sentences are drawn from CSIS' Qs and As.

[REDACTED]

\*\*\*\*\*

"On (X Date), the Federal Court released a decision regarding the CSIS Act and CSIS' authority to retain certain metadata ("associated data") collected through Federal Court issued warrants. The Federal Court found that CSIS' retention of associated data linked to third party communications found to be unrelated to threats to the security of Canada is illegal. The Federal Court also found that CSIS breached its duty of candour by failing to fully and transparently inform the Court of its retention program and the establishment of the Operational Data Analysis Centre (ODAC)."

---

**From:** [REDACTED] (PS/SP)  
**Sent:** Thursday, October 20, 2016 5:14 PM  
**To:** Grenier, Julie (PS/SP)  
**Subject:** RE: Help if you can! En Banc

I've drafted something – just waiting for John D's approval.

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Thursday, October 20, 2016 5:13 PM  
**To:** [REDACTED] (PS/SP)  
**Subject:** RE: Help if you can! En Banc

Thanks [REDACTED] Beggars can't be choosers, but any chance you could get this to me by 5:30?

Julie G

Tel : 613-993-4415 | BB : 613-410-6059

---

**From:** [REDACTED] (PS/SP)  
**Sent:** Thursday, October 20, 2016 4:56 PM  
**To:** Grenier, Julie (PS/SP)  
**Subject:** RE: Help if you can! En Banc

Stand by.

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Thursday, October 20, 2016 4:52 PM  
**To:** [REDACTED] (PS/SP); [REDACTED] (PS/SP)  
**Subject:** Help if you can! En Banc  
**Importance:** High

Do you have a one-paragraph summary of the decision that we could use as an "issue statement" at the top of key messages? PCO has asked us to include it.

Julie Grenier  
Senior Communications Advisor / Conseillère principale de communications  
Portfolio Affairs and Communications Branch/  
Secteur des affaires du portefeuille et des communications  
Public Safety Canada / Sécurité publique du Canada  
Tel : 613-993-4415 | BB : 613-410-6059

## Sayarh, Omar (PS/SP)

---

**From:** [REDACTED] PS/SP  
**Sent:** Thursday, October 20, 2016 5:50 PM  
**To:** Grenier, Julie (PS/SP)  
**Cc:** [REDACTED] PS/SP); Davies, John (PS/SP)  
**Subject:** RE: Help if you can! En Banc

Julie,

I've spoken with John D and [REDACTED]. Both are of the view that the CSIS Qs and As are sufficient for the moment and that, subject to further discussion with [REDACTED], we may provide additional Qs and As tomorrow.

Of note, we have prepared a QP note on this. We will circulate this to Parl Affairs tomorrow once John D has reviewed and approved.

Let me know if this poses problems,

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Thursday, October 20, 2016 5:42 PM  
**To:** [REDACTED] PS/SP  
**Cc:** [REDACTED] (PS/SP); Davies, John (PS/SP)  
**Subject:** RE: Help if you can! En Banc

Hi,

Heather will run it past it [REDACTED]

I have also discussed status of Qs&As with her. There is call happening at 5:45 re: Comms. They have asked that we finalize all materials tonight, and there is an expectation that we will have our own Qs&As.

Julie G  
Tel : 613-993-4415 | BB : 613-410-6059

---

**From:** [REDACTED] (PS/SP)  
**Sent:** Thursday, October 20, 2016 5:31 PM  
**To:** Grenier, Julie (PS/SP)  
**Cc:** [REDACTED] (PS/SP); Davies, John (PS/SP)  
**Subject:** RE: Help if you can! En Banc

Julie,

John D's explicit instructions were to run this by CSIS Comms before going to PCO. Are you able to do this?

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Thursday, October 20, 2016 5:29 PM  
**To:** [REDACTED] (PS/SP)

**Cc:** [REDACTED] (PS/SP)  
**Subject:** RE: Help if you can! En Banc

Thank you [REDACTED]  
Understanding that this is drawing from approved material and it's been reviewed by John, just want to confirm that this up to PCO as an "issue statement" at the top of the Key Messages document.

Julie G  
Tel : 613-993-4415 | BB : 613-410-6059

---

**From:** [REDACTED] (PS/SP)  
**Sent:** Thursday, October 20, 2016 5:25 PM  
**To:** Grenier, Julie (PS/SP)  
**Cc:** [REDACTED] (PS/SP)  
**Subject:** RE: Help if you can! En Banc

Here you go (see below)

Please run this by CSIS Comms before giving this to PCO.

Of note, the last two sentences are drawn from CSIS' Qs and As.

[REDACTED]

\*\*\*\*\*

"On (X Date), the Federal Court released a decision regarding the CSIS Act and CSIS' authority to retain certain metadata ("associated data") collected through Federal Court issued warrants. The Federal Court found that CSIS' retention of associated data linked to third party communications found to be unrelated to threats to the security of Canada is illegal. The Federal Court also found that CSIS breached its duty of candour by failing to fully and transparently inform the Court of its retention program and the establishment of the Operational Data Analysis Centre (ODAC)."

---

**From:** [REDACTED] (PS/SP)  
**Sent:** Thursday, October 20, 2016 5:14 PM  
**To:** Grenier, Julie (PS/SP)  
**Subject:** RE: Help if you can! En Banc

I've drafted something – just waiting for John D's approval.

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Thursday, October 20, 2016 5:13 PM  
**To:** [REDACTED] (PS/SP)  
**Subject:** RE: Help if you can! En Banc

Thanks [REDACTED] Beggars can't be choosers, but any chance you could get this to me by 5:30?

Julie G  
Tel : 613-993-4415 | BB : 613-410-6059

---

**From:** [REDACTED] (PS/SP)  
**Sent:** Thursday, October 20, 2016 4:56 PM  
**To:** Grenier, Julie (PS/SP)  
**Subject:** RE: Help if you can! En Banc

Stand by.

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Thursday, October 20, 2016 4:52 PM  
**To:** [REDACTED] (PS/SP); [REDACTED] PS/SP)  
**Subject:** Help if you can! En Banc  
**Importance:** High

Do you have a one-paragraph summary of the decision that we could use as an "issue statement" at the top of key messages? PCO has asked us to include it.

Julie Grenier  
Senior Communications Advisor / Conseillère principale de communications  
Portfolio Affairs and Communications Branch/  
Secteur des affaires du portefeuille et des communications  
Public Safety Canada / Sécurité publique du Canada  
Tel : 613-993-4415 | BB : 613-410-6059

**Sayarh, Omar (PS/SP)**

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Thursday, October 20, 2016 1:48 PM  
**To:** PS.F TranslationComms-TraductionComms F.SP  
**Subject:** For Translation: Key Messages - 350 words - by 9 a.m.  
**Attachments:** PS-SP-#1995114-v1F-Key\_Messages\_-\_En\_Banc\_Associated\_Data.doc

Hello,

Request to translate the attached key messages – approximately 350 words - by 9 a.m. tomorrow.

Thanks in advance,

Julie Grenier  
Senior Communications Advisor / Conseillère principale de communications  
Portfolio Affairs and Communications Branch/  
Secteur des affaires du portefeuille et des communications  
Public Safety Canada / Sécurité publique du Canada  
Tel : 613-993-4415 | BB : 613-410-6059



---

# *Media Lines*

---

## **FEDERAL COURT “EN BANC” DECISION CSIS’ Authority to Retain Metadata Collected Through Warrants**

### **Key Messages:**

- The Government accepts the Federal Court’s findings on this matter.
- It is important to underline that the associated data was collected legally through warrants. The Federal Court’s key concern relates to CSIS’ retention of such data (e.g., date, time, and phone numbers related to a call) when it is not related to a threat to the security of Canada.
- CSIS is taking immediate action to address the Federal Court’s findings. CSIS halted all access to and analysis of the associated data as it actively works to assess and address the Federal Court’s decision.
- The Government also accepts the Federal Court’s findings regarding CSIS’ duty of candour to the Federal Court. The Government takes this finding very seriously. CSIS has committed to working with the Federal Court to ensure that it is fully transparent with the Court.
- The Federal Court agreed with CSIS’ proposal to update warrants, and generally accepted the changes proposed by CSIS.
- In its decision, the Federal Court noted that the CSIS Act is now more than 30 years old and changes may need to be made to ensure that it keeps pace with changes in technology and the privacy expectations of Canadians. This is something that we will review.
- The Government is committed to keeping Canadians safe while at the same time safeguarding our freedoms, rights and values in an open and democratic society.
- We want to hear from Canadians on how we can best meet our dual objectives of security and rights. We invite all Canadians to provide us with their views and ideas on our national security framework through our online consultation, which is open until December 1<sup>st</sup>. ([www.canada.ca/national-security-consultation](http://www.canada.ca/national-security-consultation))
- Concurrently, we are taking measures to strengthen national security accountability. In June, we put forward legislation to create a National Security and Intelligence Committee of Parliamentarians which would have a broad mandate to scrutinize the activities of any federal department or agency with national security responsibilities, including operational matters.

### **Ministerial Talking Point:**



CSIS plays a vital role in keeping Canadians safe by investigating threats, and collecting and analyzing information to protect our national security. I continue to have confidence in their ability to deliver on that mandate.

## Sayarh, Omar (PS/SP)

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Thursday, October 20, 2016 12:50 PM  
**To:** [REDACTED] (PS/SP); [REDACTED] PS/SP  
**Subject:** FW: Federal Court  
**Attachments:** Director Statement re. En Banc Decision - October 2016 (ADP).docx; En Banc Decision - October 2016 - Qs As (ADP).docx

FYI

Julie G  
Tel : 613-993-4415 | BB : 613-410-6059

---

**From:** Magee, Heather (PS/SP)  
**Sent:** Thursday, October 20, 2016 12:43 PM  
**To:** Davies, John (PS/SP)  
**Cc:** Grenier, Julie (PS/SP)  
**Subject:** Fw: Federal Court

Hi John,

FYI - We just received this and we are doing a quick check to ensure the two statements work together.

Heather Magee  
Public Safety Canada / Sécurité publique Canada  
T: 613-949-6191 M: 613-302-3752  
[Heather.Magee@canada.ca](mailto:Heather.Magee@canada.ca)

---

**From:** Tomlinson, Jamie (PS/SP) <[jamie.tomlinson@canada.ca](mailto:jamie.tomlinson@canada.ca)>  
**Sent:** Thursday, October 20, 2016 12:31 PM  
**To:** Brien, Dan (PS/SP)  
**Cc:** Nichols, Megan (PS/SP); Baker3, Ryan (PS/SP); Magee, Heather (PS/SP)  
**Subject:** FW: Federal Court

fyi

---

**From:** [REDACTED]  
**Sent:** October-20-16 12:29 PM  
**To:** 'Fox, Christiane'; Tomlinson, Jamie (PS/SP); Noftle, Tracie; O'Nions, Christine  
**Cc:** Off, Shirley Anne ([ShirleyAnne.Off@justice.gc.ca](mailto:ShirleyAnne.Off@justice.gc.ca)); Magee, Heather (PS/SP); Nichols, Megan (PS/SP); Baker3, Ryan (PS/SP); [REDACTED] De Mora, Joe  
**Subject:** RE: Federal Court

Christiane, Tracie, Jamie, Shirley Anne/Joe,

Apologies for the delay, but please find attached the draft Director statement and Qs & As.

They have been reviewed up to the ADM-level here but have not yet been reviewed by the Director.

---

**From:** Fox, Christiane [mailto:Christiane.Fox@pco-bcp.gc.ca]  
**Sent:** 19-Oct-16 10:17 PM  
**To:** 'Tomlinson, Jamie (PS/SP)'; [REDACTED] Noftle, Tracie; O'Nions, Christine  
**Cc:** Off, Shirley Anne (ShirleyAnne.Off@justice.gc.ca); Magee, Heather (PS/SP); Nichols, Megan (PS/SP); Baker3, Ryan (PS/SP); [REDACTED]  
**Subject:** RE: Federal Court

Thanks everyone.

[REDACTED] for the day we go public, ideal would be for the Director to be at the NPT and the tech brief by phone works for us. Would be great to get materials asap tomorrow. Lots of interest to see drafts. Also, I have a couple of Qs on the AG review done a few years back and if not there already, that should be included in the Q&A. Is it feasible to see materials before 11am?

DoJ should also feed into the Qs&As.

Merci.

---

**From:** Tomlinson, Jamie (PS/SP) [mailto:Jamie.Tomlinson@canada.ca]  
**Sent:** October-19-16 18:48  
**To:** [REDACTED] Fox, Christiane; Noftle, Tracie; O'Nions, Christine  
**Cc:** Off, Shirley Anne (ShirleyAnne.Off@justice.gc.ca); Magee, Heather (PS/SP); Nichols, Megan (PS/SP); Baker3, Ryan (PS/SP); [REDACTED]  
**Subject:** Re: Federal Court

We will update.

Thanks

Sent from my BlackBerry 10 smartphone on the Rogers network.

---

**From:** [REDACTED]  
**Sent:** Wednesday, October 19, 2016 6:43 PM  
**To:** Tomlinson, Jamie (PS/SP); Fox, Christiane (christiane.fox@pco-bcp.gc.ca); Noftle, Tracie; O'Nions, Christine  
**Cc:** Off, Shirley Anne (ShirleyAnne.Off@justice.gc.ca); Magee, Heather (PS/SP); Nichols, Megan (PS/SP); Baker3, Ryan (PS/SP); [REDACTED]  
**Subject:** RE: Federal Court

Jamie,

A late-breaking small but important (bolded and underlined) change to recommend to one of the bullets:

- CSIS is taking immediate action to address the Federal Court's findings. CSIS halted **all access to and** analysis of **the** associated data as it actively works to assess and address the Federal Court's decision.

Thanks,

---

**From:** Tomlinson, Jamie (PS/SP) [mailto:Jamie.Tomlinson@canada.ca]  
**Sent:** 19-Oct-16 4:23 PM

**To:** Fox, Christiane ([christiane.fox@pco-bcp.gc.ca](mailto:christiane.fox@pco-bcp.gc.ca)); Noftle, Tracie; O'Nions, Christine  
**Cc:** Off, Shirley Anne ([ShirleyAnne.Off@justice.gc.ca](mailto:ShirleyAnne.Off@justice.gc.ca)); [REDACTED]; Magee, Heather (PS/SP); Nichols, Megan (PS/SP); Baker3, Ryan (PS/SP)  
**Subject:** Federal Court  
**Importance:** High

Following yesterday's discussion, we have crafted messages to respond to the federal court ruling. Ultimately, the messages could be weaved into a written Ministerial Statement or used by the Minister as talking points.

They have been approved up to our Deputy Minister [REDACTED]  
[REDACTED]

### Key Messages:

- The Government accepts the Federal Court's findings on this matter.
- It is important to underline that the associated data was collected legally through warrants. The Federal Court's key concern relates to CSIS' retention of such data (e.g., date, time, and phone numbers related to a call) when it is not related to a threat to the security of Canada.
- CSIS is taking immediate action to address the Federal Court's findings. CSIS halted all [REDACTED] associated data as it actively works to assess and address the Federal Court's decision.
- The Government also accepts the Federal Court's findings regarding CSIS' duty of candour to the Federal Court. The Government takes this finding very seriously. CSIS has committed to working with the Federal Court to ensure that it is fully transparent with the Court.
- The Federal Court agreed with CSIS' proposal to update warrants, and generally accepted the changes proposed by CSIS.
- In its decision, the Federal Court noted that the CSIS Act is now more than 30 years old and changes may need to be made to ensure that it keeps pace with changes in technology and the privacy expectations of Canadians. This is something that we will review.
- The Government is committed to keeping Canadians safe while at the same time safeguarding our freedoms, rights and values in an open and democratic society.
- We want to hear from Canadians on how we can best meet our dual objectives of security and rights. We invite all Canadians to provide us with their views and ideas on our national security framework through our online consultation, which is open until December 1<sup>st</sup>. ([www.canada.ca/national-security-consultation](http://www.canada.ca/national-security-consultation))
- Concurrently, we are taking measures to strengthen national security accountability. In June, we put forward legislation to create a National Security and Intelligence Committee of Parliamentarians which would have a broad mandate to scrutinize the activities of any federal department or agency with national security responsibilities, including operational matters.

### Ministerial Talking Point:

- CSIS plays a vital role in keeping Canadians safe by investigating threats, and collecting and analyzing information to protect our national security. I continue to have confidence in their ability to deliver on that mandate.

# STATEMENT

## *CSIS Director statement regarding decision of the Federal Court*

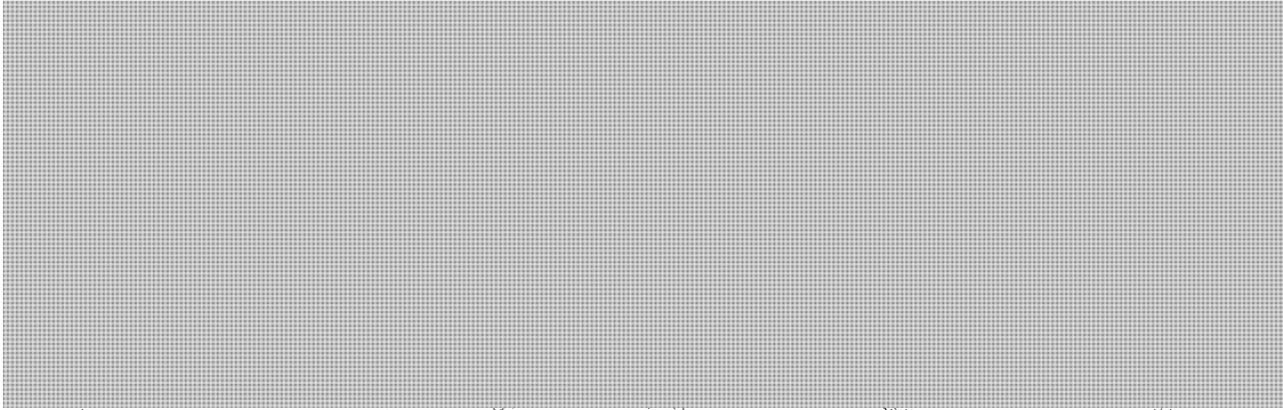
Ottawa, xxxxdays, [REDACTED] - The Director of the Canadian Security Intelligence Service (CSIS), Michel Coulombe, issued the following statement regarding the decision issued today by the Honourable Justice Noël of the Federal Court:

“The Canadian Security Intelligence Service is mandated to investigate activities which may, on reasonable grounds, be suspected of posing a threat to the security of Canada. In order to investigate these threats, CSIS may apply to the Federal Court for a warrant when the response to the threat requires more intrusive measures. Through the proceedings of the Court, over time, the provisions of warrants have changed to take into account the evolution of technology, legal developments, and investigative measures. This ensures that the powers granted by the warrants are clearly defined and that their conditions take into account the impact that the execution of the warrants [REDACTED] The Federal Court has [REDACTED]

The decision relates to [REDACTED] which authorized the interception of communications. CSIS had sought to fully analyze all of the information - both the content and the data associated [REDACTED] email addresses and telephone numbers. As is the case for many of our international partners, CSIS has developed data analytic capabilities and expertise to significantly enhance the identification and assessment of threats to the security of Canada over time and space. This includes identifying patterns of movement, communications, behaviours, significant trends, and links that are otherwise unidentifiable. When it comes to understanding and predicting the actions of the subjects of our investigations, data analytics has proven to be an effective tool. CSIS and the Department of Justice had interpreted the *CSIS Act* as enabling the retention of [REDACTED] for that important analytic work. In addition, to ensure appropriate accountability over the years, [REDACTED]

In the ruling released today, the Federal Court recognized the value of the data analytic programme and confirmed the legality of collecting telecommunications [REDACTED] pursuant to warrants. On the very specific use of associated data linked to third-party communications, the Court found that it can only be retained if it is related to threats and of use to an investigation, prosecution, national defence or international affairs. We accept this decision in full, and have taken immediate actions to respond.

Given the Court's decision, CSIS halted all access to, and analysis of, associated data while we undertake a thorough review of the decision in order to assess potential operational and legal impacts, and determine our way forward. I take seriously the concerns expressed by the Court with respect to our duty of candour. CSIS recognizes the importance of openness and transparency with the Federal Court, and we are working closely with the Department of Justice to develop measures aimed at ensuring that we meet our obligations to the Court in matters of transparency and duty of candour.



-30-

**Information:**  
Media Relations  
Canadian Security Intelligence Service  
613-231-0100

UNCLASSIFIED

Embargoed until decision is published

## Qs & As

### A. THE FEDERAL COURT DECISION

#### **1. Why did you appear before the Federal Court *en banc*?**

- CSIS appeared before the Federal Court on a warrant application with a view to amend some of the terms and conditions specified in the warrant.
- Owing to a finding in the Security Intelligence Review Committee's (SIRC) annual report (2014-15), the Court requested that the collection, use, retention and destruction of associated data (referred to by SIRC as metadata) collected under warrants also be addressed.

#### **2. Do you appear before the Federal Court *en banc* often?**

- The Service regularly applies for warrants before the Federal Court. Generally, these applications are presented to one designated Judge who will decide whether to issue the requested warrant or not.
- The Federal Court has requested that some warrant applications be heard in the presence of all designated judges of the Court. We refer to these as *en banc* hearings.

#### **3. What is the decision and how is it impacting CSIS?**

- The Court agreed with most of the terms and conditions proposed by CSIS on the warrant application that was presented to the Court.
- The Court found that CSIS breached its duty of candour by failing to fully and transparently inform the Court of its retention program and the establishment of the Operational Data Analysis Centre (ODAC).
- It also found CSIS' retention of associated data linked to third party communications found to be unrelated to threats and of no use to an investigation, prosecution, national defence or international affairs to be illegal. CSIS accepts the Court's findings in this regard.
- That said, it is important to underline that all associated data was collected legally through warrants. The Federal Court's key concern relates to CSIS' retention of associated data linked with third party communications, after it was collected.
- Further, the Court rightly acknowledged the age of the *CSIS Act* and that it may not be keeping pace with changing technology and the current threat environment.

#### **4. Why did CSIS not inform the Court of its new position on the retention of data and the creation of ODAC?**

- At various points, the Government, the Security Intelligence Review Committee and the Office of the Privacy Commissioner were made aware of CSIS' position on the retention of data and the establishment of ODAC.
- In June 2011, CSIS did advise the Federal Court that it amended the wording of warrant conditions in an effort to distinguish the content of communications from the associated data of communications. The Court found that notification to be insufficient.

UNCLASSIFIED

Embargoed until decision is published

- CSIS takes notice of the fact that the Court should have been informed earlier of the existence of ODAC and the change in the retention policy. At no point did CSIS deliberately seek to withhold this information from the Court, and the Court acknowledged that there is no evidence to that fact.

**5. What have you done to respond to the judgement?**

- On duty of candour: CSIS takes this finding very seriously and recognizes the importance of compliance with Ministerial direction and the CSIS Act, as well as openness and transparency with the Court.
- CSIS can and will do more to ensure that it is fully transparent with the Federal Court regarding the use it makes or plans to make of the information it collects pursuant to Federal Court issued warrants. To that end, it is working closely with the Department of Justice.
- On the retention of associated data linked with third party communications: CSIS immediately halted access to, and analysis of, associated data until such time as it can successfully distinguish associated data linked to third party communications from that of subject of investigation communications.

**B: Definitions**

**6. What kind of communications data does the Service collect?**

- In the course of an investigation, CSIS may obtain warrant powers against individuals or entities to authorize the use of specific investigative techniques. These powers, for example, allow CSIS to intercept communications. Execution of such warrant powers may result in the incidental collection of information from parties other than the target (i.e. third parties).
- When CSIS intercepts a communication, it obtains the content of the communication, as well as data about the communication. This could include: email addresses and telephone numbers.
- This data does not include any information that could reveal the purpose of the communication, nor any part of its content.

**7. What is the difference between associated data and metadata?**

- Metadata is the context, not the content of a communication. It is information used by computer systems to identify, describe, manage or route communications across a network.
- Associated data refers to information – or metadata – associated to a communication intercepted pursuant to a warrant.
- Neither metadata or associated data includes any information that could reveal the purpose of the communication, nor any part of its content

**8. What is associated data as defined by the Federal Court?**

- The Federal Court defines associated data as communications data collected under warrant from which the content was assessed as unrelated to threats and of no use to an investigation, prosecution, national defence or international affairs.

UNCLASSIFIED

Embargoed until decision is published

- Given the Federal Court's interpretation, the Service will undertake to review the terminology it applies to management of information collected under warrant.

**9. What is the difference between associated data and the dataset collection SIRC reviewed recently?**

- SIRC's 2016 Annual Report reviewed CSIS's non-warranted collection of datasets. This does not include communications content or data collected under Federal Court warrant.
- As an example, some non-warranted datasets are referential and provide contextual information which is publicly available. The Service also acquires other non-warranted datasets in support of mandated CSIS investigations.
- The Federal Court was concerned only with warranted collection, namely retention of third party associated data. That said, the Service is assessing the implications of this ruling for the non-warranted datasets SIRC recently reviewed.

**C. ODAC, DATA EXPLOITATION AND ASSOCIATED DATA**

**10. What is data exploitation, how does CSIS conduct data exploitation and why?**

- Data exploitation employs computers to analyze data and discover linkages, trends and patterns. These techniques enable humans to make sense of volumes of information that could not be processed without a computer's assistance.
- Data exploitation enables the Service to effectively analyze threats to the security of Canada over time. It can provide insight into subjects of investigation; identify new leads and intelligence gaps; provide context and understanding to operations and protect the security of operations and the safety of employees engaged in operations.
- The exploitation of data is invaluable in relation to the exercise of CSIS' mandate, but it must be undertaken responsibly and in accordance with our authorities. The Federal Court decision provides new direction in this regard.

**11. What is ODAC? Was anyone advised of its existence?**

- To derive more value from the data already being collected under warrant using data exploitation techniques, the Service established the Operational Data Analysis Centre in 2006.
- The necessity of creating this capability was described to the Minister of Public Safety in July 2006, noting that a basic requirement of ODAC would be the ability to retain data for extended periods of time.

**12. How long has CSIS had a formal data exploitation program?**

- The necessity of creating this capability was described to the Minister of Public Safety in July 2006 when CSIS developed the Operational Data and Analysis Centre (ODAC). This capability was created with full disclosure to the Government.

UNCLASSIFIED

Embargoed until decision is published

**13. Was SIRC aware of CSIS' data exploitation activities and collection of associated data?**

- SIRC was aware of CSIS' data exploitation activities from shortly after the establishment of ODAC in 2006. In 2007, CSIS responded to a SIRC query about ODAC and its support to operations.
- The Inspector General was provided a verbal briefing on ODAC and data exploitation in support of operations in 2011.
- SIRC reviewed CSIS' use of associated data and published its findings on the issue in its 2014-15 annual report. SIRC did not conclude that the retention of associated data was illegal.

**14. What were the Service's practices with regard to the retention of data collected under warrant prior to the Federal Court's decision?**

- Pursuant to policy, one year after collection, CSIS practice was to delete the content of communications intercepts collected under warrant assessed to be of no intelligence value.
- Though the content was destroyed, the data about the communication was retained, whether or not it was related to a third party.

**D. IMPACTS OF THE DECISION**

**15. Did CSIS collect this information illegally?**

- Any collection activity that requires the use of specific investigative techniques is authorized by warrants issued by the Federal Court. CSIS did not collect this information illegally, as confirmed in the decision.
- The Federal Court's key concern relates to CSIS' retention of associated data linked with third party communications, after it was collected.

**16. Will this decision affect the admissibility of evidence used in the cases of convicted terrorists?**

- CSIS is mandated to collect, by investigation or otherwise, to the extent that is strictly necessary, and analyze and retain information and intelligence respective activities that may on reasonable grounds be suspected of constituting threats to the security of Canada.
- CSIS collects intelligence or information for the purpose of advising the Government, providing security advice or security assessments. It does not, however, collect evidence.

**17. Were leads generated by the use of third associated data provided to the RCMP or other law enforcement partners for the purposes of counter terrorism investigations?**

- CSIS is assessing the decision in an effort to determine how it impacts operations. CSIS cannot, however, comment on the nature of its operations, and how they are impacted.

**18. Does this decision impact any current terrorism related cases?**

- CSIS is assessing the decision in efforts to determine how it impacts operations. CSIS cannot, however, comment on the nature of its operations, and how they are impacted.

UNCLASSIFIED

Embargoed until decision is published

## **E. CSIS RESPONSE TO THE DECISION**

### **19. What steps will CSIS take to implement the Court's recommended two-step process of assessment?**

- CSIS will be required to assess, within a short period, communications data to determine its relevance to a subject of investigation or threat to the security of Canada.
- Significant efforts will be required to implement policies, processes and technology that will successfully distinguish associated data (third party communications) from that of threat-related communications.

### **20. Has CSIS destroyed the data deemed illegal by the Court?**

- CSIS immediately halted analysis and use of all associated data until such time as it can successfully distinguish associated data from that linked to a threat.

## **E. BROADER IMPLICATIONS OF THE DECISION**

### **21. Are there any privacy implications noted in the decision?**

- The Federal Court did not speak to the privacy considerations of the retention of third party associated data.
- CSIS recognizes the importance of maintaining public trust and confidence in its activities. CSIS takes very seriously potential privacy considerations related to its work, and it is committed to ensuring that its activities are transparent, accountable and in compliance with privacy legislation, guidelines and best practices.
- Of note, a Privacy Impact Assessment on ODAC was completed in August 2010. Should the Office of the Privacy Commissioner be interested in investigating the privacy implications of the decision, CSIS will cooperate fully.

### **22. Will the government consult Canadians on the data exploitation activities of CSIS?**

- The Government is committed to keeping Canadians safe while at the same time safeguarding our freedoms, rights and values in an open and democratic society.
- The ongoing national security consultations represent an important opportunity to ensure that CSIS is meeting the dual objectives of security and privacy and has the tools and authorities, with appropriate oversight, to meet both.

### **23. Will the new National Security and Intelligence Committee of Parliamentarians have any role in reviewing CSIS' data exploitation activities?**

- Enhancements to the review system, including the proposed National Security and Intelligence Committee of Parliamentarians, will be properly decided by Parliament.
- As currently drafted, the Bill to establish the Committee would authorize it to review the operational activities of CSIS, including programmes such as its data exploitation activities.
- CSIS will, of course, respect and fully cooperate with this committee, should it be stood up and wish to review this issue, or any other CSIS activity.

UNCLASSIFIED

Embargoed until decision is published

## **F. CSIS USE OF ASSOCIATED DATA**

### **24. How will CSIS deal with the associated data it currently holds?**

- CSIS immediately isolated and halted analysis of all associated data until such time as it can successfully distinguish associated data from that linked to a threat.

### **25. Has or does CSIS share its associated data holdings with foreign partners?**

- CSIS does not share its associated data holdings with foreign partners.

### **26. How does or did CSIS previously ensure that data exploitation technologies did not unnecessarily target individuals NOT engaged in threat related activity?**

- Data exploitation is used in response to specific operational queries related to mandated investigations.
- Data exploitation is a tool to assist the Service in discovering linkages, trends and patterns to advance investigations.
- Determining whether or not a communication is threat-related is complex and may only become apparent as an investigation progresses.
- The Service has seen examples where communications originally assessed to have no intelligence value were later revealed to contain key threat-related information.

### **27. How is this collection different from the bulk collection of SIGINT agencies?**

- CSIS collection of communications data is authorized under Federal Court warrants and is specifically focused on an identified target of investigation.

## Sayarh, Omar (PS/SP)

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Thursday, October 20, 2016 11:03 AM  
**To:** Miller, Kevin (PS/SP)  
**Subject:** "En Banc" Key Messages  
**Attachments:** PS-SP-#1995114-v1F-Key\_Messages\_-\_En\_Banc\_Associated\_Data.doc

Hi Kevin,  
Here are the key messages, pending in MO for approval.

Julie Grenier  
Senior Communications Advisor / Conseillère principale de communications  
Portfolio Affairs and Communications Branch/  
Secteur des affaires du portefeuille et des communications  
Public Safety Canada / Sécurité publique du Canada  
Tel : 613-993-4415 | BB : 613-410-6059

**Pages 446 to / à 447  
are duplicates  
sont des duplicatas**

**Sayarh, Omar (PS/SP)**

---

**From:** [REDACTED] (PS/SP)  
**Sent:** Thursday, October 20, 2016 11:06 AM  
**To:** Grenier, Julie (PS/SP); [REDACTED] (PS/SP); [REDACTED] (PS/SP)  
**Cc:** Sousa, Michael (PS/SP); Brender, James (PS/SP)  
**Subject:** RE: Federal Court

Sounds good.

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Thursday, October 20, 2016 10:35 AM  
**To:** [REDACTED] (PS/SP); [REDACTED] (PS/SP); Davies, John (PS/SP)  
**Cc:** Sousa, Michael (PS/SP); Brender, James (PS/SP)  
**Subject:** RE: Federal Court

Hi [REDACTED]

I was just going to let you know I've been tasked with a written statement for the Minister.

I think we'll hold on sending another update to MO on the key messages (as we just sent an update less than an hour ago), but I will use this latest language in the statement.

The statement draws from the Key Messages. There should be no new language, just finesse. As such, I'll be sending straight to John D for approval, but I will be sure to copy all of you.

Thanks!

Julie G  
Tel : 613-993-4415 | BB : 613-410-6059

---

**From:** [REDACTED] (PS/SP)  
**Sent:** Thursday, October 20, 2016 10:23 AM  
**To:** Grenier, Julie (PS/SP); [REDACTED] (PS/SP); Davies, John (PS/SP)  
**Cc:** Sousa, Michael (PS/SP); Brender, James (PS/SP)  
**Subject:** RE: Federal Court

Julie,

[REDACTED]

[REDACTED]

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Thursday, October 20, 2016 10:08 AM  
**To:** [REDACTED] (PS/SP); [REDACTED] (PS/SP); Davies, John (PS/SP)  
**Cc:** Sousa, Michael (PS/SP); Brender, James (PS/SP)  
**Subject:** RE: Federal Court

Hi,

As you may already know, CSIS has provided a small but important change to the third bullet in the Key Messages. (Noted below in bold and underline)

- CSIS is taking immediate action to address the Federal Court's findings. CSIS halted **all access to and analysis of the** associated data as it actively works to assess and address the Federal Court's decision.

The updated version (attached) is with MO for approval.

Julie G

Tel : 613-993-4415 | BB : 613-410-6059

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Wednesday, October 19, 2016 6:08 PM  
**To:** [REDACTED] (PS/SP); [REDACTED] (PS/SP)  
**Subject:** Re: Federal Court

Will do.

Julie

Tel: 613-993-4415, BB: 613-410-6059

---

**From:** [REDACTED] (PS/SP)  
**Sent:** Wednesday, October 19, 2016 5:48 PM  
**To:** Grenier, Julie (PS/SP); [REDACTED] (PS/SP)  
**Subject:** RE: Federal Court

CSIS is doing a final check tonight. But for now their instruction is to only use [REDACTED]

If you don't hear from me, can you remind me before you finalize documents so that I can close the loop?

Thanks,

[REDACTED]

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Wednesday, October 19, 2016 3:49 PM  
**To:** [REDACTED] (PS/SP); [REDACTED] (PS/SP)  
**Subject:** RE: Federal Court

Yes, we can definitely make that change once the preferred language is agreed-upon. I don't think as something that would require a re-approval. Thank you!

Julie G

Tel : 613-993-4415 | BB : 613-410-6059

---

**From:** [REDACTED] (PS/SP)  
**Sent:** Wednesday, October 19, 2016 3:42 PM  
**To:** Grenier, Julie (PS/SP); [REDACTED] (PS/SP)  
**Subject:** RE: Federal Court

That should be okay. There's a bit of a discussion about whether we should be referring to "associated data," "metadata," "associated metadata," or use the terms interchangeably. Looks like we might be landing on the last option, but assuming there will still be time to make that change a bit later?



---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Wednesday, October 19, 2016 3:38 PM  
**To:** [REDACTED] (PS/SP); [REDACTED] (PS/SP)  
**Cc:** Sousa, Michael (PS/SP); Brender, James (PS/SP)  
**Subject:** RE: Federal Court

Hi [REDACTED]

Unless it's a critical correction, I think we might have to wait until the next opportunity to update the lines.

Julie G  
Tel : 613-993-4415 | BB : 613-410-6059

---

**From:** [REDACTED] (PS/SP)  
**Sent:** Wednesday, October 19, 2016 3:33 PM  
**To:** Grenier, Julie (PS/SP); [REDACTED] (PS/SP)  
**Cc:** Sousa, Michael (PS/SP); Brender, James (PS/SP)  
**Subject:** RE: Federal Court

We have one suggestion from CSIS. Will send asap.



---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Wednesday, October 19, 2016 3:27 PM  
**To:** [REDACTED] (PS/SP); [REDACTED] (PS/SP)  
**Cc:** Sousa, Michael (PS/SP); Brender, James (PS/SP)  
**Subject:** Fw: Federal Court  
**Importance:** High

As an update, lines are now with the DM via my DG.  
Thanks all for your work on this.

Up next: Qs+As. Standby as your input will be sought.

Julie  
Tel: 613-993-4415, BB: 613-410-6059

---

**From:** Tomlinson, Jamie (PS/SP) <[jamie.tomlinson@canada.ca](mailto:jamie.tomlinson@canada.ca)>  
**Sent:** Wednesday, October 19, 2016 3:20 PM  
**To:** Grenier, Julie (PS/SP)  
**Subject:** FW: Federal Court

fyi

**From:** Tomlinson, Jamie (PS/SP)  
**Sent:** October-19-16 3:19 PM  
**To:** Brown, Malcolm (PS/SP); Wilson, Gina (PS/SP)  
**Cc:** Beauregard, Monik (PS/SP); MacKinnon, Paul (PS/SP); DeSantis, Heather; Champoux, Elizabeth (PS/SP); Magee, Heather (PS/SP)  
**Subject:** Federal Court  
**Importance:** High

Malcolm,

As mentioned this morning at EXCOM, following yesterday's four corners meeting, we have crafted messages to respond to the federal court ruling. Ultimately, the messages could be weaved into a written Ministerial Statement or used by the Minister as talking points.

Once we have your feedback, we will move the messages to the Minister's Office.

CSIS is working on a statement from the Director and messaging that their officials would use in a technical briefing. I will pass along those products as soon as I receive them (CSIS was aiming for end of day).

Thank you.

#### **Key Messages:**

- The Government accepts the Federal Court's findings on this matter.
- It is important to underline that the associated data was collected legally through warrants. The Federal Court's key concern relates to CSIS' retention of such data (e.g., date, time, and phone numbers related to a call) when it is not related to a threat to the security of Canada.
- CSIS is taking immediate action to address the Federal Court's findings. CSIS halted all analysis of associated data as it actively works to assess and address the Federal Court's decision.
- The Government also accepts the Federal Court's findings regarding CSIS' duty of candour to the Federal Court. The Government takes this finding very seriously. CSIS has committed to working with the Federal Court to ensure that it is fully transparent with the Court.
- The Federal Court agreed with CSIS' proposal to update warrants, and generally accepted the changes proposed by CSIS.
- In its decision, the Federal Court noted that the CSIS Act is now more than 30 years old and changes may need to be made to ensure that it keeps pace with changes in technology and the privacy expectations of Canadians. This is something that we will review.
- The Government is committed to keeping Canadians safe while at the same time safeguarding our freedoms, rights and values in an open and democratic society.
- We want to hear from Canadians on how we can best meet our dual objectives of security and rights. We invite all Canadians to provide us with their views and ideas on our national security framework through our online consultation, which is open until December 1<sup>st</sup>. ([www.canada.ca/national-security-consultation](http://www.canada.ca/national-security-consultation))

- Concurrently, we are taking measures to strengthen national security accountability. In June, we put forward legislation to create a National Security and Intelligence Committee of Parliamentarians which would have a broad mandate to scrutinize the activities of any federal department or agency with national security responsibilities, including operational matters.

**Ministerial Talking Point:**

- CSIS plays a vital role in keeping Canadians safe by investigating threats, and collecting and analyzing information to protect our national security. I continue to have confidence in their ability to deliver on that mandate.

**Sayarh, Omar (PS/SP)**

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Thursday, October 20, 2016 11:01 AM  
**To:** [REDACTED] (PS/SP)  
**Subject:** RE: Federal Court

Got it. I can change the file name to eliminate any possible confusion.

FYI – Sent DoJ Comms the lines in our MO so everyone should have the same draft messages.

Julie G  
Tel : 613-993-4415 | BB : 613-410-6059

---

**From:** [REDACTED] (PS/SP)  
**Sent:** Thursday, October 20, 2016 10:58 AM  
**To:** Grenier, Julie (PS/SP)  
**Subject:** RE: Federal Court

Yes, and the change looks good to us.

Re. the reference to “associated data,” that’s from a policy discussion yesterday (PS, CSIS, CSE). Your material uses “associated data,” but the title refers to “metadata.” Our last conversation was that “associated data should be used throughout. [REDACTED] is policy. But maybe [REDACTED] can answer that question as well.

Thanks,

[REDACTED]

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Thursday, October 20, 2016 10:19 AM  
**To:** [REDACTED] (PS/SP)  
**Subject:** RE: Federal Court

Hi [REDACTED]

FYI -- It was [REDACTED] (DG Comms CSIS) that provided the latest update to language below. I note there is no changed to “associated data” but I guess there’s no harm in doublechecking.

Also FYI - My DG Jamie is under the impression we will get CSIS statement and supporting materials around 11 a.m. this morning.

Julie G  
Tel : 613-993-4415 | BB : 613-410-6059

---

**From:** [REDACTED] (PS/SP)  
**Sent:** Thursday, October 20, 2016 10:17 AM  
**To:** [REDACTED]  
**Cc:** Sousa, Michael (PS/SP); Brender, James (PS/SP); Grenier, Julie (PS/SP); [REDACTED] (PS/SP); Davies, John (PS/SP)  
**Subject:** RE: Federal Court

[REDACTED] per our conversation last night, have relayed to Comms that all references should be to "associated data." Are you guys still okay with that?

Thanks,

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Thursday, October 20, 2016 10:08 AM  
**To:** [REDACTED] (PS/SP); [REDACTED] (PS/SP); Davies, John (PS/SP)  
**Cc:** Sousa, Michael (PS/SP); Brender, James (PS/SP)  
**Subject:** RE: Federal Court

Hi,

As you may already know, CSIS has provided a small but important change to the third bullet in the Key Messages. (Noted below in bold and underline)

- CSIS is taking immediate action to address the Federal Court's findings. CSIS halted **all access to and** analysis of **the** associated data as it actively works to assess and address the Federal Court's decision.

The updated version (attached) is with MO for approval.

Julie G  
Tel : 613-993-4415 | BB : 613-410-6059

**Sayarh, Omar (PS/SP)**

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Thursday, October 20, 2016 10:45 AM  
**To:** 'De Mora, Joe'  
**Cc:** Sousa, Michael (PS/SP); Benoit, Nathalie; Brender, James (PS/SP); 'Gowing, Andrew'  
**Subject:** RE: [REDACTED]  
**Attachments:** [REDACTED]

Hi Joe,

[REDACTED]

Thanks,  
Julie G  
Tel : 613-993-4415 | BB : 613-410-6059

---

**From:** De Mora, Joe [mailto:Joe.DeMora@justice.gc.ca]  
**Sent:** Wednesday, October 19, 2016 4:32 PM  
**To:** Brender, James (PS/SP)  
**Cc:** Sousa, Michael (PS/SP); Grenier, Julie (PS/SP); Benoit, Nathalie  
**Subject:** RE: [REDACTED]

James,

[REDACTED]

Best

Joe

**From:** Brender, James (PS/SP) [mailto:james.brender@canada.ca]  
**Sent:** October-19-16 2:48 PM  
**To:** De Mora, Joe <Joe.DeMora@justice.gc.ca>  
**Cc:** Sousa, Michael (PS) <Michael.Sousa@canada.ca>  
**Subject:** RE: [REDACTED]

Hi Joe - [REDACTED] Thanks very much.

James Brender  
Counsel/avocat

Legal Services/service juridique  
Public Safety and Emergency Preparedness /Sécurité publique et protection civile  
269 Laurier West, 16th Floor  
Ottawa ON K1A 0P8

613-991-2883  
[james.brender@psepc.gc.ca](mailto:james.brender@psepc.gc.ca)

Solicitor / Client Privilege

---

**From:** Sousa, Michael (PS/SP)  
**Sent:** Wednesday, October 19, 2016 2:37 PM  
**To:** Brender, James (PS/SP)  
**Subject:** FW: [REDACTED]

**Michael Sousa**

Avocat général principal & Directeur exécutif  
Senior General Counsel & Executive Director  
Services juridiques ministériels, Sécurité publique Canada | Public Safety Canada Legal Services  
269 avenue Laurier ouest, 16ième étage, pièce 1800  
269, Laurier Avenue West., 16<sup>th</sup> floor, room 1800  
Ottawa (ON K1A 0P8)  
tél. | tel. (613) 991-9375 -- téléc. | fax (613) 990-8307

Solicitor-Client Privilege / Secret professionnel de l'avocat

**Page 457**

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

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

**Pages 458 to / à 459  
are duplicates  
sont des duplicatas**

## Sayarh, Omar (PS/SP)

---

**From:** Ministerial Liaison / Liaison ministerielle (PS/SP)  
**Sent:** Thursday, October 20, 2016 10:36 AM  
**To:** Brien, Dan (PS/SP); Bardsley, Scott (PS/SP); Peirce, Hilary (PS/SP)  
**Cc:** Tomlinson, Jamie (PS/SP); Magee, Heather (PS/SP); Baker3, Ryan (PS/SP); Grenier, Julie (PS/SP); Wilson, Ashleigh (PS/SP); Miller, Kevin (PS/SP); De Curtis, Laura (PS/SP); Ministerial Liaison / Liaison ministerielle (PS/SP)  
**Subject:** For Approval: "En Banc" Key Messages and Talking Point  
**Attachments:** PS-SP-#1995114-v1F-Key\_Messages\_-\_En\_Banc\_Metadata.doc

Dan, Scott, Hilary,

CSIS has provided a small but important change to the third bullet in the Key Messages. (Noted below in bold and underlined)

- CSIS is taking immediate action to address the Federal Court's findings. CSIS halted **all access to and** analysis of **the** associated data as it actively works to assess and address the Federal Court's decision.

We have updated in the attached. Please use this version for your approvals.

Please track any changes and reply all.

Thanks,  
Lucie

---

**From:** Baker3, Ryan (PS/SP)  
**Sent:** Wednesday, October 19, 2016 6:12 PM  
**To:** Brien, Dan (PS/SP); Bardsley, Scott (PS/SP); Peirce, Hilary (PS/SP)  
**Cc:** Tomlinson, Jamie (PS/SP); Magee, Heather (PS/SP); Grenier, Julie (PS/SP); Wilson, Ashleigh (PS/SP); Ministerial Liaison / Liaison ministerielle (PS/SP); Miller, Kevin (PS/SP); De Curtis, Laura (PS/SP)  
**Subject:** For approval: "En Banc" Key Messages and Talking Point

Dan, Scott, Hilary,

Attached for your approval are the proposed Key Messages and a Talking Point for the "En Banc" Federal Court decision pertaining to CSIS' retention of associated data.



Please track any changes and reply all.

Thanks,

Ryan

---

# *Media Lines*

---

## **FEDERAL COURT “EN BANC” DECISION CSIS’ Authority to Retain Metadata Collected Through Warrants**

### **Key Messages:**

- The Government accepts the Federal Court’s findings on this matter.
- It is important to underline that the associated data was collected legally through warrants. The Federal Court’s key concern relates to CSIS’ retention of such data (e.g., date, time, and phone numbers related to a call) when it is not related to a threat to the security of Canada.
- CSIS is taking immediate action to address the Federal Court’s findings. CSIS halted all access to and analysis of the associated data as it actively works to assess and address the Federal Court’s decision.
- The Government also accepts the Federal Court’s findings regarding CSIS’ duty of candour to the Federal Court. The Government takes this finding very seriously. CSIS has committed to working with the Federal Court to ensure that it is fully transparent with the Court.
- The Federal Court agreed with CSIS’ proposal to update warrants, and generally accepted the changes proposed by CSIS.
- In its decision, the Federal Court noted that the CSIS Act is now more than 30 years old and changes may need to be made to ensure that it keeps pace with changes in technology and the privacy expectations of Canadians. This is something that we will review.
- The Government is committed to keeping Canadians safe while at the same time safeguarding our freedoms, rights and values in an open and democratic society.
- We want to hear from Canadians on how we can best meet our dual objectives of security and rights. We invite all Canadians to provide us with their views and ideas on our national security framework through our online consultation, which is open until December 1<sup>st</sup>. ([www.canada.ca/national-security-consultation](http://www.canada.ca/national-security-consultation))
- Concurrently, we are taking measures to strengthen national security accountability. In June, we put forward legislation to create a National Security and Intelligence Committee of Parliamentarians which would have a broad mandate to scrutinize the activities of any federal department or agency with national security responsibilities, including operational matters.

### **Ministerial Talking Point:**

CSIS plays a vital role in keeping Canadians safe by investigating threats, and collecting and analyzing information to protect our national security. I continue to have confidence in their ability to deliver on that mandate.

**Prepared by:** Julie Grenier

**Consulted:** NS Intelligence, Legal, CSIS Policy, Justice

**Approved by:**

John Davies, DG, NS Policy (approved)

Monik Beauregard, ADM, NCSB (approved)

Heather Magee, Director, Communications (approved)

Jamie Tomlinson, DG, Communications (approved)

MO (pending)

PCO (pending)

## Sayarh, Omar (PS/SP)

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Thursday, October 20, 2016 10:04 AM  
**To:** Ministerial Liaison / Liaison ministerielle (PS/SP)  
**Subject:** FW: For approval: "En Banc" Key Messages and Talking Point  
**Attachments:** PS-SP-#1995114-v1F-Key\_Messages\_-\_En\_Banc\_Metadata.doc

It should be "a small but important change" but I'm sure you already caught that!

Julie G  
Tel : 613-993-4415 | BB : 613-410-6059

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Thursday, October 20, 2016 10:02 AM  
**To:** Ministerial Liaison / Liaison ministerielle (PS/SP)  
**Cc:** Baker3, Ryan (PS/SP); Magee, Heather (PS/SP)  
**Subject:** RE: For approval: "En Banc" Key Messages and Talking Point

Hello,  
Request to provide the below to MO ASAP.

--

Dan, Scott, Hilary,

CSIS has provided small a but important change to the third bullet in the Key Messages. (Noted below in bold and underline)

- CSIS is taking immediate action to address the Federal Court's findings. CSIS halted **all access to and** analysis of **the** associated data as it actively works to assess and address the Federal Court's decision.

We have updated in the attached. Please use this version for your approvals.

Please track any changes and reply all.

---

**From:** Baker3, Ryan (PS/SP)  
**Sent:** Wednesday, October 19, 2016 6:12 PM  
**To:** Brien, Dan (PS/SP); Bardsley, Scott (PS/SP); Peirce, Hilary (PS/SP)  
**Cc:** Tomlinson, Jamie (PS/SP); Magee, Heather (PS/SP); Grenier, Julie (PS/SP); Wilson, Ashleigh (PS/SP); Ministerial Liaison / Liaison ministerielle (PS/SP); Miller, Kevin (PS/SP); De Curtis, Laura (PS/SP)  
**Subject:** For approval: "En Banc" Key Messages and Talking Point

Dan, Scott, Hilary,

Attached for your approval are the proposed Key Messages and a Talking Point for the "En Banc" Federal Court decision pertaining to CSIS' retention of associated data.



Please track any changes and reply all.

Thanks,

Ryan

**Pages 465 to / à 466  
are duplicates  
sont des duplicatas**

## Sayarh, Omar (PS/SP)

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Wednesday, October 19, 2016 5:03 PM  
**To:** PS.F Speeches / Discours F.SP  
**Subject:** Request for support from speechwriters  
**Attachments:** PS-SP-#1995114-v1E-Key\_Messages\_-\_En\_Banc\_Metadata.doc

**Importance:** High

Hello,

Strat Comms is looking for support from Speechwriters to help fashion a short statement the Minister could read on the topic of the Federal Court's decision on CSIS' retention of associated data.

As the decision could be coming out Friday, we're looking to have something in hand by Friday morning. I can coordinate the reviews and approvals. I'm just looking for support to draft it, as I will be focusing on Qs&As for a potential teleconference with media.

Here are the key messages that we sent up to the Minister's Office this afternoon. We can discuss more first thing tomorrow.

Thanks in advance,  
Julie Grenier  
Senior Communications Advisor / Conseillère principale de communications  
Portfolio Affairs and Communications Branch/  
Secteur des affaires du portefeuille et des communications  
Public Safety Canada / Sécurité publique du Canada  
Tel : 613-993-4415 | BB : 613-410-6059



---

# *Media Lines*

---

## **FEDERAL COURT “EN BANC” DECISION CSIS’ Authority to Retain Metadata Collected Through Warrants**

### **Key Messages:**

- The Government accepts the Federal Court’s findings on this matter.
- It is important to underline that the associated data was collected legally through warrants. The Federal Court’s key concern relates to CSIS’ retention of such data (e.g., date, time, and phone numbers related to a call) when it is not related to a threat to the security of Canada.
- CSIS is taking immediate action to address the Federal Court’s findings. CSIS halted all analysis of associated data as it actively works to assess and address the Federal Court’s decision.
- The Government also accepts the Federal Court’s findings regarding CSIS’ duty of candour to the Federal Court. The Government takes this finding very seriously. CSIS has committed to working with the Federal Court to ensure that it is fully transparent with the Court.
- The Federal Court agreed with CSIS’ proposal to update warrants, and generally accepted the changes proposed by CSIS.
- In its decision, the Federal Court noted that the CSIS Act is now more than 30 years old and changes may need to be made to ensure that it keeps pace with changes in technology and the privacy expectations of Canadians. This is something that we will review.
- The Government is committed to keeping Canadians safe while at the same time safeguarding our freedoms, rights and values in an open and democratic society.
- We want to hear from Canadians on how we can best meet our dual objectives of security and rights. We invite all Canadians to provide us with their views and ideas on our national security framework through our online consultation, which is open until December 1<sup>st</sup>. ([www.canada.ca/national-security-consultation](http://www.canada.ca/national-security-consultation))
- Concurrently, we are taking measures to strengthen national security accountability. In June, we put forward legislation to create a National Security and Intelligence Committee of Parliamentarians which would have a broad mandate to scrutinize the activities of any federal department or agency with national security responsibilities, including operational matters.

### **Ministerial Talking Point:**



CSIS plays a vital role in keeping Canadians safe by investigating threats, and collecting and analyzing information to protect our national security. I continue to have confidence in their ability to deliver on that mandate.

**Prepared by:** Julie Grenier

**Consulted:** NS Intelligence, Legal, CSIS Policy, Justice

**Approved by:**

John Davies, DG, NS Policy (approved)

Monik Beauregard, ADM, NCSB (approved)

Heather Magee, Director, Communications (approved)

Jamie Tomlinson, DG, Communications (approved)

MO (pending)

PCO (pending)

**Sayarh, Omar (PS/SP)**

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Wednesday, October 19, 2016 3:49 PM  
**To:** [REDACTED] (PS/SP); [REDACTED] (PS/SP)  
**Subject:** RE: Federal Court

Yes, we can definitely make that change once the preferred language is agreed-upon. I don't think as something that would require a re-approval. Thank you!

Julie G  
Tel : 613-993-4415 | BB : 613-410-6059

---

**From:** [REDACTED] (PS/SP)  
**Sent:** Wednesday, October 19, 2016 3:42 PM  
**To:** Grenier, Julie (PS/SP); [REDACTED] (PS/SP)  
**Subject:** RE: Federal Court

That should be okay. There's a bit of a discussion about whether we should be referring to "associated data," "metadata," "associated metadata," or use the terms interchangeably. Looks like we might be landing on the last option, but assuming there will still be time to make that change a bit later?

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Wednesday, October 19, 2016 3:38 PM  
**To:** [REDACTED] (PS/SP); [REDACTED] (PS/SP)  
**Cc:** Sousa, Michael (PS/SP); Brender, James (PS/SP)  
**Subject:** RE: Federal Court

Hi [REDACTED]

Unless it's a critical correction, I think we might have to wait until the next opportunity to update the lines.

Julie G  
Tel : 613-993-4415 | BB : 613-410-6059

---

**From:** [REDACTED] (PS/SP)  
**Sent:** Wednesday, October 19, 2016 3:33 PM  
**To:** Grenier, Julie (PS/SP); [REDACTED] (PS/SP)  
**Cc:** Sousa, Michael (PS/SP); Brender, James (PS/SP)  
**Subject:** RE: Federal Court

We have one suggestion from CSIS. Will send asap.

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Wednesday, October 19, 2016 3:27 PM

**To:** [REDACTED] (PS/SP); [REDACTED] (PS/SP)  
**Cc:** Sousa, Michael (PS/SP); Brender, James (PS/SP)  
**Subject:** Fw: Federal Court  
**Importance:** High

As an update, lines are now with the DM via my DG.  
Thanks all for your work on this.

Up next: Qs+As. Standby as your input will be sought.

Julie  
Tel: 613-993-4415, BB: 613-410-6059

---

**From:** Tomlinson, Jamie (PS/SP) <jamie.tomlinson@canada.ca>  
**Sent:** Wednesday, October 19, 2016 3:20 PM  
**To:** Grenier, Julie (PS/SP)  
**Subject:** FW: Federal Court

fyi

---

**From:** Tomlinson, Jamie (PS/SP)  
**Sent:** October-19-16 3:19 PM  
**To:** Brown, Malcolm (PS/SP); Wilson, Gina (PS/SP)  
**Cc:** Beauregard, Monik (PS/SP); MacKinnon, Paul (PS/SP); DeSantis, Heather; Champoux, Elizabeth (PS/SP); Magee, Heather (PS/SP)  
**Subject:** Federal Court  
**Importance:** High

Malcolm,

As mentioned this morning at EXCOM, following yesterday's four corners meeting, we have crafted messages to respond to the federal court ruling. Ultimately, the messages could be weaved into a written Ministerial Statement or used by the Minister as talking points.

Monik has approved [REDACTED]

Once we have your feedback, we will move the messages to the Minister's Office.

CSIS is working on a statement from the Director and messaging that their officials would use in a technical briefing. I will pass along those products as soon as I receive them (CSIS was aiming for end of day).

Thank you.

### Key Messages:

- The Government accepts the Federal Court's findings on this matter.
- It is important to underline that the associated data was collected legally through warrants. The Federal Court's key concern relates to CSIS' retention of such data (e.g., date, time, and phone numbers related to a call) when it is not related to a threat to the security of Canada.
- CSIS is taking immediate action to address the Federal Court's findings. CSIS halted all analysis of associated data as it actively works to assess and address the Federal Court's decision.

- The Government also accepts the Federal Court's findings regarding CSIS' duty of candour to the Federal Court. The Government takes this finding very seriously. CSIS has committed to working with the Federal Court to ensure that it is fully transparent with the Court.
- The Federal Court agreed with CSIS' proposal to update warrants, and generally accepted the changes proposed by CSIS.
- In its decision, the Federal Court noted that the CSIS Act is now more than 30 years old and changes may need to be made to ensure that it keeps pace with changes in technology and the privacy expectations of Canadians. This is something that we will review.
- The Government is committed to keeping Canadians safe while at the same time safeguarding our freedoms, rights and values in an open and democratic society.
- We want to hear from Canadians on how we can best meet our dual objectives of security and rights. We invite all Canadians to provide us with their views and ideas on our national security framework through our online consultation, which is open until December 1<sup>st</sup>. ([www.canada.ca/national-security-consultation](http://www.canada.ca/national-security-consultation))
- Concurrently, we are taking measures to strengthen national security accountability. In June, we put forward legislation to create a National Security and Intelligence Committee of Parliamentarians which would have a broad mandate to scrutinize the activities of any federal department or agency with national security responsibilities, including operational matters.

**Ministerial Talking Point:**

- CSIS plays a vital role in keeping Canadians safe by investigating threats, and collecting and analyzing information to protect our national security. I continue to have confidence in their ability to deliver on that mandate.

**Sayarh, Omar (PS/SP)**

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Wednesday, October 19, 2016 3:39 PM  
**To:** [REDACTED] (PS/SP)  
**Subject:** RE: Federal Court  
**Attachments:** PS-SP-#1995114-v1E-Key\_Messages\_-\_En\_Banc\_Metadata.doc

You should still have access. Attached reference if you want to try again.

If you make any changes, please create a sub-version and track the change. Thanks!

Julie G  
Tel : 613-993-4415 | BB : 613-410-6059

---

**From:** [REDACTED] (PS/SP)  
**Sent:** Wednesday, October 19, 2016 3:33 PM  
**To:** Grenier, Julie (PS/SP)  
**Subject:** RE: Federal Court

Can you give me access?

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Wednesday, October 19, 2016 3:27 PM  
**To:** [REDACTED] (PS/SP); [REDACTED] (PS/SP)  
**Cc:** Sousa, Michael (PS/SP); Brender, James (PS/SP)  
**Subject:** Fw: Federal Court  
**Importance:** High

As an update, lines are now with the DM via my DG.  
Thanks all for your work on this.

Up next: Qs+As. Standby as your input will be sought.

Julie  
Tel: 613-993-4415, BB: 613-410-6059

---

**From:** Tomlinson, Jamie (PS/SP) <[jamie.tomlinson@canada.ca](mailto:jamie.tomlinson@canada.ca)>  
**Sent:** Wednesday, October 19, 2016 3:20 PM  
**To:** Grenier, Julie (PS/SP)  
**Subject:** FW: Federal Court

fyi

---

**From:** Tomlinson, Jamie (PS/SP)  
**Sent:** October-19-16 3:19 PM  
**To:** Brown, Malcolm (PS/SP); Wilson, Gina (PS/SP)  
**Cc:** Beauregard, Monik (PS/SP); MacKinnon, Paul (PS/SP); DeSantis, Heather; Champoux, Elizabeth (PS/SP); Magee,

Heather (PS/SP)

**Subject:** Federal Court

**Importance:** High

Malcolm,

As mentioned this morning at EXCOM, following yesterday's four corners meeting, we have crafted messages to respond to the federal court ruling. Ultimately, the messages could be weaved into a written Ministerial Statement or used by the Minister as talking points.

Monik has approved [REDACTED]

Once we have your feedback, we will move the messages to the Minister's Office.

CSIS is working on a statement from the Director and messaging that their officials would use in a technical briefing. I will pass along those products as soon as I receive them (CSIS was aiming for end of day).

Thank you.

**Key Messages:**

- The Government accepts the Federal Court's findings on this matter.
- It is important to underline that the associated data was collected legally through warrants. The Federal Court's key concern relates to CSIS' retention of such data (e.g., date, time, and phone numbers related to a call) when it is not related to a threat to the security of Canada.
- CSIS is taking immediate action to address the Federal Court's findings. CSIS halted all analysis of associated data as it actively works to assess and address the Federal Court's decision.
- The Government also accepts the Federal Court's findings regarding CSIS' duty of candour to the Federal Court. The Government takes this finding very seriously. CSIS has committed to working with the Federal Court to ensure that it is fully transparent with the Court.
- The Federal Court agreed with CSIS' proposal to update warrants, and generally accepted the changes proposed by CSIS.
- In its decision, the Federal Court noted that the CSIS Act is now more than 30 years old and changes may need to be made to ensure that it keeps pace with changes in technology and the privacy expectations of Canadians. This is something that we will review.
- The Government is committed to keeping Canadians safe while at the same time safeguarding our freedoms, rights and values in an open and democratic society.
- We want to hear from Canadians on how we can best meet our dual objectives of security and rights. We invite all Canadians to provide us with their views and ideas on our national security framework through our online consultation, which is open until December 1<sup>st</sup>. ([www.canada.ca/national-security-consultation](http://www.canada.ca/national-security-consultation))
- Concurrently, we are taking measures to strengthen national security accountability. In June, we put forward legislation to create a National Security and Intelligence Committee of Parliamentarians which would have a broad mandate to scrutinize the activities of any federal department or agency with national security responsibilities, including operational matters.

**Ministerial Talking Point:**

- CSIS plays a vital role in keeping Canadians safe by investigating threats, and collecting and analyzing information to protect our national security. I continue to have confidence in their ability to deliver on that mandate.



---

# *Media Lines*

---

## **FEDERAL COURT “EN BANC” DECISION CSIS’ Authority to Retain Metadata Collected Through Warrants**

### **Key Messages:**

- The Government accepts the Federal Court’s findings on this matter.
- It is important to underline that the associated data was collected legally through warrants. The Federal Court’s key concern relates to CSIS’ retention of such data (e.g., date, time, and phone numbers related to a call) when it is not related to a threat to the security of Canada.
- CSIS is taking immediate action to address the Federal Court’s findings. CSIS halted all analysis of associated data as it actively works to assess and address the Federal Court’s decision.
- The Government also accepts the Federal Court’s findings regarding CSIS’ duty of candour to the Federal Court. The Government takes this finding very seriously. CSIS has committed to working with the Federal Court to ensure that it is fully transparent with the Court.
- The Federal Court agreed with CSIS’ proposal to update warrants, and generally accepted the changes proposed by CSIS.
- In its decision, the Federal Court noted that the CSIS Act is now more than 30 years old and changes may need to be made to ensure that it keeps pace with changes in technology and the privacy expectations of Canadians. This is something that we will review.
- The Government is committed to keeping Canadians safe while at the same time safeguarding our freedoms, rights and values in an open and democratic society.
- We want to hear from Canadians on how we can best meet our dual objectives of security and rights. We invite all Canadians to provide us with their views and ideas on our national security framework through our online consultation, which is open until December 1<sup>st</sup>. ([www.canada.ca/national-security-consultation](http://www.canada.ca/national-security-consultation))
- Concurrently, we are taking measures to strengthen national security accountability. In June, we put forward legislation to create a National Security and Intelligence Committee of Parliamentarians which would have a broad mandate to scrutinize the activities of any federal department or agency with national security responsibilities, including operational matters.

### **Ministerial Talking Point:**



CSIS plays a vital role in keeping Canadians safe by investigating threats, and collecting and analyzing information to protect our national security. I continue to have confidence in their ability to deliver on that mandate.

**Prepared by:** Julie Grenier

**Consulted:** NS Intelligence, CSIS Policy, Legal, Justice

**Approved by:**

John Davies, DG, NS Policy (approved)

Monik Beauregard, ADM, NCSB (approved)

Heather Magee, Director, Communications (approved)

Jamie Tomlinson, DG, Communications (pending)

MO (pending)

PCO (pending)

## Sayarh, Omar (PS/SP)

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Wednesday, October 19, 2016 2:55 PM  
**To:** Tomlinson, Jamie (PS/SP)  
**Cc:** Magee, Heather (PS/SP)  
**Subject:** For urgent DG Approval: En Banc Key Messages & TP  
**Attachments:** PS-SP-#1995114-v1E-Key\_Messages\_-\_En\_Banc\_Metadata.doc

**Importance:** High

Hi Jamie,

Attached for your urgent approval are the proposed key messages for the "En Banc" Federal Court case. I have provided a copy-and-paste below for easier reference on BlackBerry.

Thanks in advance,  
Julie Grenier  
Senior Communications Advisor / Conseillère principale de communications  
Portfolio Affairs and Communications Branch/  
Secteur des affaires du portefeuille et des communications  
Public Safety Canada / Sécurité publique du Canada  
Tel : 613-993-4415 | BB : 613-410-6059

### Key Messages:

- The Government accepts the Federal Court's findings on this matter.
- It is important to underline that the associated data was collected legally through warrants. The Federal Court's key concern relates to CSIS' retention of such data (e.g., date, time, and phone numbers related to a call) when it is not related to a threat to the security of Canada.
- CSIS is taking immediate action to address the Federal Court's findings. CSIS halted all analysis of associated data as it actively works to assess and address the Federal Court's decision.
- The Government also accepts the Federal Court's findings regarding CSIS' duty of candour to the Federal Court. The Government takes this finding very seriously. CSIS has committed to working with the Federal Court to ensure that it is fully transparent with the Court.
- The Federal Court agreed with CSIS' proposal to update warrants, and generally accepted the changes proposed by CSIS.
- In its decision, the Federal Court noted that the CSIS Act is now more than 30 years old and changes may need to be made to ensure that it keeps pace with changes in technology and the privacy expectations of Canadians. This is something that we will review.
- The Government is committed to keeping Canadians safe while at the same time safeguarding our freedoms, rights and values in an open and democratic society.

- We want to hear from Canadians on how we can best meet our dual objectives of security and rights. We invite all Canadians to provide us with their views and ideas on our national security framework through our online consultation, which is open until December 1<sup>st</sup>. ([www.canada.ca/national-security-consultation](http://www.canada.ca/national-security-consultation))
- Concurrently, we are taking measures to strengthen national security accountability. In June, we put forward legislation to create a National Security and Intelligence Committee of Parliamentarians which would have a broad mandate to scrutinize the activities of any federal department or agency with national security responsibilities, including operational matters.

**Ministerial Talking Point:**

- CSIS plays a vital role in keeping Canadians safe by investigating threats, and collecting and analyzing information to protect our national security. I continue to have confidence in their ability to deliver on that mandate.

**Pages 480 to / à 481  
are duplicates  
sont des duplicatas**

## Sayarh, Omar (PS/SP)

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Wednesday, October 19, 2016 2:59 PM  
**To:** Beauregard, Monik (PS/SP)  
**Cc:** Davies, John (PS/SP); Brender, James (PS/SP); Sousa, Michael (PS/SP); Khouri, Lisa (PS/SP)  
**Subject:** RE: For urgent ADM approval: En Banc Key Messages  
**Attachments:** PS-SP-#1995114-v1E-Key\_Messages\_-\_En\_Banc\_Metadata.doc

Hi Monik,

As per our conversation, I have updated the third bullet of the key messages.

**Previously:** Immediate action is being taking by CSIS to address the Federal Court's findings.

**Now:** CSIS is taking immediate action to address the Federal Court's findings.

This is moving now to DG Comms for approval, and up to MO in short order. Thank you!

Julie G

Tel : 613-993-4415 | BB : 613-410-6059

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Wednesday, October 19, 2016 2:25 PM  
**To:** Beauregard, Monik (PS/SP)  
**Cc:** Davies, John (PS/SP); Brender, James (PS/SP); Sousa, Michael (PS/SP); Khouri, Lisa (PS/SP)  
**Subject:** RE: For urgent ADM approval: En Banc Key Messages

Hi Monik,

Please use this version for your approvals.

Upon review, there was one missing piece from the Four Corners discussion that would likely be requested for Ministerial TPs. Adding this message, approved by John:

- CSIS plays a vital role in keeping Canadians safe by investigating threats, and collecting and analyzing information to protect our national security. I continue to have confidence in their ability to deliver on that mandate.

Lines are updated in the attached.

Julie G

Tel : 613-993-4415 | BB : 613-410-6059

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Wednesday, October 19, 2016 1:55 PM  
**To:** Beauregard, Monik (PS/SP)  
**Cc:** Davies, John (PS/SP); Brender, James (PS/SP); Sousa, Michael (PS/SP); Khouri, Lisa (PS/SP)  
**Subject:** For urgent ADM approval: En Banc Key Messages  
**Importance:** High

Hi Monik,

Attached for your urgent approval are the proposed key messages for the En Banc case. Your team has engaged Legal (cc'd) on messaging. In addition, CSIS Policy has reviewed.

PCO is eager to see our proposed messaging ASAP. Thanks in advance!

**KEY MESSAGES:**

- The Government accepts the Federal Court's findings on this matter.
- It is important to underline that the associated data was collected legally through warrants. The Federal Court's key concern relates to CSIS' retention of such data (e.g., date, time, and phone numbers related to a call) when it is not related to a threat to the security of Canada.
- Immediate action is being taking by CSIS to address the Federal Court's findings. CSIS halted all analysis of associated data as it actively works to assess and address the Federal Court's decision.
- The Government also accepts the Federal Court's findings regarding CSIS' duty of candour to the Federal Court. The Government takes this finding very seriously. CSIS has committed to working with the Federal Court to ensure that it is fully transparent with the Court.
- The Federal Court agreed with CSIS' proposal to update warrants, and generally accepted the changes proposed by CSIS.
- In its decision, the Federal Court also noted that the CSIS Act is now more than 30 years old and changes may need to be made to ensure that it keeps pace with changes in technology and the privacy expectations of Canadians. This is something that we will review.
- The Government is committed to keeping Canadians safe while at the same time safeguarding our freedoms, rights and values in an open and democratic society.
- We want to hear from Canadians on how we can best meet our dual objectives of security and rights. We invite all Canadians to provide us with their views and ideas on our national security framework through our online consultation, which is open until December 1<sup>st</sup>. ([www.canada.ca/national-security-consultation](http://www.canada.ca/national-security-consultation))
- Concurrently, we are taking measures to strengthen national security accountability. In June, we put forward legislation to create a National Security and Intelligence Committee of Parliamentarians which would have a broad mandate to scrutinize the activities of any federal department or agency with national security responsibilities, including operational matters.

Julie Grenier

Senior Communications Advisor / Conseillère principale de communications

Portfolio Affairs and Communications Branch/

Secteur des affaires du portefeuille et des communications

Public Safety Canada / Sécurité publique du Canada

Tel : 613-993-4415 | BB : 613-410-6059

**Pages 484 to / à 485  
are duplicates  
sont des duplicatas**

**Sayarh, Omar (PS/SP)**

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Wednesday, October 19, 2016 1:48 PM  
**To:** [REDACTED] (PS/SP)  
**Cc:** [REDACTED] (PS/SP); [REDACTED] (PS/SP)  
**Subject:** RE: PS-SP-#1995114-v1C-Key\_Messages\_-\_En\_Banc\_Metadata

Thanks for confirming. I will move to Monik now.

Julie G  
Tel : 613-993-4415 | BB : 613-410-6059

---

**From:** [REDACTED] (PS/SP)  
**Sent:** Wednesday, October 19, 2016 1:45 PM  
**To:** Grenier, Julie (PS/SP)  
**Cc:** Davies, John (PS/SP); [REDACTED] (PS/SP); [REDACTED]  
**Subject:** FW: PS-SP-#1995114-v1C-Key\_Messages\_-\_En\_Banc\_Metadata

Julie, see attached key messages. Have been reviewed by CSIS; track changes is their input. John has reviewed and approved.

Thanks,

[REDACTED]

---

**From:** [REDACTED]  
**Sent:** Wednesday, October 19, 2016 1:34 PM  
**To:** [REDACTED] (PS/SP); [REDACTED] (PS/SP)  
**Cc:** [REDACTED]  
**Subject:** PS-SP-#1995114-v1C-Key\_Messages\_-\_En\_Banc\_Metadata

Hi [REDACTED]

Hope you're doing well. Attached are proposed revisions. We included the extra line proposed. Thanks, [REDACTED]

**Page 487**  
**is a duplicate**  
**est un duplicata**



---

# Media Lines

---

## FEDERAL COURT "EN BANC" DECISION CSIS' Authority to Retain Metadata Collected Through Warrants

### Key Messages:

- The Government accepts the Federal Court's findings on this matter.
- It is important to underline that all the associated data was collected legally through warrants. The Federal Court's key concern relates to CSIS' retention of associated such data (e.g., date, time, and phone numbers related to a call) that when it is not related to a threat to the security of Canada.
- Immediate action is being taking by CSIS to address the Federal Court's findings. CSIS halted all analysis of associated data as it actively works to assess and address the Federal Court's decision.  

- The Government also accepts the Federal Court's findings regarding CSIS' duty of candour to the Federal Court. The Government takes this finding very seriously. CSIS has committed to working with the Federal Court to ensure that it is fully transparent with the Court.
- The Federal Court agreed with CSIS' proposal to update warrants, and generally accepted the changes proposed by CSIS.
- In its decision, the Federal Court also noted that the CSIS Act is now more than 30 years old and changes may need to be made to ensure that it keeps pace with changes in technology and the privacy expectations of Canadians. This is something that we will review.
- The Government is committed to keeping Canadians safe while at the same time safeguarding our freedoms, rights and values in an open and democratic society.
- We want to hear from Canadians on how we can best meet our dual objectives of security and rights. We invite all Canadians to provide us with their views and ideas on our national security framework through our online consultation, which is open until December 1<sup>st</sup>. ([www.canada.ca/national-security-consultation](http://www.canada.ca/national-security-consultation))
- Concurrently, we are taking measures to strengthen national security accountability. In June, we put forward legislation to create a National Security and Intelligence Committee of Parliamentarians which would have a broad mandate to scrutinize the activities of any federal department or agency with national security responsibilities, including operational matters.



**Prepared by:** Julie Grenier

**Consulting:** NS Intelligence, CSIS Policy, Legal, Justice

**Approved by:**

John Davies, DG, NS Policy (pending)

Monik Beauregard, ADM, NCSB (pending)

Heather Magee, Director, Communications (pending)

Jamie Tomlinson, DG, Communications (pending)

MO (pending)

PCO (pending)

**Sayarh, Omar (PS/SP)**

---

**From:** [REDACTED] (PS/SP)  
**Sent:** Wednesday, October 19, 2016 1:40 PM  
**To:** Davies, John (PS/SP)  
**Cc:** Grenier, Julie (PS/SP); [REDACTED] PS/SP  
**Subject:** FW: PS-SP-#1995114-v1C-Key\_Messages\_-\_En\_Banc\_Metadata  
**Attachments:** PS-SP-#1995114-v1C-Key\_Messages\_-\_En\_Banc\_Metadata.doc

John, here are lines with CSIS input in track changes.

[REDACTED]

---

**From:** [REDACTED]  
**Sent:** Wednesday, October 19, 2016 1:34 PM  
**To:** [REDACTED] (PS/SP); [REDACTED] (PS/SP)  
**Cc:** [REDACTED]  
**Subject:** PS-SP-#1995114-v1C-Key\_Messages\_-\_En\_Banc\_Metadata

Hi [REDACTED]

Hope you're doing well. Attached are proposed revisions. We included the extra line proposed. Thanks, [REDACTED]

**Pages 491 to / à 492  
are duplicates  
sont des duplicatas**

## Sayarh, Omar (PS/SP)

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Wednesday, October 19, 2016 12:34 PM  
**To:** [REDACTED] (PS/SP)  
**Cc:** [REDACTED] PS/SP  
**Subject:** FW: En Banc - Federal Court - Key Messages

FYI – I've looped in DoJ Comms.

Julie G  
Tel : 613-993-4415 | BB : 613-410-6059

---

**From:** Gowing, Andrew [<mailto:Andrew.Gowing@justice.gc.ca>]  
**Sent:** Wednesday, October 19, 2016 12:31 PM  
**To:** Grenier, Julie (PS/SP)  
**Subject:** RE: En Banc - Federal Court - Key Messages

Hi Julie

[REDACTED]

[REDACTED] If you could share the final version of this, as well as CSIS's lines, for information when they are available, that would be great.

Thanks  
-Andrew

Andrew Gowing  
Senior Communications Advisor | Conseiller principal en communications  
Litigation and Media Relations | Litiges et Relations publiques  
Department of Justice | Ministère de la Justice  
Ottawa, Canada K1A 0H8  
[andrew.gowing@justice.gc.ca](mailto:andrew.gowing@justice.gc.ca)  
613-808-5414  
Government of Canada | Gouvernement du Canada

**From:** Grenier, Julie (PS/SP) [<mailto:julie.grenier@canada.ca>]  
**Sent:** Wednesday, October 19, 2016 12:19 PM  
**To:** Gowing, Andrew <[Andrew.Gowing@justice.gc.ca](mailto:Andrew.Gowing@justice.gc.ca)>  
**Subject:** En Banc - Federal Court - Key Messages  
**Importance:** High

Hi Andrew,

[REDACTED]

Thanks!

Julie Grenier

Senior Communications Advisor / Conseillère principale de communications

Portfolio Affairs and Communications Branch/

Secteur des affaires du portefeuille et des communications

Public Safety Canada / Sécurité publique du Canada

Tel : 613-993-4415 | BB : 613-410-6059

## Sayarh, Omar (PS/SP)

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Wednesday, October 19, 2016 12:32 PM  
**To:** 'Gowing, Andrew'  
**Subject:** RE: En Banc - Federal Court - Key Messages

Thanks Andrew!

Julie G  
Tel : 613-993-4415 | BB : 613-410-6059

---

**From:** Gowing, Andrew [<mailto:Andrew.Gowing@justice.gc.ca>]  
**Sent:** Wednesday, October 19, 2016 12:31 PM  
**To:** Grenier, Julie (PS/SP)  
**Subject:** RE: En Banc - Federal Court - Key Messages

Hi Julie

If you could share the final version of this, as well as CSIS's lines, for information when they are available, that would be great.

Thanks  
-Andrew

Andrew Gowing  
Senior Communications Advisor | Conseiller principal en communications  
Litigation and Media Relations | Litiges et Relations publiques  
Department of Justice | Ministère de la Justice  
Ottawa, Canada K1A 0H8  
[andrew.gowing@justice.gc.ca](mailto:andrew.gowing@justice.gc.ca)  
613-808-5414  
Government of Canada | Gouvernement du Canada

**From:** Grenier, Julie (PS/SP) [<mailto:julie.grenier@canada.ca>]  
**Sent:** Wednesday, October 19, 2016 12:19 PM  
**To:** Gowing, Andrew <[Andrew.Gowing@justice.gc.ca](mailto:Andrew.Gowing@justice.gc.ca)>  
**Subject:** En Banc - Federal Court - Key Messages  
**Importance:** High

Hi Andrew,

Thanks!

Julie Grenier

Senior Communications Advisor / Conseillère principale de communications

Portfolio Affairs and Communications Branch/

Secteur des affaires du portefeuille et des communications

Public Safety Canada / Sécurité publique du Canada

Tel : 613-993-4415 | BB : 613-410-6059

**Sayarh, Omar (PS/SP)**

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Tuesday, October 18, 2016 12:14 PM  
**To:** [REDACTED] (PS/SP); [REDACTED] (PS/SP)  
**Subject:** For URGENT review: En Banc Key Messages  
**Attachments:** PS-SP-#1995114-v1-Key\_Messages\_-\_En\_Banc\_Metadata.doc

**Importance:** High

Hello,  
Request to urgently review the attached key messages.

\*\*Please advise if you will coordinate [REDACTED] approval. I'm happy to take care of it, unless you think it'll be more efficient to work directly with him on it. Just let me know.

Thanks,  
Julie G  
Tel : 613-993-4415 | BB : 613-410-6059



---

# *Media Lines*

---

## **FEDERAL COURT “EN BANC” DECISION CSIS’ Authority to Retain Metadata Collected Through Warrants**

### **Key Messages:**

- The Government accepts the decision of the Federal Court on the matter of CSIS’ authority to retain metadata collected through warrants.
- Immediate action is being taking by the Canadian Security Intelligence Service to address the concerns raised in the decision and comply with the direction of the Federal Court.
- It is important to underline that all metadata was collected legally through warrants. The Government trusts that the actions being taking by CSIS in light of this decision will resolve any concerns regarding its retention.
- CSIS plays a vital role in keeping Canadians safe by investigating threats, and collecting and analyzing information to protect our national security.
- The Government is committed to keeping Canadians safe while at the same time safeguarding our freedoms, rights and values in an open and democratic society.
- We want to hear from Canadians on how we can best meet our dual objectives of security and rights. We invite all Canadians to provide us with their views and ideas on our national security framework through our online consultation, which is open until December 1<sup>st</sup>: ([www.canada.ca/national-security-consultation](http://www.canada.ca/national-security-consultation))
- We are also taking measures to strengthen our national security accountability. In June, we put forward legislation to create a National Security and Intelligence Committee of Parliamentarians which would have a broad mandate to scrutinize the activities of any federal department or agency with national security responsibilities, including operational matters.

**Prepared by:** Julie Grenier

**Consulting:** NS Intelligence

**Approved by:**



**Sayarh, Omar (PS/SP)**

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Wednesday, October 19, 2016 12:07 PM  
**To:** Magee, Heather (PS/SP)  
**Subject:** Status of En Banc key messages

Hi Heather,

The En Banc key messages have gone through a couple rounds of review (PS Policy, Legal, DoJ), but we're still waiting on CSIS' input. It's critical that we consult them, as our messaging refers to actions they are taking in light of the decision. The messages were shared from Policy-to-Policy but I've also sent them to Tahera to see if she can help accelerate things from her side.

In the meantime, I've given Monik a heads-up that an urgent approval will be coming her way.

I am doing my best to move things forward and get the messages finalized urgently.

Thanks,  
Julie Grenier  
Senior Communications Advisor / Conseillère principale de communications  
Portfolio Affairs and Communications Branch/  
Secteur des affaires du portefeuille et des communications  
Public Safety Canada / Sécurité publique du Canada  
Tel : 613-993-4415 | BB : 613-410-6059

## Sayarh, Omar (PS/SP)

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Wednesday, October 19, 2016 11:59 AM  
**To:** [REDACTED]  
**Subject:** Latest: PS En Banc Key Messages  
**Attachments:** PS-SP-#1995114-v1C-Key\_Messages\_-\_En\_Banc\_Metadata.doc; PS-SP-#1995114-v1B-Key\_Messages\_-\_En\_Banc\_Metadata.doc

**Importance:** High

Hi [REDACTED]

Attached is the latest version of our key messages. I have attached clean, as well as tracked changes from the last version I sent you.

This was just shared Policy-to-Policy, but if you can help push things along from your side that would be greatly appreciated. Also, if you see any red flags, please notify me immediately.

Julie G  
Tel : 613-993-4415 | BB : 613-410-6059

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Wednesday, October 19, 2016 11:54 AM  
**To:** [REDACTED] (PS/SP); [REDACTED] (PS/SP)  
**Subject:** RE: En Banc Key Messages

[REDACTED]

I have no concerns with revisions. The only thing I've done is remove the word "Finally" from the beginning of the 5<sup>th</sup> bullet.

I've attached latest clean and a version with your tracked changes, in case that helps you for engaging CSIS. **Can you impart the urgency with them? We need their feedback urgently.**

Julie G  
Tel : 613-993-4415 | BB : 613-410-6059

---

**From:** [REDACTED] (PS/SP)  
**Sent:** Wednesday, October 19, 2016 11:35 AM  
**To:** Grenier, Julie (PS/SP); [REDACTED] (PS/SP)  
**Subject:** RE: En Banc Key Messages

Done. Let me know if the changes work for you.

Do you want me to send the revised text to CSIS policy?

Thanks,

[REDACTED]

**From:** Grenier, Julie (PS/SP)  
**Sent:** Wednesday, October 19, 2016 11:08 AM  
**To:** (PS/SP); (PS/SP)  
**Subject:** RE: En Banc Key Messages

Hi  
Here's the reference. You can tweak directly in the document.

Julie G  
Tel : 613-993-4415 | BB : 613-410-6059

**From:** Grenier, Julie (PS/SP)  
**Sent:** Wednesday, October 19, 2016 10:25 AM  
**To:** (PS/SP); (PS/SP)  
**Subject:** RE: En Banc Key Messages

In light of the fact that you shared lines with CSIS Policy, I went ahead and shared with CSIS Comms. As this is not a joint product, was thinking it would consultation only – no approvals from their shop. What I was planning to do was share back the next version you provide me, which includes CSIS input, so that everyone is on the same page.

Noon is a target, and I know it's tight. Please do your best with that timeline and keep me updated!

Julie G  
Tel : 613-993-4415 | BB : 613-410-6059

**From:** (PS/SP)  
**Sent:** Wednesday, October 19, 2016 10:20 AM  
**To:** Grenier, Julie (PS/SP); (PS/SP)  
**Subject:** RE: En Banc Key Messages

Julie, will be looking at revised lines now.

Have not heard from CSIS. Have advised that you want to get to MO by noon. How firm is that date? Will lines go through CSIS Comms as well?

Thanks,

**From:** Grenier, Julie (PS/SP)  
**Sent:** Wednesday, October 19, 2016 10:00 AM  
**To:** (PS/SP); (PS/SP)  
**Subject:** RE: En Banc Key Messages

As I review it again, I would be in favour of a key message that is clear and categorical.

Could we say this?

Moving forward, CSIS will no longer retain "associated data" collected incidentally as a result of executing Federal Court issued warrants.

Julie G  
Tel : 613-993-4415 | BB : 613-410-6059

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Wednesday, October 19, 2016 9:46 AM  
**To:** [REDACTED] (PS/SP); [REDACTED] (PS/SP)  
**Subject:** RE: En Banc Key Messages

Hi,

In keeping with our standard process of providing key messages in a document, I have popped the revised messages back into the Media Lines template.

A few things:

- I reordered some of the bullets. I think we need to be clear off the very top that we accept the findings.
- I re-inserted a line about the importance of CSIS as an agency that helps protect Canadians. This was something MO wanted to convey as part of the overall narrative.
- I also added an indicator that Government will review outdated CSIS Act. (If this is inaccurate, strike out, but this is my understanding.)

Thanks,  
Julie G  
Tel : 613-993-4415 | BB : 613-410-6059

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Wednesday, October 19, 2016 9:32 AM  
**To:** [REDACTED] (PS/SP); [REDACTED] (PS/SP)  
**Subject:** En Banc Key Messages  
**Importance:** High

PCO is flagging they are looking for our messages ASAP. We would like to get them to MO by noon. Any chance you'll get comments back from CSIS Policy very soon? [REDACTED]

Julie G  
Tel : 613-993-4415 | BB : 613-410-6059

---

**From:** [REDACTED] (PS/SP)  
**Sent:** Tuesday, October 18, 2016 6:28 PM  
**To:** Grenier, Julie (PS/SP); [REDACTED] (PS/SP)  
**Subject:** RE: For URGENT review: En Banc Key Messages

Note that I will be out of the office tomorrow morning, but will be available via Blackberry (and I will check it frequently).

If I do not respond, then please contact [REDACTED] directly.

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Tuesday, October 18, 2016 6:25 PM  
**To:** [REDACTED] (PS/SP); [REDACTED] (PS/SP)  
**Subject:** Re: For URGENT review: En Banc Key Messages

Got them. Thank you. Let's touch base first thing tomorrow.

Julie

Tel: 613-993-4415, BB: 613-410-6059

**From:** [REDACTED] (PS/SP)  
**Sent:** Tuesday, October 18, 2016 5:53 PM  
**To:** Grenier, Julie (PS/SP) [REDACTED] (PS/SP)  
**Subject:** RE: For URGENT review: En Banc Key Messages

Here are our revised lines. We are also sending these to CSIS policy so please do not send these up the line until we have received comments from them. Note that these have been given a preliminary review by John Davies. Note that

Media Lines:

- The Federal Court agreed with CSIS' view that the warrants needed to be updated and accepted most of the changes proposed by CSIS.
- However, the Federal Court also made a clear pronouncement on the authority of CSIS to retain "associated data" collected incidentally as a result of executing Federal Court issued warrants.
- The Government accepts the Federal Court's findings on this matter.
- Immediate action is being taking by the Canadian Security Intelligence Service to address the Federal Court's findings. [REDACTED]
- It is important to underline that all associated data was collected legally through warrants. The Federal Court's key concern relates to CSIS' retention and use of associated data after it was collected. The Government trusts that the actions being taking by CSIS in light of this decision will resolve any concerns regarding its retention.
- The Government also accepts the Federal Court's findings regarding CSIS' duty of candour to the Federal Court. The Government takes this finding very seriously. CSIS can and will do more to ensure that it is fully, clearly, and substantially transparent with the Federal Court regarding the use it makes or plans to make of the information it collects pursuant to Federal Court issued warrants.
- The Federal Court has noted that the CSIS Act is now more than 30 years old and changes may need to be made to ensure that it keeps pace with changes in technology and the privacy expectations of Canadians.
- The Government is committed to keeping Canadians safe while at the same time safeguarding our freedoms, rights and values in an open and democratic society.
- We want to hear from Canadians on how we can best meet our dual objectives of security and rights. The national security consultations are an important opportunity for Canadians to make their voices heard on how we can bring the mandate and authorities of our security and intelligence agencies into the modern age. We invite all Canadians to provide us with their views and ideas on our national security framework through our online consultation, which is open until December 1<sup>st</sup>. ([www.canada.ca/national-security-consultation](http://www.canada.ca/national-security-consultation))
- We are also taking measures to strengthen our national security accountability. In June, we put forward legislation to create a National Security and Intelligence Committee of Parliamentarians which would have

a broad mandate to scrutinize the activities of any federal department or agency with national security responsibilities, including operational matters.

---

**From:** [REDACTED] (PS/SP)  
**Sent:** Tuesday, October 18, 2016 5:43 PM  
**To:** Grenier, Julie (PS/SP); [REDACTED] (PS/SP)  
**Subject:** RE: For URGENT review: En Banc Key Messages

I'm about to send you our revised lines. Can you call me once you have received them?

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Tuesday, October 18, 2016 4:02 PM  
**To:** [REDACTED] (PS/SP); [REDACTED] (PS/SP)  
**Subject:** RE: For URGENT review: En Banc Key Messages

Thanks [REDACTED]

I'll look at what you send back before sending the Qs&As. We may need to meet to discuss the latter as I don't have enough knowledge to propose responses.

Let's discuss after you send back the key messages. Thanks!

Julie G  
Tel : 613-993-4415 | BB : 613-410-6059

---

**From:** [REDACTED] (PS/SP)  
**Sent:** Tuesday, October 18, 2016 3:59 PM  
**To:** Grenier, Julie (PS/SP); [REDACTED] (PS/SP)  
**Subject:** RE: For URGENT review: En Banc Key Messages

We're on it – you should hear from us soon.

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Tuesday, October 18, 2016 3:42 PM  
**To:** [REDACTED] (PS/SP); [REDACTED] (PS/SP)  
**Subject:** RE: For URGENT review: En Banc Key Messages

Hi,

[REDACTED]  
[REDACTED] Thanks!

Julie G  
Tel : 613-993-4415 | BB : 613-410-6059

---

**From:** [REDACTED] (PS/SP)  
**Sent:** Tuesday, October 18, 2016 2:10 PM

**To:** Grenier, Julie (PS/SP); [REDACTED] (PS/SP)  
**Subject:** RE: For URGENT review: En Banc Key Messages

We will be a bit later than 2:30 pm. But a top priority for us and will move asap.

Let us know if anything changes on your end. We'll do the same.

[REDACTED]

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Tuesday, October 18, 2016 1:59 PM  
**To:** [REDACTED] (PS/SP); [REDACTED] (PS/SP)  
**Subject:** RE: For URGENT review: En Banc Key Messages

There's an expectation we'll have key messages to MO today, flowing from the direction they provided @ Four Corners Meeting this morning. PMO wants to see messaging.

If you can secure John's approval, I can coordinate Monik's approval and Comms. (If you want to me to secure John's approval, I can definitely do that – just let me know)

Any chance I can have messages back by 2:30?

Qs&As are being treated a second wave, but nevertheless a priority to finalize.

We don't yet have messaging from CSIS.

Julie G  
Tel : 613-993-4415 | BB : 613-410-6059

---

**From:** [REDACTED] (PS/SP)  
**Sent:** Tuesday, October 18, 2016 1:53 PM  
**To:** Grenier, Julie (PS/SP); [REDACTED] (PS/SP)  
**Subject:** RE: For URGENT review: En Banc Key Messages

Confirmed. What are timelines?

[REDACTED]

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Tuesday, October 18, 2016 1:52 PM  
**To:** [REDACTED] (PS/SP); [REDACTED] (PS/SP)  
**Subject:** RE: For URGENT review: En Banc Key Messages  
**Importance:** High

Hi,  
Request to please confirm you're looking at this.

I'll have a handful of Qs&As for you to review shortly.

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Tuesday, October 18, 2016 12:14 PM

**To:** ██████████ (PS/SP); ██████████ (PS/SP)  
**Subject:** For URGENT review: En Banc Key Messages  
**Importance:** High

Hello,  
Request to urgently review the attached key messages.

\*\*Please advise if you will coordinate John's approval. I'm happy to take care of it, unless you think it'll be more efficient to work directly with him on it. Just let me know.

Thanks,  
Julie G  
Tel : 613-993-4415 | BB : 613-410-6059



---

# *Media Lines*

---

## **FEDERAL COURT "EN BANC" DECISION CSIS' Authority to Retain Metadata Collected Through Warrants**

### **Key Messages:**

- The Government accepts the Federal Court's findings on this matter.
- It is important to underline that all associated data was collected legally through warrants. The Federal Court's key concern relates to CSIS' retention of associated data (e.g., date, time, and phone numbers related to a call) that is not related to a threat to the security of Canada.
- Immediate action is being taking by CSIS to address the Federal Court's findings.

- 
- The Government also accepts the Federal Court's findings regarding CSIS' duty of candour to the Federal Court. The Government takes this finding very seriously. CSIS has committed to working with the Federal Court to ensure that it is fully transparent with the Court.
  - The Federal Court agreed with CSIS' proposal to update warrants, and generally accepted the changes proposed by CSIS.
  - In its decision, the Federal Court also noted that the CSIS Act is now more than 30 years old and changes may need to be made to ensure that it keeps pace with changes in technology and the privacy expectations of Canadians. This is something that we will review.
  - The Government is committed to keeping Canadians safe while at the same time safeguarding our freedoms, rights and values in an open and democratic society.
  - We want to hear from Canadians on how we can best meet our dual objectives of security and rights. We invite all Canadians to provide us with their views and ideas on our national security framework through our online consultation, which is open until December 1<sup>st</sup>. ([www.canada.ca/national-security-consultation](http://www.canada.ca/national-security-consultation))
  - Concurrently, we are taking measures to strengthen national security accountability. In June, we put forward legislation to create a National Security and Intelligence Committee of Parliamentarians which would have a broad mandate to scrutinize the activities of any federal department or agency with national security responsibilities, including operational matters.



**Prepared by:** Julie Grenier

**Consulting:** NS Intelligence, CSIS Policy, Legal, Justice

**Approved by:**

John Davies, DG, NS Policy (pending)

Monik Beauregard, ADM, NCSB (pending)

Heather Magee, Director, Communications (pending)

Jamie Tomlinson, DG, Communications (pending)

MO (pending)

PCO (pending)

# Media Lines

## FEDERAL COURT "EN BANC" DECISION CSIS' Authority to Retain Metadata Collected Through Warrants

### Key Messages:

• The Government accepts the Federal Court's findings on this matter.

• It is important to underline that all associated data was collected legally through warrants. The Federal Court's key concern relates to CSIS' retention of associated data (e.g., date, time, and phone numbers related to a call) that is not related to a threat to the security of Canada.

Formatted: English (U.S.)

Formatted: Indent: Left: 0.25", No bullets or numbering, Tab stops: Not at 0.25"

• Immediate action is being taking by CSIS to address the Federal Court's findings.

[Redacted]

• ~~The Federal Court agreed with CSIS' view that the warrants needed to be updated and accepted most of the changes proposed by CSIS.~~

Formatted: Tab stops: 0.25", List tab + Not at 0.5"

[Redacted]

Formatted: No bullets or numbering, Tab stops: Not at 0.25"

• The Government also accepts the Federal Court's findings regarding CSIS' duty of candour to the Federal Court. The Government takes this finding very seriously. CSIS has committed to working with the Federal Court to ensure that it is fully; [Redacted] transparent with the Federal Court.

[Redacted]

• Finally, the Federal Court agreed with CSIS' proposal to update warrants, and generally accepted the changes proposed by CSIS.

Formatted: Indent: Left: 0.25", No bullets or numbering

• ~~CSIS plays a vital role in keeping Canadians safe by investigating threats, and collecting and analyzing information to protect our national security.~~

• In its decision, tThe Federal Court has also noted that the CSIS Act is now more than 30 years old and changes may need to be made to ensure that it keeps pace with changes in technology and the privacy expectations of Canadians. This is something that we will review.

- The Government is committed to keeping Canadians safe while at the same time safeguarding our freedoms, rights and values in an open and democratic society.
- We want to hear from Canadians on how we can best meet our dual objectives of security and rights. We invite all Canadians to provide us with their views and ideas on our national security framework through our online consultation, which is open until December 1<sup>st</sup>. ([www.canada.ca/national-security-consultation](http://www.canada.ca/national-security-consultation))
- ~~Concurrently, w~~~~We~~ ~~are also~~ taking measures to strengthen national security accountability. In June, we put forward legislation to create a National Security and Intelligence Committee of Parliamentarians which would have a broad mandate to scrutinize the activities of any federal department or agency with national security responsibilities, including operational matters.

**Prepared by:** Julie Grenier

**Consulting:** NS Intelligence, CSIS Policy, Legal, Justice

**Approved by:**

John Davies, DG, NS Policy (pending)

Monik Beaugard, ADM, NCSB (pending)

Heather Magee, Director, Communications (pending)

Jamie Tomlinson, DG, Communications (pending)

MO (pending)

PCO (pending)

## Sayarh, Omar (PS/SP)

---

**From:** Grenier, Julie (PS/SP)  
**Sent:** Wednesday, October 19, 2016 9:54 AM  
**To:** [REDACTED]  
**Subject:** RE: En Banc  
**Attachments:** PS-SP-#1995114-v1A-Key\_Messages\_-\_En\_Banc\_Metadata.doc

Thanks [REDACTED] We understand the decision won't come out until Friday afternoon at the earliest, but PCO is looking for PS key messages ASAP today.

It's come to my attention that PS Policy sent the draft lines to CSIS Policy late yesterday. As far as I know, they haven't heard back from your Policy shop yet. I've attached the draft for your awareness.

Thanks,  
Julie G  
Tel : 613-993-4415 | BB : 613-410-6059

---

**From:** [REDACTED]  
**Sent:** Wednesday, October 19, 2016 9:51 AM  
**To:** Grenier, Julie (PS/SP)  
**Subject:** RE: En Banc

Hi Julie,

I was out of the office yesterday. I am working on something now. I will share as soon as I have the go ahead.

Stay tuned,  
Thx  
[REDACTED]

---

**From:** Grenier, Julie (PS/SP) [<mailto:julie.grenier@canada.ca>]  
**Sent:** 18-Oct-16 3:51 PM  
**To:** [REDACTED]  
**Subject:** En Banc

Hi [REDACTED]

Wondering if you might be in a position to share your En Banc materials (ie. media lines, Qs&As)

I've been tasked with key messages and Qs&As for my Minister, and want to ensure consistency of language, where applicable.

Thanks in advance,  
Julie Grenier  
Senior Communications Advisor / Conseillère principale de communications  
Portfolio Affairs and Communications Branch/  
Secteur des affaires du portefeuille et des communications  
Public Safety Canada / Sécurité publique du Canada

Tel : 613-993-4415 | BB : 613-410-6059



---

# Media Lines

---

## FEDERAL COURT “EN BANC” DECISION CSIS’ Authority to Retain Metadata Collected Through Warrants

### Key Messages:

- The Government accepts the Federal Court’s findings on this matter.
- Immediate action is being taking by the Canadian Security Intelligence Service to address the Federal Court’s findings.
- The Federal Court agreed with CSIS’ view that the warrants needed to be updated and accepted most of the changes proposed by CSIS.
- It is important to underline that all associated data was collected legally through warrants. The Federal Court’s key concern relates to CSIS’ retention and use of associated data after it was collected. The Government trusts that the actions being taking by CSIS in light of this decision will resolve any concerns regarding its retention.
- The Government also accepts the Federal Court’s findings regarding CSIS’ duty of candour to the Federal Court. The Government takes this finding very seriously. CSIS can and will do more to ensure that it is fully, clearly, and substantially transparent with the Federal Court regarding the use it makes or plans to make of the information it collects pursuant to Federal Court issued warrants.
- CSIS plays a vital role in keeping Canadians safe by investigating threats, and collecting and analyzing information to protect our national security.
- The Federal Court has noted that the CSIS Act is now more than 30 years old and changes may need to be made to ensure that it keeps pace with changes in technology and the privacy expectations of Canadians. This is something we’ll review.
- The Government is committed to keeping Canadians safe while at the same time safeguarding our freedoms, rights and values in an open and democratic society.
- We want to hear from Canadians on how we can best meet our dual objectives of security and rights. We invite all Canadians to provide us with their views and ideas on our national security framework through our online consultation, which is open until December 1<sup>st</sup>. ([www.canada.ca/national-security-consultation](http://www.canada.ca/national-security-consultation))



- We are also taking measures to strengthen our national security accountability. In June, we put forward legislation to create a National Security and Intelligence Committee of Parliamentarians which would have a broad mandate to scrutinize the activities of any federal department or agency with national security responsibilities, including operational matters.

**Prepared by:** Julie Grenier

**Consulting:** NS Intelligence, CSIS Policy, Legal, Justice

**Approved by:**

John Davies, DG, NS Policy (pending)

Monik Beauregard, ADM, NCSB (pending)

Heather Magee, Director, Communications (pending)

Jamie Tomlinson, DG, Communications (pending)

MO (pending)

PCO (pending)



Public Safety / Sécurité publique  
Canada / Canada

Senior Assistant / Sous-ministre  
Deputy Minister / adjoint(e) principal(e)

Ottawa, Canada  
K1A 0P8

*Beek pg 1*

*J*

**SECRET**

NOV 02 2015

DATE: OCT 27 2015

File No.: 6045 / 23673 / 006779

RDIMS No.: 33676

**MEMORANDUM FOR THE DEPUTY MINISTER**

**SECURITY AND INTELLIGENCE REVIEW COMMITTEE  
2014-15 ANNUAL REPORT**

(Information Only)

**ISSUE**

To provide you with an overview of the 2014-15 Security Intelligence Review Committee (SIRC) Annual Report. (Tab A)

**BACKGROUND**

The Department received SIRC's report on September 30, 2015. In addition to certifying the annual report to the Minister from the Director of the Canadian Security Intelligence Service (CSIS), SIRC's report contains nine reviews into CSIS activities and five investigations into complaints against CSIS.

Per section 53 of the *CSIS Act*, the new Minister of Public Safety and Emergency Preparedness must table the report on one of the first 15 days on which the next Parliament sits.

**REPORT OVERVIEW**

SIRC found that, overall, the conduct of CSIS in carrying out its mandate was satisfactory. With one exception (regarding the possible contravention of the *UN Al-Qaeda and Taliban Regulations* - addressed below) SIRC found that the activities described in the Director's report complied with the law and Ministerial Direction (MD), and were reasonable and necessary. Most of the activities examined by SIRC during reviews did not raise serious concerns. In its investigations, SIRC dismissed all but one of the complaints made against CSIS. CSIS fully agreed with 10 of the 18 recommendations made by SIRC (see Tab B for more information).

However, there are also number of issues with the potential to attract media attention and controversy.

### **Concerns CSIS may have Contravened the *UN Al-Qaeda and Taliban Regulations***

SIRC found that CSIS lacks a procedure to verify whether current or past human source operations are in contravention of section 3 of the *UN Al-Qaeda and Taliban Regulations* (UNAQTR).<sup>1</sup> SIRC notes that this was the only area where it was unable to certify that CSIS activities described in the Director's report

CSIS has agreed to update its human source protocols to ensure their compliance with UNAQTR and similar legislation. However, SIRC has also invoked a rarely used clause of the *CSIS Act* to direct CSIS to review whether specific human source activities have already contravened Canadian law. The Director's 2015-16 report will contain the findings of this review and is expected to be submitted to the Minister in spring 2016.

### **A CSIS Regional Office Repeatedly Obtained Taxpayer Information without a Warrant**

The Director made an exceptional request that SIRC review an incident where an intelligence officer obtained information from the Canada Revenue Agency (CRA) without a warrant. SIRC found that "this was not an isolated incident ... there were multiple instances of a particular CSIS (regional) office obtaining from CRA absent a warrant." SIRC also found that the management of this issue by CSIS was "not adequate." Finally, SIRC found that CSIS had retained the improperly-gathered information in its holdings after informing the Minister and the Federal Court it had been deleted. SIRC also indicated that it could not make a recommendation on how to prevent a reoccurrence of this activity because CSIS did not provide, "any explanation to account for the full scope of improper collection of taxpayer information." You may wish to note that, under the *Security of Canada Information Sharing Act* (SCISA), CSIS no longer requires a warrant to obtain information from the CRA.

### **Concerns that Warrant Applications Obscure CSIS Metadata Practices**

Through its communications intercepts CSIS incidentally collects information, including communications metadata<sup>2</sup>, on persons other than warranted targets. Warrant conditions require that CSIS destroy such information unless it "may assist" with an investigation. SIRC found that CSIS interpreted the "may assist" provision as a "low threshold" which allowed CSIS to retain and use metadata which did not directly pertain to warranted targets. CSIS eventually changed the language of warrant conditions to better reflect its existing practice. According to SIRC, however, this had the effect of rendering the warrants "on questions of metadata use and retention."

<sup>1</sup> Section 3 of the UNAQTR prohibits the provision of funds to individuals associated with the Taliban or Al Qaeda. The UNAQTR implement UN Security Council Resolutions and are legally binding under the *United Nations Act*.

SECRET

- 3 -

The Federal Court raised the issue of the new warrant language in late 2011, and SIRC has received "no indication that (CSIS) was fully transparent with the Federal Court about the nature and scope of its activities with respect to metadata in the context of that discussion." SIRC's position is that CSIS metadata practices should be specifically included in warrants, as they are distinct from the traditional way in which CSIS uses communications intercepts to support investigations. CSIS disagrees with this position and its accompanying recommendation. CSIS maintains that it was fully transparent with the Court. W

### Concerns over CSIS Accountability

SIRC writes that excessive length and detail of the Director's report, "has the effect of effect of obscuring ... serious issues, challenges, and potentially controversial activities." In addition to the Director's report, CSIS is also required to notify the Minister of

SIRC found that the threshold by which CSIS determined what constituted "high risk" was likely too narrow. This may have prevented the Minister from being sufficiently informed and "taking appropriate corrective action" if necessary. SIRC notes that these issues are especially problematic in light of the new mandate for CSIS to undertake threat-reduction activities (TRAs). SIRC recommended a new MD which corrects these issues. The new MD for Operations and Accountability which came into effect in July addresses the issues raised by SIRC, but its existence is not yet public knowledge.

### Strategic Issues

SIRC emphasizes the "significant resource commitment" required to meet responsibilities such as the obligation to review TRAs, and to respond to the expanding foreign presence of CSIS. While SIRC notes in the report that it welcomes increased resources under the latest budget, in fact SIRC has yet to receive these funds because

SIRC has informally indicated to the Department that SIRC is prepared to raise this issue in the event it is the subject of a media enquiry.

SIRC's report also notes consequences of measures taken against the terrorist threat in the past year. In its review of CSIS's foreign fighter investigations, "SIRC heard concerns this significant operational shift (toward counter-terrorism) could result in a loss of investigative capacity in counter-intelligence and counter-proliferation areas in the long-term." This is a concern of the Department as well.

SECRET

RECOMMENDATION

The approval of SCISA and the updated MD for Operations and Accountability address some of the concerns SIRC has raised. One key outstanding issue, however, is

At the direction of SIRC, CSIS is currently reviewing this matter. The Director will include the findings of this review in his upcoming report to the Minister. SIRC will assess the methodology and findings of the review as part of its certification process. The Department will be in a better position to determine next steps once it has reviewed the findings of both CSIS and SIRC.

In the short term, we will provide the Minister with additional information drawn from classified SIRC reports under separate cover.

We will also enquire whether SIRC would be willing to brief the Minister on its work over the past year.

Should you require additional information, please do not hesitate to contact me or Ms. Ritu Banerjee, Acting Director General, National Security Policy Directorate, at 613-991-1979.

John Davies

Prepared by: Dashiell Dronyk

agree

① will be important to bring up in these reports in general and this one specifically  
② will be critical to explain why in some cases, the Director disagree with us as in this case, a previous that very few of us have...

SECRET / [REDACTED]

**SIRC Recommendations Fully Agreed to by CSIS**

<b>SIRC Review</b>	<b>Recommendation</b>
The "Insider Threat" and its Effect on Information Management	<ul style="list-style-type: none"> <li>• CSIS should create a more detailed policy on the conduct of Internal Security investigations</li> <li>• CSIS should ensure that decision making pertaining to internal investigations is documented appropriately</li> </ul>
CSIS's Relationship and Exchanges with DFATD	<ul style="list-style-type: none"> <li>• CSIS should establish formal mechanisms to ensure that human source operations do not contravene UNAQTR or similar Canadian statute or regulations</li> </ul>
A Counter-Terrorism Investigation	<ul style="list-style-type: none"> <li>• CSIS employees should be required record the justification for the decision to accept or dismiss internal expert advice acquired through mandatory consultation</li> </ul>
CSIS's Use of Metadata	<ul style="list-style-type: none"> <li>• CSIS should enhance feedback on the utility of specific surveillance operations to guide the future direction of this program</li> </ul>
SIRC's Inquiry to CSIS's Collection of CRA , Information	<ul style="list-style-type: none"> <li>• CSIS should conduct a post-mortem to assess the adequacy of its management of the incident in question</li> <li>• CSIS should clarify the scope of the incident to the Federal Court and the Minister</li> <li>• CSIS should advise the Privacy Commissioner of the incident</li> </ul>
Denial of CSIS Site Access Security Clearance (Complaint)	<ul style="list-style-type: none"> <li>• All regional offices should adopt the new Site Access Certification direction implemented at the regional office subject to the complaint</li> <li>• The CSIS Site Access Certification program should be reviewed in light of the new Treasury Board Standard on Security Screening</li> </ul>

SECRET

**SIRC Recommendations Rejected in Full or in Part by CSIS**

SIRC Review	Recommendations	CSIS Responses
<p>The "Insider Threat" and its Effect on Information Management</p>	<ul style="list-style-type: none"> <li>• CSIS should develop robust procedures governing access lists</li> </ul>	<ul style="list-style-type: none"> <li>• CSIS agrees in principle, but has a different approach to implementation</li> </ul>
	<ul style="list-style-type: none"> <li>• CSIS should create a robust training/mentoring program suited to the unique work of Internal Security investigators</li> </ul>	<ul style="list-style-type: none"> <li>• CSIS believes formal intelligence officer training is sufficient, but there may be an opportunity to review the current informal mentoring process and produce guidelines on best practices</li> </ul>
	<ul style="list-style-type: none"> <li>• CSIS should re-examine a specific internal investigation in its entirety in light of concerns over violations of internal policy and possible information breaches</li> </ul>	<ul style="list-style-type: none"> <li>• The Director is satisfied with the outcome of the investigation</li> </ul>
	<ul style="list-style-type: none"> <li>• CSIS Internal Security should forward final investigation reports to a group outside this branch</li> </ul>	<ul style="list-style-type: none"> <li>• CSIS believes forwarding reports to an outside unit would jeopardize the confidentiality and sensitivity of internal investigations</li> </ul>
<p>CSIS's Relationship and Exchanges with DFATD</p>	<ul style="list-style-type: none"> <li>• CSIS should renegotiate its 2007 protocol with DFATD</li> </ul>	<ul style="list-style-type: none"> <li>• CSIS will discuss the protocol during regular engagements between CSIS and DFATD senior management</li> </ul>
	<ul style="list-style-type: none"> <li>• CSIS and DFATD should create clear deconfliction guidelines</li> </ul>	<ul style="list-style-type: none"> <li>• CSIS will discuss areas where existing deconfliction processes may not be adequate during regular meetings with DFATD at all levels</li> </ul>
<p>CSIS's Use of Metadata</p>	<ul style="list-style-type: none"> <li>• CSIS should make the Federal Court aware of its specific metadata use and retention practices</li> </ul>	<ul style="list-style-type: none"> <li>• CSIS's position is that s.21 of the <i>CSIS Act</i> does not confer general supervisory authority on the Court. CSIS maintains that it clearly communicated its position on metadata to the Court in 2011</li> </ul>
<p>SIRC's Inquiry to CSIS's Collection of CRA Information</p>	<ul style="list-style-type: none"> <li>• The CSIS Audit Unit should address any substandard managerial and communication practices by the CSIS regional office involved in this incident</li> </ul>	<ul style="list-style-type: none"> <li>• CSIS believes the actions it has already taken in response to the incident are similar to those which would have been taken during an audit</li> </ul>



Public Safety Canada / Sécurité publique Canada

Deputy Minister / Sous-ministre

Ottawa, Canada  
K1A 0P8

**COPY**  
*Karime*

*Pls book a briefing  
on a priority basis  
on this topic  
key is to explain  
why 10 out of 18 recs  
are accepted  
and next  
steps*

**SECRET // CEO**

DATE:

File No.: 1307-412 / PS-003602

RDIMS No.: 34872

**MEMORANDUM FOR THE MINISTER**

**SECURITY AND INTELLIGENCE  
REVIEW COMMITTEE 2014-2015 ANNUAL REPORT**

(Signature required)

*Merci  
J*

**ISSUE**

Tabling of the Security Intelligence Review Committee (SIRC) 2014-2015 Annual Report.

JAN 18 2016

**BACKGROUND**

The Department received the report on September 29, 2015. Section 53 of the *Canadian Security Intelligence Service Act* (the Act) requires the Minister of Public Safety and Emergency Preparedness to table the Annual Report in both Houses on one of the first 15 days on which the next Parliament sits.

**REPORT OVERVIEW**

SIRC's annual report assesses Canadian Security Intelligence Service (CSIS) performance through SIRC's three key activities: certification, review, and complaints investigations.

**Certificate**

With one exception (regarding the *UN Al-Qaeda and Taliban Regulations*, addressed below) SIRC found that the activities described in the CSIS Director's Annual Report complied with the law and Ministerial Direction (MD). However, SIRC writes that excessive length and detail of the report risks obscuring "potentially controversial activities". SIRC also had concerns about CSIS's procedure for notifying you of "high risk" activities.

**Reviews**

CSIS fully agreed with 10 of the 18 recommendations made by SIRC in its report (TAB E). However, certain issues raised in the report may attract media attention and controversy.

**SECRET** [REDACTED]

- 2 -

**SIRC found that SCRS lacks a procedure to verify whether current or past human source operations are in contravention of section 3 of the *UN Al-Qaeda and Taliban Regulations (UNAQTR)*.**<sup>1</sup> SIRC notes that this was the only area where it was unable to certify that CSIS activities described in the Director's report did not contravene the law or MD. CSIS is updating human source protocols in light of these findings. However, SIRC has also invoked a rarely used clause of the *CSIS Act* to direct CSIS to review its compliance with laws and regulations implementing the decisions of international organizations of which Canada is a member. The next Director's report (expected in spring 2016) will contain the findings of this review.

**SIRC found that, on multiple occasions, a CSIS regional office obtained taxpayer information without a warrant.** The Director made the exceptional request that SIRC review an incident where an intelligence officer improperly obtained information from the Canada Revenue Agency. SIRC found that this was not an isolated case and that CSIS's management of the incident was "not adequate". SIRC also found that CSIS did not explain "the full scope of improper collection of taxpayer information", and that CSIS had retained the improperly-gathered information after informing the Minister and the Federal Court otherwise. CSIS agreed to conduct a post-mortem of the incident and provided its findings to SIRC. CSIS also agreed to clarify the scope of the incident to your predecessor and the Federal Court, and to advise the Privacy Commissioner of these events.

**SIRC found that CSIS may not have been fully transparent with the Federal Court regarding CSIS's use and retention of metadata.** SIRC's report notes that CSIS has long interpreted warrant conditions to allow CSIS to retain and use communications metadata<sup>2</sup> incidentally collected through intercepts on warranted targets. CSIS eventually reworded warrant conditions in way which rendered them [REDACTED] on this issue, according to SIRC. SIRC's position is that CSIS's metadata practices are distinct enough to be specifically included in warrant applications. CSIS disagrees with this position and maintains it has been fully transparent with the Court.

**The report notes a key challenge for CSIS going forward.** In its review of a foreign fighters investigation SIRC noted concerns from SIRC that its recent "significant operational shift" toward counter-terrorism could degrade its investigative capacity in the counter-intelligence and counter-proliferation areas in the long-term.

### **Complaints**

SIRC dismissed all but one of the complaints made against CSIS. The exception involved an individual whom SIRC determined had been erroneously denied a site access clearance for a CSIS location. In light of SIRC's findings, CSIS has agreed to review its Site Access Certificate Program.

---

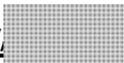
<sup>1</sup> Section 3 of the UNAQTR prohibits the provision of funds to individuals associated with the Taliban or Al Qaeda. The UNAQTR implement UN Security Council Resolutions and are legally binding under the *United Nations Act*.



Public Safety    Sécurité publique  
Canada            Canada

Deputy Minister    Sous-ministre

Ottawa, Canada  
K1A 0P8

**SECRET** / 

DATE: **JAN 26 2016**

File No.: 1307-412 / PS-003602

RDIMS No.: 34872

**MEMORANDUM FOR THE MINISTER**

**SECURITY AND INTELLIGENCE  
REVIEW COMMITTEE 2014-2015 ANNUAL REPORT**

(Signature required)

**ISSUE**

Tabling of the Security Intelligence Review Committee (SIRC) 2014-2015 Annual Report.

**BACKGROUND**

The Department received the report on September 29, 2015. Section 53 of the *Canadian Security Intelligence Service Act* (the Act) requires the Minister of Public Safety and Emergency Preparedness to table the Annual Report in both Houses on one of the first 15 days on which the next Parliament sits.

**REPORT OVERVIEW**

SIRC's annual report assesses Canadian Security Intelligence Service (CSIS) performance through SIRC's three key activities: certification, review, and complaints investigations.

**Certificate**

With one exception (regarding the *UN Al-Qaeda and Taliban Regulations*, addressed below) SIRC found that the activities described in the CSIS Director's Annual Report complied with the law and Ministerial Direction (MD). However, SIRC writes that excessive length and detail of the report risks obscuring "potentially controversial activities". SIRC also had concerns about CSIS's procedure for notifying you of "high risk" activities.

**Reviews**

CSIS fully agreed with 10 of the 18 recommendations made by SIRC in its report (TAB E). However, certain issues raised in the report may attract media attention and controversy.

**Canada**

**SECRET**

- 2 -

**SIRC found that SCRS lacks a procedure to verify whether current or past human source operations are in contravention of section 3 of the *UN Al-Qaeda and Taliban Regulations (UNAQTR)*.**<sup>1</sup> SIRC notes that this was the only area where it was unable to certify that CSIS activities described in the Director's report did not contravene the law or MD. CSIS is updating human source protocols in light of these findings. However, SIRC has also invoked a rarely used clause of the *CSIS Act* to direct CSIS to review its compliance with laws and regulations implementing the decisions of international organizations of which Canada is a member. The next Director's report (expected in spring 2016) will contain the findings of this review.

**SIRC found that, on multiple occasions, a CSIS regional office obtained taxpayer information without a warrant.** The Director made the exceptional request that SIRC review an incident where an intelligence officer improperly obtained information from the Canada Revenue Agency. SIRC found that this was not an isolated case and that CSIS's management of the incident was "not adequate". SIRC also found that CSIS did not explain "the full scope of improper collection of taxpayer information", and that CSIS had retained the improperly-gathered information after informing the Minister and the Federal Court otherwise. CSIS agreed to conduct a post-mortem of the incident and provided its findings to SIRC. CSIS also agreed to clarify the scope of the incident to your predecessor and the Federal Court, and to advise the Privacy Commissioner of these events.

**SIRC found that CSIS may not have been fully transparent with the Federal Court regarding CSIS's use and retention of metadata.** SIRC's report notes that CSIS has long interpreted warrant conditions to allow CSIS to retain and use communications metadata<sup>2</sup> incidentally collected through intercepts on warranted targets. CSIS eventually reworded warrant conditions in way which rendered them [REDACTED] on this issue, according to SIRC. SIRC's position is that CSIS's metadata practices are distinct enough to be specifically included in warrant applications. CSIS disagrees with this position and maintains it has been fully transparent with the Court.

**The report notes a key challenge for CSIS going forward.** In its review of a foreign fighters investigation SIRC noted concerns from SIRC that its recent [REDACTED]

### **Complaints**

SIRC dismissed [REDACTED] made against CSIS. The exception involved an individual whom SIRC determined had been erroneously denied a site access clearance for a CSIS location. In light of SIRC's findings, CSIS has agreed to review its Site Access Certificate Program.

---

<sup>1</sup> Section 3 of the UNAQTR prohibits the provision of funds to individuals associated with the Taliban or Al Qaeda. The UNAQTR implement UN Security Council Resolutions and are legally binding under the *United Nations Act*.

**SECRET** / [REDACTED]

- 3 -

**CURRENT STATUS**

Enclosed are materials in preparation for the tabling of the Annual Report including:

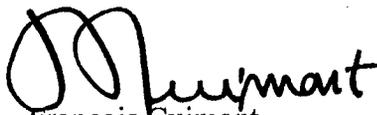
- The Annual Report in both official languages (**TAB A**);
- correspondence from the Executive Director of SIRC transmitting the annual report (**TAB B**);
- letters for your signature to the Clerks of the House of Commons and Senate in both official languages (**TAB C**);
- a Question Period Note (**TAB D**); and
- a summary table of SIRC recommendations and CSIS responses (**TAB E**).

The Parliamentary Affairs Division has retained the necessary copies for depositing the report with the Clerks of the Senate and the House of Commons. Parliamentary Affairs is also prepared to provide you with a statement, should you wish to table the report during Routine Proceedings.

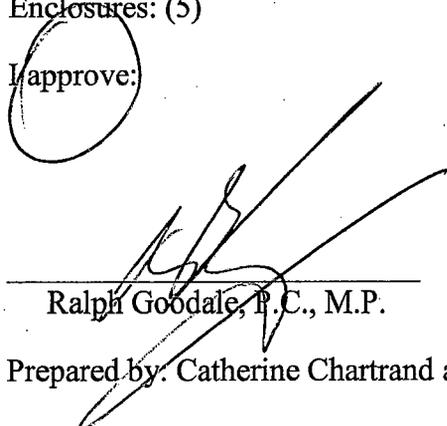
**RECOMMENDATION**

It is recommended that you table the Annual Report at the earliest convenience or by the statutory deadline of February 3, 2016.

Should you require additional information, please do not hesitate to contact me or John Davies, Acting Senior Assistant Deputy Minister, National and Cyber Security Branch, at 613-990-4976.

  
François Guimont

Enclosures: (5)

I approve: 

I do not approve:

\_\_\_\_\_  
Ralph Goodale, P.C., M.P.

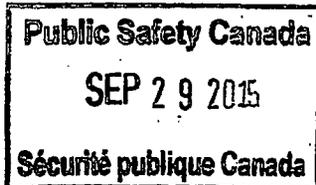
\_\_\_\_\_  
Ralph Goodale, P.C., M.P.

Prepared by: Catherine Chartrand and [REDACTED]

Security Intelligence  
Review Committee



Comité de surveillance des activités  
de renseignement de sécurité



CONFIDENTIAL (with att.)

File no.: 1630-1/15

September 29, 2015

The Honourable Steven Blaney, P.C., Q.C, M.P.  
Minister of Public Safety  
Bank of Montreal Building  
269 Laurier Avenue West, 16<sup>th</sup> Floor  
Ottawa, Ontario  
K1A 0A6

COPY

Dear Minister Blaney:

On behalf of the Chair and Members of the Security Intelligence Review Committee (SIRC), I am pleased to provide you with ten (10) copies of SIRC's Annual Report for 2014-2015. Pursuant to s. 53 of the *CSIS Act*, SIRC's Annual Report must be submitted to you no later than September 30, for tabling in Parliament within 15 sitting days.

Yours sincerely,

Michael Doucet  
Executive Director

Encl. (10)

cc: Mr. John Davies  
A/Senior Assistant Deputy Minister  
National and Cyber Security Branch  
Public Safety Canada



Ministre de la Sécurité publique

Minister of Public Safety

Ottawa, Canada K1A 0P8

28 JAN. 2016

Monsieur Gary W. O'Brien  
Greffier du Sénat et greffier des Parlements  
Édifice du centre, pièce 185-S  
Sénat du Canada  
Édifices du Parlement  
Ottawa (Ontario) K1A 0A4

CLERK OF THE SENATE  
28 JAN 28 AM 10 08  
GREFFIER DU SENAT

Monsieur,

Vous trouverez sous pli deux exemplaires du Rapport annuel du Comité de surveillance des activités de renseignement de sécurité, pour l'exercice fiscal 2014-2015, dans les deux langues officielles, qui doit être déposé conformément à l'article 53 de la *Loi sur le Service canadien du renseignement de sécurité*.

Je vous prie d'agréer, Monsieur, mes salutations distinguées.

L'honorable Ralph Goodale, C.P., député

Pièces jointes : 2

Canada

Minister of Public Safety



Ministre de la Sécurité publique

Ottawa, Canada K1A 0P8

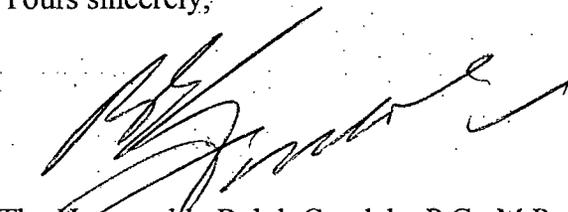
28 JAN. 2016

Mr. Gary W. O'Brien  
Clerk of the Senate and Clerk of the Parliaments  
Centre Block, Room 185-S  
Senate of Canada  
Parliament Buildings  
Ottawa, Ontario K1A 0A4

Dear Mr. O'Brien:

Please find enclosed two copies of the 2014-2015 Security Intelligence Review  
Committee Annual Report, in both official languages, to be tabled in accordance with  
section 53 of the *Canadian Security Intelligence Service Act*.

Yours sincerely,



The Honourable Ralph Goodale, P.C., M.P.

Enclosures: (2)

CLERK OF THE SENATE  
28 JAN 28 AM 10 08  
GREFFIER DU SENAT

Canada

000528

**Page 529**  
**is not relevant**  
**est non pertinente**

Minister of Public Safety



Ministre de la Sécurité publique

Ottawa, Canada K1A 0P8

28 JAN. 2016

Mr. Marc Bosk  
Acting Clerk of the House of Commons  
Centre Block, Room 228-N  
House of Commons  
Parliament Buildings  
Ottawa, Ontario K1A 0A6

Dear Mr. Bosk:

Please find enclosed two copies of the 2014-2015 Security Intelligence Review Committee Annual Report, in both official languages, to be tabled in accordance with section 53 of the *Canadian Security Intelligence Service Act*.

This report is permanently referred to the Standing Committee on Public Safety and National Security.

Yours sincerely,

A handwritten signature in black ink, appearing to read 'R. Goodale', written over a horizontal line.

The Honourable Ralph Goodale, P.C., M.P.

Enclosures: (2)

Canada

000530

QUESTION PERIOD NOTE

Date:  
Classification: UNCLASSIFIED  
Branch/Agency : NCSB

Question Period Note

**Security Intelligence Review Committee 2014-2015 Annual Report**

**ISSUE:** Tabling of the 2014-2015 SIRC Annual Report

**PROPOSED RESPONSE:**

- **The Security Intelligence Review Committee annual report includes the Committee's findings and recommendations based on the reviews and complaint investigations it has performed.**
- **I would like to assure Canadians that the Security Intelligence Review Committee's findings and recommendations will be carefully considered by my officials.**

***If pressed about Canadian Security Intelligence Service's compliance with the United Nations Al-Qaeda and Taliban Regulations:***

- **The Canadian Security Intelligence Service is undertaking a review of its human source operations in light of the Security Intelligence Review Committee's report, and will report its findings to me. The Security Intelligence Review Committee will then assess the Canadian Security Intelligence Service's findings. Going forward, I will be seeking advice from my officials on the work of both the Canadian Security Intelligence Service and the Security Intelligence Review Committee.**

***If pressed about Canadian Security Intelligence Service's collection of the Canadian Revenue Agency information without a warrant:***

- **In light of the issues identified by the Security Intelligence Review Committee, the Canadian Security Intelligence Service conducted a post-mortem of the incident and provided a copy of its report to the Committee. The Canadian Security Intelligence Service has also taken steps to make its compliance reporting regime more robust.**

***If pressed about Canadian Security Intelligence Service's transparency with the Court regarding metadata:***

- **The Canadian Security Intelligence Service takes seriously its duty of candour before the Court, and maintains that it was fully transparent regarding the matter in question.**

**Page 532**  
**is not relevant**  
**est non pertinente**

## Security Intelligence Review Committee (SIRC) 2014-2015 Annual Report

### BACKGROUND:

SIRC is an external review body that reports to Parliament on the activities of the Canadian Security Intelligence Service (CSIS). SIRC's purpose is to ensure democratic accountability: it exists to provide assurance to the Ministers and Parliament that CSIS activities comply with the law and Ministerial Direction (MD). It also provides expert advice to lawmakers and policymakers on CSIS's performance.

SIRC is comprised of a committee of five Privy Councillors, supported by a small group of officials and administrative staff, and has three basic roles.

SIRC certifies the Annual Report to the Minister from the Director of CSIS, which provides an overview of operations in the past year. The Certificate states the extent to which SIRC is satisfied with the report, and indicates whether any the described activities involved an unreasonable or unnecessary exercise of CSIS powers, or contravened the law or MD. SIRC also reviews a sample of CSIS activities for their compliance with the law and MD. Finally, SIRC investigates complaints made against CSIS regarding any action taken by CSIS or the denial of security clearances.

Pursuant to section 53 of the *CSIS Act*, SIRC must submit to the Minister a report on its activities during the preceding fiscal year no later than September 30 of each year. The report must be tabled by the Minister before both Houses within 15 sitting days of its receipt. The Department received SIRC's 2014-2015 annual report on September 29, so it must be tabled within the first 15 days on which the next Parliament sits.

The annual report summarizes, at the unclassified level, SIRC's Certificate, reviews and investigations. It also contains recommendations from SIRC accompanied by CSIS's responses. This year's report indicates that, overall, SIRC was satisfied with CSIS's conduct. CSIS fully agreed to 10 of the 18 recommendations made by SIRC, and partially agreed with others. SIRC dismissed all but one of the complaints against CSIS, which involved the denial of a security clearance for CSIS site access. The report contains CSIS's response to each recommendation.

In its Certificate, SIRC identified certain issues which, according to SIRC, had negative implications in terms of CSIS's accountability to the Minister. These included the length and level of detail of the Director's annual report, and issues with the way in which CSIS notifies the Minister of high-risk activities. CSIS is working to address these issues.

In one review SIRC found that CSIS could not verify whether current or past human source operations are in contravention of the *UN Al-Qaeda and Taliban Regulations (UNAQTR)* and therefore in contravention of Canadian law. SIRC has asked CSIS undertake a broader review of this issue, and efforts are currently underway.

While there are no provisions within the *CSIS Act* through which CSIS can compel SIRC to undertake a review, SIRC did agree to conduct an inquiry into an incident where an intelligence officer obtained taxpayer information from the Canada Revenue Agency without a warrant. SIRC's review found that a certain CSIS regional office had in fact engaged in this action on multiple occasions. CSIS has since taken corrective action.

In another review SIRC found that CSIS may not have been fully transparent with the Federal Court with respect to CSIS's retention and use of communications metadata. CSIS maintains that it was fully transparent with the Court.

<b>CONTACTS:</b>			
Prepared by	Tel. no.	John Davies A/Senior Assistant Deputy Minister, National and Cyber Security Branch	Tel. no. (613) 990-4976
[REDACTED]			

SECRET /

COPY

**SIRC Recommendations Fully Agreed to by CSIS**

<b>SIRC Review</b>	<b>Recommendation</b>
The "Insider Threat" and its Effect on Information Management	<ul style="list-style-type: none"> <li>• CSIS should create a more detailed policy on the conduct of Internal Security investigations</li> <li>• CSIS should ensure that decision making pertaining to internal investigations is documented appropriately</li> </ul>
CSIS's Relationship and Exchanges with DFATD	<ul style="list-style-type: none"> <li>• CSIS should establish formal mechanisms to ensure that human source operations do not contravene UNAQTR or similar Canadian statute or regulations</li> </ul>
A Counter-Terrorism Investigation	<ul style="list-style-type: none"> <li>• CSIS employees should be required record the justification for the decision to accept or dismiss internal expert advice acquired through mandatory consultation</li> </ul>
CSIS's Use of Metadata	<ul style="list-style-type: none"> <li>• CSIS should enhance feedback on the utility of specific surveillance operations to guide the future direction of this program</li> </ul>
SIRC's Inquiry to CSIS's Collection of CRA Information	<ul style="list-style-type: none"> <li>• CSIS should conduct a post-mortem to assess the adequacy of its management of the incident in question</li> <li>• CSIS should clarify the scope of the incident to the Federal Court and the Minister</li> <li>• CSIS should advise the Privacy Commissioner of the incident</li> </ul>
Denial of CSIS Site Access Security Clearance (Complaint)	<ul style="list-style-type: none"> <li>• All regional offices should adopt the new Site Access Certification direction implemented at the regional office subject to the complaint</li> <li>• The CSIS Site Access Certification program should be reviewed in light of the new Treasury Board Standard on Security Screening</li> </ul>

SECRET //

**SIRC Recommendations Rejected in Full or in Part by CSIS**

SIRC Review	Recommendations	CSIS Responses
<p>The "Insider Threat" and its Effect on Information Management</p>	<ul style="list-style-type: none"> <li>• CSIS should develop robust procedures governing access lists</li> </ul>	<ul style="list-style-type: none"> <li>• CSIS agrees in principle, but has a different approach to implementation</li> </ul>
	<ul style="list-style-type: none"> <li>• CSIS should create a robust training/mentoring program suited to the unique work of Internal Security investigators</li> </ul>	<ul style="list-style-type: none"> <li>• CSIS believes formal intelligence officer training is sufficient, but there may be an opportunity to review the current informal mentoring process and produce guidelines on best practices</li> </ul>
	<ul style="list-style-type: none"> <li>• CSIS should re-examine a specific internal investigation in its entirety in light of concerns over violations of internal policy and possible information breaches</li> </ul>	<ul style="list-style-type: none"> <li>• The Director is satisfied with the outcome of the investigation</li> </ul>
	<ul style="list-style-type: none"> <li>• CSIS Internal Security should forward final investigation reports to a group outside this branch</li> </ul>	<ul style="list-style-type: none"> <li>• CSIS believes forwarding reports to an outside unit would jeopardize the confidentiality and sensitivity of internal investigations</li> </ul>
<p>CSIS's Relationship and Exchanges with DFATD</p>	<ul style="list-style-type: none"> <li>• CSIS should renegotiate its 2007 protocol with DFATD</li> </ul>	<ul style="list-style-type: none"> <li>• CSIS will discuss the protocol during regular engagements between CSIS and DFATD senior management</li> </ul>
	<ul style="list-style-type: none"> <li>• CSIS and DFATD should create clear deconfliction guidelines</li> </ul>	<ul style="list-style-type: none"> <li>• CSIS will discuss areas where existing deconfliction processes may not be adequate during regular meetings with DFATD at all levels</li> </ul>
<p>CSIS's Use of Metadata</p>	<ul style="list-style-type: none"> <li>• CSIS should make the Federal Court aware of its specific metadata use and retention practices</li> </ul>	<ul style="list-style-type: none"> <li>• CSIS's position is that s.21 of the <i>CSIS Act</i> does not confer general supervisory authority on the Court. CSIS maintains that it clearly communicated its position on metadata to the Court in 2011</li> </ul>
<p>SIRC's Inquiry to CSIS's Collection of CRA Information</p>	<ul style="list-style-type: none"> <li>• The CSIS Audit Unit should address any substandard managerial and communication practices by the CSIS regional office involved in this incident</li> </ul>	<ul style="list-style-type: none"> <li>• CSIS believes the actions it has already taken in response to the incident are similar to those which would have been taken during an audit</li> </ul>



Public Safety    Sécurité publique  
Canada            Canada

Deputy Minister    Sous-ministre

Ottawa, Canada  
K1A 0P8

TOP SECRET 

DATE:

File No.: 6210 / PS-013589

MEMORANDUM FOR THE MINISTER

**MINISTERIAL BRIEFINGS ON CSIS' OPERATIONAL DATA ANALYSIS  
CENTRE SINCE JULY 2006**

(Information only)

ISSUE

Your office has requested that the Department provide you with a timeline of Ministerial briefings regarding CSIS' Operational Data Analysis Centre since 2006.

A timeline of these briefings has been enclosed (TAB A).

CURRENT STATUS

On November 3, 2016, the Federal Court released to the public an unclassified version of its October 4, 2016 decision regarding CSIS' legal authority to retain non threat related "associated data" collected pursuant to Federal Court warrants. Among other things, the Federal Court decision examined CSIS' retention of this data and its use by CSIS' Operational Data Analysis Centre (ODAC). ODAC processes and analyses "associated data" and other information 

*Ministerial Briefings on ODAC*

ODAC was first established by CSIS in April 2006. CSIS and Public Safety Canada records indicate that the Minister of Public Safety was first apprised of the program via a letter to the Minister from the Director of CSIS on July 20, 2006.

Records further suggest that Ministers of Public Safety (including yourself) have received at least seven written documents (including the July 2016 letter) in which ODAC was explicitly discussed.

Canada

.../2 

TOP SECRET

- 4 -

Additionally, CSIS provided a verbal briefing on ODAC to Minister Toews in March 2010.

Separately, Ministers of Public Safety have also received, at least, six other written documents that, while not explicitly referencing ODAC, discussed CSIS' use and retention of metadata.

At the same time, CSIS first acknowledged the existence of ODAC in its 2007-2008 Public Report (TAB B). The report stated that "CSIS' Operational Data Analysis Centre (ODAC) provides support to the Service's operational branches by performing advanced analysis of data that is collected on subjects of investigation".

### CONSIDERATIONS

With regard to the seven written documents that explicitly discuss ODAC, it should be noted that these documents mention ODAC in the context of a broad overview of all of CSIS' operations (i.e. ODAC was mentioned as part of the Director of CSIS' classified Annual Reports to various Ministers). Moreover, while some of these written materials stated that ODAC "relies on data obtained under warrant powers", none of these documents discuss CSIS' legal authority to retain "associated data" or any related legal risks.

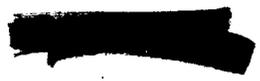
At the same time, records of the verbal briefing to Minister Toews do not provide any information as to whether the Minister was briefed on CSIS' legal authority to retain "associated data" or any related legal risks.

Should you require additional information, please do not hesitate to contact me or Monik Beauregard, Senior Assistant Deputy Minister, National and Cyber Security, at 613-990-4976.

Malcolm Brown

Enclosures: (2)

Prepared by 



**TOP SECRET**  
For Internal Use Only

Timeline of Ministerial Briefings on ODAC

Date	Action
July 2006	CSIS Director's letter to former Minister of Public Safety (Stockwell Day) advising him of the creation of ODAC
25 July 2007	CSIS Classified 2006-07 Annual Report to Minister of Public Safety (Stockwell Day)
14 November 2007	Revised version of classified 2006-07 Annual Report Minister of Public Safety (Stockwell Day)
24 August 2009	CSIS Classified 2008-09 Annual Report to Minister of Public Safety (Peter Van Loan)
8 March 2010	Verbal Briefing on ODAC and the Information Operations Centre to Vic Toews, former Minister of Public Safety
19 August 2010	CSIS Classified 2009-10 Annual Report to Minister of Public Safety (Vic Toews)
5 November 2014	CSIS Classified 2013-14 Annual Report to Minister of Public Safety (Steven Blaney)
January 2016	Minister of Public Safety meetings with the Chair of SIRC and, separately, the Director of CSIS to discuss SIRC's 2014-15 Annual Report and related issues
October 16, 2016	Public Safety Canada and CSIS Briefing Notes to Minister of Public Safety on the <i>en banc</i> Federal Court decision



Public Safety    Sécurité publique  
Canada            Canada

Deputy Minister    Sous ministre

Ottawa, Canada  
K1A 0P8

TOP SECRET

DATE:

File No.: 6210 / 24100 / PS-012958

MEMORANDUM FOR THE MINISTER

FEDERAL COURT DECISION: CSIS' AUTHORITY TO RETAIN  
METADATA COLLECTED THROUGH WARRANTS

(Information only)

ISSUE

The Federal Court has issued an important decision in which, among other matters, the Court ruled that the Canadian Security Intelligence Service's (CSIS) retention of certain metadata ("associated data") collected incidentally as a result of the execution of CSIS warrants is illegal.

The decision will be made public, potentially as early as October 18, 2016, and will likely result in negative media coverage.

The Director of CSIS has written to you to update you on the Federal Court decision and the preliminary actions taken by CSIS in response to the decision (TAB A).

CURRENT STATUS

The *En Banc* hearings began as a result of a December 2015 CSIS application for section 12 warrants in which CSIS proposed certain amendments to the standard templates for CSIS warrants. These amendments had been brought forward by CSIS to update the warrant templates to reflect changes in technology and to respond to certain questions that the Federal Court had raised, particularly in relation to the definition of "destroyed" in warrants, and the period of time that CSIS has to assess third party information that it collects through warrants.

At the same time, following the tabling of the Security Intelligence Review Committee's (SIRC) 2014-2015 Annual Report, the Federal Court indicated that it also wanted to explore issues related to CSIS retention and use of associated data. In particular, the Federal Court wanted to address SIRC's finding that "SIRC was given no indication that [CSIS] was fully transparent with the Federal Court about the nature

Canada

.../2



**TOP SECRET**

- 2 -

and scope of its activities with respect to metadata in the context of [a particular hearing before the Federal Court]”.

The *En Banc* hearings were held over four days in February, March, and April 2016. The Director of CSIS and the Deputy Minister of Justice also appeared before an *En Banc* hearing on June 10, 2016 to address concerns raised by the Court regarding CSIS' duty of candour in these matters.

On October 4, 2016, Justice Simon Noel, the designated judge selected to lead the *En Banc* proceedings issued a 136 page decision addressing the matters that were put before the Court (**TAB B**).

### **CSIS' RETENTION AND USE OF ASSOCIATED DATA**

The Federal Court's enquiries into "associated data" focused primarily on CSIS' retention and use of data associated with telecommunications and other communications that CSIS intercepts pursuant to *CSIS Act* warrants.

Up to this point, CSIS' practice has been to: (1) assess the contents of all communications intercepts conducted and retain only the contents of communications intercepts that are relevant to a threat to the security of Canada; and (2) retain *all* associated data related to these communications regardless of whether they are threat-related or not.

Since 2006, therefore, CSIS has used associated data from threat-related and non-threat-related communications to support the operations of its Operational Data Analysis Centre (ODAC), which processes and analyses "associated data" and other information

The Minister of Public Safety was informed of the creation of the ODAC and CSIS' intention to use "associated data" in July 2006 (**TAB C**). In 2011, CSIS further sought and obtained amendments to the standard *CSIS Act* warrant templates to clarify that the warrant conditions only applied to the *content* of communications and not the *associated data*. In his decision, Justice Noel raised significant concerns regarding how CSIS legal counsel described these proposed amendments in their submissions to the Federal Court. Justice Noel notes that CSIS counsel described these amendments as "minor" and "technical" when, in fact, according to Justice Noel, these amendments were not minor [Para 93-95].

.../3

**TOP SECRET**

- 3 -

## ANALYSIS

The key aspects of the Federal Court's decision are as follows:

1. The Federal Court ruled that CSIS' retention of "associated data" obtained incidentally as a result of CSIS warrants, but subsequently found not to be related to a threat to the security of Canada, is illegal;
2. The Federal Court found that CSIS breached its duty of candour in not informing the Court that it was retaining this data and had been doing so since 2006;
3. The Federal Court was critical of CSIS' views regarding the Federal Court's role in overseeing CSIS activities, particularly CSIS' contention that "Section 21 of the *CSIS Act* does not confer any general supervisory authority to the Federal Court"; and,
4. The Federal Court largely accepted CSIS' proposals regarding technical amendments to *CSIS Act* warrant templates.

The Director of CSIS' briefing note addresses the Federal Court's findings in further detail.

## CONSIDERATIONS

### *CSIS' duty of candour to the Federal Court*

This is the second time since 2013 that the Federal Court has raised concerns regarding CSIS' duty of candour to the Court.

In November 2013, the Federal Court issued a decision with important similarities to Justice Noel's current decision. In this decision (referred to as the "Mosley decision"), Justice Mosley ruled that CSIS had breached its duty of candour in not informing the Federal Court that it was undertaking certain activities that, in his view, were not authorized by the *CSIS Act* and went beyond the scope of certain *CSIS Act* warrants he had issued. In particular, Justice Mosley ruled that CSIS had not met its duty of full and frank disclosure by not specifying that, in addition to asking the Communication Security Establishment (CSE) to intercept the telecommunications of warranted targets outside of Canada (which was authorized by *CSIS Act* warrants), CSIS was also asking foreign partners to intercept such telecommunications as well (which Justice Mosley found was not authorized). Justice Mosley's decision was appealed to the Federal Court of Appeal and provided the impetus for amendments to the *CSIS Act* that were brought forward through Bill C-44.

In the current October 2016 decision, Justice Noel referenced Justice Mosley's decision and stated that he agreed with SIRC's conclusion from its 2014-2015 Annual

.../4

**TOP SECRET**

- 4 -

Report. He found that CSIS, over the period 2006 to the present, had multiple opportunities to inform the Federal Court that it retained and made use of associated data that it assessed as non-threat related. Justice Noel was particularly critical of CSIS' claim that it informed the Court of these activities in December 2011. On this issue, he wrote: "I absolutely disagree with the CSIS' suggestion that the Court was informed 'clearly and transparently'" [Para 103]. The extent of Justice Noel's concerns regarding CSIS' candour with the Federal Court since 2013 was further demonstrated when he wrote: "Must a contempt of Court proceeding, with all its related consequences, be necessary in the future?" [Para 108].

*Privacy implications and potential for future legal challenges*

The Federal Court's decision includes notable comments regarding the privacy implications of CSIS' retention and use of this data. It stated that the analysis conducted by CSIS "reveals specific, intimate details on the life and environment of the persons CSIS investigates" [Para 42].

*Communications and implications for other national security legislative initiatives.*

The judgment is likely to attract a lot of media attention. It has been written in a manner that would likely be understandable for non-experts and multiple passages in the decision could be picked up as quotes in newspaper articles.

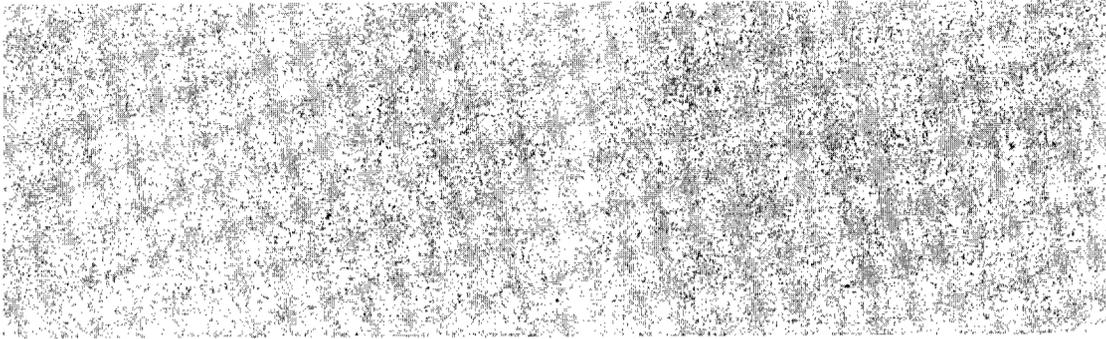
**NEXT STEPS**

The Federal Court has indicated that it will publicly release an unclassified version of its decision once CSIS and the *amici curiae* have made submissions regarding what

.../5

- 5 -

information can be released. Given the timelines established by the Court, the decision could be released publicly as early as October 18, 2016.

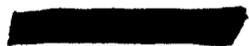


Should you require additional information, please do not hesitate to contact me or Monik Beauregard, Senior Assistant Deputy Minister, National and Cyber Security, at 613-990-4976.

Malcolm Brown

Enclosures: (3)

Prepared by: 

A solid black horizontal bar used to redact a signature or name.

Canadian Security  
Intelligence Service



Service canadien du  
renseignement de sécurité

Director / Directeur

CCM #25140  
TOP SECRET  
For Information

OCT 14 2016

MEMORANDUM TO THE MINISTER

EN BANC: FEDERAL COURT DECISION ON WARRANT CONDITIONS AND  
RETENTION OF DATA ASSOCIATED WITH THIRD PARTY COMMUNICATIONS

SUMMARY

- Further to my memoranda of April 11 and June 29, to inform that on October 4, 2016 the Federal Court issued its judgement and reasons in relation to the Canadian Security Intelligence Service's (CSIS) proposed amendments to section 12 warrant conditions, as well as its retention of data associated to third party communications.
- Though the Court accepted a number of the Service's proposed wording changes to warrant conditions, it found that CSIS breached its duty of candour by failing to fully and transparently inform the Court of its retention program, and that its retention of associated data linked to third party communications found to be unrelated to threats and of no use to an investigation, prosecution, national defence or international affairs is illegal.

BACKGROUND:

In December 2015, CSIS sought to renew and obtain new warrants for targeted individuals, while also proposing amendments to certain warrant conditions. The application was heard *en banc*, or as a panel. Owing to a finding in the Security Intelligence Review Committee's (SIRC) annual report (2014-15) that the Service's transparency with the Federal Court regarding the collection, use, retention and destruction of associated data (referred to by SIRC as metadata) collected under warrants was insufficient, the Court requested that this matter also be addressed.

it is defined as data collected through warranted operations from which the content was assessed as unrelated to threats and of no use to an investigation, prosecution, national defence or international affairs.

The *en banc* hearings on these matters were held over four days in February, March and April 2016. Five affidavits were filed and three affiants were examined, and both written and oral submissions were made addressing the establishment of the Operational Data Analysis Centre (ODAC), the retention of associated data, and operational reasoning behind the proposed wording changes to warrant conditions.

Following an exchange of letters between the Assistant Deputy Attorney General and the Chief Justice of the Federal Court, the Court called for another *en banc* hearing to address perceived issues arising from CSIS' candour towards the Court in relation to the retention program of associated data and other related concerns. Thus, on June 10, I appeared before the Federal Court along with the Deputy Minister of Justice.

#### DISCUSSION:

The Federal Court's decision, which was issued by the Honourable Justice Noël on October 4, deals with three particular issues. These include: whether the Service breached its duty of candour toward the Court when it established and ran the Operational Data Analysis Centre (ODAC) program; whether the Service is legally authorized to retain associated data linked to third party (i.e. non-target) communications unrelated to threats and of no use to an investigation, prosecution, national defence or international affairs; and whether the Service's proposed amendments to warrant conditions were acceptable.

Though no evidence indicated this was deliberate, the Court found that CSIS breached its duty of candour by omitting to inform the Court, between 2006 and 2016, of the Service's new position on the retention of data, as well as ODAC's creation. I take seriously the concerns of the Court, and commit to, going forward, advise the Court of changes in policy or practice relevant to the exercise of our warrants without delay. That said, since its establishment, the Service has sought to provide the necessary policy and guidance for employees to ensure compliance with the law and Ministerial Direction. To that end, CSIS has, through its dealings with the Court, acted based on consistent advice from the Department of Justice. As the Court acknowledges, however, the *CSIS Act* of 1984 was not drafted to account for the enormous and unforeseen technological advances of the last decade.

The Court also found that the Service's retention of associated data linked to third party communications is illegal. The decision argues that the 'strictly necessary' qualifier in s.12 of the *CSIS Act* applies to both collection under s.12 and retention of collected information, including that which is obtained pursuant to a warrant issued under s.21. From this perspective, incidental collection of associated data linked to third parties not found to be related to any threats is not considered to meet the 'strictly necessary' qualifier.

Associated data linked to third parties not found to be related to any threats is susceptible to being collected as a consequence of a warranted operation on a target. Justice Noël concludes,

[REDACTED]

however, that as this is not within the scope of the warrant, nor is it the reason for the warrant to be granted, a determination must be done, within a short period, to assess the relevance of this data to the target or threats to the security of Canada.

Though the Service may continue to retain associated data linked to a target's communications, it will no longer be able to retain associated data linked to third party communications found to be unrelated to threats and of no use to an investigation, prosecution, national defence or international affairs. This is a shift from current practice, as since 2006, CSIS has retained all associated data and inserted it into ODAC for future investigative purposes.

Given the decision, CSIS has halted internal use and analysis of all associated data.

Given the requirement to assess, within a short period, relevance to targets or threats to the security of Canada, the Service has been given three months to implement a two-step process of assessment. As outlined in the decision, upon successful decryption or decoding, the Service will have six months to assess information and communications that are obviously unrelated to a target or a threat. The Service will continue to have 12 months for other communications and information.

Of note, the Court was satisfied with a number of the Service's proposed amendments to s.12 warrant conditions. Amongst other things, it accepted the Service's proposal to:

As these proposals to amend warrant conditions initiated the *en banc* hearings, this aspect of the decision is positive.

**NEXT STEPS:**

[REDACTED]

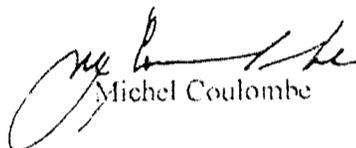
Though not directly related, I have also exerted particular emphasis on employee responsibilities as it pertains to operational compliance. This, given that it is the foundation for maintaining the trust and confidence of CSIS' domestic and foreign partners, the Court and the Canadian public. Work is therefore underway to enhance the Service's compliance management framework for all of its operational activities, as well as increase resources dedicated to operational compliance

A redacted version of the Federal Court's judgement and reasons could be made available to the public as early as October 18, though this will depend on the Court's review of the redactions due that day. This will likely garner attention and, given the Court's critical stance, there will likely be reputational impact on the Service at a moment when the public and stakeholders have been actively engaged by you. In addition to the heightened attention brought by the consultations, the Privacy Commissioner, who recently tabled his annual report addressing Bill C-51, amongst other things, will also be interested in this decision.

[REDACTED]

I wish to reiterate that the Service recognizes the importance of compliance with Ministerial Direction and the *CSIS Act*, as well as openness and transparency with the Court. Moreover, I wish to emphasize that CSIS will improve its practices involving the Court to ensure that duty of candour-related issues do not occur again.

As always, please do not hesitate to contact me should you require further information.

  
Michel Coulombe

cc.: National Security Advisor  
Deputy Minister, Public Safety

This document constitutes a record which may be subject to mandatory exemption under the *Access to Information Act* or the *Privacy Act*. The information or intelligence may also be protected by the provisions of the *Canada Evidence Act*. The information or intelligence must not be disclosed or used as evidence without prior consultation with the Canadian Security Intelligence Service.

[REDACTED]



Sécurité publique    Public Safety  
Canada                    Canada

Sous-ministre            Deputy Minister

Ottawa, Canada  
K1A 0P8

**TOP SECRET** 

DATE:

File No.: 6210 / 23746 / 008209

**MEMORANDUM FOR THE MINISTER**

**SECURITY INTELLIGENCE REVIEW COMMITTEE ANNUAL REPORT**

(Signature Required)

**ISSUE**

On January 27, 2016, you will meet with Pierre Blais, Chair of the Security Intelligence Review Committee (SIRC), to discuss SIRC's 2014-2015 Annual Report. Following your meeting with Mr. Blais, you will also meet with the Director of the Canadian Security Intelligence Service (CSIS).

We have attached talking points (**TAB A**), Mr. Blais' biography (**TAB B**), Mr. Blais' letter to you (**TAB C**), and a proposed reply (**TAB D**), as well as the Director of CSIS' briefing note to you regarding SIRC's Annual Report (**TAB E**).

**BACKGROUND**

Every year SIRC reviews a sample of CSIS activities to ensure that CSIS is complying with the law and exercising its powers in a reasonable and necessary way. SIRC also investigates any complaints made against CSIS. SIRC summarizes its review and investigation activities in its Annual Report to Parliament.

The *CSIS Act* also requires that SIRC provide you with a Certificate on the Annual Report from the Director of CSIS. The Certificate states the extent to which SIRC is satisfied with the Report; whether CSIS operations complied with the law and Ministerial Direction (MD); and whether any operations involved an unnecessary or unreasonable use of CSIS powers.

**CURRENT STATUS**

The Department received SIRC's Annual Report on September 29, 2015. As Parliament resumed on December 3, you must table the Annual Report before both Houses by **February 3, 2016**, pursuant to section 53 of the *CSIS Act*.

Overall, SIRC found that, with one exception, CSIS activities did not contravene the *CSIS Act* or Ministerial Direction, and represented a reasonable exercise of CSIS' authorities. SIRC arrived at this conclusion after conducting eight reviews and

**Canada** 

.../2

000548  
000548

concluding five investigations into complaints against CSIS. SIRC dismissed all complaints against CSIS, except one. At the request of the Director of CSIS, SIRC also conducted an inquiry into an incident involving CSIS employees. The volume of CSIS reviews and investigations is consistent with volumes from previous years.

SIRC's Annual Report includes 18 recommendations. Public Safety Canada (PS) estimates that CSIS has fully or partially agreed with 14 of SIRC's recommendations and disagreed with the remaining four (TAB F). Though not legally binding, PS estimates that CSIS implements 75% of SIRC recommendations.

### ANALYSIS OF SIRC ANNUAL REPORT

SIRC's Annual Report raises four issues that have important policy and legislative considerations and may give rise to criticism in the media.

#### 1. **Some CSIS** [REDACTED]

As part of its review entitled "CSIS' Relationship with the Department of Foreign Affairs, Trade, and Development" (SIRC Review 2014-07), [REDACTED] discussions between CSIS and DFATD regarding [REDACTED]

[REDACTED]

**SIRC Recommendation:** [REDACTED]  
[REDACTED] (CSIS fully agrees)

**PS view:** [REDACTED]

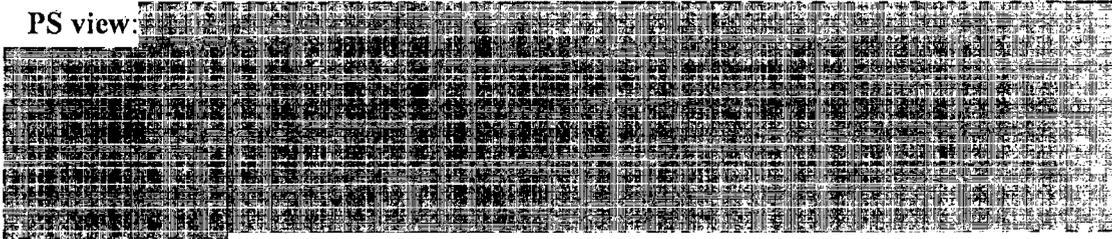
#### 2. **SIRC believes that CSIS should provide information to the Federal Court regarding how it uses metadata**

In its "Review of CSIS' Use of Metadata" (SIRC Study 2014-03), SIRC examined CSIS' exchanges with the Federal Court regarding the retention and use of metadata

collected pursuant to warrants. SIRC's report noted that CSIS has stated to the Federal Court that it does retain metadata, but it is not clear that CSIS has told the Federal Court how it uses that metadata. CSIS, however, believes that it has been sufficiently transparent with the Federal Court. CSIS further believes that it does not need to provide further information since the *CSIS Act* does not confer the Federal Court with oversight or supervisory authority over CSIS.

**SIRC Recommendation:** CSIS disagrees with SIRC's recommendation that it advise the Federal Court how it uses metadata collected pursuant to warrants.

PS view:



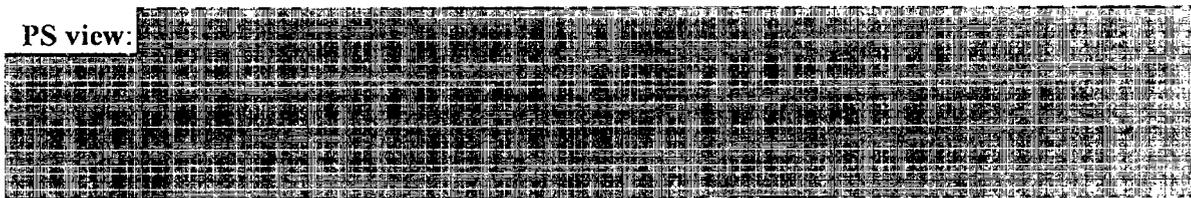
**3. CSIS is taking appropriate action to address insider threats, but procedures regarding internal security investigations should be improved**

SIRC undertook a comprehensive review of CSIS' internal security practices. It found that CSIS addresses its physical security appropriately and has introduced improvements in IT security. However, SIRC found shortcomings related to internal security investigations. In particular, SIRC raised concerns regarding an internal security investigation



**SIRC Recommendations:** CSIS has disagreed with two of SIRC's recommendations, including that CSIS: (1) undertake a full review of [redacted] and, (2) forward final investigation reports to another unit within CSIS for review.

PS view:



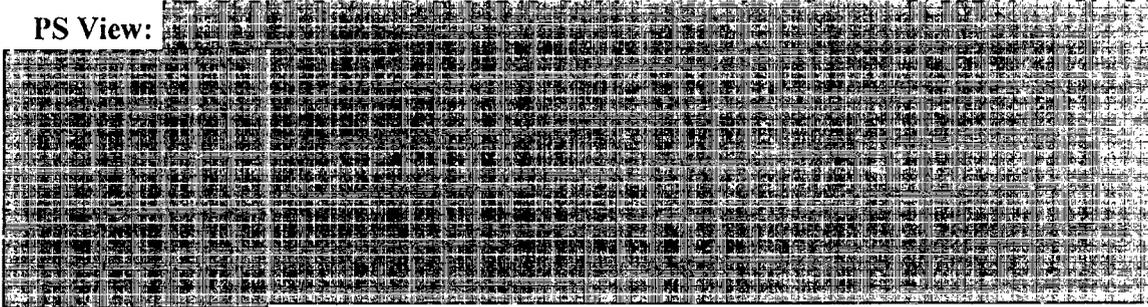
**4. SIRC found that a CSIS regional office obtained taxpayer information without a warrant on multiple occasions.**

As a result of a question asked by the Federal Court during proceedings pursuant to an application for warrants under the *CSIS Act*, CSIS discovered that an employee at its [redacted] office had obtained information from the Canada Revenue Agency (CRA) without a warrant. The Director of CSIS responded by asking SIRC to conduct an inquiry. SIRC's inquiry found a total of [redacted] of disclosure of taxpayer information without a warrant. While CSIS has concluded that these incidents were

the result of human error (the CSIS and CRA employees involved were unaware that a warrant was required), SIRC found that CSIS' initial management of the incident was "not adequate".

**SIRC Recommendations:** CSIS has fully or partially agreed with all of SIRC's recommendations and has advised the Privacy Commissioner of the issue.

**PS View:**

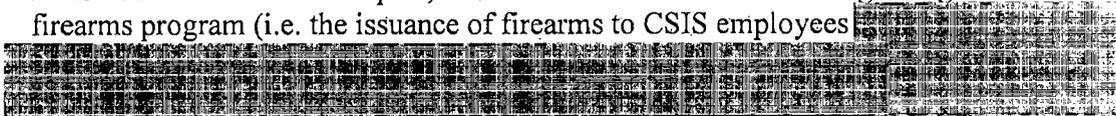


**ADDITIONAL CONSIDERATIONS**

The following three issues may also come up during your meetings with the Chair of SIRC and the Director of CSIS:

**1. CSIS' Firearms Program**

In its 2013-2014 Annual Report, SIRC cited numerous concerns regarding CSIS' firearms program (i.e. the issuance of firearms to CSIS employees



and a failure to properly brief your predecessor. PS wrote to you on this issue in December 2015 (TAB G).



**2. SIRC Funding**

Budget 2015 allocated \$12.5 million over 5 years and \$2.5 million ongoing to support SIRC.



**3. Office of the Communications Security Establishment Commissioner (OCSEC) 2014-2015 Annual Report**

Our understanding is that the OCSEC Annual Report may be tabled in Parliament the same week that SIRC's report is tabled. This year's Annual Report will include the results of the Commissioner's review of the Communications Security Establishment's use of metadata. It is likely that the Commissioner's findings will attract media attention and may be linked to SIRC's findings regarding CSIS' retention and use of metadata.

RECOMMENDATION

We recommend that you sign the attached correspondence to Mr. Blais.

Should you require additional information, please do not hesitate to contact me or  
Monik Beauregard, Senior Assistant Deputy Minister, National and Cyber Security, at  
613-990-4976.

François Guimont

Attachments: (5)

I approve:

I do not approve:

\_\_\_\_\_  
Ralph Goodale, P.C., M.P.

\_\_\_\_\_  
Ralph Goodale, P.C., M.P.

Prepared by: 

Ministre de la Sécurité publique



Minister of Public Safety

Ottawa, Canada K1A 0P8

The Honourable Pierre Blais, P.C.  
Chairperson, Security Intelligence Review Committee  
PO BOX 22430 Station D  
Ottawa, ON,  
K1P 5W5

Dear Mr. Blais,

Thank you for your correspondence dated November 9, 2015, which I read with great interest.

Our Government is committed to striking the right balance between ensuring our rights and freedoms, and our collective security. The Security Intelligence Review Committee (SIRC) plays a vital role in this regard and, on behalf of Canadians, I would like to thank you for the Committee's excellent work.

As you know the Government has a number of priorities which may be of interest to SIRC. My officials have briefed me on SIRC's Annual Report for 2014-2015, and on the classified reports produced in the last year.

I look forward to meeting with you to discuss SIRC's activities over the past year, and the situation going forward. I would welcome your perspective on SIRC's recommendations to the Canadian Security Intelligence Service in the Annual Report, and the Service's response to the recommendations. I would also be interested in your views on the challenges and opportunities that may lie ahead for SIRC.

Ralph Goodale, P.C., M.P.  
Minister of Public Safety and Emergency Preparedness

Canada

000553  
000553

Canadian Security  
Intelligence Service



Service canadien du  
renseignement de sécurité

Director - Directeur

CCM #22653  
TOP SECRET/  
For Information



NOV 17 2015

**MEMORANDUM TO THE MINISTER**

**SECURITY INTELLIGENCE REVIEW COMMITTEE ANNUAL REPORT 2014-2015**

**SUMMARY**

- Pursuant to s.53 of the *Canadian Security Intelligence Service Act (CSIS Act)*, SIRC is required to submit to you an Annual Report of its activities, which must be tabled in the House of Commons within fifteen sitting days of receipt.
- The SIRC Report contains unclassified summaries of SIRC's reviews of the Service's activities, as well as findings related to complaints. While the report includes a number of favorable reviews, it also identifies concerns, some of which may attract media attention.

**BACKGROUND:**

The *CSIS Act* did more than create Canada's civilian security intelligence agency. The Act also created the Security Intelligence Review Committee (SIRC), an independent, external review body reporting to the Minister and Parliament on CSIS operations. In broad terms, SIRC conducts reviews, investigates complaints and, since the dissolution of the position of Inspector General in 2012, certifies the Director's Report to the Minister.

By statute, SIRC is also required to submit to you an Annual Report of its activities, to be tabled in the House of Commons within fifteen sitting days of receipt. The Annual Report includes a summary of SIRC's certification of the Director's Report, as well as unclassified summaries of the Committee's in-depth classified reviews and investigations.

To fulfill its mandate, SIRC has access to all information held by the Service, with the exception of Cabinet confidences. Steps have also been taken in the last year to support SIRC research by providing direct access to relevant databases. This is also intended to address SIRC concerns with regard to the fulsomeness of their access to Service information. In addition to document review, SIRC regularly meets with and interviews CSIS staff, and formally questions CSIS witnesses in a quasi-judicial complaints process.

The Service has established a productive relationship with SIRC, whose ongoing reviews contribute to a culture of continual learning and improvement. While the Service is not required by law to adopt SIRC recommendations, the results of SIRC reviews and complaints are regularly discussed among members of the CSIS Executive and routinely inform Service policies and practices.

In 2012, SIRC assumed responsibility for some functions of the former Inspector General of CSIS. At that time, SIRC identified as a potential challenge the need to maintain arms' length independence while simultaneously briefing the Minister of Public Safety on any matter related to the performance of the Service, including through the annual certification process. In last year's report, however, SIRC noted that contrary to its initial concerns, its more frequent interactions with you and the Department have enhanced its role and, by extension, accountability within the system.

In this year's report, *Broader Horizons; Preparing the Groundwork for Change in Security Intelligence Review*, SIRC notes that the new legislative landscape introduced by the *Protection of Canada from Terrorists Act* and *Anti-terrorism Act* presents a more complex workload for SIRC's research and legal teams. Certainly, this year's Annual Report will be considered against a backdrop of heightened public interest in national security, not only in relation to legislative change, but also questions of review and accountability.

### DISCUSSION:

Though the Act limits SIRC's certification to activities described therein, SIRC considers it an opportunity to offer a more "global" assessment of the legality, reasonableness and necessity of the Service's operational activities. This year, SIRC expressed its overall satisfaction with the Director's Report, finding that CSIS activities did not contravene the *CSIS Act* or Ministerial Direction and were reasonable and necessary, with one exception; SIRC identified a potential legal concern regarding compliance of CSIS human source operations with the *United Nations Al Qaeda Taliban Regulations (UNAOIR)*.

The Service takes this finding very seriously and, in addition to launching a s.40 review of its current human source operations, is working closely with the Department of Justice and Global Affairs Canada to identify international obligations adopted into Canadian law and associated carve outs to inform the development of a mechanism to be incorporated into relevant operational policies and procedures. The results are to be included in the Director's report to you for 2015-2016, and will be reviewed by SIRC in next year's certification process.

In its certification, SIRC also recommended that consideration be given to CSIS' assessment of risk, as well as the format and structure of my report to you. With respect to risk, SIRC concluded that the Service's calculation of risk may be too narrow for the purpose of ensuring Ministerial accountability. Similarly, SIRC concluded that the length and level of detail included in recent Director's reports have the effect of obscuring issues worthy of Ministerial attention. While CSIS may take issue with the assumptions underpinning these conclusions, there is strong recognition of the need to appropriately support the exercise of Ministerial accountability.

As such, and in accordance with recent Ministerial Direction, CSIS is revising its suite of operational policies, including in relation to the assessment of risk and related approval, consultation and notification requirements. With respect to this year's Director's Report, it reflects a concerted effort to adopt a new approach, taking into consideration the concerns raised by SIRC. It also addresses recently issued Ministerial Direction.

This year's report contains unclassified summaries of eight reviews and one inquiry, as well as five investigations into complaints against the Service (Annex). Section 54 of the *CSIS Act* identifies that SIRC may, at any time, furnish the Minister with a specific report relating to performance of its duties and functions. Two of SIRC's reviews during the period resulted in s. 54 reports: the "Insider Threat" and CSIS's Relationship and Exchanges with the Department of Foreign Affairs, Trade and Development. Further, with regard to CSIS' retention of metadata, SIRC found the Service's transparency with the Federal Court insufficient. Though CSIS and our legal counsel from the Department of Justice disagree with this finding, the issue could garner attention. In this regard, I would reiterate that the Service takes its duty of candour very seriously.

4

SIRC reached positive conclusions for some of CSIS's most complex, intensive and demanding programs, including: foreign fighters, *CSIS Act* section 16 (collection of information on foreign states and persons in support of the Minister of National Defence or Minister of Foreign Affairs), counter-proliferation and foreign-based human sources. SIRC further highlighted the "exceptional" request made by the Director for SIRC to conduct an inquiry into an incident involving a CSIS Intelligence Officer who obtained taxpayer information from the Canada Revenue Agency without a Federal Court warrant. In addition, SIRC highlighted an overall improvement in the provision and disclosure of information by CSIS to SIRC, whereas this had previously been highlighted as a challenge.

5

Regarding the various areas SIRC identified for improvement, work is actively underway to update CSIS' operational policies and procedures to give effect to legislative change and Ministerial Direction, as well as the majority of SIRC's recommendations. In some cases, such as accounting for Canada's international obligations, the requirements may be complex. Given its unique mandate and the challenging environment in which it operates, the Service recognizes the importance of ensuring that its activities are grounded in clear policies and procedures, including a robust risk-assessment framework.

Communication requirements that arise from the release of the SIRC report, and particularly those in relation to the Canada Revenue Agency and Global Affairs Canada, will be promptly addressed through existing channels and procedures.

As always, please do not hesitate to contact me should you require further information.

  
Michel Coulombe

**Enclosure:**

Annex: SIRC Annual Report 2014-2015 – Summary

c.c.: National Security Advisor  
Deputy Minister, Public Safety

This document constitutes a record which may be subject to mandatory exemption under the *Access to Information Act* or the *Privacy Act*. The information or intelligence may also be protected by the provisions of the *Canada Evidence Act*. The information or intelligence must not be disclosed or used as evidence without prior consultation with the Canadian Security Intelligence Service.

TOP SECRET

ANNEX

SIRC Annual Report 2014-2015  
Summary of Reviews, Recommendations, Complaints and CSIS Responses

**SIRC Review: The "Insider Threat" and Its Effect on Information Management -- Section 54 Report**

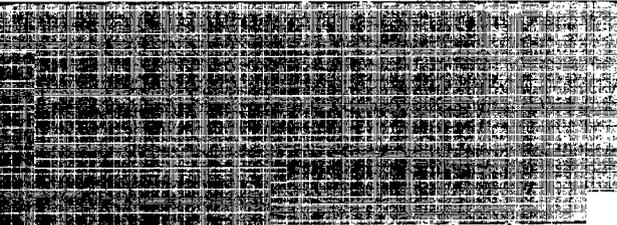
With a focus on information management, this review examined the Service's efforts to mitigate insider threats. SIRC reviewed policies and procedures as well as the operations of the Service's Internal Security (IS) unit. It also reviewed a sample of related internal investigations. SIRC found a decrease in security violations and that the Service addressed its physical security appropriately. However, SIRC found there was insufficient training, gaps in policies and procedures and unsatisfactory thresholds for internal investigations. It also found the Service did not maintain proper documentation on decision making surrounding internal investigations. In a specific case, SIRC found that CSIS failed to give the case an appropriate level of attention and scrutiny. As a result of these findings, SIRC made a number of recommendations and intends to examine CSIS' internal security activities on a regular basis.

*SIRC Recommendation:*

SIRC recommended that CSIS immediately develop robust procedures governing access lists.

*CSIS Response:*

CSIS agreed in principle with the recommendation.



The Service is in the process of determining what interim steps are required to satisfy security requirements.

*SIRC Recommendation:*

SIRC recommended that CSIS create a robust training and mentoring program suited to the unique work of Internal Security employees who are expected to conduct sensitive investigations into suspected violations and/or breaches of security.

*CSIS Response:*

CSIS partially agreed with this recommendation; while it is not believed that further training of Intelligence Officers is required, Internal Security is reviewing whether the current informal mentoring process within the branch meets requirements and will develop a guideline of best practices for IS investigators.

TOP SECRET

*SIRC Recommendation:*

SIRC recommended that CSIS create more detailed policy on the conduct of Internal Security investigations into suspected violations and/or breaches of security.

*CSIS Response:*

*ajed* CSIS agreed with this recommendation. Since the recommendation was made, the Service has revised the policy on *Internal Security Administrative Investigations* and procedures on *Internal Security Administrative Investigations* to address these concerns. Of note, the Service Policy on *Physical Security* is currently being revised, as are related procedures on *Security Searches of Individuals, Workspace Searches and Removal of Designated or Classified Information or Equipment*.

*SIRC Recommendation:*

SIRC recommended that CSIS take immediate action to ensure that all decision making pertaining to internal investigations be documented appropriately, in accordance with Treasury Board standards.

*CSIS Response:*

*ajed* CSIS agreed with this recommendation, and since the recommendation was made, procedures on Administrative Investigations were revised to include detailed requirements for initiating and documenting an investigation, as well as reporting and approval requirements. The *Service Policy on Internal Security Administrative Investigations* was also updated and sets out the high-level requirement to document all findings from an Injury Assessment report.

*SIRC Recommendation:*

SIRC recommended that CSIS re-examine a specific case in its entirety, guided by six specific concerns regarding violations of internal policy and possible information breaches.

*CSIS Response:*

*X* CSIS disagreed with this recommendation. The Director was satisfied with the outcome of the investigation. [REDACTED] The allegations were also not substantiated and were not significant from the Service's perspective. Given the passage of time, the Service assessed that returning to the issue could be construed as harassment or abuse of authority.

*SIRC Recommendation:*

SIRC recommended that [REDACTED] forward final investigation reports to an external unit for review to ensure investigations are complete, objective and well-documented.

*CSIS Response:*

*X* CSIS disagreed with this recommendation and is of the view that third party review of formal investigations would jeopardize confidentiality and sensitivity of investigations, impede timely and objective conclusion of investigations and impede the Director's authority in the management of personnel.

TOP SECRET 

### SIRC Review: CSIS's Investigation of Canadian Foreign Fighters

SIRC examined the Service's investigation of the "foreign fighter" threat by focusing on targeting, advice to government and information exchange. To conduct the study, SIRC met with a number of CSIS employees, including in regions , as well as with RCMP members. SIRC found that CSIS continues to adjust to the threat by shifting resources, reprioritizing investigations and engaging domestic partners. With regard to the latter, SIRC found that CSIS conducts frequent deconfliction meetings with the RCMP and engages in intelligence production for partners. SIRC found that CSIS' targeting in these investigations complied with operational policies, Ministerial Direction and relevant legislation. It also examined  warrant applications and found that CSIS followed relevant policies and procedures in applying for and executing those warrants. SIRC noted that the reprioritization to CT could result in a loss of capacity in counter-intelligence and counter-proliferation investigations. SIRC flagged its intention to review in the coming year the overseas element of the "foreign fighter" investigation and the challenge of returnees and frustrated travelers in addition to the impact of the amendment to the *CSIS Act* on Service investigations.

*SIRC Recommendations:*  
None.

*CSIS Response:*  
N/A

### SIRC Review: CSIS' Relationship and Exchanges with DFATD – Section 54 Report

SIRC reviewed the evolution of the Service's relationship with DFATD and found the relationship at overseas missions to be generally positive. It identified two key challenges in the relationship: issues relating to information disclosure and insufficient operational and program deconfliction. Further, it identified potential legal concerns with respect to the Service's activities in relation to the United Nations Al Qaeda Taliban Regulations (UNAQTR) and, more broadly, compliance with Canadian laws and regulations implementing Canada's international obligations. It recommended the Service undertake a s.40 *CSIS Act* review of the latter and to report its findings in the next Annual Report to the Minister.

*SIRC Recommendations:*  
SIRC recommended that CSIS renegotiate the 2007 Protocol with DFATD on *Cooperation in Respect of Consular Cases Involving Canadians Detained Abroad as Part of a National Security or Terrorism-Related Case* to reach agreement on issues impeding its functionality.

*CSIS Response:*  
*agree?* CSIS agreed partially with this recommendation and has enhanced its engagement with DFATD, now Global Affairs Canada (GAC), at senior levels. In addition, detailed staff-level discussions are underway to  including  appropriate protocols  Once established, CSIS will work with GAC to determine if updates to the protocol are required.

TOP SECRET



*SIRC Recommendations:*

SIRC recommended the development of clear deconfliction guidelines between CSIS and DFATD where there is potential for operational or program entanglement.

*CSIS Response:*

The Service agreed with SIRC on the importance of deconfliction, but not on the need for guidelines. In the context of implementing Ministerial Direction associated with CSIS' threat reduction mandate, the consultation process with DFATD has been enhanced.

*SIRC Recommendations:*

SIRC recommended that CSIS put in place formal mechanisms to ensure that none of its human source operations are in contravention of the UNAQTR or any similar Canadian statute or regulation.

*CSIS Response:*

*agreed*

CSIS agreed with this recommendation and is working with Global Affairs Canada and the Department of Justice to identify relevant Canadian statutes and regulations, as well as legal carve outs (i.e., permits, exemptions, etc.). Steps have also been taken to ensure the Service is informed of new requirements in a timely manner. Based on this work, and informed by the conduct of the Service's s.40 review of current human source operations, CSIS will develop a mechanism to assess human source operations against UNATR and other similar legal obligations.

*SIRC Recommendations:*

SIRC directed the Service to undertake a Section 40(1)(a) review of the specific activities involving compliance with Canadian laws and regulations implementing measures, decisions, resolutions or recommendations of an international organization of states of which Canada is a member. The findings will be included in the Director's classified Annual Report to the Minister.

*CSIS Response:*

*agreed*

CSIS agreed with this direction and has initiated the Section 40 review. To fulfil the obligations in a timely manner, and to minimize the impact on ongoing operations, the review will focus on ongoing human source operations over the 2015-16 fiscal year. Results, final or preliminary, will be included in the next Annual Report to the Minister.

**SIRC Review: Review of a Counter-Terrorism Investigation**

With the realignment of the Service's [redacted] investigation [redacted]

[redacted] SIRC undertook a comprehensive assessment of the Service's [redacted] investigations and found it to be run soundly with operational activities reasonable and proportional to the threat. [redacted]

TOP SECRET

*SIRC Recommendation:*

SIRC recommended that CSIS document the decision-making or rationale for choosing not to follow expert advice [REDACTED]

*CSIS Response:*

CSIS agreed with the recommendation. [REDACTED]

[REDACTED] procedures are currently under review. Updates to these procedures and associated approval forms will include enhanced documentation on the assessment of risk.

**SIRC Review: CSIS' Section 16 Program**

Section 16 of the *CSIS Act* authorizes CSIS to assist the Minister of National Defence or the Minister of Foreign Affairs with the collection, in Canada, of intelligence relating to foreign states and persons. In 2014, to respond to GoC changes to coordinate and streamline intelligence requirements, priorities and collection, CSIS changed its internal procedures. This year SIRC examined several facets of the Service's section 16 activities including Ministerial Direction, requests for assistance, prioritization, collection, record-keeping and dissemination. SIRC found significant improvements to the Service's foreign intelligence collection function since changes were instituted in 2014, not only with regard to process but vis-à-vis the relevance and utility of the information collected. Among the improvements noted was a clearer distinction between s.12 and s.16 collection. SIRC's examination of [REDACTED] specific s.16 targets suggested the new process ensures collection responds to wider GoC intelligence priorities and requirements and reflects the Service's capacity to collect.

*SIRC Recommendation:*

None.

*CSIS Response:*

N/A

**SIRC Review: CSIS' Counter-Proliferation Strategy**

Canada does not currently have a Counter-Proliferation (CP) Strategy; however, counter-proliferation is a GoC intelligence priority. SIRC reviewed CSIS' investigation of proliferation and procurement attempts by state and non-state actors and examined the Service's [REDACTED]. SIRC found the Service works to maintain cooperative relationships on CP issues with domestic and foreign partners and identified two main challenges in CSIS' CP investigations: managing joint operations with partners of varying capabilities and priorities and balancing risk with intelligence gain. SIRC also found that a GoC strategy would be highly beneficial for CSIS and its partners.

*SIRC Recommendation:*

None.

*CSIS Response:*

N/A

TOP SECRET

**SIRC Review (Baseline): CSIS' Use of Metadata**

SIRC examined CSIS' collection and use of metadata and related authorities and accountability structures guiding its collection, use and retention. It focused on two areas of metadata use: use of metadata collected to support the Service's larger data exploitation program and the Service's interception [redacted] information. SIRC did not draw any adverse conclusions with respect to the retention and use of metadata collected under warrant. However, SIRC found the Service's transparency with the Federal Court on the issue of metadata insufficient. It also found that there was no formal process for tabulating and sharing the results of intercept operations [redacted]

[redacted]

*SIRC Recommendation:*

SIRC recommended that the Service advise the Federal Court of its activities with respect to metadata collected under the authority of its warrant.

*CSIS Response:*

X CSIS disagrees with this recommendation; it is the Service's position that it has been fully transparent with the Court. This recommendation suggests SIRC believes the CSIS Act confers general supervisory authority to federal court judges; the Department of Justice, which provides legal advice to CSIS, does not agree. Section 21 of the CSIS Act confers discretion to issue or refuse to issue a warrant but does not confer any oversight or supervisory authority. Of note, however, during a hearing on 16 December 2011, the Service, through its legal counsel, informed seven designated judges of the Federal Court that "metadata is not destroyed and is retained no matter what happens to the communications, except for solicitor-client, which will be destroyed." The Service considers its position to have been communicated to the Court clearly and transparently.

[redacted]

*SIRC Recommendation:*

SIRC [redacted] continue to work with [redacted] to enhance feedback on the utility of [redacted] and, based on these findings, that the 2012 internal assessment be updated to guide the future direction of the program.

*CSIS Response:*

agreed CSIS agreed with this recommendation. The Service acknowledges that [redacted] is a new program and is in the process of developing new procedures and processes to better manage [redacted] and subsequent reporting to ensure they are standardized, comprehensive and value-added.

TOP SECRET



### SIRC Review (Core): CSIS' Foreign-Based Human Sources

SIRC undertook a comprehensive assessment of the Service's human source program with the objective of understanding the contribution the program has made to the Service's overall intelligence collection and production. SIRC found that the Service's accountability framework in the area of human source management was sound and concurred with the Service decision to develop policies and procedures applicable to all human sources regardless of location. SIRC did identify some issues of concern pertaining to the approval process for a specific operation, the

#### *SIRC Recommendation:*

None.

#### *CSIS Response:*

While SIRC did not make any formal recommendations in this review, it did indicate that it could not fully verify the Service's adherence to reporting requirements for contact between CSIS employees and

Further, it identified an issue with respect to the approval process for an operation involving a human source.

To reflect the new protection for Human Source identity in the *CSIS Act*, the Service revising its human source policy suite; amendments include new requirements to document decision-making as well as. These changes also reflect related Ministerial Direction issued to CSIS on 31 July 2015.

### SIRC Inquiry: CSIS' Collection of Canada Revenue Agency (CRA) Information

In August 2014, SIRC was asked to conduct a review of an instance in which the CRA disclosed taxpayer information without a warrant.

that a 1987 Memorandum of Understanding (MOU) between CSIS and the CRA permitted sharing of information without a warrant. The Service responded formally to these recommendations on 11 May, 2015, which elicited a follow up from SIRC on 2 June, 2015, in which it expressed concern with the Service's response. Following further discussion between SIRC and the Service to clarify the areas of contention, an amended response was provided to SIRC on 14 July, 2015.

TOP SECRET

*SIRC Recommendation:*

SIRC recommended that CSIS task Internal Audit to address any substandard managerial or communications practices by the district in question.

*CSIS Response:*

*agree* CSIS agreed with the spirit of SIRC's recommendation to conduct an audit, and had already conducted an internal review of the incident which examined the policies in place at the time and the managerial practices of the regional office in question. It was determined the improper collection of CRA information was the result of human error and the unique nature of the prohibition on collecting taxpayer information.

*SIRC Recommendation:*

SIRC recommended that CSIS conduct a post-mortem of the incident.

*CSIS Response:*

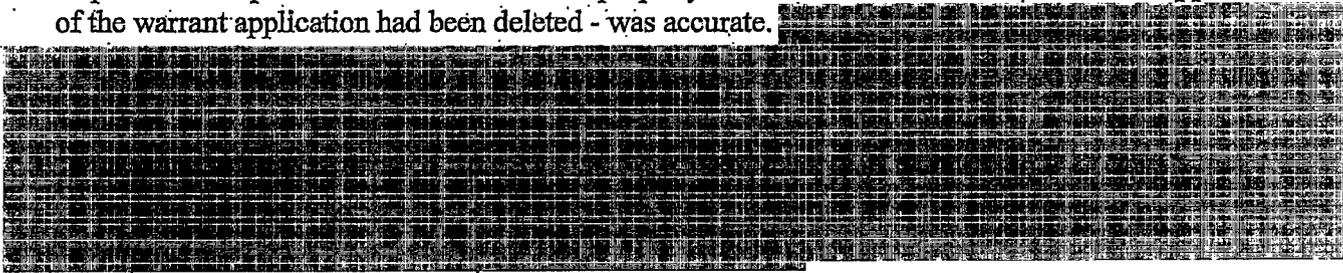
*agree* CSIS conducted a post-mortem of the incident, and will be enhancing the compliance reporting regime to ensure any instances of non-compliance are reported in a timely manner, in addition to on an annual basis.

*SIRC Recommendation:*

SIRC recommended that CSIS clarify the scope of the incident to the Minister and the Federal Court.

*CSIS Response:*

*agree* The Service provided an update to the Minister in August 2015 on the situation. CSIS initially did not see the need to revisit the issue given that the information provided to the Federal Court in response to its specific concern – that the improperly collected CRA information used in support of the warrant application had been deleted - was accurate.



*SIRC Recommendation:*

SIRC recommended that CSIS advise the Privacy Commissioner of the issue.

*CSIS Response:*

*agree* While the Service initially declined to engage the Privacy Commissioner as the disclosures were made by CRA, in the interests of full transparency, a letter was sent to the Privacy Commissioner by the Service on 13 July 2015 advising of the full extent of the disclosures. The Privacy Commissioner has responded requesting additional information; CSIS will continue to work with the Privacy Commissioner to the extent possible.

TOP SECRET



**SIRC Investigation: Denial of a Security Clearance (1)**

SIRC investigated a complaint under s.42 of the CSIS Act regarding denial of a Top Secret security clearance which brought into question the complainant's loyalty and reliability. The complainant was denied a security clearance at any level, including reliability, based on the findings of the investigation. As such, the complainant was informed that they could not be employed by the Department. SIRC found that the information with respect to the complainant's loyalty was not supported by the evidence and was not persuaded the complainant had lacked candour in related proceedings. However, SIRC found there were reasonable grounds to question the complainant's reliability and recommended that the decision to deny the clearance be upheld.

*SIRC Recommendation:*

None.

*CSIS Response:*

N/A

**SIRC Investigation: Denial of a Security Clearance (2)**

SIRC investigated a complaint under s.42 of the CSIS Act regarding denial of a security clearance at any level. The decision was based on investigations carried out both by the Service and the Department which identified concerns with the complainant's associations with a foreign intelligence service. SIRC found there were reasonable grounds to deny the security clearance and was satisfied with the procedural fairness afforded the complainant during the CSIS screening and Department review process. SIRC rejected complaints with regard to the conduct of the CSIS interviewer during one of the interviews based on a review of the interview tapes.

*SIRC Recommendation:*

None

*CSIS Response:*

N/A

**SIRC Investigation: Denial of a Security Clearance (3)**

SIRC investigated a complaint under s.42 of the CSIS Act regarding denial of a secret level security clearance. The complainant, who was working in the position prior to obtaining the clearance, was terminated after the denial. SIRC found there were reasonable grounds to question the complainant's reliability as it related to loyalty and recommended the denial be upheld.

*SIRC Recommendation:*

None.

*CSIS Response:*

N/A

TOP SECRET/



**SIRC Investigation: Denial of Site Access Security Clearance**

SIRC investigated a complaint under s.41 of the CSIS Act in which the complainant was denied Site Access Certification to the [redacted] Office. The complainant had previously been granted clearance to the location but was denied the two following years. SIRC found that CSIS did not consider all relevant information in its holdings and that the complainant should have been granted access. SIRC recommended that the complainant's next application be granted unless new adverse information came to light.

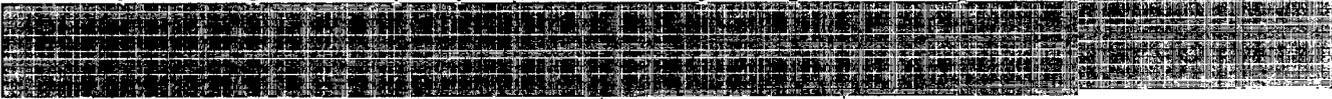
*SIRC Recommendation:*

SIRC recommended that a new Site Access Certification Direction, which was adopted in the [redacted] office, be adopted in all regional offices with the required modifications and that the program be reviewed in light of the new Standard on Security Screening.

*CSIS Response:*

*agreed*

CSIS agreed with the recommendation and sent a memo to all regional offices to ensure any Site Access Certification denials were made at the appropriate level of authority. The SA Certification process is being replaced with policies and procedures in keeping with the new Treasury Board Security Screening Standard (2014) which has a three-year implementation period.



**SIRC Investigation: Allegation of harassment, discrimination and profiling**

SIRC investigated a complaint under s.41 of the CSIS Act in which the complainant alleged he had been the victim of harassment, discrimination and profiling following three interviews by CSIS intelligence officers (IOs). SIRC found that the allegations were without merit and that the IOs had acted in accordance with the CSIS Act, Ministerial Direction and relevant CSIS policies.

*SIRC Recommendation:*

None.

*CSIS Response:*

N/A

# SIRC Recommendations Fully Agreed by CSIS



BUILDING A SAFE AND RESILIENT CANADA

TOP SECRET //



## CSIS' Relationship and Exchanges with DFATD (Key Issue #1)

- Establish mechanisms to ensure that human source operations do not contravene UNAQTR or other Governor-in-Council regulations

- CSIS is working with Global Affairs Canada and the Department of Justice to identify relevant statutes



## CSIS' Use of Metadata

- Enhance feedback on utility of [REDACTED]

- CSIS is developing new procedures and processes to enhance feedback



(This recommendation is not related to Key Issue #2)

## The "Insider Threat" and its Effect on Information Management (Key Issue #3)

- Create a more detailed policy on conduct of Internal Security investigations
- Ensure proper documentation of decision making pertaining to internal investigations

- CSIS internal policy has been revised
- CSIS internal policy have been revised

## CSIS collection of CRA Information (Key Issue #4)

- Conduct a post-mortem to assess adequacy of CSIS' management of the incident
- Clarify the scope of the incident to the Federal Court and the Minister
- Advise the Privacy Commissioner of the incident

- CSIS conducted a post-mortem of the incident; internal policy changes have been made
- CSIS wrote a letter to the Federal Court in July 2015; Minister was given an update in August 2015
- CSIS sent a letter to the Privacy Commissioner in July 2015



# SIRC Recommendations Fully Agreed by CSIS (Continued)



BUILDING A SAFE AND RESILIENT CANADA

TOP SECRET // [REDACTED]

## A Counter-Terrorism Investigation [REDACTED]

- Require CSIS employees to document their rationale for choosing not to follow internal expert advice obtained through mandatory consultations required by CSIS policy.

- CSIS agreed. [REDACTED]

## Denial of CSIS Site Access Clearance (Complaint)

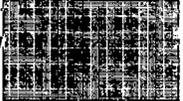
- All regional offices should adopt the Site Access Certification direction implemented at the [REDACTED] Office
- The CSIS Site Access Certification program should be reviewed in light of the new Treasury Board Security Screening Standard

- All Regional Offices have been sent a memo to ensure any Site Access Certification denials were made at the appropriate level of authority
- Policies and procedures consistent with the new Treasury Board Security Screening Standard are being put in place



# SIRC Recommendations Partially Agreed by CSIS



BUILDING A SAFE AND RESILIENT CANADA  
**TOP SECRET** / 

## CSIS' Relationship and Exchanges with DFATD

- CSIS and GAC should create clear deconfliction guidelines (This recommendation is not related to Key Issue #1)

- CSIS will discuss areas where existing deconfliction processes may not be adequate during regular meetings with GAC

## The "Insider Threat" and its Effect on Information Management (Key Issue #3)

- CSIS should develop robust procedures governing access lists (i.e. access to documents)
- CSIS should create a robust training/mentoring program suited to the unique work of Internal Security investigators

- CSIS agrees in principle, but has a different approach to implementation
- CSIS believes that formal intelligence officer training is sufficient, but there may be an opportunity to review the current informal mentoring process and produce guidelines on best practices

## CSIS collection of CRA Information (Key Issue #4)

- The CSIS Internal Audit unit should be tasked to address any substandard managerial or communications practices identified in the  office

- CSIS has already conducted an internal review of the incident (in lieu of an audit).

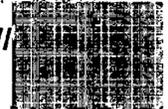




# SIRC Recommendations Rejected by CSIS

BUILDING A SAFE AND RESILIENT CANADA

TOP SECRET //



## CSIS' Relationship and Exchanges with DFATD

- CSIS should renegotiate its 2007 protocol with Global Affairs Canada (GAC) (This recommendation is not related to Key Issue #1)

- CSIS will discuss the protocol during regular engagements between CSIS and GAC senior management

## CSIS' Use of Metadata (Key Issue #2)

- CSIS should make the Federal Court aware of its specific metadata use and retention policies

- CSIS' position is that the fact that CSIS retains metadata has been clearly communicated to the Federal Court. CSIS further believes that there is no need to provide additional information regarding how metadata is used since the *CSIS Act* does not confer the Federal Court with oversight or supervisory authority over CSIS.

## The "Insider Threat" and its Effect on Information Management (Key Issue #3)

- CSIS undertake a full review of an internal investigation regarding a CSIS employee
- CSIS Internal Security should forward final investigation reports to an external unit (within CSIS) for review

- CSIS conducted a partial review and is satisfied with the outcome of the investigation.
- CSIS believes that forwarding reports to an outside unit would jeopardize the confidentiality and sensitivity of internal investigations



Public Safety  
Canada

Sécurité publique  
Canada

**Pages 571 to / à 572**  
**are withheld pursuant to sections**  
**sont retenues en vertu des articles**

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

**Pages 573 to / à 575**  
**are withheld pursuant to sections**  
**sont retenues en vertu des articles**

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

**Page 576**

**is withheld pursuant to sections  
est retenue en vertu des articles**

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



Public Safety    Sécurité publique  
Canada            Canada

Deputy Minister    Sous-ministre

Ottawa, Canada  
K1A 0P8

**TOP SECRET**

DATE:

File No.: 6210/008920

**MEMORANDUM FOR THE MINISTER**

**EN BANC HEARING OF THE FEDERAL COURT IN RELATION TO CSIS  
WARRANT APPLICATION ( [REDACTED] )**

(For Information)

**ISSUE**

To provide an update on the Federal Court *en banc* hearing regarding CSIS warrant application [REDACTED] as well as issues related to CSIS' use and retention of metadata, which occurred February 25-26, 2016.

**BACKGROUND**

CSIS' warrant application [REDACTED] which you approved on February 20, 2016, proposed to amend certain warrant conditions. As you will recall, the proposed amendments sought to address questions the Federal Court has asked over the past year, particularly regarding the definition of "destroyed" in warrants, and the period of time that CSIS has to assess third party information that it collects through warrants.

In hearing this warrant application, the Court also explored issues raised by the Security Intelligence Review Committee (SIRC) related to the retention and use of metadata, as well as SIRC's comments regarding CSIS' transparency with the Court on this issue.

**CURRENT STATUS**

The *en banc* hearing proceeded on February 25-26, before the eleven designated judges of the Federal Court, with Noël J. presiding over the application for warrants. Two *amici curiae* were appointed by the Court, and participated in the hearing.

The Court was satisfied that the threat to the security of Canada posed by the activities being investigated had been established. However, the Court indicated that the warrants sought will only be issued for a period of [REDACTED] since the Court wishes to thoroughly examine the impact that section 12 warrants, in general, may have on third parties.

Through this application, the Court is taking the opportunity to review the standard wording for all s.12 warrants, especially when it comes to the incidental collection of third party information and the conditions dealing with the collection, destruction and retention of such information.

The hearing is to resume at the end of March, when the Court expects to receive additional detailed evidence on the manner in which CSIS exercises the powers granted by warrants, notably in relation to the manner in which they affect third parties. Legal submissions will be filed for this hearing.

The Court also remains interested in exploring issues related to transparency with respect to metadata. The approach it will take to do so has yet to be confirmed.

#### NEXT STEPS

Departmental officials will continue to work with CSIS to learn more about the implications of the Court's decision on the warrant application. We will keep you apprised of further developments as they occur.

Should you require additional information, please do not hesitate to contact me or Monik Beauregard, Senior Assistant Deputy Minister, National and Cyber Security, at 613-990-4976.

François Guimont

Prepared by: [REDACTED]

Canadian Security Intelligence Service



Service canadien du renseignement de sécurité

Director - Directeur

CCM # 23637  
TOP SECRET  
For Information

AVR 1-1 2016

MEMORANDUM TO THE MINISTER

FEDERAL COURT WARRANT EXAMINATION: EN BANC HEARING

SUMMARY

- On 25 and 26 February, the Canadian Security Intelligence Service (CSIS) appeared in an *en banc* hearing before the Federal Court in relation to proposed amendments to six section 12 warrant conditions and to the category of employees that may make determinations pursuant to [REDACTED]. The matter was continued on 31 March and 1 April.
- The Federal Court expressed appreciation with the information provided by the Service thus far. The Court requested legal submissions on issues that will require further evidence on the utility of associated data and the circumstances surrounding the Service's decisions on retention of associated data since 2006.

BACKGROUND:

In the course of an investigation, CSIS may obtain warrant powers against targets to authorize the use of specific investigative techniques. These powers allow CSIS to intercept communications destined to, received by, or originating from, devices or accounts that are owned by a target. [REDACTED]

[REDACTED] Execution of any of these warrant powers may result in the incidental collection of information from parties other than the target (i.e. third parties).

When the Service intercepts communications, it obtains the content of the communication, as well as its associated data [referred to by the Security Intelligence Review Committee (SIRC) as metadata]. Associated data is information, in structured fields, linked with a communication. Examples include email addresses, telephone numbers, [REDACTED] as well as duration, dates and [REDACTED]

times of phone calls or Internet sessions. It does not include any information that could reveal the purpose of the communication, nor any part of its content.

Existing policies and procedures require that, subject to the exception for data related to solicitor-client communications, which is deleted immediately, information and communications intercepts collected under warrant, whether from a third party or not, found to be of no intelligence value be destroyed [REDACTED]. This policy, however, does not apply to associated data.

### DISCUSSION:

On 25-26 February 2016, CSIS sought to renew and obtain new warrants for targeted individuals, while also proposing amendments to warrant conditions. The application was heard *en banc*, or as a panel. While the Court was satisfied that the threat to the security of Canada posed by the activities being investigated had been established, it did not render a decision on the Service's proposed amendments to warrant conditions.

At that hearing, the Court indicated that it wished to more thoroughly examine the impact that section 12 warrants may have on third parties. It also requested that the Service provide further evidence regarding the collection, use, retention and destruction of associated data collected under warrants issued by the Court. This, owing to a finding in SIRC's annual report (2014-15) that the Service's transparency with the Federal Court in this regard was insufficient.

Further to the hearing and in response to the Court's request, CSIS filed two supplemental affidavits. The first described the process used to manage the way in which the Service conducts its warranted collection. [REDACTED]

[REDACTED] particular emphasis was placed on the manner in which CSIS may execute warrants related to [REDACTED]

The second affidavit addressed the Service's collection, processing, use and retention of associated data, including several examples of the foregoing and an analysis of its investigative value. Through this affidavit, CSIS also proposed that associated data related to third party communications intercepts found to be of no intelligence value be retained for a period of [REDACTED]

[REDACTED] This is a shift from current practice, whereby no such limit exists. Both affidavits included several examples aimed at demonstrating that there is an operational need that justifies the retention of associated data and that measures are in place to limit the impact on third parties.

The hearing resumed on 31 March and 1 April. While the Court was appreciative of the Service's illustration that associated data is valuable, questions remain regarding the value of retaining associated data over time. As such, CSIS will be offering further evidence to address this issue.

The Court requested written submissions to determine whether the wording of warrants, as proposed, strikes an appropriate balance between CSIS operational needs and third party privacy rights. The Court also requested submissions pertaining to the legal basis pursuant to which CSIS has retained associated data since 2006, when this practice appears to have begun. In response,

the Service will file an affidavit including evidence of the circumstances surrounding the Service's decisions related to the retention of associated data since 2006.

It is anticipated that the Court will be satisfied with the proposed amendments to section 12 warrant conditions, with minimal amendments to the proposed wording. These allow the Service to

[REDACTED]  
[REDACTED]  
[REDACTED] Other new conditions specifically govern [REDACTED]  
[REDACTED] prevent the Service from retrieving information that was destroyed pursuant to a warrant condition; and, alter the designated employees in warrant conditions relating to the retention of information and communications.

**NEXT STEPS:**

On 7 April, the Service advised the Court that it will be filing two additional affidavits. The first will pertain to the utility of associated data and the second will pertain to the circumstances surrounding CSIS' decision to, in 2006, retain associated data. Provided that the Court is in agreement with this proposal, both affidavits will be filed by 21 April. CSIS will submit legal submissions shortly after, at a date to be set by the Court.

Of note, on 7 April, the Attorney General of Canada provided information to the Court related to SIRC's findings regarding the Service's transparency with the Court on issues related to associated data. This was provided in response to a 23 March request from the Honourable Chief Justice Crampton, who requested this information to assist the Court in understanding the basis upon which SIRC formulated its recommendation. It is possible that the information provided by the Attorney General will further inform the designated judges sitting in the *en banc* hearing.

I wish to reiterate that the Service takes its duty of candour very seriously and will continue to work in a forthright manner with the Court. I will keep you apprised of any new developments. As always, please do not hesitate to contact me should you require further information.

  
Michel Coulombe

cc.: National Security Advisor  
Deputy Minister, Public Safety

This document constitutes a record which may be subject to mandatory exemption under the *Access to Information Act* or the *Privacy Act*. The information or intelligence may also be protected by the provisions of the *Canada Evidence Act*. The information or intelligence must not be disclosed or used as evidence without prior consultation with the Canadian Security Intelligence Service.

Canadian Security  
Intelligence Service



Service canadien du  
renseignement de sécurité

Director - Directeur

CCM #24382  
TOP SECRET  
For Information

JUN 29 2016

MEMORANDUM TO THE MINISTER

UPDATE ON *EN BANC* HEARINGS AND THE SERVICE'S RETENTION AND  
DESTRUCTION OF WARRANTED COLLECTION

ISSUE:

Further to my memorandum of April 11, to provide an update regarding the Canadian Security Intelligence Service's (CSIS) involvement in *en banc* hearings, as well as related engagements with the Federal Court.

BACKGROUND:

In early 2016, CSIS sought to renew and obtain new warrants for targeted individuals, while also proposing amendments to warrant conditions. The application was heard *en banc*, or as a panel. At that hearing, the Court indicated that it wished to more thoroughly examine the impact that section 12 warrants may have on third parties. The hearing resumed on March 31 and April 1 and the Court requested written submissions to determine whether the wording of warrants, as proposed, strikes an appropriate balance between CSIS operational needs and third party privacy rights. The Court also requested submissions pertaining to the legal basis pursuant to which CSIS has retained associated data since 2006. In support of these requirements, CSIS filed two affidavits on April 21 and submissions on June 22.

DISCUSSION:

The Court has continued to issue warrants

r. A decision is not expected until fall 2016

As we do not expect a decision from the Court in these matters before the last part of October,

In addition, my previous memorandum noted that the Attorney General of Canada provided information to the Court regarding the Security Intelligence Review Committee's (SIRC)

TOP SECRET

findings regarding the Service's transparency with the Court on issues related to associated data filed on June 8.

On June 10, I appeared before the Federal Court with the Deputy Minister of Justice to address issues identified by the Court in relation to transparency and duty of candor. We presented a series of measures proposed to address the issues identified by the Court, including the adoption of a joint policy on the duty of candour in *ex parte* proceedings and the review of collection, retention, and destruction practices related to the execution of warrants.

In addition, I undertook to advise the Court promptly of matters relevant to applications for warrants as they may become identified pursuant to internal audits or SIRC reviews. I also reiterated CSIS' commitment to resolving the matters identified by the Court, and to implement corrective measures as they are identified. Throughout, I emphasized full mindfulness of the Service's duties in terms of candour and the rule of law.

On a related matter, further to my May 26 memorandum to you regarding the [REDACTED]

[REDACTED] The Court acknowledged having received the report.

**NEXT STEPS:**

[REDACTED] The objective is to identify and address any gaps to guarantee the highest level of assurance of compliance with warrant conditions, including a governance mechanism with clear points of accountability. An initial report is scheduled to be provided to me in late September, 2016.

I wish to reiterate that the Service has and will continue to take its duty of candour very seriously and will continue to work in a forthright manner with the Court. I will keep you apprised of any new developments.

As always, please do not hesitate to contact me should you require further information.

  
Michel Coulombe

cc.: Deputy Minister, Public Safety

This document constitutes a record which may be subject to mandatory exemption under the *Access to Information Act* or the *Privacy Act*. The information or intelligence may also be protected by the provisions of the *Canada Evidence Act*. The information or intelligence must not be disclosed or used as evidence without prior consultation with the Canadian Security Intelligence Service.



Public Safety    Sécurité publique  
Canada            Canada

Deputy Minister    Sous-ministre

Ottawa, Canada  
K1A 0P8

**TOP SECRET // SI //**

DATE: AUG - 5 2018

File No.: 6210 / 24011 / 011246

**MEMORANDUM FOR THE MINISTER**

**SECURITY INTELLIGENCE REVIEW COMMITTEE REPORTS IN 2015-16  
AND CERTIFICATE OF 2014-15 CSIS DIRECTOR'S REPORT**

(Information only)

**ISSUE**

Reviews and complaints completed by the Security Intelligence Review Committee (SIRC) in 2015-16 (TAB A), and SIRC's Certificate for the 2014-15 Annual Report of the Director of the Canadian Security Intelligence Service (CSIS) (TAB B).

**BACKGROUND**

SIRC carries out its mandate through three main activities: 1) SIRC reviews a sample of CSIS activities to ensure that CSIS is complying with the law and exercising its powers in a reasonable and necessary way; 2) SIRC investigates any complaints against CSIS and; 3) SIRC provides you with a Certificate on the Director's Report on operational activities, stating the extent to which SIRC is satisfied with the Report and whether the activities described therein complied with the law and Ministerial Direction (MD). SIRC summarizes these activities in its Annual Report to Parliament.

Over the course of the year, we immediately provide you with memoranda of advice on any SIRC reports that raise significant issues. This year, we have already provided you with two such studies under separate cover. One concerned CSIS's foreign fighters investigation, [REDACTED] (TAB C). The other reviewed CSIS threat reduction activities (TRAs) (TAB D).

This note provides you with our analysis of the issues raised across the seven remaining reviews and one complaint investigation SIRC completed this year. It also addresses the issues SIRC raised in its Certificate of the 2014-15 Director's Report.

.../2

**Canada**



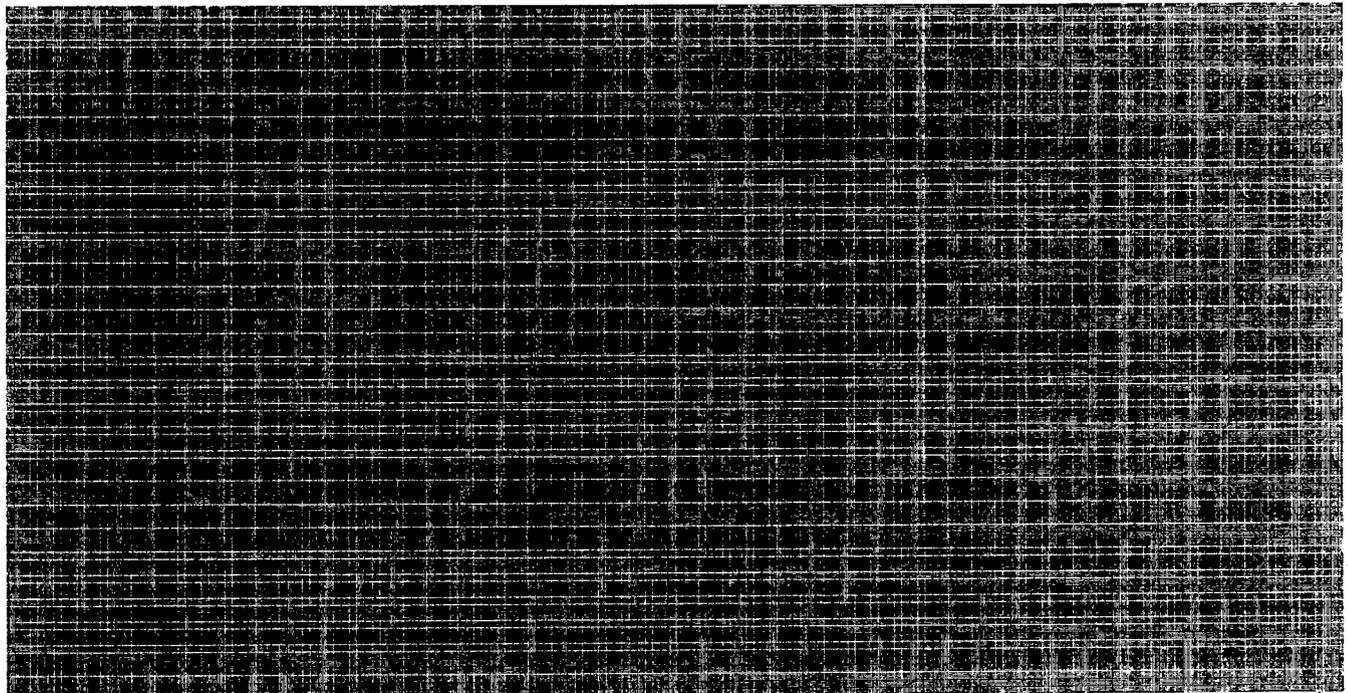
**CURRENT STATUS**

We have attached a table containing the SIRC's findings and recommendations in all reviews at **TAB E**. SIRC's findings were generally positive in six of the nine reviews; more problematic reviews (discussed below) pertained to CSIS's foreign fighter investigation, its bulk data-related activities, and [REDACTED]. SIRC's positive findings were that CSIS has sound policies and procedures for information sharing with foreign entities, [REDACTED] and for TRAs. SIRC also found that [REDACTED] has a constructive relationship with its partners; and that CSIS soundly managed its relationship with the Canada Border Services Agency. Finally, SIRC found there was "overwhelming" evidence to dismiss the complaint it completed investigating this year.

*Certificate*

SIRC was satisfied, overall, with the Director's Report, finding that it was accurate, fulfilled Ministerial reporting requirements, and placed information in its proper context. SIRC has also highlighted improvements to the Report. Last year SIRC concluded that the "Director's [R]eport had become less effective as a tool for Ministerial responsibility" and recommended the Minister provide "more specific instructions to [CSIS] with respect to format and structure". This was a key consideration for Public Safety Canada (PS) in developing the 2015 MD on *Operations and Accountability*. SIRC found the latest Director's Report to be "more concise and focused on issues of ministerial concern", as was intended in the new MD.

SIRC concluded in its Certificate that, "notwithstanding a few exceptions," (discussed below) the activities described in the Director's Report, and examined in SIRC's reviews, complied with the law, MD, and "did not constitute an unreasonable or unnecessary exercise of CSIS's powers."



*CSIS's Data Acquisition Program Raises Significant Concerns*

CSIS supports its investigations through the acquisition and analysis of bulk datasets that contain vast amounts of information [REDACTED]

[REDACTED] In its review on this matter, SIRC raised concerns regarding the compliance of these activities with the principle of proportionality anchored in s.12 of the *CSIS Act*, which stipulates that CSIS shall collect information "to the extent that it is strictly necessary." SIRC believes that this provision creates a high threshold under which the expected value of information must be sufficient to justify the intrusion on privacy associated with its collection. According to SIRC, this in turn requires "an assessment of whether the information could not reasonably be obtained by less intrusive means."

With these principles in mind, SIRC raised similar concerns with regard to the several different bulk dataset-related activities it examined: 1) CSIS's dataset acquisition effectively constituted collection of information on people [REDACTED]

[REDACTED] 2) CSIS framed its justification for such collection in terms of the information's [REDACTED]

SIRC believes there is a long-term potential for these practices to result in [REDACTED]

[REDACTED] SIRC has recommended that CSIS finalize work on a governance framework, giving due consideration to the principle of proportionality.

You may wish to note that SIRC also raised concerns regarding bulk data practices last year, specifically regarding CSIS's use of metadata collected under warrant.

[REDACTED] *Incident of Non-Compliance with the CSIS Act*

One review included a non-compliance incident that SIRC also discusses in its Certificate. The incident involved [REDACTED]

[REDACTED] SIRC did not find that this was the result of any deliberate effort on CSIS's part to violate the warrant, but rather reflected "confusion" on the part of CSIS managers. SIRC is satisfied with CSIS's efforts to address this issue. CSIS has also reported the incident to your predecessor, pursuant to s.20 of the *CSIS Act*; PS prepared a note of advice for him at that time (TAB H)

*Framework for Information Sharing with Foreign Entities*

SIRC's findings in its review of CSIS's governance framework for the 2011 MD on *Information Sharing with Foreign Entities* were generally positive. As you know, this MD has been the subject of public criticism. In its review, however, SIRC did not

**TOP SECRET // SI //**

identify problems with the MD itself. SIRC also found that CSIS had "acted quickly to implement a sound information-sharing framework" in response to the MD. Furthermore, SIRC found that senior CSIS executives appropriately managed all cases that were referred to the Information Sharing Evaluation Committee (ISEC).

SIRC did, however, identify examples of errors and inconsistencies in the application of the framework at the Deputy Director General (DDG) level. [REDACTED]

[REDACTED] in its Certificate, SIRC also "cautioned" CSIS on the limits of caveats and assurances in mitigating the risks of engaging with countries with poor human rights records.

*Resource Issues*

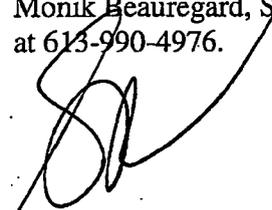
For the second year in a row, SIRC has highlighted issues related to CSIS's constrained resources and the impact [REDACTED]

In this year's review of economic security intelligence activities, SIRC found that limited resources were among the challenges for CSIS [REDACTED]

**NEXT STEPS**

SIRC's statutory deadline to submit its Annual Report to you is September 30 and you are required to table the Report in Parliament within fifteen sitting days of its receipt. We will provide you with tabling advice when we receive the Report.

Should you require additional information, please do not hesitate to contact me or Monik Beaugard, Senior Assistant Deputy Minister, National and Cyber Security, at 613-990-4976.

  
Malcolm Brown

Enclosure: (8)

Prepared by [REDACTED]

Security Intelligence  
Review Committee



Comité de surveillance des activités  
de renseignement de sécurité

Office of the Chairman

Bureau du président

**TOP SECRET** 

File No.: 2800-200

July 13, 2016

The Honourable Ralph Goodale  
Minister of Public Safety and Emergency Preparedness  
Public Safety Canada  
Minister's Office  
269 Laurier Avenue West  
Ottawa, Ontario  
K1A 0P8

Dear Minister:

**RE: CERTIFICATION OF THE DIRECTOR'S ANNUAL REPORT TO THE  
MINISTER OF PUBLIC SAFETY**

---

Pursuant to subsection 38(2) of the *Canadian Security Intelligence Service Act (CSIS Act)*, SIRC is required to submit to you, the Minister of Public Safety, a Certificate stating the extent to which it is satisfied with the CSIS Director's report; whether the operational activities described in the Director's report contravened the *CSIS Act* or Ministerial Directions; and whether the activities described in the report involved any unreasonable or unnecessary use of CSIS's powers. Our Certificate therefore provides an important high-level assessment of the legality, reasonableness and necessity of CSIS's operational activities.

To fulfill its responsibility for the certification process, SIRC relies on a carefully designed and rigorous research methodology. To assess its satisfaction with the Director's report, SIRC situates the statements made in the report against SIRC's knowledge of CSIS's operations and challenges. To that end, SIRC conducted an extensive review of CSIS information holdings and requested briefings with CSIS officials to ensure that the information in the Director's report is placed in its proper context. SIRC grounds its assessment of CSIS's compliance with the *CSIS Act* and Ministerial Directions and whether SIRC considers any use by CSIS of its powers to be

P.O. Box / C.P. 2430, Station / Succursale "D"  
Ottawa, Canada K1P 5W5  
613 990-8441

000588  
000585

unreasonable or unnecessary in reviews of several specific operations and activities referred to in the Director's report, as well as a sample of core CSIS activities. In addition, SIRC's on-going review work, which yields important findings and recommendations, directly supports the certification process.

## **SATISFACTION WITH THE DIRECTOR'S ANNUAL REPORT**

SIRC's approach to the certification process has evolved in the past three years. Last year, as CSIS was entering a period of change with the expansion of its mandate, the Committee undertook to study the question of whether the Director's report was serving well the requirements of Ministerial responsibility. Of particular concern to the Committee was whether the report remained true to its original intent - to make available to the Minister important information as to the functioning of CSIS. The Committee believed that the proper flow of information to the Minister is especially important in the current context.

The Committee concluded that the Director's report had become less effective as a tool of Ministerial responsibility in that the level of detail contained in the report had the effect of obscuring the more important information for Ministerial consideration, including serious issues, challenges, and potentially controversial activities. To address this, SIRC recommended that "the Minister make his expectations with respect to both the Director's Annual Report and the system of notifications explicit in the form of a new Ministerial Direction on Responsibility and Accountability with more specific instructions to the Service with respect to the format and structure, as well as the timing, of the Director's Report."

SIRC is pleased that its observations, and recommendation, were well received: new and more explicit direction to the Director with respect to the report is included in the Ministerial Direction issued in July 2015. The Committee believes that the new format for the report adopted by CSIS is a more effective support to your responsibility for the activities undertaken by CSIS: the report is more concise and focused on issues of ministerial concern. As a result, the Committee believes that SIRC has an even stronger foundation on which to organize its work in support of the Certificate.

Accordingly, SIRC's satisfaction with the Director's report is based on its assessment of the extent to which the report provides you with information to assist in exercising Ministerial responsibility for CSIS. To make this assessment, SIRC used several criteria. First, SIRC examined whether the report met the Ministerial reporting requirements set out in the 2008 Ministerial Direction on Operations and the 2014-2016 Ministerial Direction on Intelligence Priorities. Second, SIRC assessed whether the report included due attention to issues of Ministerial concern and put the information in

its proper context. It did so by reviewing the statements in the report against CSIS information holdings, submitting questions, as well as requesting additional documentation and briefings on specific areas of CSIS activities. Third, SIRC assessed whether the report provided an accurate representation of CSIS activities and was factually accurate. To this end, SIRC conducted a sample review of the facting materials and submitted requests for statistics and information on CSIS operational activities.

**Overall, SIRC was satisfied with the Director's report. The Committee found that it fulfilled Ministerial reporting requirements, that information was placed in its proper context and was factually accurate.** With respect to the new format of the report, SIRC acknowledges CSIS's work toward revising the format of the report to better support your requirements.

### **COMPLIANCE WITH THE CSIS ACT AND MINISTERIAL DIRECTIVES AND EXERCISE OF CSIS'S POWER**

The *CSIS Act* also requires SIRC to state whether, in its opinion, the operational activities described in the Director's report contravened the *CSIS Act* or Ministerial Directions and whether the activities involved any unreasonable or unnecessary use of the Service's powers. To make this assessment, SIRC reviewed Ministerial Direction to CSIS, including an examination of your Ministerial Direction on operations and that on intelligence priorities, as well as the Ministerial Direction on Information Sharing with Foreign Entities. In addition, SIRC reviewed several specific operations and activities referred to in the Director's report, as well as a sample of the core CSIS activities that support the operations described in the report, described below.

SIRC examined a sample of CSIS's collection on [REDACTED]

[REDACTED]

SIRC examined a sample of [REDACTED]

[REDACTED] which authorizes CSIS to obtain [REDACTED] where there are "reasonable grounds to believe [REDACTED]

[REDACTED]" SIRC was satisfied with the justifications provided and that the collection advanced CSIS's investigation into threat-related activity.

In addition, SIRC looked at several [REDACTED], including the [REDACTED]

[REDACTED] SIRC found that the decision to use [REDACTED]

SIRC questioned whether the risk assessment could have been completed in a more timely manner as this would have allowed the Minister to be "consulted" as required by Ministerial Direction instead of "informed." [REDACTED]

Finally, SIRC conducted a full length study to evaluate CSIS's compliance with the Ministerial Direction on Information Sharing with Foreign Entities. SIRC found that, overall, CSIS has implemented a sound framework for sharing information with foreign entities where there may be a risk of mistreatment. At the same time, however, SIRC found that there were gaps in both the application of CSIS's internal directive on information sharing and in CSIS's recording of the decision-making process. SIRC also cautioned CSIS to keep in mind that risk mitigation techniques, like caveats and assurances, have their limitations. [REDACTED]

[REDACTED] In view of the seriousness of this issue, SIRC will continue to make CSIS's information-sharing policies and practices an integral component of SIRC's annual reviews and certification process.

**SIRC is of the opinion that, notwithstanding a few exceptions identified in the report, some of which are described below, the activities described in the Director's report and those assessed as part of SIRC's review activities complied with the *CSIS Act* and Ministerial Directions and did not constitute an unreasonable or unnecessary exercise of CSIS's powers.**

#### **Subsection 20(2) incident of non-compliance with *CSIS Act***

The Director's report contains an incident that CSIS assessed to be non-compliance with the *CSIS Act* pursuant to subsection 20(2). Upon notification, SIRC commenced a review of the incident. SIRC agreed with CSIS [REDACTED]

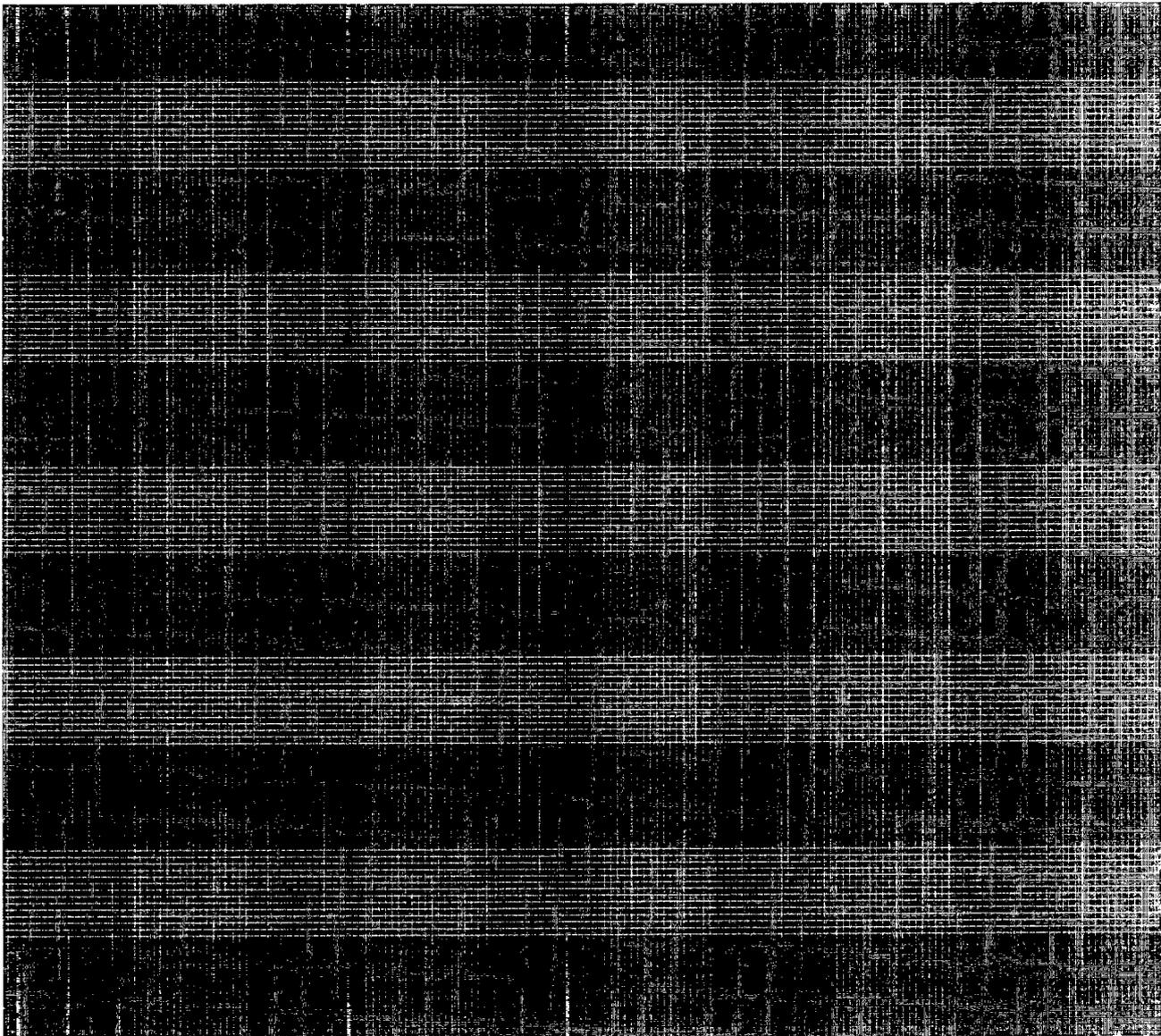
[REDACTED] SIRC also agrees with the actions undertaken by CSIS in response, described in the Director's report, [REDACTED]

[REDACTED] In its review, however, SIRC went a step further and made several recommendations to address deficiencies it observed, including the use of [REDACTED] changes to operational policy [REDACTED] and improved access [REDACTED]

to legal opinions. SIRC also noted that CSIS lacked a formal process for subsection 20(2) incidents and recommended that one be put in place.

**Improperly Obtaining Information from the Canadian Revenue Agency (CRA)**

SIRC reviewed the circumstances in which CSIS obtained taxpayer information from the Canadian Revenue Agency (CRA) without a warrant. During the review, SIRC found that the scope of the incident was wider than had been initially implied to SIRC. SIRC found that the Federal Court had similarly not been advised of the full scope. Although there was no evidence that there was a systemic problem, SIRC found that the incident was not managed adequately. The review resulted in several recommendations, including an internal audit of the regional office in question.



## THREAT REDUCTION ACTIVITIES

The *Anti-terrorism Act, 2015* confers on SIRC the responsibility to "each fiscal year, review at least one aspect of the Service's performance in taking measures to reduce threats to the security of Canada." To that end, SIRC's first review examined CSIS efforts to "operationalize" its new powers. SIRC found that CSIS has put in place a governance structure to guide its threat reduction activities. SIRC assesses the governance structure positively.

SIRC also assessed whether the governance structure adequately supports the direction provided to CSIS by you, in particular with respect to deconfliction and coordination with partners. SIRC is of the opinion that the Ministerial Direction related to threat reduction activities has established clear triggers for consultation with the RCMP and GAC and that CSIS has responded appropriately to this direction. At the same time, however, SIRC found that there is a need to further outline its own formal consultation process involving other implicated government departments and agencies and has made a recommendation to CSIS to that effect.

SIRC reviewed all the threat reduction activities completed by CSIS at the time of writing, [REDACTED] SIRC found that CSIS has taken a cautious approach to this new area of responsibility and that the activities undertaken thus far by CSIS complied with the *CSIS Act*, Ministerial Direction and operational policies. SIRC will continue to monitor on an on-going basis whether this remains the case going forward as the scope of CSIS's threat reduction activities expands.

## NEW MINISTERIAL DIRECTION TO CSIS

The Committee would like to take the opportunity to offer a few comments on selected elements of the new Ministerial Direction. As indicated, SIRC is pleased that more explicit direction has been given to CSIS with respect to the Director's report and accountability more generally. SIRC assesses that the new format for the report better supports your needs as Minister, as well as SIRC's own work under the Certificate. SIRC is also pleased with the direction to CSIS to include in the report an overview of CSIS operational activities abroad, which echoes SIRC's comments from previous Certificates with respect to the deficiency of information in the report on foreign operations.

From SIRC's perspective, the new Ministerial Direction is a better grounding for CSIS operations in the current context of change and expanding risk. To that end, SIRC notes your direction to CSIS with respect to its assessment of risk. SIRC's review of CSIS's Investigation of Canadian Foreign Fighters is a case in point: as [REDACTED]

[REDACTED] there is a corresponding need to fortify the risk assessment processes that must support those operations. Assessing CSIS's management of these new requirements with regard to risk will be a high priority for SIRC.

Similarly, SIRC notes the changes to the annex on [REDACTED]

[REDACTED] For

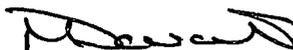
its part, SIRC will continue to look at this relationship closely.

### CONCLUSION

SIRC is aware that efforts are now underway at CSIS to "operationalize" your expectations as set out in the new Ministerial Direction in more concrete terms. The Committee looks forward to the opportunity of the next Certificate to offer its assessment of this effort insofar as it must support compliance with your direction and the exercise of ministerial responsibility.

In addition, the Committee would welcome the opportunity to be consulted in light of the important changes that are occurring in the national security environment. With 30 years of experience in review of security intelligence activities, SIRC brings much to the table. Indeed, SIRC's expertise and position allow it to provide objective information and advice, alongside its assurances to Parliament and to the Canadian public.

Yours sincerely,



for

The Honourable Pierre Blais, P.C.  
Chair



Public Safety    Sécurité publique  
Canada            Canada

Deputy Minister    Sous-ministre

Ottawa, Canada  
K1A 0P8

**COPY**

**SPECIAL HANDLING**

**TOP SECRET** / 

DATE:

File No.: 6210 / NI 23977 / CCM 010701

**MEMORANDUM FOR THE MINISTER**

**SIRC STUDY 2015-09: CSIS'S INVESTIGATION OF  
CANADIAN FOREIGN FIGHTERS**

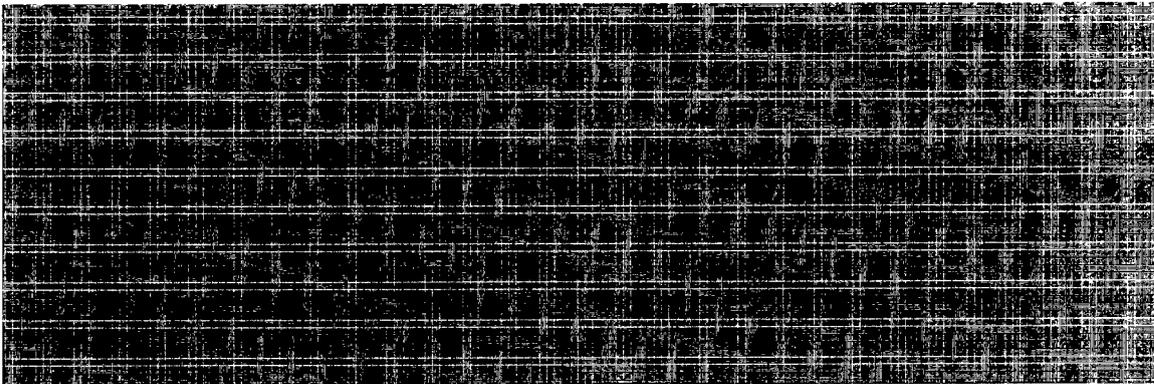
(Information only)

**ISSUE**

The Security Intelligence Review Committee (SIRC) has completed a study entitled "CSIS's Investigation of Canadian Foreign Fighters" 

 (TAB A):

**BACKGROUND**



.../2

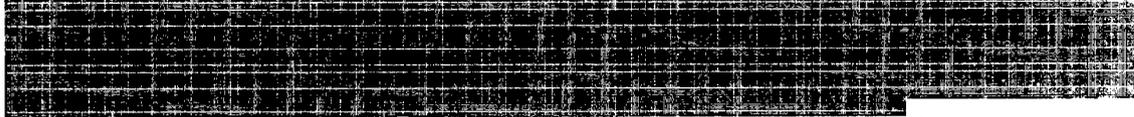
**Page 596**

**is withheld pursuant to sections  
est retenue en vertu des articles**

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

**NEXT STEPS**

The Director of CSIS plans to brief you on the SIRC study. 



Should you require additional information, please do not hesitate to contact me or  
Monik Beauregard, Senior Assistant Deputy Minister, National and Cyber Security,  
at 613-990-4976.

Malcolm Brown

Enclosure: (2)

Prepared by: 



Public Safety    Sécurité publique  
Canada            Canada

Deputy Minister    Sous-ministre

Ottawa, Canada  
K1A 0P8

**COPY**

**TOP SECRET // SI** 

DATE:

File No.: 6045 / NI 23982 / CCM 010731

**MEMORANDUM FOR THE MINISTER**

**SIRC STUDY 2015-07: REVIEW OF CSIS'S  
THREAT REDUCTION ACTIVITIES**

(Information only)

**ISSUE**

The Security Intelligence Review Committee (SIRC) has submitted its first "Review of CSIS's Threat Reduction Activities" (TAB A).

**BACKGROUND**

The *Anti-terrorism Act, 2015* conferred on CSIS a new mandate to reduce threats to the security of Canada. It also made corresponding adjustments to SIRC's mandate. Specifically, subsection 38(1.1) of the *CSIS Act* now requires SIRC to review at least one aspect of CSIS's performance in taking measures to reduce threats to the security of Canada each year.

In fulfilment of this legislative requirement, SIRC has produced its first review of CSIS's threat reduction activity. SIRC focused its study on how CSIS has operationalized its new mandate by examining the governance structures that have been put into place. SIRC also examined several threat reduction measures taken to date.

**CONSIDERATIONS**

Overall, SIRC found that CSIS's use of its new powers has complied with the *CSIS Act*, Ministerial Direction and internal operational policies. SIRC is also broadly satisfied with the governance structures now in place. Nonetheless, it cites a number of areas where CSIS could make improvements. In particular, it recommends that CSIS

.../2

**Canada**

expedite work to strengthen and formalize its mechanisms for coordinating threat reduction activity with other departments and agencies.

**NEXT STEPS**

SIRC will summarize its review in a future annual public report. SIRC's generally positive first impression of CSIS's threat reduction mandate will likely attract public attention.

SIRC notes that CSIS has not yet taken any threat reduction measures requiring a court warrant, but that CSIS could do so in future. At the conclusion of its review, SIRC commits to examining future warrant cases carefully.

Given the importance of CSIS's new mandate, you may wish to request briefings from the Director of CSIS and the Executive Director of SIRC on this report.

Should you require additional information, please do not hesitate to contact me or Monik Beauregard, Senior Assistant Deputy Minister, National and Cyber Security, at 613-990-4976.

Malcolm Brown

Enclosure: (1)

Prepared by: 

**Pages 600 to / à 604  
are withheld pursuant to sections  
sont retenues en vertu des articles**

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

**Pages 605 to / à 607  
are withheld pursuant to sections  
sont retenues en vertu des articles**

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



Sécurité publique Canada / Public Safety Canada

Sous-ministre / Deputy Minister

Ottawa, Canada  
K1A 0P8

**COPY**

TOP SECRET//SI



DATE: Nov 26, 2014

File No.: 6210/23232/001451

**MEMORANDUM FOR THE MINISTER**

**CANADIAN SECURITY INTELLIGENCE SERVICE WARRANT ISSUES**

(Signature Required)

**ISSUE**

To inform you of two recent Canadian Security Intelligence Service (CSIS) activities undertaken without proper warrant authorities, including one that the Director considers unlawful.

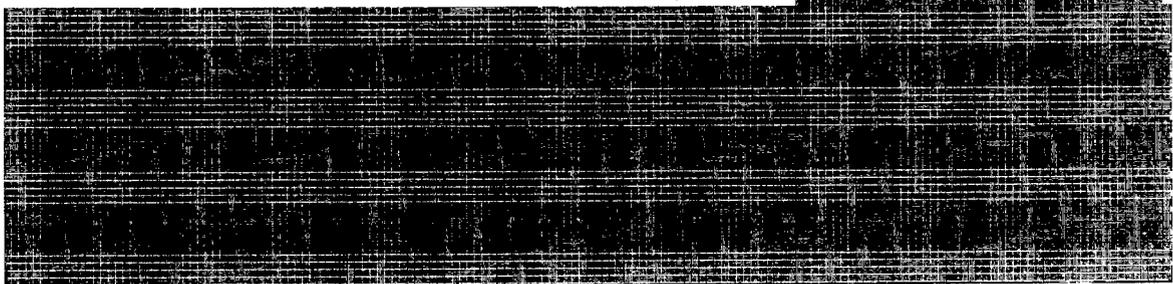
**BACKGROUND**

Pursuant to section 20 of the *CSIS Act*, when the Director is of the opinion that [redacted] he must inform you, [redacted] and in turn you must report the unlawful activity to the Attorney General of Canada and provide a copy of that report to the Security Intelligence Review Committee (SIRC).

**CURRENT STATUS**

**Unlawful Activity**

On October 16, 2014, the Director wrote to inform you of an [redacted]



.../2

**TOP SECRET**

Section 16 warrants authorize collection activities [REDACTED]

Public Safety Canada (PS) officials have discussed this incident with their CSIS counterparts, and agree that there was [REDACTED]

Since then, CSIS has deleted the intercept of the communication. CSIS has also issued a memorandum to all Directors General, clarifying responsibilities for section 16 operations; and it has issued a directive to all personnel on roles, responsibilities, and procedures for section 16 collection. In addition, CSIS is planning to undertake an internal review of section 16 warrants to ensure they are being interpreted consistently across the organization.

#### Collection of Information Without a Warrant

On October 28, 2014, the Director wrote to inform you of an incident relating to the unauthorized disclosure of Canada Revenue Agency (CRA) information to CSIS (Tab B).

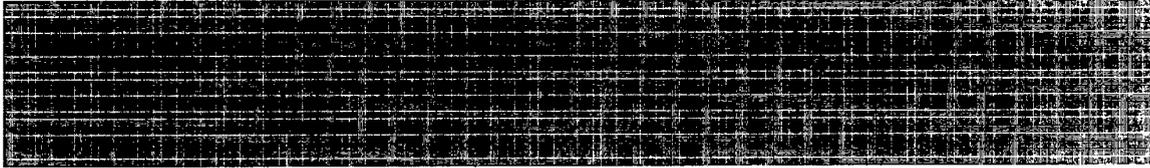
CSIS had filed an affidavit in support of a warrant application [REDACTED]. One sentence of the affidavit contained CRA information. A CRA employee had originally shared this information [REDACTED]. The CSIS officer [REDACTED] a CSIS-CRA MOU permitted information sharing without a warrant. CSIS does not believe its officer's conduct was unlawful [REDACTED]. Because there is no belief that the conduct was unlawful, there is no requirement for the Minister of Public Safety to send a letter to the Attorney General.

In March 2014, [REDACTED]

[REDACTED] as well as whether it had informed the Security Intelligence Review Committee (SIRC), the Privacy Commissioner, and/or the CRA Commissioner. In May, CSIS responded to the judge that it would issue a reminder to all personnel that a warrant is required for CRA to disclose taxpayer information, and that it would inform SIRC (which it has since done). CSIS has also engaged the CRA on this issue.

**TOP SECRET**

**RECOMMENDATION**



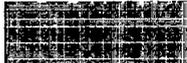
It is also recommended that you sign the letter to the Chair of SIRC, providing her with a copy of your letter to the Attorney General of Canada (**Tab D**).

Should you require additional information, please do not hesitate to contact me or Lynda Clairmont, Senior Assistant Deputy Minister, National and Cyber Security, at 613-990-4976.

  
Francis Guimont

Enclosures: (4)

Prepared by:



**TOP SECRET // SI // 1** [REDACTED]

SIRC Review	SIRC's Findings	SIRC's Recommendations
<p><b>"CSIS's Warranted Collection of Information:</b> [REDACTED]</p>	<p>[REDACTED] CSIS complied with Federal Court warrants, the <i>CSIS Act</i>, Ministerial Direction, and operational policy during the execution [REDACTED]</p>	<p>In addition to continuing to refine training, there is also opportunity for the [REDACTED] Policy Centre at CSIS Headquarters to develop other standardized processes to guide the future of [REDACTED]</p>
	<p>SIRC found no evidence to suggest that any CSIS employee deliberately acted in violation of the Federal Court's warrant(s) in the [REDACTED] where there were issues regarding compliance with warrants.</p>	
	<p>[REDACTED]</p>	<p>[REDACTED]</p>
	<p>There is no clear process within CSIS for accessing legal opinions and/or advice that have been issued by CSIS's Directorate of Legal Services.</p>	<p>CSIS should implement a process to ensure that relevant stakeholders have knowledge of, and access to, legal opinions and/or advice.</p>
<p>CSIS lacked a formal process for s.20 incidents.</p>	<p>CSIS should create a formal process for suspected s.20 incidents.</p>	

**TOP SECRET // SI**

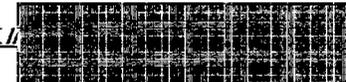


SIRC Review	SIRC's Findings	SIRC's Recommendations
<p><b>“Review of CSIS’s Use of Data Management and Exploitation Activities”</b></p>	<p>There is no governance framework guiding CSIS’s collection, retention, and use of bulk data. [REDACTED] bulk datasets did not meet CSIS’s own criteria regarding referential data, and as such, constituted “collection” as understood in s.12 of the <i>CSIS Act</i>.</p>	<p>The governance framework for bulk dataset acquisition be finalized and implemented no later than [REDACTED]. CSIS cease to acquire any additional bulk datasets until it has put in place a formal and documented process to assess whether such acquisitions are collected to the extent that is “strictly necessary,” taking into account SIRC’s considerations. This process also should be implemented no later than [REDACTED].</p>
	<p>CSIS Legal Services has not provided formal legal guidance regarding whether or not the acquisition of bulk datasets was consistent with CSIS’s mandate as outlined in s.12 of the <i>CSIS Act</i>.</p>	<p>Should the process noted above not be in place by [REDACTED] CSIS should discontinue its use of bulk datasets under the Data Acquisition Program until such time as a process is in place.</p>
	<p>There is no evidence to indicate that CSIS’s data acquisition program has appropriately considered the threshold of “strictly necessary” as required in the <i>CSIS Act</i>.</p>	<p>CSIS should assesses the acquisition of [REDACTED] bulk datasets against the “strictly necessary” threshold. CSIS should re-evaluate all referential bulk dataset acquisitions to ensure that they meet the criteria for inclusion in the referential category. Those that do not meet such criteria should be assessed to ensure the information was collected to the extent that was “strictly necessary.”</p>

TOP SECRET // SI // [REDACTED]

SIRC Review	SIRC's Findings	SIRC's Recommendations
<p><b>"Review of Ministerial Direction and CSIS Directives on Information Sharing"</b></p>	<p>Overall, CSIS acted quickly to implement a sound information sharing framework. However, that framework could be strengthened through more rigorous and consistent application of the relevant Deputy Director, Operations Directive and recordkeeping of the decision-making process especially by Deputy Directors General.</p>	<p>The CSIS Executive should prioritize the development of action plan to address the issue of maintain records of decision-making within this fiscal year.</p>
	<p>While CSIS had records of decision-making in the cases SIRC reviewed, there were no records of the deliberations of DDG assessments, contrary to the DDO Directive.</p>	<p>CSIS should ensure records of decision-making include all deliberations at the DDG level, as well as any concerns raised in foreign arrangement profiles or in CSIS internal documentation about respect of human rights.</p>
	<p>There were inconsistencies in the application of the DDO Directive and in the decision-making process at the DDG level.</p>	<p>CSIS should make its assessment of the capacity of foreign entities to fulfil proposed assurances in its records of decision-making.</p>
	<p>All cases that were referred to the Information Sharing Evaluation Committee were managed appropriately at the senior executive level.</p>	
	[REDACTED]	

TOP SECRET // SI //



SIRC Review	SIRC's Findings	SIRC's Recommendations
<p><b>"Review of CSIS's Collection of Economic Security Intelligence"</b></p>	<p>CSIS collected intelligence on [REDACTED] in accordance with its mandate and authorities, and in line with the Government's priorities and intelligence requirements.</p> <p>CSIS's internal guidebook on its role in the <i>Investment Canada Act</i> review process provided adequate advice on CSIS's role and process within national security reviews.</p>	<p>CSIS should use consistent language in all its <i>Investment Canada Act</i> reviews.</p>
<p><b>"CSIS's Traditional and Non Traditional Foreign Partners"</b></p>	<p>The procedures in place around joint operations are clear and detailed, with room for discussion between CSIS HQ and regional offices, reflected the value of both strategic and tactical aspects of operational planning.</p> <p>In some cases, CSIS showed produced in establishing s.17 arrangements with smaller units within foreign agencies that presented human rights concerns. In others CSIS started with a broad arrangement.</p> <p>In [REDACTED] SIRC reviewed, CSIS followed policy and was mindful that its mandate requires there to be a nexus to a threat to Canada.</p> <p>[REDACTED] CSIS did not followed policy and approved leveraging an existing s.17 arrangement to cooperate with a foreign agency with which it did not have such an arrangement.</p>	<p>If faced with the necessity to cooperate with partners in countries with human rights concerns, CSIS should begin with an arrangement with a narrowly defined unit within the foreign agency before considering expanding the arrangement to the broader agency.</p> <p>CSIS should no longer leverage its relationship with a third party in order to cooperate with a foreign agency with which it does not have a valid s.17 arrangement.</p>

**Page 615**

**is withheld pursuant to sections  
est retenue en vertu des articles**

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

TOP SECRET // SI // [REDACTED]

SIRC Review	SIRC's Findings	SIRC's Recommendations
<p><b>"CSIS Threat Reduction Activities"</b></p>	<p>As SIRC's review unfolded, CSIS provided regular up-to-date information, thus allowing for a full assessment of threat reduction activity (TRA) cases.</p> <p>The new consultation process between CSIS and GAC, related specifically to TRA, is a positive development.</p> <p>There is a need to further outline how formal TRA consultation will transpire with other departments and agencies.</p> <p>CSIS has created satisfactory training modules for employees and has devised a sound set of policies and procedures to help guide the conduct of TRA.</p> <p>The TRA cases SIRC examined complied with the <i>CSIS Act</i>, Ministerial Direction, and operational policies.</p> <p>[REDACTED] lacked certain details which should be present in future submissions.</p>	<p>CSIS should prioritize the development of formal mechanisms on TRA consultation with other departments and agencies.</p> <p>CSIS should create a mechanism for tracking best practices and/or lessons learned within each TRA category.</p>
<p><b>"CSIS's Relationship and Exchanges with CBSA"</b></p>	<p>Despite engagement on the [REDACTED] there was no clear centre of responsibility managing the process within CSIS at the time of SIRC's review.</p> <p>SIRC requests to be made aware of instances when CSIS's collaborative endeavours or information sharing practices rely on SIRC as an accountability mechanism.</p> <p>In general, the policies and procedures for the [REDACTED] CSIS-CBSA information sharing programs SIRC reviewed were sound.</p> <p>Having a unit dedicated to managing the bulk of requests to the [REDACTED] is of benefit to CSIS both in terms of quality control and managing the relationship.</p>	<p>CSIS should work closely with CBSA to expedite the finalization of the annexes underpinning the agencies' 2015 memorandum of understanding.</p> <p>It is incumbent upon CSIS to ensure that its requests for [REDACTED] disclosure are tied to an active investigation.</p>

**Page 617**

**is withheld pursuant to sections  
est retenue en vertu des articles**

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

[REDACTED]

**From:** Davies, John  
**Sent:** October-05-16 12:05 PM  
**To:** [REDACTED]  
**Subject:** FW: PRELIMINARY SUMMARY - EN BANC JUDGMENT AND REASONS

CLASSIFICATION:TOP SECRET

**From:** [REDACTED] mailto:[REDACTED]  
**Sent:** Wednesday, October 05, 2016 11:08 AM  
**To:** Davies, John  
**Cc:** [REDACTED]  
**Subject:** PRELIMINARY SUMMARY - EN BANC JUDGMENT AND REASONS

**Classification:** Top Secret  
**Classification:** Très secret  
**Restriction / Restriction d'accès:** NR / AR  
**File Number / No. de dossier:** [REDACTED]

(Please kindly provide copy to Michael Sousa.)

This note summarizes key aspects of the decision issued by Justice Noël on October 3, 2016, in Federal Court file no. [REDACTED] and sets out general comments.

[REDACTED]

**Pages 619 to / à 623  
are withheld pursuant to sections  
sont retenues en vertu des articles**

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

**Davies, John**

---

**From:** [REDACTED]  
**Sent:** Friday, October 21, 2016 1:31 PM  
**To:** Davies, John  
**Subject:** FW: En Banc - Q&A answer requested re SIRC advice

**Classification: Top Secret**  
**Classification: Très secret**  
**Not for PA / Ne pas classer**

Just for your interest.

---

**From:** [REDACTED]  
**Sent:** 21-Oct-16 8:40 AM  
**To:** [REDACTED]  
**Cc:** [REDACTED]  
**Subject:** RE: En Banc - Q&A answer requested re SIRC advice

**Classification: Top Secret**  
**Classification: Très secret**  
**Not for PA / Ne pas classer**

There would be two reasons for this.

It is SIRC that overviews the activities of the CSIS and not the Federal Court. This stems from a strict interpretation of the CSIS Act. It is now clear that the Federal Court disagrees with such an interpretation.

The Service was under the impression that the Federal Court had been advised of the retention of associated data in 2011. The Court also disagreed with this assessment.

[REDACTED]

---

**De :** [REDACTED]  
**Envoyé :** 21-Oct-16 8:08 AM  
**À :** [REDACTED]  
**Cc :** [REDACTED]  
**Objet :** RE: En Banc - Q&A answer requested re SIRC advice

**Classification: Top Secret**  
**Classification: Très secret**  
**Not for PA / Ne pas classer**

Hi [REDACTED]  
Need an answer to this question.. all around town are asking it.  
Thanks,  
[REDACTED]

---

**From:** [REDACTED]  
**Sent:** 21-Oct-16 7:32 AM  
**To:** [REDACTED]  
**Cc:** [REDACTED]  
**Subject:** RE: En Banc - Q&A answer requested re SIRC advice

**Classification:** Top Secret  
**Classification:** Très secret  
**Not for PA / Ne pas classer**

As indicated on the external side, fwd to [REDACTED] as she is the one who assisted the Service and dealt with SIRC further to its review.

[REDACTED]  
Avocate-conseil /Senior Counsel  
DAJ-Services juridiques / ADL-Legal Services  
Tél. [REDACTED] /Pièce : [REDACTED]

---

**From:** [REDACTED]  
**Sent:** 20-Oct-16 7:07 PM  
**To:** [REDACTED]  
**Cc:** [REDACTED]  
**Subject:** En Banc - Q&A answer requested re SIRC advice  
**Importance:** High

**Classification:** Top Secret  
**Classification:** Très secret  
**Not for PA / Ne pas classer**

Hi [REDACTED]

There are a few urgent updates and we need to have the Q&As ready for tonight. A Q&A has been identified for DLS given. Can you please provide an answer to the following (can be found paragraph 99)?

**SIRC recommended that the Service advise the Federal Court of activities relating to metadata collected under warrant. CSIS, however believed that SIRC's recommendation was both inappropriate and unwarranted given that section 21 of the CSIS Act does not confer any general supervisory authority to Federal Court judges. Why did CSIS take this position?**

Regards,

[REDACTED]  
Senior Communications Advisor / Conseiller principal de communication

[REDACTED]

\*\*\*

**Page 626**

**is withheld pursuant to sections  
est retenue en vertu des articles**

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

**From:** Davies, John  
**Sent:** October-25-16 9:16 AM  
**To:** [REDACTED]  
**Subject:** FW: Status Report , En Banc Hearing and Correspondance with Chief Justice (CSIS)

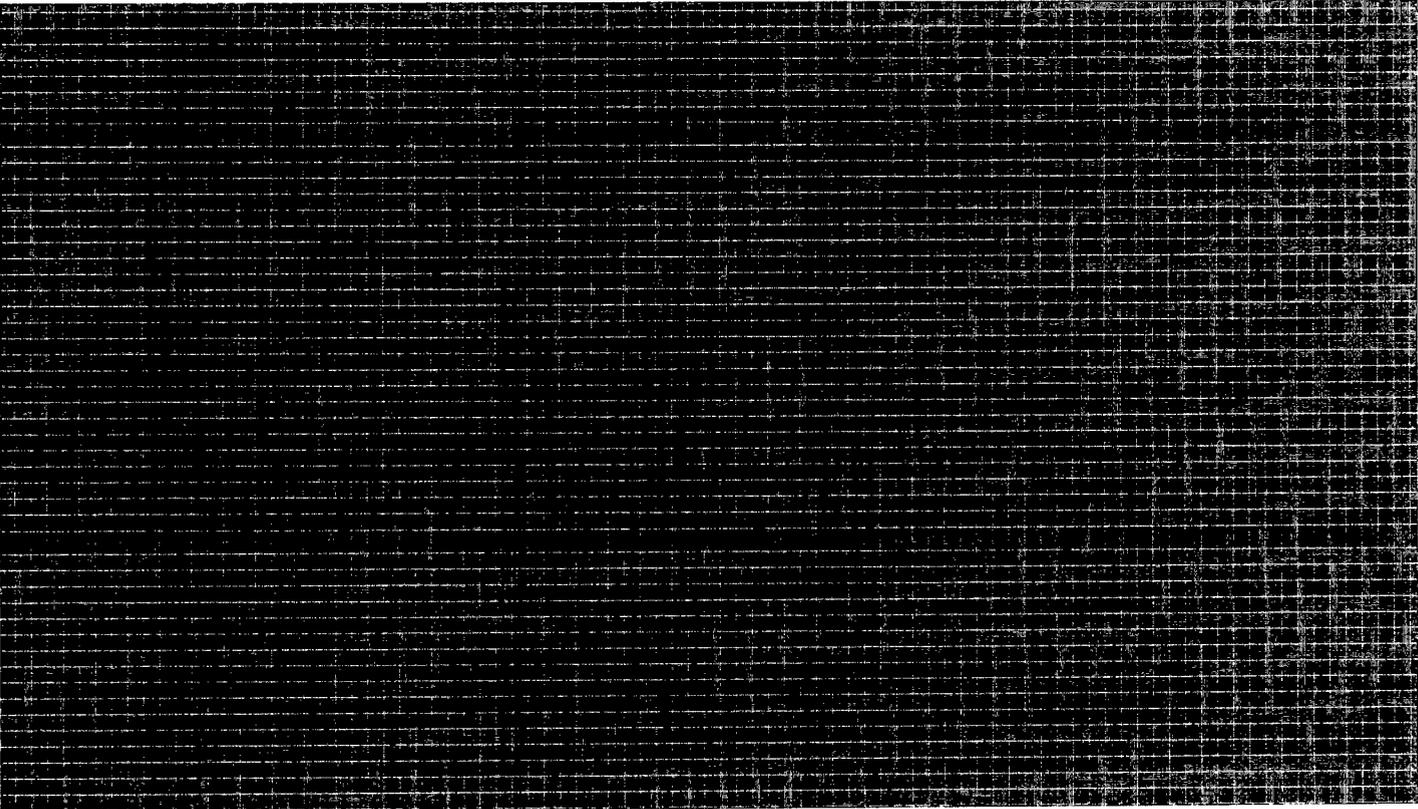
CLASSIFICATION:TOP SECRET

Here is the answer to third party concern origins...

**From:** [REDACTED]  
**Sent:** Friday, April 08, 2016 2:52 PM  
**To:** Sudunasiri, Shalin; Davies, John; Gauthier, Linda M. (JUSTICE)  
**Cc:** [REDACTED]  
**Subject:** Status Report , En Banc Hearing and Correspondance with Chief Justice (CSIS)

**Classification:** Top Secret//Solicitor-Client Privilege  
**Classification:** Très secret//Secret professionnel de l'avocat  
**Restriction / Restriction d'accès:** NR / AR  
**File Number / No. de dossier:** [REDACTED]

Shalin: for Michael also please  
Linda: for Elisabeth and Michael please



**Page 628**

**is withheld pursuant to sections  
est retenue en vertu des articles**

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



2016-2017 Supplementary Estimates (B)

FEDERAL COURT DECISION ON ASSOCIATED DATA

PROPOSED RESPONSE

- **The Government welcomes the Federal Court's findings related to CSIS' retention of "associated data". The decision will not be appealed.**
- **It is important to note that the associated data was collected legally through warrants. The Federal Court's concern relates to CSIS' retention of this data when it is determined not to be related to a threat to the security of Canada.**
- **CSIS took immediate action to address the Federal Court's findings; it has halted all access to and analysis of associated data as it works to assess and address the Federal Court's findings.**
- **I have asked the Security and Intelligence Review Committee (SIRC) to monitor this process and they have agreed to do so.**
- **I take very seriously the Federal Court's finding regarding CSIS' duty of candour, and I will be pursuing this criticism with the executive management of the Service.**
- **CSIS will be working with the Department of Justice and the Federal Court to ensure that it is fully transparent with the Court.**
- **Our Government is committed to hearing from Canadians on how we can best meet our dual objectives of keeping Canadians safe, while safeguarding our freedoms, rights, and values.**
- **Through Bill C-22, the *National Security and Intelligence Committee of Parliamentarians Act*, we are also moving forward to strengthen national security accountability.**

**Backgrounder:**

*Federal Court En Banc Hearings*

The En Banc hearings began as a result of a December 2015 CSIS application for section 12 warrants in which CSIS proposed certain amendments to CSIS warrants. At the same time, following the tabling of the Security Intelligence Review Committee's (SIRC) 2014-2015 Annual Report, the Federal Court indicated that it also wanted to explore issues related to CSIS retention and use of "associated data". In particular, the Federal Court wanted to address SIRC's finding that "SIRC was given no indication that [CSIS] was fully transparent with the Federal Court about the nature and scope of its activities with respect to metadata in the context of [a particular hearing before the Federal Court]".

The En Banc hearings were held over four days in February, March, and April 2016. The Director of CSIS and the Deputy Minister of Justice also appeared before an En Banc hearing on June 10, 2016 to address concerns raised by the Court regarding CSIS' duty of candour in these matters. On October 4, 2016, Justice Simon Noel, the designated judge selected to lead the En Banc proceedings issued a classified, 136 page decision addressing the matters that were before the Court. An unclassified version was released to the public on November 3, 2016.

*CSIS' Retention and Use of Associated Data*

"Associated data" is metadata collected incidentally through the execution of telecommunications and other communications intercepts conducted by CSIS pursuant to CSIS Act warrants. It consists of, for example, information about the date, time, and phone numbers related to a phone call, or the email addresses, dates, and times of an email. It does not include content.

CSIS uses associated data to support investigations into threats to the security of Canada. It is used to, among other things, help identify links between subjects of investigation and identify where they were located at particular points in time.

Prior to the Federal Court's decision, CSIS' practice had been to: (1) assess the contents of all communications intercepts conducted and retain the contents of communications intercepts that are relevant to a threat to the security of Canada; (2) delete content deemed not to be related to a threat, within one year after collection; and (3) retain all associated data related to these communications regardless of whether it is threat-related or not.

*Key Findings of the Federal Court*

The key aspects of the decision are:

- (1) CSIS' retention of non-threat related "associated data" is illegal;
- (2) CSIS breached its duty of candour in not informing the Court that it was retaining this data and had been doing so since 2006;
- (3) The Federal Court was critical of CSIS' views regarding the Federal Court's role in overseeing CSIS activities, particularly CSIS' contention that "Section 21 of the CSIS Act does not confer any general supervisory authority to the Federal Court"; and,
- (4) The Federal Court largely accepted CSIS' proposals regarding technical amendments to CSIS Act warrant templates.

*The Government's Response to the Federal Court's Decision*

The Government accepts the Federal Court's ruling that CSIS' retention of non-threat related associated data is not authorized by the CSIS Act and further accepts the Court's finding that CSIS breached its duty of candour. The decision will not be appealed.

CSIS has taken immediate action to address the Federal Court's findings and has halted all access to and analysis of associated data until CSIS can further assess the decision and put in place measures to comply with the Federal Court's ruling. CSIS is also working with Justice Canada to ensure that it is fully transparent with the Court.

On November 3, 2016 the Director of CSIS and Robert Frater, Chief General Counsel for Justice Canada, conducted a news conference to discuss the decision and the Government's response. The Director subsequently issued statements to the media on November 3 and November 6.

**CONTACTS:**

Prepared by

[Redacted]

Tel. no.

[Redacted]

Approved by

Monik Beauregard,  
Senior Assistant Deputy Minister,  
National and Cyber Security Branch

Tel. no.

613-990-4976

2016-2017 Supplementary Estimates (B)

**FEDERAL COURT DECISION ON ASSOCIATED DATA**

**PROPOSED RESPONSE**

- **The Government accepts the Federal Court's findings related to CSIS' retention of "associated data". The decision will not be appealed.**
- **It is important to note that the associated data was collected legally through warrants. The Federal Court's concern relates to CSIS' retention of this data when it is determined not to be related to a threat to the security of Canada.**
- **CSIS is taking immediate action to address the Federal Court's findings; it has halted all access to and analysis of associated data as it works to assess and address the Federal Court's findings.**
- **I have asked the Security and Intelligence Review Committee (SIRC) to monitor this process and they have agreed.**
- **The Government also accepts the Federal Court's findings regarding CSIS' duty of candour to the Federal Court. CSIS is working with the Department of Justice and the Federal Court to ensure that it is fully transparent with the Court.**
- **It is also important to note that the Federal Court agreed with most of the terms and conditions proposed by CSIS in the warrant application that was presented to the Court.**
- **Our Government is committed to hearing from Canadians on how we can best meet our dual objectives of keeping Canadians safe, while safeguarding our freedoms, rights, and values.**
- **Through Bill C-22, the National Security and Intelligence Committee of Parliamentarians Act, we are also moving forward to strengthen national security accountability.**

**Page 732**  
**is a duplicate**  
**est un duplicata**

**Chiasson, Carole (PS/SP)**

---

**From:** Michel COULOMBE <[REDACTED]>  
**Sent:** Saturday, November 05, 2016 10:02 PM  
**To:** Brown, Malcolm (PS/SP)  
**Attachments:** STATEMENT.docx

FYI - attached statement has been approved by PMO, PCO and MinO. MINO sent the statement to Min for his Ok. Once received statement will be sent to media outlets tomorrow morning.

Sent from my BlackBerry 10 smartphone on the Rogers network.

## STATEMENT

Ottawa, November 5, 2016

The Director of the Canadian Security Intelligence Service, Michel Couombe, issued the following statement today regarding the recent Federal Court decision and the Service's Operational Data Analysis Centre (ODAC):

~~"Given recent media coverage, as I indicated in my previous statement (hyperlink), and in the news conference when the Federal Court's ruling was issued, I would like to reiterate that all associated data was legally collected under warrants. CSIS, in consultation with the Department of Justice, interpreted the CSIS Act to allow for the retention of non-threat related associated data linked with third party communications that were collected while under warrant. The Federal Court has disagreed with this interpretation and we accept their decision. I would like to reiterate~~ make it clear that the Service was not knowingly exceeding the scope of the CSIS Act.

~~As for ODAC, it was created in 2006 to derive more value from the data already being collected under warrant using data exploitation techniques.~~

I would like to address the apparent perception that the Service created and operated ODAC without the knowledge of key government stakeholders. As for ODAC, it was created in 2006 to derive more value from the data already being collected under warrant using data exploitation techniques.

The creation of ODAC and this core operational capability was presented to the Minister of Public Safety in July 2006, explaining the requirement for advanced data analytics and the ability of ODAC to retain data, including metadata, for extended periods of time. The Minister was also briefed on the program in March 2010. Information was also shared over the years with various government stakeholders, including the Security Intelligence Review Committee (SIRC), the Privacy Commissioner, including a Privacy Impact Assessment, and the Inspector General. ~~was also aware of ODAC and its data exploitation activities soon after its establishment.~~

The CSIS 2007-08 Public Report (hyperlink) also refers to ODAC, describing the support being provided to its operational branches through the performance of advanced analysis of data, and the program was described over the years in the Directors' Annual Reports to the Minister.

~~In March 2010, another Minister of Public Safety was briefed on ODAC and the data analytics program.~~

~~The Privacy Commissioner was informed of ODAC and the data analytics program when a Privacy Impact Assessment on ODAC was submitted in August 2010. The Inspector General was also provided a verbal briefing on ODAC and data exploitation in support of operations in 2011. It should also be noted that ODAC's existence, capabilities, and operations were described over the years in the Directors' Annual Reports to the Minister. These references vary from narrative descriptions of the activities to specific contributions to operations.~~

Given the Service and Department of Justice interpretation that the activity in question was within the scope of the CSIS Act, these briefings may not have specifically addressed the retention of the sub-set of associated data on which the Court has now ruled. The intent of the Service, however, was to ensure key stakeholders were aware of ODAC, its capabilities, and intentions around retention.

SIRC reviewed CSIS' use of associated data and published its findings on the issue in its 2014-15 annual report. SIRC did not conclude that the retention of associated data was illegal, but did suggest that the Federal Court be made aware.

| As I noted in my previous statement, CSIS agrees that the Court should have been informed earlier of the existence of ODAC and the approach to data retention, and acknowledges this was a significant omission. At no point did CSIS deliberately seek to withhold this information from the Court, and the Court acknowledged that there is no evidence to suggest ~~we~~ CSIS did.

CSIS recognizes the importance of maintaining public trust and confidence in its activities. CSIS takes very seriously the privacy considerations related to its work, and it is committed to ensuring that its activities are in compliance with all legislation and Ministerial Direction.”

**Contact:**

CSIS Media Relations

[media-medias@smtp.gc.ca](mailto:media-medias@smtp.gc.ca)

613-231-0100

**Chiasson, Carole (PS/SP)**

---

**From:** Brown, Malcolm (PS/SP)  
**Sent:** Friday, October 21, 2016 10:12 AM  
**To:** De Santis, Heather (PS/SP)  
**Subject:** Re: SIRC Letter

Hx.

Sent from my BlackBerry 10 smartphone on the Rogers network.

---

**From:** De Santis, Heather (PS/SP)  
**Sent:** Friday, October 21, 2016 10:10 AM  
**To:** Brown, Malcolm (PS/SP)  
**Subject:** RE: SIRC Letter

Yep, it was understood

---

**From:** Brown, Malcolm (PS/SP)  
**Sent:** Friday, October 21, 2016 10:02 AM  
**To:** De Santis, Heather (PS/SP)  
**Subject:** Re: SIRC Letter

I said circ. I meant csis.

Sent from my BlackBerry 10 smartphone on the Rogers network.

---

**From:** De Santis, Heather (PS/SP)  
**Sent:** Friday, October 21, 2016 10:00 AM  
**To:** Brown, Malcolm (PS/SP)  
**Subject:** RE: SIRC Letter

She's on it

---

**From:** Brown, Malcolm (PS/SP)  
**Sent:** Friday, October 21, 2016 9:37 AM  
**To:** De Santis, Heather (PS/SP)  
**Subject:** Re: SIRC Letter

No need. That's monik's job to work with circ. And time is short.

Sent from my BlackBerry 10 smartphone on the Rogers network.

---

**From:** De Santis, Heather (PS/SP)  
**Sent:** Friday, October 21, 2016 9:35 AM  
**To:** Brown, Malcolm (PS/SP)  
**Subject:** Re: SIRC Letter

Yes, waiting for more. I can collate all comments

Sent from my BlackBerry 10 smartphone on the Rogers network.

---

**From:** Brown, Malcolm (PS/SP)  
**Sent:** Friday, October 21, 2016 9:22 AM  
**To:** De Santis, Heather (PS/SP)  
**Subject:** Re: SIRC Letter

I think this incomplete.

Sent from my BlackBerry 10 smartphone on the Rogers network.

---

**From:** De Santis, Heather (PS/SP)  
**Sent:** Friday, October 21, 2016 9:21 AM  
**To:** Brown, Malcolm (PS/SP)  
**Subject:** FW: SIRC Letter

John's first thoughts

---

**From:** Davies, John (PS/SP)  
**Sent:** Friday, October 21, 2016 9:08 AM  
**To:** De Santis, Heather (PS/SP); Beauregard, Monik (PS/SP); Sousa, Michael (PS/SP)  
**Cc:** [REDACTED] (PS/SP)  
**Subject:** RE: SIRC Letter

I am going to 4C meeting now. [REDACTED] s here if they want our input.

John

---

**From:** De Santis, Heather (PS/SP)  
**Sent:** Friday, October 21, 2016 8:54 AM  
**To:** Beauregard, Monik (PS/SP); Sousa, Michael (PS/SP)  
**Cc:** Davies, John (PS/SP)  
**Subject:** FW: SIRC Letter  
**Importance:** High

Monik/Mike –

Pls see attached letter the Minister will send to SIRC at 11 am.

Can you pls have a look for and reflag/comments. DM will also speak to Marci. I will call you on this shortly. I will also send to CSIS.

Thanks!

## **De Santis, Heather (PS/SP)**

---

**From:** Tomlinson, Jamie (PS/SP)  
**Sent:** Thursday, October 20, 2016 12:36 PM  
**To:** Brown, Malcolm (PS/SP); Wilson, Gina (PS/SP)  
**Cc:** Beauregard, Monik (PS/SP); MacKinnon, Paul (PS/SP); DeSantis, Heather  
**Subject:** FW: Federal Court  
**Attachments:** Director Statement re. En Banc Decision - October 2016 (ADP).docx; En Banc Decision - October 2016 - Qs As (ADP).docx

Malcolm,

Here are the draft CSIS products. They are currently being reviewed by the Minister's Office.

There is discussion happening at the centre in terms of how the roll-out will happen once the court decision is public. Specifically, the discussion is whether the Director and Minister will appear together.

**Pages 739 to / à 746**

**are duplicates**

**sont des duplicatas**

## **De Santis, Heather (PS/SP)**

---

**From:** Tomlinson, Jamie (PS/SP)  
**Sent:** Sunday, October 23, 2016 5:59 PM  
**To:** Brown, Malcolm (PS/SP); Wilson, Gina (PS/SP); Beaugard, Monik (PS/SP)  
**Cc:** MacKinnon, Paul (PS/SP); De Santis, Heather (PS/SP)  
**Subject:** Federal Court - Comms update  
**Attachments:** PS-SP-#1997213-v1C-Minister\_-\_Statement\_on\_En\_Banc\_Decision.doc; PS-SP-#1997111-1-Minister - Federal Court Decision - En Banc.docx

I am just off a conference call with PCO, CSIS and Justice.

CSIS is working to finalize communications products - Director's Statement and Qs & As. The hope is to have them ready tonight.

Our MO has approved the attached Minister's Statement. We have also developed talking points for the Minister to use for a pre or post Question Period scrum.

Depending on the timing that the ruling goes public, sequencing - if it were to be tomorrow - could be as follows:

**Pages 748 to / à 753  
are duplicates  
sont des duplicatas**

**De Santis, Heather (PS/SP)**

---

**From:** Beauregard, Monik (PS/SP)  
**Sent:** Monday, October 24, 2016 4:17 PM  
**To:** Brown, Malcolm (PS/SP)  
**Cc:** De Santis, Heather (PS/SP); Champoux, Elizabeth (PS/SP)  
**Subject:** Fw: CSIS Federal Court decision - update

Looks like we have another 48hrs or so.  
M.

Sent from my BlackBerry 10 smartphone on the Rogers network.

---

**From:** Davies, John (PS/SP) <john.davies@canada.ca>  
**Sent:** Monday, October 24, 2016 4:06 PM  
**To:** Tomlinson, Jamie (PS/SP); Magee, Heather (PS/SP); Grenier, Julie (PS/SP); Beauregard, Monik (PS/SP); Beecher, Sophie (PS/SP); [REDACTED] (PS/SP); [REDACTED] (PS/SP); De Santis, Heather (PS/SP); Sousa, Michael (PS/SP)  
**Subject:** FW: CSIS Federal Court decision - update

fyi

---

**From:** [REDACTED]  
**Sent:** Monday, October 24, 2016 3:12 PM  
**To:** Bouzigon, Mylène; Matte, Daniel; Vigneault, David; Rogers, Daniel; [REDACTED] Noftle, Tracie; O'Nions, Christine; Off, Shirley Anne; Ghiz, Joanne; Webber, Grégoire; Tomlinson, Jamie (PS/SP); Hurl, David (PS/SP); Davies, John (PS/SP); Brien, Dan (PS/SP); [REDACTED] Gowing, Andrew; [REDACTED] (PS/SP); Brender, James (PS/SP); Allen, Kristine; Frater, Robert; [REDACTED] Leclerc, Caroline  
**Cc:** Bustros, Katia; Farkas, Jennifer; Benoit, Nathalie  
**Subject:** Re: CSIS Federal Court decision - update

Bonjour à tous,

[REDACTED]

Thank you.

[REDACTED]

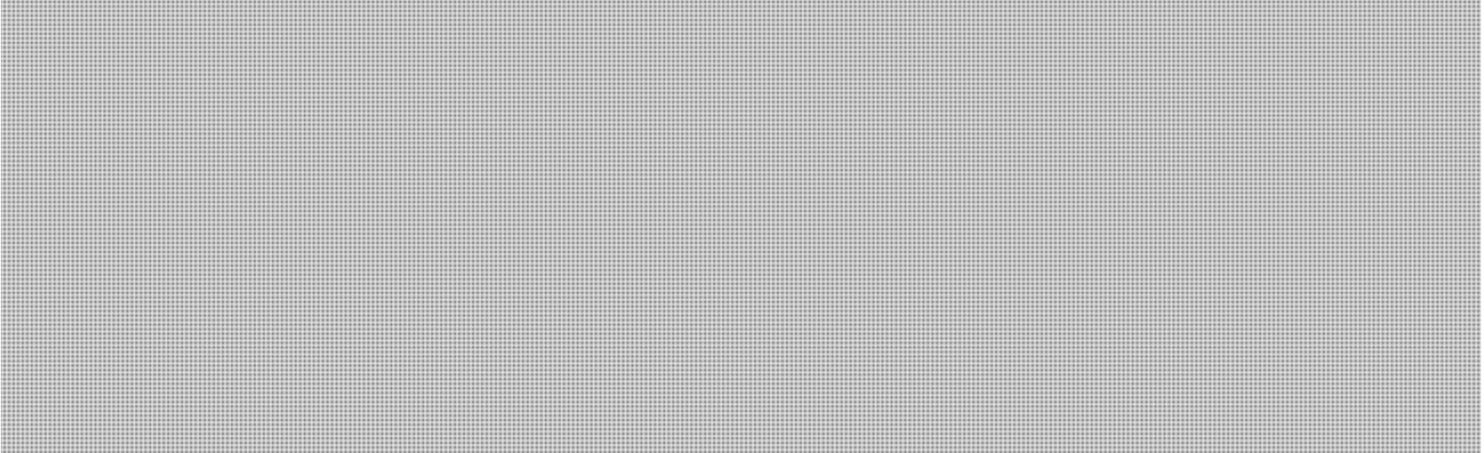
Envoyé de mon smartphone BlackBerry 10 sur le réseau Rogers.

---

**De:** Bouzigon, Mylène  
**Envoyé:** vendredi 21 octobre 2016 1:32 PM  
**À:** Matte, Daniel; Vigneault, David; Rogers, Daniel; [REDACTED] Noftle, Tracie; O'Nions, Christine; Off, Shirley Anne; Ghiz, Joanne; Webber, Grégoire; 'jamie.tomlinson@canada.ca'; 'david.hurl@canada.ca'; john.davies@canada.ca; 'dan.brien@canada.ca'; Andrew Swift; [REDACTED] Gowing, Andrew; [REDACTED] (PS/SP); 'Brender, James (PS/SP)'; Allen, Kristine; Frater, Robert; Amy JOHNSON; Leclerc, Caroline  
**Cc:** Bustros, Katia; Farkas, Jennifer; Benoit, Nathalie

**Objet:** CSIS Federal Court decision - update

Good afternoon,



Thank you.

MB

**Me Mylène Bouzigon**

Senior General Counsel | Avocate générale principale

(613) 842-1197 / (613) 231-0027 | [bouzigon.mylene@justice.gc.ca](mailto:bouzigon.mylene@justice.gc.ca) | Facsimile - télécopieur: (613) 842-1345

*This communication contains information that may be confidential, exempt from disclosure, subject to litigation privilege or protected by the privilege that exists between lawyers and their clients. If you are not the intended recipient, you should not read, rely on, retain, or distribute it. Please delete or otherwise destroy this communication and all copies of it immediately, and contact the sender.*

*Ce message contient des renseignements qui pourraient être confidentiels, soustraits à la communication, ou protégés par le privilège relatif au litige ou par le secret professionnel liant l'avocat à son client. S'il ne vous est pas destiné, vous êtes priés de ne pas le lire, l'utiliser, le conserver ou le diffuser. Veuillez sans tarder le supprimer et en détruire toute copie, et communiquer avec l'expéditeur.*

**De :** Benoit, Nathalie

**Envoyé :** 20 octobre 2016 15:52

**À :** Matte, Daniel <Daniel.Matte@justice.gc.ca>; Benoit, Nathalie <Nathalie.Benoit@justice.gc.ca>; Vigneault, David <David.Vigneault@pco-bcp.gc.ca>;

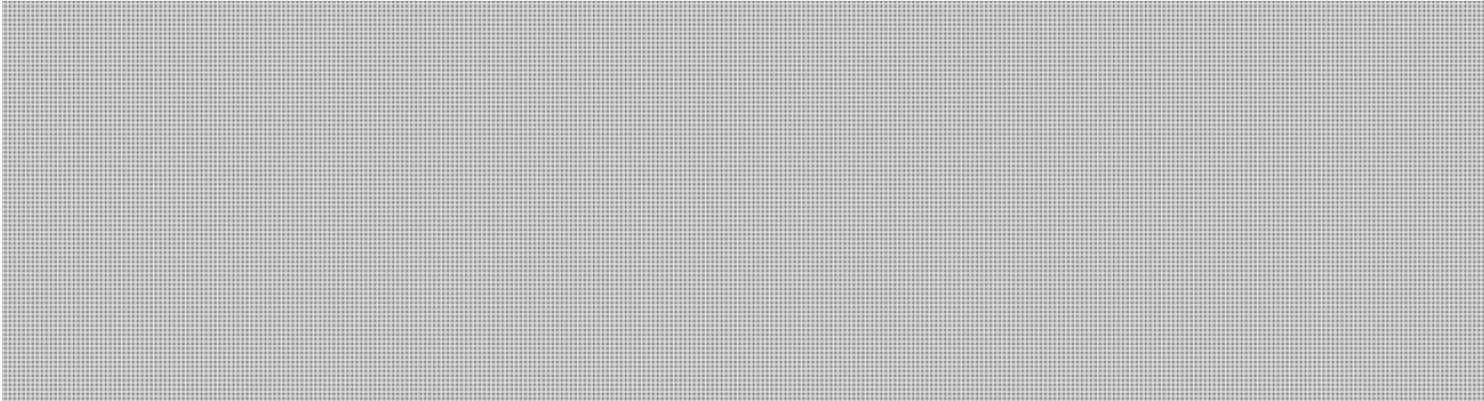
[redacted] Nofle, Tracie <Tracie.Nofle@pco-bcp.gc.ca>; O'Nions, Christine <Christine.O'Nions@pco-bcp.gc.ca>; Off, Shirley Anne <ShirleyAnne.Off@justice.gc.ca>; Ghiz, Joanne <Joanne.Ghiz@justice.gc.ca>; Webber, Grégoire <Gregoire.Webber@justice.gc.ca>; 'jamie.tomlinson@canada.ca' <jamie.tomlinson@canada.ca>; 'david.hurl@canada.ca' <david.hurl@canada.ca>; john.davies@canada.ca; 'dan.brien@canada.ca' <dan.brien@canada.ca>;

[redacted] Gowing, Andrew <Andrew.Gowing@justice.gc.ca>; [redacted] (PS/SP) [redacted] @canada.ca>; Brender, James (PS/SP) <james.brender@canada.ca>; Allen, Kristine <Kristine.Allen@justice.gc.ca>; Frater, Robert <Robert.Frater@justice.gc.ca>; [redacted] Leclerc, Caroline <Caroline.Leclerc@justice.gc.ca>

**Cc :** Bouzigon, Mylène <Mylene.Bouzigon@justice.gc.ca>; Bustros, Katia <Katia.Bustros@justice.gc.ca>

**Objet :** CSIS Federal Court decision - update

Good afternoon,



Salutations,

**Nathalie Benoit**  
General Counsel, NLSAG  
613-369-2499.

**AVIS DE CONFIDENTIALITÉ**

Le contenu de ce courrier électronique est confidentiel et strictement réservé à l'usage des personnes auxquelles il s'adresse. Ce message peut contenir de l'information privilégiée protégée par le secret professionnel avocat-client. Si vous avez reçu ce message par erreur, contactez immédiatement l'expéditeur afin de confirmer que vous avez détruit le message original et toute copie. Veuillez noter qu'il est strictement interdit de divulguer, reproduire ou diffuser le contenu de ce message ou de prendre des mesures en conséquence. Tout nouvel envoi, reproduction ou usage de ce message par une personne autre que le destinataire est strictement interdit. Merci.

**CONFIDENTIALITY NOTICE**

The contents of this electronic mail message are confidential and strictly reserved for the sole use of its intended recipients. This message may contain information protected by the solicitor-client privilege. If you receive this message in error, please notify the sender immediately in order to confirm that the original message as well as all copies have been deleted. Any disclosure, copying, distribution or reliance on the contents of the information is strictly prohibited. Thank you.

**De Santis, Heather (PS/SP)**

---

**From:** Beauregard, Monik (PS/SP)  
**Sent:** Friday, October 21, 2016 5:18 PM  
**To:** Brown, Malcolm (PS/SP)  
**Cc:** De Santis, Heather (PS/SP); Champoux, Elizabeth (PS/SP)  
**Subject:** FW: Letter to Blais oct 2016 v2\_CSIS input  
**Attachments:** Letter to Blais oct 2016 v2\_CSIS input.docx

Malcom,  
As requested, here is the CSIS version of the letter to SIRC.  
M.

---

**From:** Khouri, Lisa (PS/SP)  
**Sent:** Friday, October 21, 2016 5:08 PM  
**To:** Champoux, Elizabeth (PS/SP); Beauregard, Monik (PS/SP); De Santis, Heather (PS/SP)  
**Subject:** FW: Letter to Blais oct 2016 v2\_CSIS input

---

**From:** [REDACTED] (PS/SP)  
**Sent:** Friday, October 21, 2016 5:08 PM  
**To:** Khouri, Lisa (PS/SP)  
**Subject:** FW: Letter to Blais oct 2016 v2\_CSIS input

First version was ours. This one is CSIS'.

[REDACTED]

---

**From:** [REDACTED]  
**Sent:** Friday, October 21, 2016 12:58 PM  
**To:** [REDACTED] (PS/SP)  
**Cc:** [REDACTED]  
**Subject:** Letter to Blais oct 2016 v2\_CSIS input

Hi [REDACTED]

Please find attached our proposed revision. Happy to discuss.

It is still with one of our Exec's, but in the interest of time am sending and will let you know of anything further.

Thanks  
[REDACTED]

The Hon. Pierre Blais, PC  
Chair of the Security Intelligence Review Committee  
P.O. Box 2430, Station "D"  
Ottawa, ON K1P 5W5

Formatted: French (Canada)

21 October, 2016

Dear Mr. Blais,

As you know, the government is guided by two overarching principles in the domain of national security: keeping Canadians safe and safeguarding rights and freedoms.

We know that effective oversight review is key to meeting these objectives by providing accountability and transparency. In light of SIRC's important contributions in this regard, I am requesting that you, as Chair, take on a specific mandate with respect to CSIS's ~~collection~~ retention of "associated data".

In December 2015, CSIS notified the Federal Court that changes to the warrant application would be presented; this, in response to previous questions from the Federal Court related to the definition of "destroyed" and the period of time allowed to assess whether information may be retained or must be destroyed (the assessment period). Proposed changes to the warrant conditions were presented in early 2016 and were heard *en banc*, in the presence of all designated judges.

In the interim, ~~Following SIRC's recommendation in its 2014-15 annual report, SIRC recommended~~ that "the Service make the Court aware of the particulars of the Service's retention and use of metadata collected under warrant," CSIS ~~undertook to improve the warrant process. The Service created a new warrant template designed to ensure that it includes the full spectrum of what data will be retained. It presented that template to the court when requesting a warrant in early 2016. In light of this, and in the context of the ongoing *en banc* process, the Federal Court called on the Service to justify the assessment period and to fully explain its practices with respect to associated data.~~

Formatted: Font: Italic

~~The Service has also informed me that as result of the Federal Court's decision of October 4, 2016, it has segregated, halted access to and use of isolated the all relevant database containing (PS policy and LSU) the associated meta-data associated with communications intercepts that was lawfully obtained under warrants. I understand that CSIS is actively working to restore access to associated data that is threat-related and that, in parallel, is working to develop policies, processes and technology to meet operational requirements in a manner that complies with the Federal Court's ruling. between 2006 and 2015. This~~

Formatted: Font: Bold

~~"fence" will prevent analysis or use of that data as the Service determines how to extract the information threat related associated data that was properly retained in the database from the data that should have later been destroyed non threat related associated data that the Federal Court has ruled should not have been retained (PS policy and LSU).~~

Formatted: Font: Bold

~~Pursuant to section 54(2) of the CSIS Act, to ask that SIRC I am writing to request that SIRC review monitor the Service's response to the Federal Court decision of October 4, and that a special report be provided to me in relation to this matter. "fence" as well as the process of removing separating the lawfully retained information threat related associated data while destroying the improperly retained information non threat related associated data (PS policy and LSU). Once the process is complete I am requesting a special report be provided to me.~~

Formatted: Font: Italic

Formatted: Font: Bold

Thank you for your attention to this matter.

Sincerely,

Hon. Ralph Goodale, PC, MP  
Minister of Public Safety and Emergency Preparedness

## De Santis, Heather (PS/SP)

---

**From:** Brien, Dan (PS/SP)  
**Sent:** Friday, October 21, 2016 12:47 PM  
**To:** Brown, Malcolm (PS/SP)  
**Cc:** Surkes, Marci (PS/SP)  
**Subject:** FW: Goodale statement on CSIS

Draft from last night.

-----Original Message-----

**From:** Ralph Goodale [mailto: ]  
**Sent:** Thursday, October 20, 2016 10:32 PM  
**To:** Surkes, Marci (PS/SP); Brien, Dan (PS/SP); Hurl, David (PS/SP)  
**Subject:** Goodale statement on CSIS

Here's a draft. Getting on plane soon. This is probably not done yet, but wanted to get you this cut. RG

STATEMENT BY PUBLIC SAFETY MINISTER RALPH GOODALE ON THE RULING OF THE FEDERAL COURT OF CANADA, PUBLISHED OCTOBER XX, 2016, WITH RESPECT TO THE CANADIAN SECURITY INTELLIGENCE SERVICE (CSIS) AND THE HANDLING OF "ASSOCIATED DATA"

October XX, 2016 - I welcome the decision in this matter rendered by Mr. Justice Noel on behalf of the Federal Court, en banc. The court's insight and guidance are timely, coming in the midst of the public consultations we now have underway about Canada's national security framework.

CSIS plays a critical role in keeping Canadians safe. As it investigates threats to our national security, the Service collects a considerable amount of information, with full legal authorization pursuant to the CSIS Act and warrants issued by the Federal Court. When the information is intercepted communications, it can often include "associated data" of third-parties such as phone numbers and email addresses.

The court has ruled that while legally collected, such "associated data" cannot be retained and utilized by CSIS unless it relates to a specific threat to the security of Canada and is of use to an investigation, prosecution, national defence or foreign affairs.

The Service has confirmed that it is taking immediate steps to address the court's decision. It has blocked all access to and analysis of any associated data, while it considers its next steps. As Minister of Public Safety, I am asking the Security Intelligence Review Committee (SIRC) to monitor the situation carefully to ensure compliance.

I also take very seriously the explicit finding by Justice Noel that CSIS had failed in its duty to be candid with the court. I will be perusing this criticism with the executive management of the Service. In matters of security and intelligence, Canadians need to have confidence that all the departments and agencies of the Government of Canada are being effective at keeping Canadians safe, and equally, that they are safeguarding our rights and freedoms.

I also take note of the court's observation that the CSIS Act is now more than 30 years old and showing its age as global affairs, threat profiles, technology and public expectations have rapidly evolved. In his judgement, Justice Noel did not

dispute the potential value of "associated data" to the important work CSIS does in this challenging world, but he could find not existing legislative authority permitting its retention and use.

-30-

Sent from my iPad

## De Santis, Heather (PS/SP)

---

**From:** De Santis, Heather (PS/SP)  
**Sent:** Friday, October 21, 2016 12:41 PM  
**To:** Brown, Malcolm (PS/SP)  
**Subject:** FW: En Banc Comms

Preview for you

---

**From:** Tomlinson, Jamie (PS/SP)  
**Sent:** Friday, October 21, 2016 12:23 PM  
**To:** Beauregard, Monik (PS/SP); De Santis, Heather (PS/SP)  
**Cc:** Magee, Heather (PS/SP)  
**Subject:** RE: En Banc Comms

Just in from Dan. Monik we will move this to you and your folks for quick review.

STATEMENT BY PUBLIC SAFETY MINISTER RALPH GOODALE ON THE RULING OF THE FEDERAL COURT OF CANADA, PUBLISHED OCTOBER XX, 2016, WITH RESPECT TO THE CANADIAN SECURITY INTELLIGENCE SERVICE (CSIS) AND THE HANDLING OF "ASSOCIATED DATA"

October XX, 2016 - I welcome the decision in this matter rendered by Mr. Justice Noel on behalf of the Federal Court, en banc. The court's insight and guidance are timely, coming in the midst of the public consultations we now have underway about Canada's national security framework.

CSIS plays a critical role in keeping Canadians safe. As it investigates threats to our national security, the Service collects a considerable amount of information, with full legal authorization pursuant to the CSIS Act and warrants issued by the Federal Court. When the information is intercepted communications, it can often include "associated data" of third-parties such as phone numbers and email addresses.

The court has ruled that while legally collected, such "associated data" cannot be retained and utilized by CSIS unless it relates to a specific threat to the security of Canada and is of use to an investigation, prosecution, national defence or foreign affairs.

The Service has confirmed that it is taking immediate steps to address the court's decision. It has blocked all access to and analysis of any associated data, while it considers its next steps. As Minister of Public Safety, I am asking the Security Intelligence Review Committee (SIRC) to monitor the situation carefully to ensure compliance.

I also take very seriously the explicit finding by Justice Noel that CSIS had failed in its duty to be candid with the court. I will be perusing this criticism with the executive management of the Service. In matters of security and intelligence, Canadians need to have confidence that all the departments and agencies of the Government of Canada are being effective at keeping Canadians safe, and equally, that they are safeguarding our rights and freedoms.

I also take note of the court's observation that the CSIS Act is now more than 30 years old and showing its age as global affairs, threat profiles, technology and public expectations have rapidly evolved. In his judgement, Justice Noel did not dispute the potential value of "associated data" to the important work CSIS does in this challenging world, but he could find not existing legislative authority permitting its retention and use.

-30-

---

**From:** Beauregard, Monik (PS/SP)  
**Sent:** October-21-16 12:17 PM  
**To:** De Santis, Heather (PS/SP); Tomlinson, Jamie (PS/SP)  
**Subject:** RE: En Banc Comms

Heather,  
According to Julie, the Min has rewritten his statement and Comms is waiting for the electronic version.  
M.

---

**From:** De Santis, Heather (PS/SP)  
**Sent:** Friday, October 21, 2016 12:17 PM  
**To:** Tomlinson, Jamie (PS/SP); Beauregard, Monik (PS/SP)  
**Subject:** En Banc Comms

Jamie, Min asking for draft lines. Can you give me a status update/draft?

Thx  
Sent from my BlackBerry 10 smartphone on the Rogers network.



---

# Statement

---

## Statement from Public Safety Minister Ralph Goodale regarding the Federal Court's "En banc" Decision

**Ottawa, October 21, 2016** - "Given the current focus on matters related to our security and rights and freedoms, I want to address the Federal Court's findings in the "En Banc" decision, which looked at CSIS' authority to retain associated data it collected through warrants.

First, I want to stress the vital role CSIS plays in keeping Canadians safe. It does this by investigating threats, and collecting and analyzing information to protect our national security. This is their *raison d'être*, and I continue to have confidence in their ability to deliver.

The Government of Canada accepts the Federal Court's findings.

It is important to underline that the associated data was collected legally through warrants. The Court's key concern relates to CSIS' retention of data, such as date, time, and phone numbers related to a call, when it is not related to a threat to the security of Canada.

I am assured that CSIS is taking immediate action to address the Federal Court's findings. CSIS halted all access to and analysis of the associated data as it actively works to assess and address the Federal Court's decision.

The Government also accepts the Federal Court's findings regarding CSIS' duty of candour to the Federal Court. The Government takes this finding very seriously. CSIS has committed to working with the Federal Court to ensure that it is fully transparent with the Court.

The Federal Court agreed with most of the terms and conditions proposed by CSIS on the warrant application that was presented to the Court.

In its decision, the Court noted that the CSIS Act is now more than 30 years old and changes may be needed to ensure that it keeps pace with changes in technology and the privacy expectations of Canadians. This is something that we will review.

I want to also emphasize our Government's dual objective to keep Canadians safe, while at the same time safeguarding our freedoms, rights and values in an open and democratic society.

We are listening to Canadians about how best we can achieve this dual objective. We invite all Canadians to provide us with their views and ideas on our national security framework through our [online consultation](#), which is open until December 1st.

At the same time, we are taking measures to strengthen national security accountability. In June, we put forward legislation to create a National Security and Intelligence Committee of Parliamentarians, which would have a broad mandate to scrutinize the activities of any



- 2 -

federal department or agency with national security responsibilities, including operational matters.”

-30-

Follow Public Safety Canada ([@Safety\\_Canada](https://twitter.com/Safety_Canada)) on Twitter.

For more information, please visit the website [www.publicsafety.gc.ca](http://www.publicsafety.gc.ca).

**Information:**

Scott Bardsley  
Office of the Minister of Public Safety and Emergency Preparedness  
613-998-5681

Media Relations  
Public Safety Canada  
(613) 991-0657

## **De Santis, Heather (PS/SP)**

---

**From:** Tomlinson, Jamie (PS/SP)  
**Sent:** Thursday, October 20, 2016 5:37 PM  
**To:** Brown, Malcolm (PS/SP); Wilson, Gina (PS/SP)  
**Subject:** Federal Court  
**Attachments:** PS-SP-#1997213-v1-Minister\_-\_Statement\_on\_En\_Banc\_Decision.doc

We have developed a statement for the Minister using the messages developed yesterday. One scenario for tomorrow (if ruling goes public) is to issue this written statement - sequencing of timing with Director's statement and CSIS tech briefing, to be confirmed.

Statement is being reviewed by MO and PCO.

**De Santis, Heather (PS/SP)**

---

**From:** Beauregard, Monik (PS/SP)  
**Sent:** Friday, October 14, 2016 7:21 AM  
**To:** Sousa, Michael (PS/SP)  
**Cc:** De Santis, Heather (PS/SP); Brown, Malcolm (PS/SP)  
**Subject:** Re: En Banc Decision

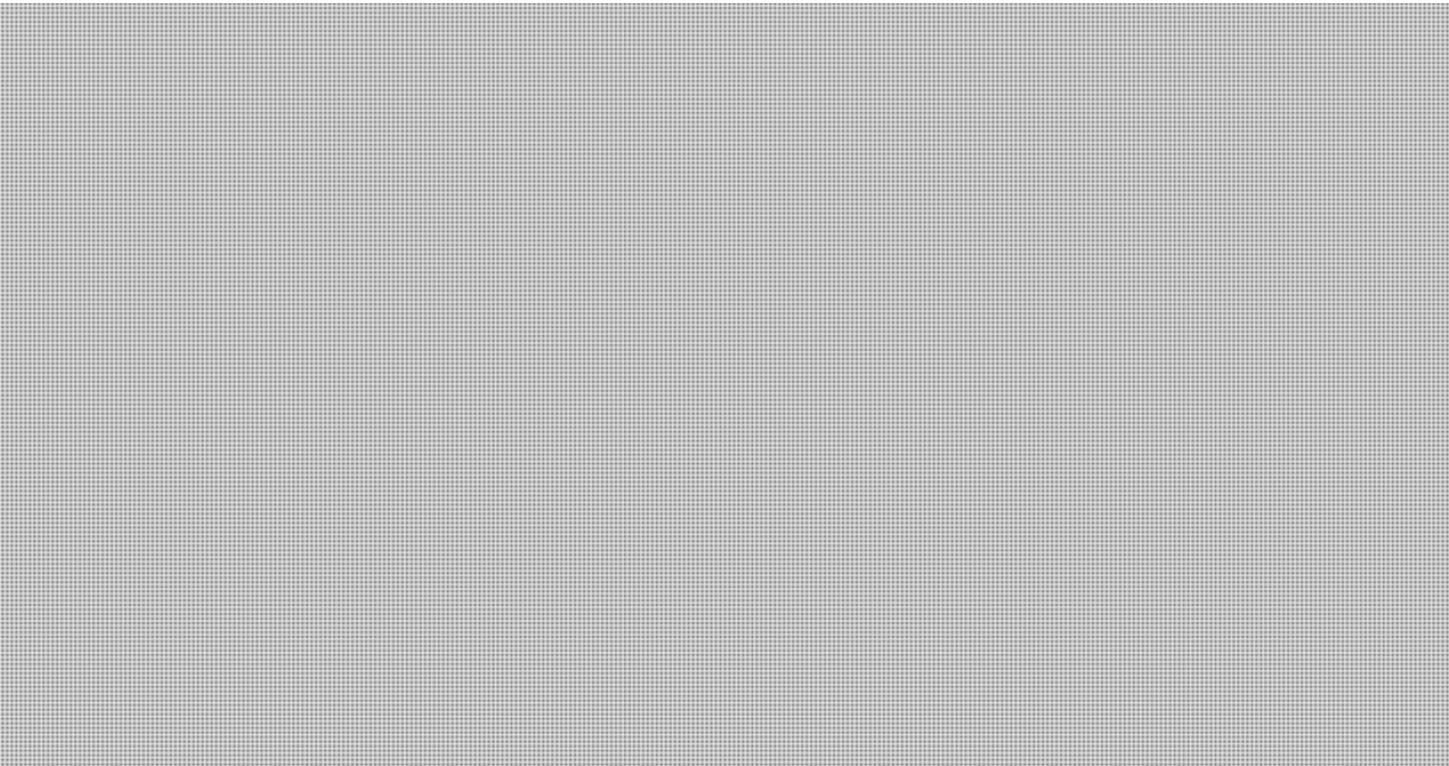
Thx Mike,   
M.

Sent from my BlackBerry 10 smartphone on the Rogers network.

---

**From:** Sousa, Michael (PS/SP)  
**Sent:** Friday, October 14, 2016 7:14 AM  
**To:** Beauregard, Monik (PS/SP)  
**Subject:** RE: En Banc Decision

Monik.



Cheers,

Mike

**Michael Sousa**  
Avocat général principal & Directeur exécutif  
Senior General Counsel & Executive Director

Services juridiques ministériels, Sécurité publique Canada | Public Safety Canada Legal Services  
269 avenue Laurier ouest, 16ième étage, pièce 1800  
269, Laurier Avenue West., 16<sup>th</sup> floor, room 1800  
Ottawa (ON K1A 0P8  
tél. | tel. (613) 991-9375 -- téléc. | fax (613) 990-8307

Solicitor-Client Privilege / Secret professionnel de l'avocat

**De Santis, Heather (PS/SP)**

---

**From:** Beauregard, Monik (PS/SP)  
**Sent:** Friday, October 14, 2016 8:42 AM  
**To:** Brown, Malcolm (PS/SP); Wilson, Gina (PS/SP)  
**Cc:** De Santis, Heather (PS/SP); Champoux, Elizabeth (PS/SP)  
**Subject:** Fw: Briefing

Malcolm,  
Appears NSA will be briefed on en banc this pm. Pushing to get invited.

Gina heads up on this if your calendar allows, or I can step in.  
I can fill you in early afternoon as off to CSE this morning. But if you have no other window I will get someone else to go to the CSE mtg.  
M.

Sent from my BlackBerry 10 smartphone on the Rogers network.

---

**From:** Beauregard, Monik (PS/SP) <[monik.beauregard@canada.ca](mailto:monik.beauregard@canada.ca)>  
**Sent:** Friday, October 14, 2016 8:33 AM  
**To:** [REDACTED] Davies, John (PS/SP)  
**Subject:** Re: Briefing

Malcolm is out of town with Min so either Gina or me.  
Thx

Sent from my BlackBerry 10 smartphone on the Rogers network.

---

**From:** [REDACTED]  
**Sent:** Friday, October 14, 2016 8:32 AM  
**To:** Beauregard, Monik (PS/SP); Davies, John (PS/SP)  
**Subject:** RE: Briefing

It is this afternoon at 2:30. It was organized by the legal people – we invited ourselves and [REDACTED] Who should be invited?

Thanks!  
Nada

---

**From:** Beauregard, Monik (PS/SP) [<mailto:monik.beauregard@canada.ca>]  
**Sent:** October-14-16 8:10 AM  
**To:** [REDACTED] Davies, John (PS/SP)  
**Subject:** Re: Briefing

Nada,  
Is this today or Monday?  
We are brfg MIn Monday as out of town today. Would be good if PS was present to ensure all on same page.  
Thx  
M.

Sent from my BlackBerry 10 smartphone on the Rogers network.

---

**From:** [REDACTED]  
**Sent:** Friday, October 14, 2016 8:07 AM  
**To:** Davies, John (PS/SP)  
**Cc:** Beauregard, Monik (PS/SP)  
**Subject:** Re: Briefing

Just to be clear, invitation was sent to [REDACTED] but he is not in the office today.

---

**From:** [REDACTED]  
**Sent:** Friday, October 14, 2016 08:02 AM  
**To:** 'John.Davies@canada.ca' <[John.Davies@canada.ca](mailto:John.Davies@canada.ca)>  
**Cc:** 'monik.beauregard@canada.ca' <[monik.beauregard@canada.ca](mailto:monik.beauregard@canada.ca)>  
**Subject:** Re: Briefing

At Assistant Secretary level, DMs not attending - except as I heard late yesterday, Dir C.

---

**From:** Davies, John (PS/SP) [<mailto:John.Davies@canada.ca>]  
**Sent:** Friday, October 14, 2016 07:53 AM  
**To:** [REDACTED]  
**Cc:** Beauregard, Monik (PS/SP) <[monik.beauregard@canada.ca](mailto:monik.beauregard@canada.ca)>  
**Subject:** FW: Briefing

[REDACTED] – do you know who is attending the briefing at 230pm? i.e., is PMO going to be there?  
Was our DM invited? Thanks. John

---

**From:** [REDACTED]  
**Sent:** Friday, October 14, 2016 7:40 AM  
**To:** Davies, John (PS/SP)  
**Subject:** Fw: Briefing

Hi,

As discussed. I'm a little unclear as to whether it's just a briefing for the NSA and pco, or if pmo is invited....  
maybe you should follow up with Nada?

---

**From:** [REDACTED]  
**Sent:** Thursday, October 13, 2016 8:35 PM  
**To:** [REDACTED]  
**Cc:** [REDACTED]  
**Subject:** Briefing

DIR will attend. 2:30.

Sent from my BlackBerry 10 smartphone on the Rogers network.

**Chiasson, Carole (PS/SP)**

---

**From:** Brown, Malcolm (PS/SP)  
**Sent:** Friday, October 21, 2016 12:29 PM  
**To:** Surkes, Marci (PS/SP); Goodale, Ralph - Personal  
**Cc:** Beauregard, Monik (PS/SP); De Santis, Heather (PS/SP); Brien, Dan (PS/SP)  
**Subject:** Re: Decision

Thx.

Sent from my BlackBerry 10 smartphone on the Rogers network.

---

**From:** Surkes, Marci (PS/SP)  
**Sent:** Friday, October 21, 2016 12:16 PM  
**To:** Brown, Malcolm (PS/SP); Goodale, Ralph - Personal  
**Cc:** Beauregard, Monik (PS/SP); De Santis, Heather (PS/SP); Brien, Dan (PS/SP)  
**Subject:** Re: Decision

Will share latest draft.  
Adding Dan.

Sent from my BlackBerry 10 smartphone on the Rogers network.

---

**From:** Brown, Malcolm (PS/SP)  
**Sent:** Friday, October 21, 2016 12:14 PM  
**To:** Goodale, Ralph - Personal; Surkes, Marci (PS/SP)  
**Cc:** Beauregard, Monik (PS/SP); De Santis, Heather (PS/SP)  
**Subject:** Re: Decision

I have not seen anything today. But I will ask for it.

Sent from my BlackBerry 10 smartphone on the Rogers network.

---

**From:** Goodale, Ralph - Personal  
**Sent:** Friday, October 21, 2016 12:12 PM  
**To:** Surkes, Marci (PS/SP); Brown, Malcolm (PS/SP)  
**Cc:** Beauregard, Monik (PS/SP); De Santis, Heather (PS/SP)  
**Subject:** Re: Decision

Indeed! Any thoughts on the draft of my possible response to media. RG

-----  
Sent using BlackBerry

---

**From:** Surkes, Marci (PS/SP) [<mailto:marci.surkes@canada.ca>]  
**Sent:** Friday, October 21, 2016 10:10 AM  
**To:** Brown, Malcolm (PS/SP) <[malcolm.brown@canada.ca](mailto:malcolm.brown@canada.ca)>; Goodale, Ralph - Personal  
**Cc:** Beauregard, Monik (PS/SP) <[monik.beauregard@canada.ca](mailto:monik.beauregard@canada.ca)>; De Santis, Heather (PS/SP) <[heather.desantis@canada.ca](mailto:heather.desantis@canada.ca)>

**Subject:** Re: Decision

Thank you.

MS

Sent from my BlackBerry 10 smartphone on the Rogers network.

---

**From:** Brown, Malcolm (PS/SP)  
**Sent:** Friday, October 21, 2016 12:07 PM  
**To:** Surkes, Marci (PS/SP); Ralph Goodale  
**Cc:** Beauregard, Monik (PS/SP); De Santis, Heather (PS/SP)  
**Subject:** Fw: Decision

Fyi.

Sent from my BlackBerry 10 smartphone on the Rogers network.

---

**From:** Michel COULOMBE [REDACTED]  
**Sent:** Friday, October 21, 2016 11:58 AM  
**To:** Brown, Malcolm (PS/SP)  
**Subject:** Decision

Redacted version is not going to Court until late this aft (3:30) so today seems increasingly unlikely.

Sent from my BlackBerry 10 smartphone on the Rogers network.

**Chiasson, Carole (PS/SP)**

---

**From:** Brown, Malcolm (PS/SP)  
**Sent:** Friday, October 21, 2016 1:24 PM  
**To:** Michel COULOMBE  
**Subject:** Re: Decision

You too.

Sent from my BlackBerry 10 smartphone on the Rogers network.

---

**From:** Michel COULOMBE  
**Sent:** Friday, October 21, 2016 1:21 PM  
**To:** Brown, Malcolm (PS/SP)  
**Subject:** Re: Decision

Will do.

Since almost certain it will not be released today, I am off to Mtl. Reachable via BlackBerry and 90 minutes away if I have to come back.  
Have a good weekend.

Sent from my BlackBerry 10 smartphone on the Rogers network.

---

**From:** Brown, Malcolm (PS/SP)  
**Sent:** Friday, October 21, 2016 13:18  
**To:** Michel COULOMBE  
**Subject:** Re: Decision

Good for you. You should let the minister know.

Sent from my BlackBerry 10 smartphone on the Rogers network.

---

**From:** Michel COULOMBE  
**Sent:** Friday, October 21, 2016 1:13 PM  
**To:** Brown, Malcolm (PS/SP)  
**Subject:** Re: Decision

FYI - we will be sending a note to [REDACTED] on the court decision. In addition, as a courtesy (do not want him to learn about this via media) I have called him for a heads up. He is on his way back from overseas and I left a msg for him to call me back.

Sent from my BlackBerry 10 smartphone on the Rogers network.

---

**From:** Brown, Malcolm (PS/SP)  
**Sent:** Friday, October 21, 2016 12:18  
**To:** Michel COULOMBE  
**Subject:** Re: Decision

Thx.

Sent from my BlackBerry 10 smartphone on the Rogers network.

**From:** Michel COULOMBE  
**Sent:** Friday, October 21, 2016 11:58 AM  
**To:** Brown, Malcolm (PS/SP)  
**Subject:** Decision

Redacted version is not going to Court until late this aft (3:30) so today seems increasingly unlikely.

Sent from my BlackBerry 10 smartphone on the Rogers network.

**Chiasson, Carole (PS/SP)**

---

**From:** Michel COULOMBE <[REDACTED]>  
**Sent:** Friday, October 21, 2016 1:26 PM  
**To:** Ralph Goodale  
**Cc:** Surkes, Marci (PS/SP); Brown, Malcolm (PS/SP)  
**Subject:** Decision

Minister,

FYI - Regarding the recent Court decision, we will be sending a note to the Privacy Comm. In addition, as a courtesy (do not want him to learn about this via media) I have called him for a heads up. He is on his way back from [REDACTED] and I left a msg for him to call me back.

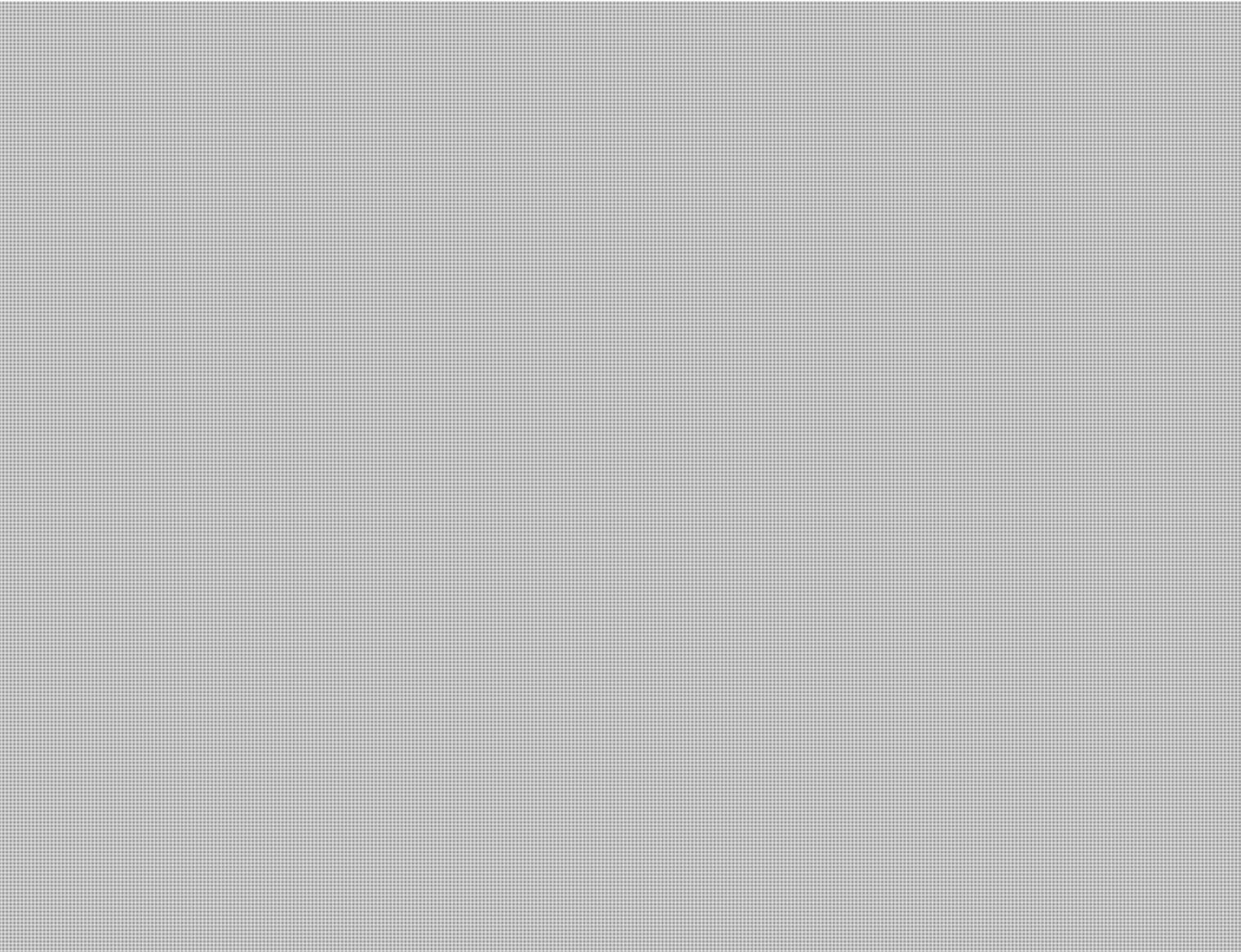
Sent from my BlackBerry 10 smartphone on the Rogers network.

**Davies, John**

---

**From:** [REDACTED]  
**Sent:** Sunday, February 28, 2016 8:18 PM  
**To:** Davies, John; Sugunasiri, Shalin; Baker, Christine (JUSTICE); Duffy, Michael W. (JUSTICE)  
**Cc:** [REDACTED] (CSIS-SCRS); [REDACTED]  
**Subject:** Report on en banc hearing of the Federal Court in application for warrants [REDACTED]

**Classification:** Secret  
**Classification:** Secret  
**Restriction / Restriction d'accès:** NR / AR  
**File Number / No. de dossier:** [REDACTED]



**Page 777**

**is withheld pursuant to sections  
est retenue en vertu des articles**

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

**Davies, John**

---

**From:** [REDACTED]  
**Sent:** Monday, June 13, 2016 8:54 AM  
**To:** [REDACTED]; Davies, John; [REDACTED]  
**Cc:** [REDACTED]  
**Subject:** RE: en banc

**Classification:** Confidential  
**Classification:** Confidential  
**Not for PA / Ne pas classer**

I believe John's already on the Hill, but not to worry, I sent him something on the other system (a version of the download you had provided on the external system on Friday).

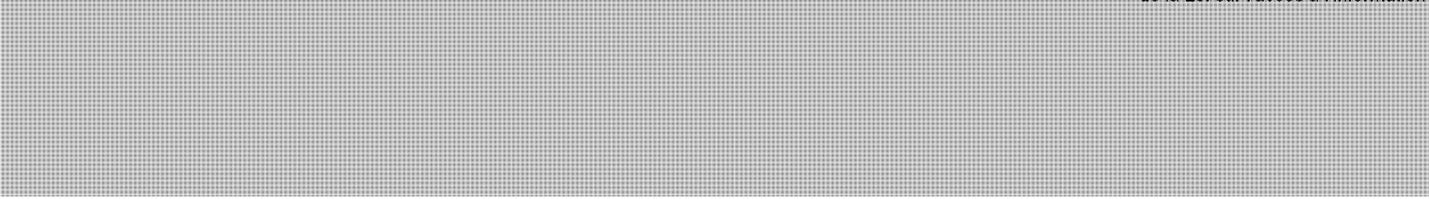
---

**From:** [REDACTED]  
**Sent:** 13-Jun-16 8:50 AM  
**To:** John Davies (PSEPC-SPPCC); [REDACTED]  
**Cc:** [REDACTED]  
**Subject:** RE: en banc

**Classification:** Confidential  
**Classification:** Confidential  
**Not for PA / Ne pas classer**

John

[REDACTED]



**Mylène Bouzigon**

Senior General Counsel (Justice Department) | Avocate générale principale (Ministère de la Justice)  
ADL | DAJ

*This message may be covered by solicitor-client privilege or litigation privilege. It should not be shared outside of the Government of Canada without prior verification.  
Ce message peut être couvert par le secret professionnel de l'avocat ou par privilège relatif au litige. Il ne devrait pas être partagé à l'extérieur du Gouvernement du Canada sans vérification préalable.*

---

**De :** Davies, John [mailto:

**Envoyé :** 13-Jun-16 7:16 AM

**À :** 

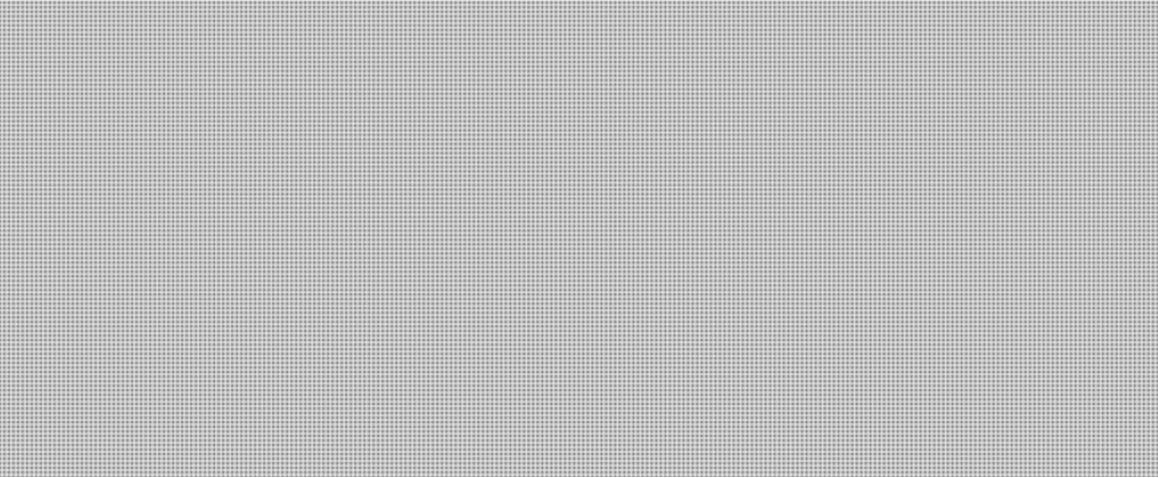
**Cc :** 

**Objet :** en banc

CLASSIFICATION:SECRET

I am seeing the MIN at 9am; he may ask me about the en banc. Can you let me know if there is anything I can relay in that regards? Thanks.

john



**Davies, John (PS/SP)**

---

**From:** Davies, John (PS/SP)  
**Sent:** Monday, June 13, 2016 9:13 AM  
**To:** [REDACTED]  
**Subject:** Re: en banc proceedings

Tks. He didn't ask me about it so good.

Sent from my BlackBerry 10 smartphone on the Rogers network.

**From:** [REDACTED]  
**Sent:** Monday, June 13, 2016 8:52 AM  
**To:** Davies, John (PS/SP)  
**Subject:** Re: en banc proceedings

Mylène just sent you something on the internal... not much more detail, to be honest....

[REDACTED]

**From:** Davies, John (PS/SP)  
**Sent:** Monday, June 13, 2016 8:45 AM  
**To:** [REDACTED]  
**Subject:** Re: en banc proceedings

Ok tks

Sent from my BlackBerry 10 smartphone on the Rogers network.

**From:** [REDACTED]  
**Sent:** Monday, June 13, 2016 8:25 AM  
**To:** Davies, John (PS/SP)  
**Subject:** Re: en banc proceedings

I haven't anything else yet, i'm afraid.

**From:** [REDACTED]  
**Sent:** Monday, June 13, 2016 7:19 AM  
**To:** Davies, John (PS/SP)  
**Subject:** Fw: en banc proceedings

Here's what I have (don't forward, pls). Will see if there is anything more when I get in to the office.

**From:** [REDACTED]  
**Sent:** Friday, June 10, 2016 7:42 PM  
**To:** [REDACTED]  
**Cc:** [REDACTED]  
**Subject:** Fw: en banc proceedings

Below fyi

DIR also advised separately that he and DM Pentney both thought that, overall and all things considered, it went well.

Sent from my BlackBerry 10 smartphone on the Rogers network.

**From:** [REDACTED]

**Sent:** Friday, June 10, 2016 7:37 PM

**To:** [REDACTED]

Karen ROBERTSON

**Cc:** Michel COULOMBE; [REDACTED]

**Subject:** en banc proceedings

Bonsoir

[REDACTED]

Bonne fin de semaine

[REDACTED]

**Davies, John (PS/SP)**

---

**From:** Davies, John (PS/SP)  
**Sent:** Friday, October 14, 2016 8:03 AM  
**To:** Beauregard, Monik (PS/SP)  
**Subject:** RE: Briefing

Yes same subject but it looks like DIR going over to see NSA and maybe PMO today (I think). DM should probably be aware, maybe you should insinuate into that meeting.

---

**From:** Beauregard, Monik (PS/SP)  
**Sent:** Friday, October 14, 2016 8:02 AM  
**To:** Davies, John (PS/SP)  
**Subject:** Re: Briefing

John I have a 2:30 Monday in my calendar with MIN + DM for en banc. We talking the same?

Sent from my BlackBerry 10 smartphone on the Rogers network.

---

**From:** Davies, John (PS/SP)  
**Sent:** Friday, October 14, 2016 7:53 AM  
**To:** [REDACTED]  
**Cc:** Beauregard, Monik (PS/SP)  
**Subject:** FW: Briefing

Nada – do you know who is attending the briefing at 230pm? i.e., is PMO going to be there? Was our DM invited? Thanks. John

---

**From:** [REDACTED]  
**Sent:** Friday, October 14, 2016 7:40 AM  
**To:** Davies, John (PS/SP)  
**Subject:** Fw: Briefing

Hi,

As discussed. I'm a little unclear as to whether it's just a briefing for the NSA and pco, or if pmo is invited... maybe you should follow up with Nada?

---

**From:** [REDACTED]  
**Sent:** Thursday, October 13, 2016 8:35 PM  
**To:** [REDACTED]  
**Cc:** [REDACTED]  
**Subject:** Briefing

DIR will attend. 2:30.

Sent from my BlackBerry 10 smartphone on the Rogers network.

**Howell, John**

---

**From:** Davies, John  
**Sent:** October-18-16 5:33 PM  
**To:** [REDACTED]  
**Subject:** [REDACTED]

**Attachments:** [REDACTED]

CLASSIFICATION:SECRET

**From:** [REDACTED]  
**Sent:** Tuesday, October 18, 2016 5:28 PM  
**To:** [REDACTED] Schmidt, Emily A. (JUSTICE);  
Davies, John  
**Cc:** Matte, Daniel R. (JUSTICE); [REDACTED]  
**Subject:** [REDACTED]

Classification: Secret//Solicitor-Client Privilege  
Classification: Secret//Secret professionnel de l'avocat  
Restriction / Restriction d'accès: NR / AR  
File Number / No. de dossier: [REDACTED]

[REDACTED]

Thank you,

[REDACTED]  
Executive Assistant (EA) / Chef du Cabinet  
Assistant Director, Legal Services (ADL)  
Senior General Counsel, Department of Justice  
[REDACTED]

**Pages 785 to / à 791  
are withheld pursuant to sections  
sont retenues en vertu des articles**

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

**Davies, John**

---

**From:** [REDACTED]  
**Sent:** Wednesday, October 19, 2016 7:46 PM  
**To:** Davies, John  
**Cc:** [REDACTED]  
**Subject:** OPC and SIRC and En Banc

**Classification: Secret**  
**Classification: Secret**  
**Not for PA / Ne pas classer**

John,  
Now that we have gotten through the crush of the first wave of comms products, my staff are taking a look at our engagement with the OPC on this issue back in 2010-2011 time period, including the submission of a formal PIA. We CAN safely say that they were properly engaged on this, and have an exchange of correspondence with them. We'll try to get this sorted in the next day or two to figure out how best to position this issue, and whether there is value to an informal chat with them shortly after the ruling is released. Also, we have lots of info on how and when SIRC was engaged, and we should discuss that, as well. I think the Federal Court story isn't great, but I would say that the existence of the programme itself, the acknowledgment and consideration of privacy interests and government engagement/awareness of our abilities and intent is a good one.

[REDACTED]

---

**From:** Davies, John  
**Sent:** October-20-16 8:01 AM  
**To:** [REDACTED]  
**Subject:** FW: Briefing Note for Ministers - Assessment of Impact of Federal Court Decision (CSIS) of October 4, 2016  
**Attachments:** Note to Minister about CSIS warrant\_ES.docx; Note to Minister about CSIS Warrants\_Oct\_19\_2016.docx

CLASSIFICATION:SECRET

Could you get copies to SADM, DMO and LSU? I assume we should just get a copy to MO now as well, but will check. Thanks

**From:** [REDACTED]  
**Sent:** Wednesday, October 19, 2016 5:41 PM  
**To:** Davies, John  
**Cc:** Matte, Daniel R. (JUSTICE); [REDACTED]  
**Subject:** Briefing Note for Ministers - Assessment of Impact of Federal Court Decision (CSIS) of October 4, 2016

**Classification:** Secret  
**Classification:** Secret  
**Restriction / Restriction d'accès:** NR / AR  
**File Number / No. de dossier:** 51000-931

Please find enclosed copy of the BN sent to the Minister of Justice for the purpose of sending it on to the Minister of Public Safety as discussed. I understand that the minister of PS will be informed that the same note is provided to his colleague. I gather the note is the same the one provided to DMs, with the exception of first possible release date pushed to the 21.

I also include the executive summary which may be used in preparing the cover note for PS.

Would be grateful if you could share a copy of this with Michael Sousa. I will share this with the Service as well.

Thank you

[REDACTED]

Senior General Counsel (Justice Department) | Avocate générale principale (Ministère de la Justice)  
ADL | DAJ

*This message may be covered by solicitor-client privilege or litigation privilege. It should not be shared outside of the Government of Canada without prior verification.  
Ce message peut être couvert par le secret professionnel de l'avocat ou par privilège relatif au litige. Il ne devrait pas être partagé à l'extérieur du Gouvernement du Canada sans vérification préalable.*

[REDACTED]

**Pages 794 to / à 795  
are withheld pursuant to sections  
sont retenues en vertu des articles**

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

**Pages 796 to / à 801  
are withheld pursuant to sections  
sont retenues en vertu des articles**

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

[REDACTED]

---

**From:** Davies, John  
**Sent:** October-20-16 4:55 PM  
**To:** [REDACTED]  
**Subject:** FW: CSIS and PS Timelines  
**Attachments:** PS Timeline - Draft.docx; 2016 10 20 - Timeline - 3 Pager.docx

CLASSIFICATION:SECRET

[REDACTED]

---

**From:** [REDACTED]  
**Sent:** Thursday, October 20, 2016 4:47 PM  
**To:** [REDACTED]  
**Cc:** [REDACTED]  
**Subject:** CSIS and PS Timelines

Classification: Secret  
Classification: Secret  
Not for PA / Ne pas classer

[REDACTED]

For the attention of [REDACTED]

Tricia has asked that I provide you with, for background, attached timelines prepared by both Public Safety and CSIS. Please note that these remain DRAFT, Secret and for internal use only.

Thanks,

[REDACTED]  
Analyst, Strategic Policy  
[REDACTED]

[REDACTED]

**Pages 803 to / à 806  
are withheld pursuant to sections  
sont retenues en vertu des articles**

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

**Page 807**

**is withheld pursuant to sections  
est retenue en vertu des articles**

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

(PS/SP)

**From:** Davies, John (PS/SP)  
**Sent:** Monday, October 24, 2016 8:24 AM  
**To:** Grenier, Julie (PS/SP); Tomlinson, Jamie (PS/SP); Magee, Heather (PS/SP)  
**Cc:** [REDACTED]  
**Subject:** FW: Updated Products  
**Attachments:** Backgrounder ADP Approved.docx; Backgrounder ADP Approved-French.docx; Director Opening Remarks ADP approved French.docx; Director Statement ADP approved.docx; Director Statement ADP approved-French.docx; Q&A ADP approved..docx; Q&A ADP approved.-TEF.DOCX

I assume you have these already, but just in case.

Can you let us know where things are at from your perspective? Do we owe you any comments etc? Does MO have all they need?

Thanks.

John

---

**From:** [REDACTED]  
**Sent:** Sunday, October 23, 2016 8:25 AM  
**To:** Davies, John (PS/SP); [REDACTED]  
**Cc:** [REDACTED]  
**Subject:** Fw: Updated Products

Hi guys,

John and Nada, your comms folks have these and for version control and coordination, probably easiest for you to feed specific comments or any suggested changes directly to them (that said, we are at disaster check stage) and you may even want to wait for whatever pmo or mo consulted version they want to send you, first. Still may see some dm level edits as well. That said, if after reading these you have questions or comments more generally, please let me know. Happy to do by email or with a call, preferably this afternoon.

---

**From:** [REDACTED]  
**Sent:** Saturday, October 22, 2016 4:45 PM  
**To:** [REDACTED]  
**Cc:** [REDACTED]  
**Subject:** Updated Products

As discussed, please find attached the updated and translated products. I will now send them to DG Comms at Justice, Public Safety and PCO.

I have printed copies for yourself, the ADE, the Director and [REDACTED] and will bring them to the retreat tomorrow.

# Backgrounder

*Federal Court ruling on the retention of associated data linked to third party information.*

## **IMPACT OF THE DECISION ON CSIS:**

- The Canadian Security Intelligence Service is mandated to investigate activities which may, on reasonable grounds, be suspected of posing a threat to the security of Canada. In order to investigate these threats, CSIS may apply to the Federal Court for a warrant when the response to the threat requires more intrusive measures.
- Through the proceedings of the Court, over time, the provisions of warrants have changed to take into account the evolution of technology, legal developments, and investigative measures.
- This ensures that the powers granted by the warrants are clearly defined and that their conditions take into account the impact that the execution of the warrants and the retention of the information may have on third parties.
- The decision relates to certain information that has been legally collected via the execution of warrants, issued by the Court, which authorized the interception of communications.
- CSIS had sought to fully analyze all of the information - both the content and the associated data - for example, email addresses and telephone numbers.
- As is the case for many of our international partners, CSIS has developed data analytic capabilities and expertise to significantly enhance the identification and assessment of threats to the security of Canada over time and space. This includes identifying patterns of movement, communications, behaviours, significant trends, and links that are otherwise unidentifiable.

- When it comes to understanding and predicting the actions of the subjects of our investigations, data analytics has proven to be an effective tool.
- In the ruling released today the Federal Court recognized the value of the data analytic programme and confirmed the legality of collecting telecommunications associated data pursuant to warrants.
- On the very specific issue of associated data linked to third-party communications, the Court found that it can only be retained if it is related to threats or of use to an investigation, prosecution, national defence or international affairs.
- CSIS, in consultation with the Department of Justice, had interpreted the *CSIS Act* as enabling the retention of this sub-set of associated data to allow for that important analytic work. All laws must be interpreted in the circumstances and when the *CSIS Act* was written, it did not conceive of current technologies and the potential for data analytics.
- At no time did the Service believe this to be inconsistent with the *CSIS Act*.
- It is now clear that the Federal Court disagrees with this interpretation of the *Act*.
- We accept this decision in full, and have taken immediate actions to respond.
- In response to the decision, CSIS halted all access to, and analysis of, associated data while we undertake a thorough review of the decision in order to assess potential operational and legal impacts, and determine our way forward.
- CSIS takes seriously the concerns expressed by the Court with respect to our duty of candour and recognizes the importance of openness and transparency with the Federal Court.
- CSIS is working closely with the Department of Justice to develop measures aimed at ensuring that we meet our obligations to the Court in matters of transparency and duty of candour.

**Pages 811 to / à 813  
are not relevant  
sont non pertinentes**

UNCLASSIFIED  
NON CLASSIFIÉ

## **Opening Remarks on Federal Court *En Banc* Decision**

### **National Press Gallery**

#### **Mot d'ouverture sur la décision rendue en banc par la Cour fédérale**

#### **Tribune de la presse nationale**

- **Thank you Andrew. Bonjour Mesdames et Messieurs. Today (or TBD) the Federal Court issued an *En Banc* Decision. I am here to explain what this decision means.**
- **I would like to start off by saying, first and foremost, that the Canadian Security Intelligence Service accepts in full the Court's decision, and have taken immediate actions to respond.**
- **I deeply regret the Court's serious concerns with respect to our duty of candour and I commit to continuing my efforts, with the Deputy Minister of Justice, to fully address this concern.**
- **CSIS recognizes the importance of openness and transparency with the Federal Court, and we are working closely with the Department of Justice to develop measures aimed at ensuring that**

UNCLASSIFIED  
NON CLASSIFIÉ

**we meet our obligations to the Court in matters of transparency and duty of candour.**

- **Given the Court's decision with respect to third-party data, CSIS has halted all access to, and analysis of, associated data while we undertake a thorough review of the decision in order to assess potential operational and legal impacts, and determine our way forward.**
- **Let me be clear that all associated data collected, under warrant, was done so legally. The Court's key concern related to our retention of non-threat related associated data linked with third party communications, after it was collected.**
- **CSIS, in consultation with the Department of Justice, interpreted the CSIS Act to allow for the retention of this sub-set of associated data.**
- **It is now clear that the Federal Court disagrees with this interpretation; a decision which we fully accept.**

UNCLASSIFIED  
NON CLASSIFIÉ

- **All laws must be interpreted in the circumstances, and when the Act was written, current technologies and the potential for data analytics could not have been anticipated.**
- **The Court rightly acknowledged the age of the CSIS Act and that it may not be keeping pace with changing technology and the current threat environment, contributing to this challenge.**
- **That said, again, we fully accept the decision of the Court.**
- **As Canada's national intelligence agency, CSIS investigates activities which may, on reasonable grounds, be suspected of posing a threat to the security of Canada.**
- **One of the ways we investigate these threats is through warrants issued by the Federal Court which authorize the interception of communications. This includes analysis of all of the information - both the content and the associated data.**
- **Associated data includes information such as: email addresses and telephone numbers but never the content.**

UNCLASSIFIED  
NON CLASSIFIÉ

- **It is useful in identifying patterns of movement, communications, behaviours, significant trends, and links that are otherwise unidentifiable.**
- **As is the case for many of our international partners, CSIS has developed data analytic capabilities and expertise to exploit associated data and enhance its capacity to identify and assess threats to the security of Canada over time.**
- **When it comes to understanding and predicting the actions of the subjects of our investigations, data analytics has proven to be an effective tool.**
- **In the ruling released today the Federal Court recognized the value of the data analytic programme and confirmed the legality of collecting telecommunications associated data pursuant to warrants.**
- **I would add that, like the threats we face today, technologies and associated privacy implications have also evolved.**
- **The retention and analysis of information is a significant public policy issue, not just in Canada, but also among our closest allies.**

UNCLASSIFIED  
NON CLASSIFIÉ

- **I would like to say, that the trust of Canadians is fundamental to our ability to deliver on our mandate.**
- **Because the nature of our business is principally secret, Canadians are largely unaware of the professionalism and outstanding dedication the men and women of CSIS show every day as they carry out intelligence work. As the Director of CSIS, I am extremely proud of the people with whom I work. Canadians, too, should be proud of those who work tirelessly to keep this great country safe.**
- **We appreciate the confidence the government invests in CSIS, and it remains for us a privilege to protect Canadians and Canada's interest at home and abroad.**
- **The ongoing national security consultations represent an important opportunity to ensure that CSIS is meeting the dual objectives of security and privacy, and has the tools and authorities, with appropriate oversight, to meet both.**
- **(REPEAT IN FRENCH)**
- **(RÉPÉTER EN FRANÇAIS)**

**Pages 819 to / à 823  
are not relevant  
sont non pertinentes**

UNCLASSIFIED  
NON CLASSIFIÉ

- **With that, I will be happy to answer some questions.**
- **Je répondrai maintenant à vos questions avec plaisir.**

**Pages 825 to / à 826  
are duplicates  
sont des duplicatas**

**Pages 827 to / à 828  
are not relevant  
sont non pertinentes**

UNCLASSIFIED

Embargoed until decision is published

## Qs & As

### A. THE FEDERAL COURT DECISION

#### 1. Why did you appear before the Federal Court?

- The Canadian Security Intelligence Service is mandated to investigate activities which may, on reasonable grounds, be suspected of posing a threat to the security of Canada. In order to investigate these threats, CSIS may apply to the Federal Court for a warrant when the response to the threat requires more intrusive measures. Late 2015, CSIS applied to renew and obtain new warrants as well as propose amendments to warrant conditions.
- In light of the finding in the Security Intelligence Review Committee's (SIRC) annual report (2014-15), the Court requested that the collection, use, retention and destruction of associated data (referred to by SIRC as metadata) collected under warrants also be addressed.
- These issues were heard en banc.

#### 2. What is the decision?

- The Court agreed with most of the terms and conditions proposed by CSIS on the warrant application that was presented to the Court.
- The Court found that CSIS failed to fully and transparently inform the Court of its retention program and the establishment of the Operational Data Analysis Centre (ODAC), but did not find evidence that this had been done deliberately.
- The Court also determined that CSIS' retention of associated data linked to third-party communications found to be unrelated to threats or of no use to an investigation, prosecution, national defence or international affairs to be illegal.
- That said, it is important to underline that all associated data was collected legally through warrants. The Federal Court's key concern relates to CSIS' retention of non-threat related associated data linked with third party communications, after it was collected.
- Further, the Court rightly acknowledged the age of the *CSIS Act* and that it may not be keeping pace with changing technology and the current threat environment.

#### 3. What is the Government's duty of candour?

- In all instances where only one party is before the Court, without having all of the other interested parties present (known as an "*ex parte*" or "*in private*" hearing), that the party is under a duty of utmost good faith in the representations it makes to the Court.

UNCLASSIFIED

Embargoed until decision is published

- The evidence presented must be complete and thorough and no relevant information adverse to the interests of the party may be withheld.
- The Federal Court has noted that this duty is heightened when hearings take place behind closed doors, rather than in public, as often occurs in cases related to national security.
- The duty of candour applies to all parties, not just the Government.

**4. So the Government breached its duty of candour in this case?**

- Department of Justice lawyers, who represented CSIS in this matter, strive to uphold the highest standards of the legal profession in their representation of the Government interests in the Courts.
- In this case, the Government accepts the Federal Court's findings that regarding CSIS's duty of candour and is taking immediate action to address those findings.
- CSIS can and will do more to ensure that it is fully transparent with the Federal Court regarding the use it makes or plans to make of the information it collects pursuant to Federal Court issued warrants. To that end, it is working closely with the Department of Justice.

**5. This is not the first incident of CSIS being found to be in breach of Duty of Candour. Why and what is being done to address this?**

- CSIS recognizes the importance of openness and transparency with the Federal Court.
- Overtime the provisions of the warrants have changed to take into account the evolution of technology, legal developments and investigate measures.
- The *CSIS Act* defines the Service's relationship with the Court. The means to approach the Court is through a warrant application, which creates a very focused type of interaction.
- Given the Court's findings, we are seized with these concerns and are working closely with the Department of Justice to develop measures aimed at ensuring that we meet our obligations to the Court in matters of transparency and duty of candour.

**6. What is CSIS doing to address the duty of candour issues and why should they be trusted given that this is a second breach of this nature?**

- CSIS is committed to improve its practices involving the Court to ensure it fully meets its duty of candour

UNCLASSIFIED

Embargoed until decision is published

- In consultation with the Department of Justice, we are working to develop measures aimed at ensuring that we meet our obligations to the Court in matters of transparency and duty of candour.

**7. Why did CSIS not inform the Court of its new position on the retention of data and the creation of the Operational Data Analysis Centre (ODAC)?**

- At various points, the Government, the Security Intelligence Review Committee and the Office of the Privacy Commissioner were made aware of CSIS' position on the retention of data and the establishment of ODAC.
- In June 2011, CSIS did advise the Federal Court that it amended the wording of warrant conditions in an effort to distinguish the content of communications from the associated data of communications. The Court found that notification to be insufficient.
- CSIS takes notice of the fact that the Court should have been informed earlier of the existence of ODAC and the change in the retention policy and acknowledges this was a significant omission. At no point did CSIS deliberately seek to withhold this information from the Court, and the Court acknowledged that there is no evidence to that fact.
- The development of this new capability evolved over time as has our understanding of our obligations towards the Federal Court in this regard, which CSIS determines in close consultation with the Department of Justice.

**8. SIRC recommended in their 2014-15 Report that the Service advise the Federal Court of activities relating to metadata collected under a warrant. CSIS, however believed that SIRC's recommendation was both inappropriate and unwarranted given that section 21 of the CSIS Act does not confer any general supervisory authority to Federal Court judges. Why did CSIS take this position?**

- It is SIRC that reviews the activities of CSIS and not the Federal Court. This stems from a strict interpretation of the *CSIS Act*. It is now clear that the Federal Court disagrees with such an interpretation. The Service accepts this finding.
- The Service was under the impression that the Federal Court had been sufficiently advised of the retention of associated data in 2011. The Court also disagreed with this assessment. The Service accepts this finding.

**9. Has CSIS briefed this Minister on this matter?**

- In the context of an update on the en banc hearing, the current Minister of Public Safety has been briefed a number of times.
- At various points, previous Ministers, the Security Intelligence Review Committee and the Office of the Privacy Commissioner were made aware of CSIS' position on the retention of data and the establishment of ODAC.

UNCLASSIFIED

Embargoed until decision is published

**10. Did CSIS purposely mislead the Court in this case?**

- The Court found that CSIS failed to fully and transparently inform the Court of its retention program and the establishment of the Operational Data Analysis Centre (ODAC), but did not find evidence that this had been done deliberately.

**11. Can CSIS be held in “contempt of court” for not disclosing this information?**

- (Answer to be provided by DoJ)

**CSIS RESPONSE TO THE DECISION**

**12. What have you done to respond to the judgement?**

- On duty of candour: CSIS takes this finding very seriously and recognizes the importance of compliance with Ministerial Direction and the *CSIS Act*, as well as openness and transparency with the Court.
- CSIS can and will do more to ensure that it is fully transparent with the Federal Court regarding the use it makes or plans to make of the information it collects pursuant to Federal Court issued warrants. To that end, it is working closely with the Department of Justice.
- On the retention of non-threat related associated data linked with third-party communications: CSIS immediately halted access to, and analysis of, associated data until such time as it can successfully distinguish associated data linked to third-party communications from that of subject of investigation communications.

**13. What steps will CSIS take to implement the Court’s recommended two-step process of assessment?**

- CSIS will be required to assess, within a short period, communications data to determine its relevance to a subject of investigation or threat to the security of Canada.
- Significant efforts will be required to implement policies, processes and technology that will successfully distinguish between threat related and non-threat related associated data. ~~associated data (third party communications) from that of threat related communications.~~

**14. Has CSIS destroyed the data deemed illegal by the Court?**

- The Court did not order CSIS to destroy third-party associated data from its databases and recognized that the retention and analysis of associated data has yielded useful intelligence results in the past.

UNCLASSIFIED

Embargoed until decision is published

- CSIS immediately halted analysis and use of all associated data until such time as it can successfully distinguish associated data from that linked to a threat.
- We are assessing the application of the Court's finding in this regard.

### **IMPACTS OF THE DECISION**

#### **15. Did CSIS collect this information legally?**

- Any collection activity that requires the use of specific investigative techniques is authorized by warrants issued by the Federal Court. CSIS collected this information legally, as confirmed in the decision.
- The Federal Court's key concern relates to CSIS' retention of non-threat related associated data linked with third-party communications, after it was collected.

#### **16. Why was CSIS retaining this third party associated data if it was not authorized by the CSIS Act?**

- All laws must be interpreted in the circumstances and when the CSIS Act was written, it did not conceive of current technologies and the potential for data analytics.
- CSIS, in consultation with the Department of Justice, interpreted the CSIS Act to allow for the retention of this data.
- It is now clear that the Federal Court disagrees with this interpretation.
- CSIS fully accepts the Court's ruling and has taken appropriate steps to respond.

#### **17. Will this decision affect the admissibility of evidence used in the cases of convicted terrorists?**

- CSIS is mandated to collect, by investigation or otherwise, to the extent that is strictly necessary, and analyze and retain information and intelligence regarding activities that may on reasonable grounds be suspected of constituting threats to the security of Canada.
- CSIS collects intelligence or information for the purpose of advising the Government, providing security advice or security assessments. It does not, however, collect evidence.

#### **18. Were leads generated by the use of third-party associated data provided to the RCMP or other law enforcement partners for the purposes of counter terrorism investigations?**

- CSIS is assessing the decision in an effort to determine how it impacts operations. CSIS cannot, however, comment on the nature of its operations, and how they are impacted.

UNCLASSIFIED

Embargoed until decision is published

**19. Does this decision impact any current terrorism related cases?**

- CSIS is assessing the decision in an effort to determine how it impacts operations. CSIS cannot, however, comment on the nature of its operations, and how they are impacted.

**20. How many Canadians were impacted?**

- It is impossible to quantify the number of individuals linked to the associated data, much less identify personal details such as citizenship.
- The associated data in question is associated with communications lawfully intercepted under warrant in relation to the investigation of threats to the security of Canada.
- Associated data does not reveal the purpose of the communication, nor any part of the content and, on its own, does not identify individuals who are party to the communication.
- This speaks directly to the nature of associated data, which, on its own, does not readily identify an individual.

**BROADER IMPLICATIONS OF THE DECISION**

**21. Are there any privacy implications noted in the decision?**

- The Federal Court did not speak to the privacy considerations of the retention of third-party associated data.
- CSIS recognizes the importance of maintaining public trust and confidence in its activities. CSIS takes very seriously potential privacy considerations related to its work, and it is committed to ensuring that its activities are transparent, accountable and in compliance with privacy legislation, guidelines and best practices.
- Of note, a Privacy Impact Assessment on ODAC was completed in August 2010. Should the Office of the Privacy Commissioner be interested in investigating the privacy implications of the decision, CSIS will cooperate fully.

**22. How can Canadians have confidence in the organization?**

- CSIS recognizes the importance of maintaining public trust and confidence, and has a strong record of responsibly exercising its authorities and has matured as an organization over its 30 year history.
- SIRC, and the Inspector General before it, has consistently found that the Service has carried out its duties in accordance with the CSIS Act and Ministerial Direction and that the exercise of its activities has been reasonable and necessary.
- CSIS maintains a productive relationship with SIRC. SIRC's findings and recommendations have demonstrably shaped the conduct of CSIS operations and continue to do so.
- And in the context of warrant powers, CSIS must also answer to the Federal Court.
- As CSIS adapts to an ever-changing environment, challenges do emerge, demanding continual improvement to operational policies and procedures, supported by a robust governance framework.

UNCLASSIFIED

Embargoed until decision is published

- CSIS operates in a rigorous system of checks and balances. These layers of accountability are mutually reinforcing, which is certainly highlighted in this instance and will be bolstered by enhanced oversight by the proposed Committee of Parliamentarians.

**23. Will the government consult Canadians on the data exploitation activities of CSIS?**

- The Government is committed to keeping Canadians safe while at the same time safeguarding our freedoms, rights and values in an open and democratic society.
- The ongoing national security consultations represent an important opportunity to ensure that CSIS is meeting the dual objectives of security and privacy and has the tools and authorities, with appropriate oversight, to meet both.

**24. Will the new National Security and Intelligence Committee of Parliamentarians have any role in reviewing CSIS' data exploitation activities?**

- Enhancements to the review system, including the proposed National Security and Intelligence Committee of Parliamentarians, will be properly decided by Parliament.
- As currently drafted, the Bill to establish the Committee would authorize it to review the operational activities of CSIS, including programmes such as its data exploitation activities.
- CSIS will, of course, respect and fully cooperate with this committee, should it be stood up and wish to review this issue, or any other CSIS activity.

**ODAC, DATA EXPLOITATION AND ASSOCIATED DATA**

**25. What kind of communications data does the Service collect?**

- In the course of an investigation, CSIS may obtain warrant powers against individuals or entities to authorize the use of specific investigative techniques. These powers, for example, allow CSIS to intercept communications. Execution of such warrant powers may result in the incidental collection of information from parties other than the target (i.e. third-parties).
- When CSIS intercepts a communication, it obtains the content of the communication, as well as data about the communication. This could include: email addresses and telephone numbers.
- This data does not include any information that could reveal the purpose of the communication, nor any part of its content.

**26. What is the difference between associated data and metadata?**

- There is no difference. Associated data – or metadata – refers to information associated to a communication intercepted pursuant to a warrant.

UNCLASSIFIED

Embargoed until decision is published

- Neither metadata or associated data includes any information that could relate to content.
- Metadata is the context, not the content of a communication. It is information used by computer systems to identify, describe, manage or route communications across a network.

**27. What is associated data as defined by the Federal Court?**

- CSIS had applied the term associated data to all metadata associated to a communication intercepted under warrant.
- The Federal Court, however, diverged from the Service's definition.
- The Federal Court defines associated data as communications data collected under warrant from which the content was assessed as unrelated to threats and of no use to an investigation, prosecution, national defence or international affairs.
- Given the Federal Court's interpretation, the Service will undertake to review the terminology it applies to management of information collected under warrant.

**28. What is the difference between associated data and the dataset collection SIRC reviewed recently?**

- SIRC's 2016 Annual Report reviewed CSIS's non-warranted collection of datasets. This does not include communications content or data collected under Federal Court warrant.
- As an example, some non-warranted datasets are referential and provide contextual information which is publicly available. CSIS has developed a rigorous governance framework for the collection of non-referential datasets. This framework sets out clear requirements and a decision-making process to ensure that our collection in this regard respects *CSIS Act* requirements and the Charter, including privacy considerations.
- The Federal Court was concerned only with warranted collection, namely retention of third party associated data. That said, the Service is assessing the implications of this ruling for the non-warranted datasets SIRC recently reviewed.

**CSIS USE OF ASSOCIATED DATA**

**29. How will CSIS deal with the associated data it currently holds?**

- CSIS immediately halted all access to, and analysis of, all associated data until such time as it can successfully distinguish associated data from that linked to a threat.

**30. Has or does CSIS share its associated data holdings with foreign partners?**

- CSIS does not share raw associated data with foreign or domestic partners.
- Associated data that has been analysed and determined to be related to a threat could have been shared with domestic and foreign partners in accordance with our national security mandate.

UNCLASSIFIED

Embargoed until decision is published

- Although raw associated data would not have been shared with partners, it is used to inform our investigations as well as intelligence products which may be discussed and shared with partners.
- In this context the associated data would have been deemed threat related and thus is authorized to be retained by the Service.

**31. How is this collection different from the bulk collection of SIGINT agencies?**

- CSIS collection of communications data is authorized under Federal Court warrants and is specifically focused on an identified target of investigation.

**32. How does or did CSIS previously ensure that data exploitation technologies did not unnecessarily target individuals NOT engaged in threat related activity?**

- Data exploitation is used in response to specific operational queries related to mandated investigations.
- Data exploitation is a tool to assist the Service in discovering linkages, trends and patterns to advance investigations.
- Determining whether or not a communication is threat-related is complex and may only become apparent as an investigation progresses.
- The Service has seen examples where communications originally assessed to have no intelligence value were later revealed to contain key threat-related information.

**33. What is third party information?**

- Subjects of investigation communicate with a whole range of people for a whole range of purposes, which may or may not be threat-related.
- When these communications are intercepted, it is not immediately known whether or not the communication is related to the threat.
- The Court acknowledged that in executing warrant powers, CSIS will by necessity collect third party information; information that is not directly associated with a subject of investigation.
- Some third party information is threat-related and provides essential investigative leads. Some, however, has no intelligence value
- CSIS policy and practice is to delete the content of communications intercepts collected under warrant assessed to be of no intelligence value.
- Though the content was destroyed, the data about the communication was retained, whether or not it was related to a third party.
- On the very specific issue of non-threat related associated data linked to third-party communications, the Court found that it can only be retained if it is related to threats or of use to an investigation, prosecution, national defence or international affairs.

UNCLASSIFIED

Embargoed until decision is published

**34. What is data exploitation, how does CSIS conduct data exploitation and why?**

- Data exploitation employs computers to analyze data and discover linkages, trends and patterns. These techniques enable humans to make sense of volumes of information that could not be processed without a computer's assistance.

Data exploitation enables the Service to effectively analyze threats to the security of Canada over time. It can provide insight into subjects of investigation; identify new leads and intelligence gaps and provide context and understanding to operations.

- The exploitation of data is invaluable in relation to the exercise of CSIS' mandate, but it must be undertaken responsibly and in accordance with our authorities. The Federal Court decision provides new direction in this regard.

**35. What is ODAC? Was anyone advised of its existence?**

- To derive more value from the data already being collected under warrant using data exploitation techniques, the Service established the Operational Data Analysis Centre in 2006.
- The necessity of creating this capability was described to the Minister of Public Safety in July 2006, noting that a basic requirement of ODAC would be the ability to retain data for extended periods of time.
- CSIS also informed subsequent ministers, the Inspector General, the Privacy Commissioner and SIRC.

**36. How long has CSIS had a formal data exploitation program?**

- The necessity of creating this capability was described to the Minister of Public Safety in July 2006 when CSIS developed the Operational Data and Analysis Centre (ODAC). This capability was created with full disclosure to the Government.

**37. Was SIRC aware of CSIS' data exploitation activities and collection of associated data?**

- SIRC was aware of CSIS' data exploitation activities from shortly after the establishment of ODAC in 2006. In 2007, CSIS responded to a SIRC query about ODAC and its support to operations.
- The Inspector General was provided a verbal briefing on ODAC and data exploitation in support of operations in 2011.
- SIRC reviewed CSIS' use of associated data and published its findings on the issue in its 2014-15 annual report. SIRC did not conclude that the retention of associated data was illegal.

**38. What were the Service's practices with regard to the retention of data collected under warrant prior to the Federal Court's decision?**

UNCLASSIFIED

Embargoed until decision is published

- Pursuant to policy, one year after collection, CSIS practice was to delete the content of communications intercepts collected under warrant assessed to be of no intelligence value.
- Though the content was destroyed, the data about the communication was retained, whether or not it was related to a third-party.

### **FEDERAL COURT, "EN BANC" HEARINGS**

#### **39. What is an "en banc" hearing and why are they used?**

- These are hearings where all available judges, in this case designated judges of the Federal Court, attend, participate, and hear evidence. These hearings are a longstanding judicial practice which is utilized in Courts around the world. For example, all Supreme Court of Canada hearings are conducted "en banc".
- Sitting "en banc" is helpful because it avoids the need to repeat evidence in similar applications in the future. In reaching a decision, judges also have the benefit of one another's perspectives.

#### **40. Why are "en banc" hearings being held in relation to national security issues? What was the Governments' role?**

- The Federal Court of Canada, which has requested that some warrant applications be heard in the presence of all designated judges, determines when en banc hearings occur.
- Representatives of CSIS and the Attorney General of Canada attended these hearings in order to fully understand the Court's expectations and to be in the best possible position to meet them in future ex parte proceedings involving warrants requested by CSIS.

#### **41. Why were these hearings held in secret?**

- There are many reasons why court proceedings may be held privately (also known as "in-camera"), including the protection of national security. This is a common practice which applied to all types of hearings, not just "en banc" hearings.
- In this case, the hearing was held in-camera pursuant to section 27 of the *CSIS Act*

**Pages 840 to / à 852  
are not relevant  
sont non pertinentes**