A-2014-555
<table>
<thead>
<tr>
<th>Subject-Sujet</th>
<th>Priority-Priorité</th>
<th>Record of Consultation</th>
<th>Comments-Commentaires</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>DDO and Director,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Please find attached.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>s. 13 security assessment</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>While this particular assessment is not being provided to your attention due to a specific recommendation being made by the Service, I believe you will want to be aware of its content and associated fact gathering.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Available to discuss at your convenience.</td>
</tr>
</tbody>
</table>

Chief GSS

DDG Ops

DG SSB

CCM# 02501
Table of Contents

TAB 1: Table of Contents
MEMO

TO:   Director (via ADH)  
FROM: Review Committee  

SUBJECT: Mobility Review - Transfer of Service employee submitted to the ADH a request to not relocate. As per the Service's Mobility of Intelligence Officers procedures, section 5.3, which is governed by the Recruiting and Staffing policy, the employee submitted two written rationales in support of her request for the cancellation of the transfer (attached).

Further to request, and pursuant to the Service's Mobility of Intelligence Officers procedures, section 5.4, the ADH designated the undersigned to form a Mobility Review Committee with the mandate of evaluating if the grounds submitted by the employee are compassionate or compelling enough to postpone or cancel the relocation.

Committee members reviewed the employee's written submissions. This process included convening as a formal committee to evaluate the employee's documented reasoning, which was considered in the context of relative policy and organizational requirements. Finally, was interviewed by committee members on 2015 01 20 in NHQ during which time answered questions and provided additional information and context relevant to this determination.

Subsequent to these steps, the Mobility Review Committee has arrived at the following recommendation:

Postponing the Transfer to the summer of 2016

While there have been discussions with management, no steps were taken to relocate.
Committee members believe that there are compelling and compassionate reasons to postpone transfer. It should be noted that the Committee had a discussion around cancelling the transfer but decided against it given that mobility is a condition of employment for IOs in order to meet the Service's operational requirements.

Recommendation is: □ Accepted ☒ Not Accepted

Michel Coulombe
Director
2018.02.05
Dear

I am writing to inform you of my decision with respect to your request to cancel your transfer.

In arriving at a decision in this matter, I have taken into account all of the points you raised in your written submission to the ADH, as well as the recommendation of the Mobility Review Committee.

Given the unique circumstances of your particular situation, combined with the fact that mobility for 10 employees is subject to review as part of the Special Project on Operational Transformation, I have decided to postpone indefinitely your transfer.

Notwithstanding the foregoing, should your personal situation change and you find yourself in a position to revisit this matter, please advise your Regional Director General.

Michel Coulombe
<table>
<thead>
<tr>
<th>Action / Donnez suite</th>
<th>Priority / Priorité</th>
<th>Deadline / Délai</th>
<th>Comments / Commentaires</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Please find attached a BN requesting the Director's authorization to request a waiver to the pension reduction for two employees who are affected by the recent workforce adjustment.

Attached: a form providing the necessary information. The average, in recent years, the reduction for each employee is 3% on their financial record. For each employee, this is an improvement in the cost of the PS and I fully support the request.

DG HR/D
Director/Dir

CSIS / SCRS
FEB 1 2015
20507

Please process ASAP

DG HR/D
1/3/117
TO: Director, via ADH

FROM: DG HRS

BRIEFING NOTE

SUBJECT: WORKFORCE ADJUSTMENT (WFA)- PENSION REDUCTION WAIVER REQUEST FORM

BACKGROUND:
As a result of the Workforce Adjustment in the employees listed below, a request can be made to allow the employee to draw a full pension without penalty as long as they meet the eligibility criteria of being between the ages of 55 and 59, with at least 10 years of service. Employees listed below meet the eligibility criteria and have not received an educational allowance or a reasonable job offer. The Pension Reduction Waiver Request must be signed by the Deputy Head, and sent to the Pension Center for processing.

RECOMMENDATION:
The Director sign the Waiver forms (attached) for the following two employees affected by the recent workforce adjustment action in

PREPARED BY:
Chef, Pay Section

Att.
cc. ADC
This application is being processed in accordance with the Public Service
Superannuation Act (PSA) for the purpose of certifying that the employee listed above
is entitled to a reduction in their pension for the reasons indicated on this
application. This information will be filed in a personal information file pursuant to
Privacy Act, R.S.C. 1985, c. P-5. This application must be supported by evidence in
collection under the Privacy Act (s. 7 of the PSA). If the application is incomplete
or incorrect, it will be returned to the applicant.

Employee’s Service and Given Names - Name of person employed

The above-named individual was at least 55 at termination and has
been employed in the public service for at least 10 years. I certify that the
individual concerned has met the requirements for a waiver of the reduction
in his pension as indicated below:

1. An employee to whom the Work Force Adjustment Directive (WFAD) or the
Work Force Adjustment Appendix (WFAA) applies and who:
   a. has not received a reasonable job offer under the WFAD or the WFAA and who
is, or is entitled to receive, a reasonable job offer during the period of reduction
in annuity
   b. is not entitled to receive a reasonable job offer under the WFAD or the WFAA and who
remains in the public service;
   c. an employee whose severance pay will be paid for at least one year if he
must be paid a reasonable job offer under the WFAD or the WFAA and who
remains in the public service;
   d. an employee whose annuity is no longer required by reason of a
transfer or layoff during the period of reduction in annuity
2. An employee who has been declared surplus, who has not received an
officer of the public service and who is not
   a. an employee who is not entitled to receive a reasonable job offer under the WFAD or the WFAA and who
remains in the public service;
   b. an employee whose severance pay will be paid for at least one year if he
must be paid a reasonable job offer under the WFAD or the WFAA and who
remains in the public service;
   c. an employee whose annuity is no longer required by reason of a
transfer or layoff during the period of reduction in annuity
3. A departmental or an employee to whom the Public Service
Superannuation Act (PSA) applies and who
   a. has not received a reasonable job offer under the WFAD or the WFAA and who
is, or is entitled to receive, a reasonable job offer during the period of reduction
in annuity
   b. is not entitled to receive a reasonable job offer under the WFAD or the WFAA and who
remains in the public service;
   c. an employee whose severance pay will be paid for at least one year if he
must be paid a reasonable job offer under the WFAD or the WFAA and who
remains in the public service;
   d. an employee whose annuity is no longer required by reason of a
transfer or layoff during the period of reduction in annuity
4. A term employee whose term has ended and who will have
   a. an employee who is not entitled to receive a reasonable job offer under the public service
was, or is entitled to receive, a reasonable job offer during the period of reduction
in annuity
   b. an employee whose severance pay will be paid for at least one year if he
must be paid a reasonable job offer under the public service
was, or is entitled to receive, a reasonable job offer during the period of reduction
in annuity
   c. an employee whose annuity is no longer required by reason of a
transfer or layoff during the period of reduction in annuity

Further certifies that this employee has not received an
educational allowance under the PSA, or a
pre-retirement allowance job offer,

Signature of Deputy Head or Designated Authority

Signature of administrative employee by date

Contact Person - Person in charge

Telephone no. - No. of telephone

Signature of Employment Canada

Title - Title of person

Department - Department

CSIS

FaceMix - No. of telephone

PWGS-183-PC 2123.128975

PENSION REDUCTION WAIVER REQUEST

DEMANDE D'EXONERATION DE LA REDUCTION A UNE PENSION

La personne concernée était âgée de moins de 55 ans à la fin de son
emploi et a été à l'emploi de la fonction publique depuis au moins 10 ans.
Je certifie que la personne concernée a respecté les exigences qui sont
indiquées ci-dessous, qui lui donnent droit à une exonération de la
réduction de sa pension.

1. Un employé visé par la Directive sur la restructuration des effectifs (DRE)
ou l'Arrêté sur le rapprochement des effectifs (ARE) et qui
a:
   a. reçu un offre d'emploi raisonnable sous la DRE ou l'ARE et qui a été
accepté ou un offert d'emploi raisonnable sous la DRE ou l'ARE et qui a été
accepté ou un offre d'emploi raisonnable sous la DRE ou l'ARE et qui a été
accepté;
   b. qui a reçu une offre d'emploi raisonnable sous la DRE ou l'ARE et qui a été
accepté;
   c. qui a reçu une offre d'emploi raisonnable sous la DRE ou l'ARE et qui a été
accepté;
   d. qui a reçu une offre d'emploi raisonnable sous la DRE ou l'ARE et qui a été
accepté;
2. Un employé dont l'offre d'emploi raisonnable sous la DRE ou l'ARE a été
acceptée et qui a reçu une offre d'emploi raisonnable sous la DRE ou l'ARE et qui a été
acceptée;
3. Un employé dont l'offre d'emploi raisonnable sous la DRE ou l'ARE a été
acceptée et qui a reçu une offre d'emploi raisonnable sous la DRE ou l'ARE et qui a été
acceptée;
4. Un empl.

PENSION REDUCTION WAIVER REQUEST

DEMANDE D'EXONÉRATION DE LA RÉDUCTION À UNE PENSION

This information is being collected in accordance with the Public Service Superannuation Act (PSSA) for the purpose of determining if the employee meets the requirements for a waiver of the reduction in his pension, when a reduction results. This information will be stored in Personal Information Bank number PSSPC PC 702. It is protected from disclosure to unauthorized persons in accordance with the provisions of the Privacy Act. Under the Act you have the right to request access to your personal information held by a federal government institution and, upon request, corrections should be made. This information cannot be used for any purpose other than the one for which it was collected. Personal information should be accurate to the extent known to the person under the Privacy Act.

Employees Surname and Given Names - Nom et prénoms de l'employé

The above-named individual will at least 55 at termination and has been employed in the public service for at least 10 years. I certify that the individual concerned has met the requirements for a waiver of the reduction in his pension as indicated below:

1. An employee with the transition adjustment directive (TAD) or the transition adjustment appendix (TAA) who is:
   a. a surplus employee who has not received a guarantee of a reasonable job offer under the TAD or the TAA and who is laid-off, or in other circumstances, is paid a payment representing payment at a level of surplus employees;
   b. an employee whose services will no longer be required because of a work force adjustment situation, who has not received a guarantee of a reasonable job offer and who is in transition adjustment in accordance with the TAD or the TAA and who is no longer employed by the public service;
   c. an employee whose services are no longer required because of a layoff, who has not received a reasonable job offer and who is in transition adjustment in accordance with the TAD or the TAA and who is no longer employed by the public service;
   d. an employee affected by relocation of a work unit and who has not received a reasonable job offer and who is in transition adjustment in accordance with the TAD or the TAA and who is no longer employed by the public service;
   e. an employee whose services are no longer required because of a transfer or relocation to another position, and who has not received a reasonable job offer and who is in transition adjustment in accordance with the TAD or the TAA and who is no longer employed by the public service;
   f. an employee who has been declared surplus, who has not received an offer of alternative employment in the public service and does not receive a negotiated settlement that includes compensation for a reduction in the amount of benefits payable under the public service pension plan and who is otherwise employed;
   g. a Governor-in-Council appointment whose position is abolished and who may receive a negotiated settlement that includes compensation for a reduction in the amount of benefits payable under the public service pension plan;
   h. a terminated employee whose term has ended and who is immediately eligible for a reduction in his pension.

I further certify that this employee has not received an educational allowance, work not in receipt of a reasonable job offer or other guaranteed reasonable job offer.

Signature of Deputy Head or Delegated Authority

Prix et - Tissus

Directeur

Département - Ministère

CSIS

Contact Pension - Personne-ressource

Téléphone no. - N° de téléphone

Pension no. - N° de télécopieur
MEMORANDUM TO THE DIRECTOR

MINISTERIAL BRIEFING ON BILL C-44
23 February 2015, 10:50 - 11:15
Minister's Board Room, 269 Laurier

• You have been invited to attend a Ministerial Briefing to discuss Bill C-44 in advance of the upcoming appearance before the Senate National Security and Defence Committee (SECD) on or after 2015 03 09. Along with the DM of Public Safety, you will support the Minister for the first hour of the appearance and then remain to answer questions for the second hour.
• Key messages remain the same for C-44, although new language has been developed to address communication issues arising from the introduction of C-51.

BACKGROUND:

Bill C-44 has received third and final reading in the House of Commons and was sent to the Senate where it was introduced at first reading on 2015 02 03. It is expected to be sent shortly to SECD for review. It is expected that SECD will consider the bill at several committee hearings before the full Senate will consider the bill a third and final time. After this, the bill, if voted on and approved, would be sent to the Governor General for Royal Assent;

DISCUSSION:
Of note, you have a bilateral meeting with the Minister on 25 February at which you have the opportunity to further discuss/clarify issues arising out of this meeting.

**KEY MESSAGES ON C-44**

- These amendments bring the legal certainty required for us to effectively fulfill our mandate.
- The world reminds us on a daily basis the extent to which our national security is inextricably linked to events and persons abroad.
- To ensure the safety and security of Canadians, we must be able to investigate and advise on threats to the security of Canada and Canadians, whether they originate at home or abroad.
- This legislation provides the express legal authority for CSIS to do so.
- Source and employee identity protection is vital for reasons of personal safety and to maintain CSIS’ operational effectiveness.
- These dedicated individuals need to feel confident in the protection offered, which requires a strong and clear basis in law.
- Recent Court decisions created significant uncertainty for certain of CSIS’ investigative activities and necessitated an urgent legislative response.
- Nothing in Bill C-44 alters CSIS’ mandate, duties or functions. Rather, these amendments put our investigations and authority to seek a warrant for activities in Canada and abroad on a clear footing.
- Nothing in C-44 or C-51 changes the threats CSIS is authorized to investigate.
- CSIS will continue to investigate the threats it was charged with 30 years ago – including terrorism, espionage, and foreign interference. Nothing in either of these bills would change that.

As always, please do not hesitate to contact me should you require further information.

__________________________
Tom Venner
Assistant Director Policy and Strategic Partnership

**Enclosures:**
- Tab I: Agenda
- SECD Briefing Binder

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.
| TAB 1 | Bill C-44: The Protection of Canadians from Terrorism Act |
| TAB 2 | Minister's Opening Remarks and Key Issue Cards |
| TAB 3 | Media Scan of CSIS and Bill C-44 |
| TAB 4 | Highlights of C-44 Debate in the House of Commons |
| TAB 5 | Highlights of Question Period |
| TAB 6 | Highlights and Transcript of Minister and Director's Appearance before SECU, 24 November 2014 |
| TAB 7 | Highlights, Summary, and Transcript of Academics' Appearance before SECU, 26 November 2014 |
| TAB 8 | Transcript of ADP Appearance before SECD, 17 November 2014 |
| TAB 9 | Transcript of ADP Appearance before SECD, 27 October 2014 |
| TAB 10 | Highlights and Transcript of DDO Appearance before SECD, 20 October 2014 |
| TAB 11 | Highlights of DIR Appearance before SECU, 8 October 2014 |
| TAB 12 | SECD Membership |
BILL C-44

An Act to amend the Canadian Security Intelligence Service Act and other Acts

HOUSE OF COMMONS OF CANADA

C-44

Second Session, forty-first Parliament.
62-63 Elizabeth II, 2013-2014

MINISTER OF PUBLIC SAFETY AND EMERGENCY PREPAREDNESS

C-44

CHAMBRE DES COMMUNES DU CANADA

PROJET DE LOI C-44

Lui modifiant la Loi sur le Service canadien du renseignement de sécurité et d'autres lois

MINISTRE DE LA SÉCURITÉ PUBLIQUE ET DE LA PROTECTION CIVILE
SUMMARY

This enactment amends the Canadian Security Intelligence Service Act to give greater protection to the Canadian Security Intelligence Service's human sources. Also, so as to enable the Service to more efficiently investigate threats to the security of Canada, the enactment clarifies the scope of the Service’s mandate and confirms the jurisdiction of the Federal Court to hear warrants that have been issued outside Canada. In addition, it makes a consequential amendment to the Access to Information Act.

The enactment also amends the Canadian Citizenship Act to allow for the coming into force of provisions relating to the revocation of Canadian citizenship on a different day than the day on which certain other provisions of that Act come into force.


Le texte modifie également la Loi concernant la citoyenneté canadienne afin de permettre que le jour d’entrée en vigueur des dispositions portant sur la révocation de la citoyenneté canadienne soit distinct de celui d’autres dispositions de cette loi.

Available on the Parliament of Canada Web Site at the following address:

http://www.parl.gc.ca

Disponible sur le site Web du Parlement du Canada à l’adresse suivante :

http://www.parl.gc.ca

HOUSE OF COMMONS OF CANADA

BILL C-44

An Act to amend the Canadian Security Intelligence Service Act and other Acts

Her Majesty, by and with the advice and consent of the Senate and House of Commons of Canada, enacts as follows:

SHORT TITLE

1. This Act may be cited as the Protection of Canada from Terrorists Act:

CANADIAN SECURITY INTELLIGENCE SERVICE ACT

2. Section 1 of the Canadian Security Intelligence Service Act is amended by adding the following in alphabetical order:

"human source" means an individual who, having received a promise of confidentiality, has provided, or is likely to provide, information to the Service;

3. Section 12 of the Act is renumbered as subsection 12(1) and is amended by adding the following:

(2) For greater certainty, the Service may perform its duties and functions under subsection (1) within or outside Canada.

4. Section 15 of the Act is renumbered as subsection 15(1) and is amended by adding the following:

(2) For greater certainty, the Service may conduct the investigations referred to in subsection (1) within or outside Canada.
5. (1) Paragraph 16(1)(b) of the French version of the Act is replaced by the following:

b) d'une personne qui n'appartient à aucune des catégories suivantes:

5. (1) L'article 16(1)b) de la version française de la même loi est remplacé par ce qui suit:

b) d'une personne qui n'appartient à aucune des catégories suivantes:

6. Subsection 18(1) of the Act is replaced by the following:

6. Le paragraphe 18(1) de la même loi est remplacé par ce qui suit:

18. (1) Subject to subsection (2), no person shall knowingly disclose any information that they obtained or to which they had access in the course of the performance of their duties and functions under this Act or their participation in the administration or enforcement of this Act and from which could be inferred the identity of an employee who was, is or is likely to become engaged in covert operational activities of the Service or the identity of a person who was an employee engaged in such activities.

18. (1) Sous réserve du paragraphe (2), nul ne peut secon centement communiquer des informations qu'il a acquises ou auxquelles il avait accès dans l'exercice de leurs fonctions qui les ont rendues, de confidences, de la présente loi ou lors de sa participation à l'exécution ou au contrôle d'application de cette loi et qui permettraient de découvrir l'identité d'un employé qui a participé, participe ou pourrait participer à des activités opérationnelles coûteuses du Service ou l'identité d'une personne qui était un employé et qui a participé à de telles activités.

7. The Act is amended by adding the following after section 18:

7. La même loi est modifiée par adjonction, après l'article 18, de ce qui suit:

18.1 (1) The purpose of this section is to ensure that the identity of human sources is kept confidential in order to protect their life and security and to encourage individuals to provide information to the Service.

18.1 (1) Le présent article vise à préserver l'anonymat des sources humaines afin de protéger leur vie et leur sécurité et d'encourager les personnes physiques à fournir des informations au Service.

(2) Subject to subsections (3) and (8), no person, shall, in a proceeding before a court, person of body with jurisdiction to compel the production of information, disclose the identity of a human source or any information from which the identity of a human source could be inferred.

(2) Sous réserve des paragraphes (3) et (8), nul ne peut, dans une instance devant un tribunal, un organisme ou une personne qui ont le pouvoir de contraindre à la production d'informations, révéler l'identité d'une source humaine ou toute information qui permettrait de découvrir cette identité.
La partie à une instance visée au paragraphe (2), l'uniras en iea nomme dans cette instance eu l'avocat spécial nommé sous le régime de la Loi sur l'immigration a lu protection de'srrjugrev demander a tin 10 tige de décimer, par onlonunoe. si une lelle delararion eti pCrrinoue dans l'insrancc:

a) qu'une personne physique n'est pas une ounee humaine ou qu'une infummititm ne permettrait plis de décusi rit l'identité d'une 15 gourcs 'humaine; Iss dans le cas où l'instance eel une poursuite peitr infreclion, que la alanmünicalion de t'identitC d'une source humaine ou d'une information qui pain vrai t do &couvrir adné 20 identity est essentielle pour i ]iaitilir l'iono-

(3) The identity of a human source or a human source information from which the identity of a human source could be inferred may be discussed in a proceeding referred to in subsection (2) if the proceeding is under the Immigration and Refugee Protection Act and the director consents in the disclosure of that information.

(4) A party to a proceeding referred to in subsection (2), an amicus curiae who is appointed by order of the judge for the purpose of acting as a special advocate if the proceeding is under the Immigration and Refugee Protection Act may apply to a judge for one of the following orders if it is relevant to the proceeding:

(a) an order declaring that an individual is not a human source or that information is not information from which the identity of a human source could be inferred, or

(b) if the proceeding is a prosecution of an offence, an order declaring that the disclosure of the information would be necessary to establish the accused's innocence and that it may be disclosed in the proceeding:

(3) L'identité d'une source humaine ou une information qui permettrait de découvrir l'identité peut être communiquée dans une instance visée au paragraphe (2) si la source humaine ou le directeur y consentent.

(4) A la partie à une instance visée au paragraphe (2), l'amicae curiae nommé dans cette instance ou l'avocat spécial nommé sous le régime de la Loi sur l'immigration ou la protection des réfugiés peut demander à un juge de déclarer, par ordonnance, si une telle déclaration est pertinente dans l'instance:

a) qu'une personne physique n'est pas une source humaine ou qu'une information ne permettrait pas de découvrir l'identité d'une source humaine;

b) dans le cas où l'instance est une poursuite pour infraction, que la communication de l'identité d'une source humaine ou d'une information qui permettrait de découvrir cette identité est essentielle pour établir l'innocence de l'accusé et que cette communication peut être faite dans la procédure;

(5) La demande et l'affidavit déposant les faits sur lesquels il fonde cette 25 demande seront déposés au greffe de la Cour fédérale. Sans délai après le dépôt, le demandeur signifie copie de la demande et de l'affidavit au procureur général du Canada.

(6) Le procureur général du Canada est réputé être partie à la demande dès que celui-ci lui est signifié.

(7) La demande est entendue à huis clos et en l'absence du demandeur et de son avocat, sauf si le juge en ordonne autrement.

(8) Si le juge accorde la demande présentée au titre de l'alinéa 44.1, il peut ordonner la communication qu'il estime indiquée sous réserve des conditions qu'il précise.

(9) Si la demande présentée au titre du 40(e) est accueillie, l'ordonnance prend effet après l'expiration du délai prévu.
Protection of Canada from Terrorism

6. (1) Subsection 21(1) of the Act is replaced by the following:

21. (1) If the Director or any employee designated by the Minister for the purpose believes, on reasonable grounds, that a warrant under this section is required to enable the Service to investigate, within or outside Canada, a threat to the security of Canada or to permit the Director or employee to, after having obtained the Minister’s approval, make an application in accordance with subsection (2) to a judge for a warrant under this section.

(2) Section 21 of the Act is amended by adding the following after subsection (3):

(3.1) Without regard to any other law, including that of any foreign state, a judge may, in a warrant issued under subsection (3), authorize activities outside Canada to enable the Service to investigate a threat to the security of Canada.

9. The portion of subsection 39(2) of the Act before paragraph (a) is replaced by the following:

4. (1) The judge shall ensure the confidentiality of the following:

(a) the identity of any human source and any information from which the identity of a human source could be inferred; and
(b) information and other evidence provided in respect of the application if, in the judge’s opinion, its disclosure would be injurious to national security or endanger the safety of any person.

5. (1) The portion of paragraph (a) is replaced by the following:

The judge shall ensure the confidentiali

(1) If the order is appealed and is confirmed, until either the time provided to apply for a review of the order has expired or all review rights have been exhausted.

Confidentialité

Confidentiality

Confidentialité

Confidentiality

Confidentialité

Confidentiality

Confidentiality

Confidentialité

Confidentiality

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialité

Confidentialità
(2) Despite subsection 18.1(2), any other Act of Parliament or any privilege under the law of evidence, but subject to subsection (3), the Review Committee is entitled to have any other information of Parliament or any privilege under the law of evidence, subject to reserve of the paragraph (3), the committee of surveillance;

STRENGTHENING CANADIAN CITIZENSHIP ACT

10. Subsection 24(5) of the Strengthening Canadian Citizenship Act is replaced by the following:

(5) Paragraphs 27(7) to (f) of the Act are replaced by the following:

(r) providing for the number of copies of any 10 declarative, certificate, or other document made, issued or provided under this Act or prior legislation that any person is entitled to have;

(s) respecting the provision under paragraph 12(1)(h) or (2)(h) of a means of establishing citizenship other than a certificate of citizenship;

(t) providing for the surrender and retention of certificates, citizenship, certificates of naturalization and certificates of renunciation issued or granted under this Act or prior legislation and of documents provided under paragraph 12(1)(h) or (2)(h) if there is reason to believe that their holder may not be entitled to have them or has contravened any of the provisions of this Act;

(u) providing for the renunciation of citizenship by persons

(i) who are citizens under paragraph 30(1)(g) or (i),

(ii) who are citizens under any of paragraphs 30(1)(h) to (r) and who did not, before the coming into force of this subparagraph, become citizens by way of grant or deemed in subsection 30(9), or

(iii) who are citizens under paragraph 30(1)(h) for the sole reason that one or both parents are persons referred to in any of paragraphs 30(1)(h) to (r) and who did not, before the coming into force of this subparagraph, become citizens by way of grant or deemed in subsection 30(9),

(3) Malgré le paragraphe 18.1(2), toute autre loi fédérale ou toute immunité reconnaissable par le droit de la preuve, mais sous réserve du paragraphe (3), le comité de surveillance;

LOI RENFORÇANT LA CITIZENNETÉ CANADIENNE

10. Le paragraphe 24(5) de la Loi renforçant la citoyenneté canadienne est remplacé par ce qui suit:

(5) Les alinéas 27(7) à (f) de la même loi sont remplacés par ce qui suit:

(i) à préciser le nombre de copies de déclarations, certificats ou autres documents accessibles, délivrés ou fournis en vertu de la présente loi ou de la législation antérieure qui une personne a le droit d'avoir;

(ii) régir la fourniture, en application des alinéas 12(1)(h) et (2)(h), des moyens de prouver la qualité de citoyen autres que les certificats de citoyenneté;

(iii) régir la restitution et la rétention des certificats de citoyenneté, de naturalisation, de renunciation ou de répudiation délivrés ou fournis en vertu de la présente loi ou de la législation antérieure ou des documents fournis en application des alinéas 12(1)(h) et (2)(h), l'incident que leur titulaire n'a pas 25 ans à leur date d'émission ou a enfreint la présente loi;

(iv) régir la répudiation de la citoyenneté de quiconque:

(i) a qualité de citoyen au titre des alinéas 3(1)(f) ou (g),

(ii) a qualité de citoyen au titre des alinéas 3(1)(h) à (r) et n'a pas obtenu, avant l'entrée en vigueur du présent sous-alinéa, la citoyenneté par attribution au sens du paragraphe 3(9),

(iii) a qualité de citoyen en vertu de l'alinéa 3(1)(h) pour la seule raison que son père ou sa mère ou ses deux parents sont visés à l'un des alinéas 3(1)(h) à (r) et n'a pas obtenu, avant l'entrée en vigueur 40 du présent sous-alinéa, la citoyenneté par attribution au sens du paragraphe 3(9);
(5.1) Section 27 of the Act is amended by adding the following after paragraph (j.1): 15

(j.2) prescribing the factors that the Minister shall consider in forming an opinion as to whether a hearing is required under subsection 10(4); 5

(5.2) Paragraph 27(1) of the Act is replaced by the following: 5

(k.1) providing for the surrender and cancellation of certificates and documents referred to in paragraph (i) if their holder is not entitled to them; 10

(k.2) providing for the collection, retention, use, disclosure and disposal of information for the purposes of this Act; 15

(k.3) providing for the disclosure of information for the purposes of national security, the defence of Canada or the conduct of international affairs, including the implementation of an agreement or arrangement entered into under section 5 of the Department of Citizenship and Immigration Act; 20

(k.4) providing for the disclosure of information to verify the citizenship status or identity of any person for the purposes of administration of any federal or provincial law or law of another country; 25

(k.5) providing for the disclosure of information for the purposes of cooperation within the Government of Canada and between the 30

Government of Canada and the government of a province; 30

(k.6) respecting the disclosure of information relating to the professional or ethical conduct of a person referred to in any of paragraphs 21.1(1)(a) to (c) in connection with a proceeding — other than a proceeding before a superior court — or application under this Act to a body that is responsible for governing or investigating that conduct, for the purposes of ensuring that persons referred to in those paragraphs offer and provide professional and ethical 35

(5.1) L'article 27 de la même loi est modifié par adjonction, après l'alinéa (j.7), de ce qui suit: 7

(j.2) établir les facteurs dont le ministre doit tenir compte pour former sa décision quant à la nécessité de la tenue d'une audience visée au paragraphe 10(4); 5

(5.2) L'alinéa 27(1) de la même loi est remplacé par ce qui suit: 5

(k.1) prévoir la collecte, la conservation, l'utilisation, la communication et la destruction de renseignements pour l'application de la présente loi; 15

(k.2) prévoir la communication de renseignements aux fins de sécurité nationale, de défense du Canada, de conduite des affaires internationales, y compris la mise en œuvre d'accords ou d'engagements conclus au titre de l'article 5 de la Loi sur le ministère de la Citoyenneté et de l'Immigration. 20

(k.3) prévoir la communication de renseignements aux fins de vérification du statut de citoyenneté et de l'identité d'une personne dans le cadre de l'administration de toute loi fédérale, provinciale ou étrangère; 25

(k.4) prévoir la communication de renseignements aux fins de coopération au sein de l'administration publique fédérale et entre l'administration publique fédérale et celle d'une province; 30

(k.5) régir la communication de renseignements relatifs à la conduite, sur le plan professionnel ou de l'éthique, d'une personne visée à l'un des alinéas 21.1(2)(a) à (c) relativement à une demande ou à une instance prévue par la présente loi — à l'exception de l'une des instances devant une cour supérieure — à l'organisme qui régir la conduite de cette personne ou à l'organisme ou à la personne qui enquête sur cet élément conduite, et ce en vue de veiller à ce que la personne visée à l'un ou à 45

l'autre de ces alinéas représente ou conseille des personnes, ou offre de le faire, en
CONSEQUENTIAL AMENDMENT TO THE ACCESS TO INFORMATION ACT

13. Schedule II to the Access to Information Act is amended by replacing the reference to "section 18" opposite the reference to "Canadian Security Intelligence Service Act" with a reference to "sections 18 and 18.1".

MODIFICATION CORRÉLATIVE À LA LOI SUR L'ACCÈS À L'INFORMATION

13. L'annexe II de la Loi sur l'accès à l'information est modifiée par remplacement de la mention «article 18», figurant en regard de la mention «Loi sur le Service canadien du renseignement de sécurité», par les articles 18 et 18.1.
Anti-Terror Legislation—News Coverage

Meet the professors behind the swift assault on C-51

Maclean's Magazine, John Geddes, 2015 03 04

Prime Minister Stephen Harper must wonder what hit him. When Harper announced Bill C-51, known at the Anti-Terrorism Act, at a campaign-style event in Richmond Hill, Ont., on Jan. 30, he might reasonably have judged that his government's response to what he called "violent jihadism" was a sure political winner. After all, polls show his Conservatives enjoy a solid edge over the New Democrats and Liberals on the fighting-terrorism file. On the policy details, the experts in security law at his disposal inside the federal public service easily outgun anyone in the opposition parties' research bureaus. What the Conservatives didn't figure into their calculations, however, was the scheduling of academic sabbaticals.

It happens that both the University of Toronto's Kent Roach and the University of Ottawa's Craig Forcese—arguably the country's two top law professors when it comes to national security—are both on breaks from their usual teaching duties. That gave Roach and Forcese ample time to join forces and mount a swift assault on C-51 unlike anything seen in a federal policy debate in recent memory. They set up a
website, under the stolid banner "Canada's Antiterrorism Act: An Assessment," on which they have posted a series of devastatingly comprehensive critiques of the bill—taking everything from how it would chill free speech, to how it would undermine privacy, to how it would undermine the independent position of authorizing Charter of Rights and Freedoms violations by Canada's spy agency. Roach, 53, has been studying the Canadian Security Intelligence Service from the time it was born—ever a bit before. As an undergraduate political science student at the University of Toronto in the early 1960s, he came under the thrill of Prof. Peter Russell, who had been director of research for the landmark McDonald Commission on the RCMP. It was the McDonald Commission's recommendation that a civilian national security agency be split off from the Mounties that led to the creation of CSIS in 1984: the year Roach handed in his undergraduate thesis on the brand-new intelligence service.

Grand Chief Phillip, Palmater invited to testify on anti-terror bill before committees of MPs

Ottawa - The House of Commons committee studying the Harper government's anti-terror bill has invited Stewart Philip and Pam Palmater to appear as witnesses, according to a list obtained by APTN National News. Philip, president of the Union of British Columbia Indian Chiefs, and Palmater, a Mikmaq professor and lawyer, are on a list of about 70 potential witnesses who have been asked to appear before the Commons public safety committee. The committee is studying Bill C-51, the Harper government's proposed anti-terror bill that would give more powers to agencies like the Canadian Security Intelligence Service (CSIS), the RCMP and Canada Border Services Agency (CBSA). The Assembly of First Nations drafted an analysis of the proposed bill which concluded the proposed law could lead to the labeling of Indigenous activists as "terrorists."

Former PMs not on C-51 witness list

Globe and Mail, Daniel Leblanc, 2015 03 04

Ottawa - A parliamentary committee will hear from strong supporters and vocal critics of the government's anti-terrorism bill, but not from four former prime ministers who have denied the lack of increased oversight in the legislation. Bill C-51 would beef up the powers of the Canadian Security Intelligence Service (CSIS), criminalize the promotion of terrorism and provide the RCMP with new powers of preventative arrest. But critics charge it goes too far and risks ensnaring environmentalists and First Nations in the fight against terrorism. The public safety committee of the House will hear from 50 witnesses between March 9 and March 31 as part of its study of the bill, starting with Public Safety Minister Steven Blaney and Justice Minister Peter MacKay. The 48 remaining slots will be filled from a list of 70 potential witnesses, based on their availability. According to the list obtained by The Globe and Mail, witnesses will come from a wide range of society, including government, academia, law enforcement and various non-governmental organizations. For example, the committee could hear from former public safety ministers (Liberal Anne McLellan and Conservative Stockwell Day), current and past members of the House public safety committee, current and past privacy commissioners, and retired judges John Major and Louise Arbour. The list of potential witnesses includes fierce critics of C-51, namely Maher Arar, who was tortured in Syria after being flagged as a security risk in Canada, and law professors Kent Roach and Craig Forcese. NDP MP Randall Garrison said he concerned the committee will only have two hours with Mr. Blaney, Mr. MacKay and their officials, including RCMP Commissioner Bob Paulson and CSIS director Michel Coulombe.

Witness list long on anti-terror law

Toronto Star, Alex Boutilier, 2015 03 04

Ottawa - The House of Commons committee studying the Conservatives' controversial new anti-terrorism law is expected to call retired spies, former politicians and some of Bill C-51's harshest critics to testify. A draft witness list obtained by the Star shows the committee will invite about 76 people to fill the 48 speaking slots on the bill. The list includes former Supreme Court justices, lawyers and academics, as well as retired police and security officials, both active and retired, who are also expected to appear to discuss the legislation. High-ranking officials from some of Canada's closest security partners will also be invited to testify. But the list does not include four former prime ministers - John Turner, Joe Clark, Jean Chrétien and Paul Martin - who have been publicly critical of the bill. The New Democrats hoped to call the four to testify before the committee. According to the committee's list, other potential witnesses include: Maher Arar, whose rendition and torture in Syria led to a federal inquiry into Canada's security agencies' co-operation with American spies. Justice Dennis O'Connor, the former associate chief justice of Ontario who led the Arar inquiry. Chuck Strahl and Deborah Grey, the former and current head of CSIS's review committee, respectively, and former Conservative politicians. U.S. Department of Homeland Security Secretary Jeh Johnson, Craig Forcese and Kent Roach, two academics who have raised serious concerns about Bill C-51; Louise Arbour, a retired Supreme Court justice. Anne McLellan, a former Liberal cabinet minister who oversaw the implementation of Canada's 2001 anti-terrorism regime.

Ottawa didn't learn Air India lesson, says ex-judge

Globe and Mail, Sean Fine, 2015 03 02

The former Supreme Court judge who headed an inquiry into Canada's worst terrorism incident says the federal government's new anti-terrorism legislation is flawed because it fails to ensure that CSIS and the RCMP share information on unfolding threats. John Major says the crucial lack of cooperation between the two agencies that occurred before the 1985 Air India explosion is still a concern and that a security overseer is needed to ensure information-sharing takes place. In his 2010 report into the disaster, he said a national security adviser with enhanced powers should be appointed to settle disputes and ensure intelligence is shared between the Canadian Security Intelligence Service, the RCMP and 14 other security agencies and departments. The Conservative government rejected that recommendation at the time. "They may be entitled to do more than simple intelligence gathering," he said of CSIS under the
proposed new law, "if that's the case, it can lead to other problems of overlap. The RCMP get a little annoyed and think, 'Well, let CSIS do it.' And CSIS doesn't do it. When you have it, you're usually involved, it's a recipe for confusion unless there's somebody steering the ship.' A spokesman for Public Safety Minister Steven Blaney, however, said greater information-sharing is a pillar of the proposed law. "This Act fulfills the government's commitment to introduce information-sharing legislation as part of the Air India Inquiry Action Plan," JeanChristophe de Le Rue said. But Mr. Major said he saw nothing in the bill that gives a national security adviser the authority necessary to ensure the information is actually shared.

Le SCR a peu de pouvoir pour arrêter le recrutement de terroristes, selon des experts
Radio Canada Nouvelles. 2015 02 26
Ottawa - Le Service canadien du renseignement de sécurité (SCR) dispose de peu de marge de manœuvre dans son mandat actuel pour prévenir le recrutement par des groupes radicaux tels que le groupe armé État islamique, selon des experts en sécurité. «Ce n'est pas illégal de quitter le pays», soutient le professeur à l'Université MacEwan d'Edmonton Jean-Christophe Boucher. «Ce n'est pas illégal de payer le billet d'avion de quelqu'un d'autre. Ce n'est pas illégal, à certaines conditions, de convaincre quelqu'un de partir à l'étranger», fait-il valoir. Cette semaine, Radio-Canada a révélé plusieurs cas de jeunes femmes qui ont quitté le pays pour rejoindre les rangs du groupe armé État islamique (EI). Dans l'une de ces révélations, une femme d'Edmonton s'est dite furieuse que sa sœur, qui était surveillée par le SCR, ait pu quitter le pays l'été dernier pour rallier l'EI. «Je ne comprends pas pourquoi ils ne l'ont pas arrêtée à l'aéroport de Toronto. Elle a même répondu à une conversation qu'elle avait suivie tout au long de son voyage», elle a affirmé.

Rules spat puts hearings on anti-terror bill up in air
Ottawa Citizen, Ian MacLeod. 2015 02 28
Ottawa - The slant of public hearings on the government's anti-terror bill is in question after the NDP complained Friday that Conservatives broke parliamentary rules during a committee vote on the bill. NDP House Leader Peter Julian formally asked deputy House of Commons speaker Joe Comartin to void a Thursday vote by the Commons' public safety committee. Comartin said House Speaker Andrew Scheer would respond "as quickly as possible." With Parliament now on a weeklong break, Scheer's response isn't expected until Monday, March 9. Public hearings on Bill C-51 were to start the following day and continue through March 11. The contentious committee vote came just before 5 p.m. Thursday, after more than seven hours of bickering between government and NDP MPs on the timing of hearings to listen to expert witnesses on the anti-terror legislation. The proposed legislation gives CSIS, Canada's top spy agency, the ability to conduct "no-fly list" powers, crack down on terrorist propaganda and remove barriers to sharing security-related information.

Canadian anti-terror bill opens door for human rights abuses, law scholars argue
The Guardian.co.uk, John Barber. 2015 02 28
Toronto - More than 100 Canadian law professors have warned the prime minister, Stephen Harper, that a sweeping new anti-terror law introduced by his Conservative government is a "dangerous piece of legislation" that threatens to undermine the rule of law, human rights and democracy itself. Although one poll showed that four out of five Canadians supported the proposed law shortly after it was tabled last month, criticisms that originated with scattered human-rights groups have since been amplified by a growing chorus of the nation's leading jurists, academics, editorial-writers and opinion-makers. Bill C-51 significantly loosens current restrictions on police and spies seeking to disrupt terrorist activity. But critics claim that it also opens the way for the Canadian Security and Intelligence Service (CSIS) to target legitimate dissent, making criminals of environmentalists, native people and other protesters hostile to the government.

'People are afraid' Health minister switches to terrorism during health speech
Canadian Press, Bill Gravesland. 2015 02 25
Calgary - Federal Health Minister Rona Ambrose made an unexpected leap Friday from talking about health-care innovation to fears over the threat of the Islamic State. Ambrose was discussing health care in a speech to the Calgary Chamber of Commerce when she abruptly changed topics. We're also proud of our record of making careful, principled choices reflecting the values of Canadians whether it's economic and financial security or creating and protecting jobs but also keeping Canada and Canadians safe in a dangerous and uncertain world, Ambrose said. We know it's on a lot of people's minds and the truth is we are again at war with a very dangerous enemy. ISIL's campaign of what is unspeakable atrocities, whether it's beheadings or rape or slavery on the most innocent of people including women and children. Her comments come as Ottawa pushes ahead with Bill C-51, which seeks to increase the powers of police and spy agencies in the name of fighting terrorism. Ambrose lauded actions the Conservative government took, including changes to the Citizenship Act as well as the new anti-terrorism bill. The bill would give CSIS the ability to disrupt terror plots. It makes it easier to limit the movements of a suspect, expand no-fly list powers, crack down on terrorist propaganda, and remove barriers to sharing security-related information.

Tories use majority to limit study of terror bill to eight days
Toronto Star, Alex Boutilier. 2015 02 27
Ottawa - Conservatives used their majority to limit a House of Commons study of their controversial new terrorism bill to just eight meetings. After a day of delay tactics from the NDP in an attempt to expand the study of Bill C-51, the Conservative members of the public safety committee overruled their own committee chair to force a vote on the schedule. The opposition was suggesting at least 25 meetings to study the bill that would drastically increase the mandate of Canada's spies. On Tuesday, the government offered only four meetings. In the end, the Conservatives permitted eight meetings on the bill, which they say will allow for about 50 witnesses to testify. NDP public safety critic Rosanne DORS Leefebvre called that
a small victory, but said eight meetings -- including one with Public Safety Minister Steven Blaney and Justice Minister Peter MacKay -- is still not enough. "We were trying to have a full debate on the study, so we were pushing for that," Doré Lefebvre told reporters Thursday. "We could have met evenings and weekends, and have a full study. But unfortunately we didn't get what we wanted, but it's still a small victory in the end."

ISIS recruits' beliefs usually known by families, Steven Blaney says

CBC.CA, Laura Payton, 2015 02 27

Ottawa - In most cases where someone is willing to travel for terrorist-related reasons, those around them are aware of those beliefs, Public Safety Minister Steven Blaney said Thursday, as he urged people to report those cases to officials. "We all have a responsibility and our studies clearly demonstrate that in 80 per cent of the cases, when an individual is willing to travel for a terrorist purpose, the people around are aware or informed of that situation," Blaney said outside the House of Commons. "It is important to report it to the authorities for the well-being of that individual, for not being further radicalized and also saving human lives."

CBC News reported Wednesday on a woman in Edmonton who recruited a Canadian woman to join ISIS. On Thursday, media reports said six Quebecers had travelled to Turkey and are believed to be on their way to Syria to join jihadists there. Blaney said Wednesday that Canada "cannot become an exporter of terrorism" by letting Canadians travel to join ISIS. Blaney urged MPs to move faster on Bill C-51, his proposed anti-terrorism legislation, which would vastly expand the powers of the Canadian Security Intelligence Service (CSIS). One power would be the ability to disrupt suspected terrorist activities, with very few limits. New Democrat public safety critic Randall Garrison questioned the need for some of the powers proposed in the bill, arguing that Canada's security and law enforcement agencies already have the power to stop Canadians from leaving to join terrorist activities.

CSIS needs power to stop high-risk travellers, says Steven Blaney

CBC News, Staff reporter, 2015 02 26

Canada must take action to prevent its citizens from travelling abroad for terrorist purposes, Public Safety Minister Steven Blaney said after a CBC News investigation revealed a 23-year-old Edmonton woman travelled to Syria after being radicalized. "Clearly, Canada cannot become an exporter of terrorists. This is not the Canadian way of living," Blaney said Wednesday. The woman, whom CBC News is calling Aisha, to protect her identity, made the journey to Syria to join up with ISIS last summer, after taking an online course to study the Qur'an taught by a woman based in Edmonton, according to her older sister Rabia (whose name has also been changed). Blaney said the Conservative-backed Bill C-61 -- which would expand the CSIS's powers, allowing the security agency to disrupt the travel plans or financial transactions of Canadians the agency believes have been radicalized -- is aimed at preventing stories just like Aisha's. "In Bill C-51, there are provisions that enable our intelligence officers to interact with the families and the communities, not only to engage in a discussion but to reduce the threat and prevent individuals from travelling," he said. "Currently, we are not able to prevent a high-risk traveller from boarding an airplane. With the bill, we will be able to prevent those individuals from getting on board."

Work on better spy monitoring still underway four years after promise; news

Canadian Press, Jim Bronskill, 2015 02 25

Ottawa - The Conservative government says it is working on more comprehensive monitoring of Canadian intelligence agencies over four years after committing to do so. In December 2010, the government promised to allow the review of national security activities involving multiple departments and agencies. The goal was to eliminate barriers that prevent spy watchdogs from talking to each other. It also pledged to create an internal mechanism to ensure accountability and compliance with the laws and policies governing national security information-sharing. The commitments were included in the Harper government's response to a federal commission of inquiry into the 1985 Air India bombing that killed 329 people, most of them Canadians. Josee Sirois, a Public Safety Department spokeswoman, says the government it still developing options for inter-agency security review, adding she has no details on how the government might be done. "The government of Canada recognizes the importance of independent review in maintaining Canadians' trust in our national security activities," Sirois said. While there are efforts to improve information exchanges between intelligence agencies, calls to break down walls between the watchdogs that keep an eye on those agencies have largely gone unheard. Plans for new rules that would permit greater co-operation between watchdogs have come from Chuck Strahl, former head of the Security Intelligence Review Committee, which monitors CSIS, and Robert Decary, who once led the oversight agency for the Communications Security Establishment, the electronic spy service.

Small boost for security, even less for watchdogs

Ottawa Citizen, Ian Macleod, 2015 02 25

Ottawa - The government plans modest spending increases for key national security agencies in the coming year despite proposed legislation to dramatically expand their powers and scope, according to federal spending estimates released Tuesday. What's more, as the Conservatives continued their weeklong defence of anti-terror Bill C-51 in the Commons Tuesday by insisting that rights and freedoms will be protected by robust, independent oversight, Treasury Board revealed that Canada's two national security oversight organizations are to receive a combined total of just $18.3 million in additional funding in the next fiscal year. By comparison, Canada's "human" spy agency, the Canadian Security Intelligence Service (CSIS), and the electronic spy agency, the Communications Security Establishment (CSE), are to get a combined total of almost $37 million more in annual net spending for 2015-16. CSIS is to see a net $20.6 million, or 3.6 per cent, boost, bringing planned spending to $537 million for 2015-16. The CSE is to
get $16.1 million, or three per cent more, for total spending of $538.2 million. The Canada Border Services Agency’s (CBSA) net spending is to rise $37 million, or 2.2 per cent, to $1,76 billion. The RCMP, which has responsibility for criminal national security investigations, is to see a $4.1 million, or 0.2 per cent, spending increase.

**Tories move to limit study of terror bill**

**Toronto Star, Alex Boutilier, 2015 02 25**

Ottawa - The Conservatives are seeking to limit testimony on their wide-ranging terrorism bill to just four days, sources say, with Prime Minister Stephen Harper urging MPs to pass the bill "as quickly as possible." The parliamentary committee studying Bill C-51 met for several hours behind closed doors Tuesday to discuss potential witnesses and schedule meetings. Because the discussion was held in secret, MPs are prohibited from speaking publicly about the debate. But several sources told the Star the government wants only three meetings to hear expert witnesses, plus one appearance from Public Safety Minister Steven Blaney and Justice Minister Peter MacKay. That would amount to only four days for the most dramatic changes to Canada's security legislation since 2001. No deadlines were made on Tuesday, and Blaney's office said it's up to the committee - on which the government enjoys a majority - to determine how many meetings they'll hold. In the House of Commons, NDP Leader Thomas Mulcair demanded that the bill be given a full study. "Rushing C-51 through without improved oversight is reckless," The Conservatives introduced Bill C-51 in January, suggesting the Canadian Security Intelligence Service needs expanded powers to combat terrorist threats to Canada. Critics also point out that while CSIS will be given a larger mandate and expanded powers - including the ability to break the law or violate Charter rights, with judicial approval - the government refused to add more oversight.

**Harper urges swift passage of anti-terror bill as NDP calls for full study**

**Canadian Press, Jim Bronskill, 2015 02 25**

Ottawa - Prime Minister Stephen Harper is urging a House of Commons committee to study the government's anti-terror bill as quickly as possible, in spite of accusations the Conservatives are using their majority to move the legislation onto the books. NDP Leader Tom Mulcair told the Commons on Tuesday it is essential to scrutinize the bill, and asked Harper to ensure that security and human rights experts are not only heard, but also heeded. The Conservatives brought in the bill - which would significantly expand the powers of Canada's spy agency - following the murders of two Canadian soldiers last October. The bill would also make it easier for authorities to control the movements of terror suspects, expand no-fly lists, crack down on extremist propaganda and outlaw encouraging someone to commit a terrorist act. The bill was introduced in January, suggesting the Canadian Security Intelligence Service needs expanded powers to combat terrorist threats to Canada. Critics also point out that while CSIS will be given a larger mandate and expanded powers - including the ability to break the law or violate Charter rights, with judicial approval - the government refused to add more oversight. Harper dismissed Mulcair's criticisms and said the public strongly supports the proposals. "I would urge the committee to study this bill as quickly as possible, in order to ensure the adoption of these measures to ensure the security and safety of Canadians," Harper said. The NDP hopes to call anywhere from 80 to 100 witnesses to testify on the bill during more than two dozen meetings, and as of Tuesday had finalized a preliminary roster of 20 names. They include four former prime ministers and several retired Supreme Court justices who recently published a statement calling for increased oversight of Canadian intelligence activities. The New Democrats also want to hear from Eva Plunkett, the former inspector general of the Canadian Security Intelligence Service, whose office was abolished as a cost-cutting measure. Critics including the NDP and Liberals have called for more robust oversight to complement the work of the Security Intelligence Review Committee, the remaining watchdog charged with keeping an eye on CSIS.

**Spy agency's review group has no clout**

**Ottawa Citizen, Ian MacLeod, 2015 02 24**

Ottawa - The small group watching over Canada's spy agency says it was purposely devised to be a limited, after-the-fact "review" body - not an all-seeing "oversight" committee that would vet spy operations. During three days of lively debate in the Commons over the controversial anti-terror Bill C-51, the Security Intelligence Review Committee (SIRC) - which MPs have now sent to committee for study - has already characterized the Security Intelligence Review Committee (SIRC) as providing oversight of the spy agency, known as the Canadian Security Intelligence Service (CSIS). The committee was only heard, but also heeded. Yet SIRC has no such mandate, its spokeswoman said Monday. "We review CSIS. We look at past activities," to ensure they are lawful, appropriate and effective, SIRC's Lindsay Jackson said. "Recently the terms 'oversight' and 'review' have become almost interchangeable, but they do actually mean separate things. 'Direct oversight' implies a certain amount of involvement in the active political decision-making of the operational decision-making, and we are not involved in the operational decision-making," at CSIS. Under C-51, which MPs have now sent to committee for study - CSIS agents would be allowed to actively disrupt threats to national security, a significant expansion from their current mandate of producing security intelligence for government. CSIS would only be required to obtain judicial "threat disruption" warrants in instances where the activity was expected to be illegal or unconstitutional.

**Bill's terrorist propaganda provisions overly broad: law professors**

**Canadian Press, Jim Bronskill, 2015 02 24**

Ottawa - A federal proposal to scrub terrorist propaganda from the Internet risks sweeping in too much speech that doesn't lie in violent threats, says a new analysis. The definition of propaganda in the government anti-terrorism bill is dangerously broad, law professors Craig Forcese and Kent Roach say in their paper. The bill, introduced late last month, proposes giving the RCMP power to seek a judge's order to remove terrorist propaganda from websites. Forcese, of the University of Ottawa, and Roach, who teaches at the University of Toronto, say while they support the idea in principle, it should be rooted in actual or threatened violence. The Conservatives brought in the bill which would also significantly expand
the powers of Canada’s spy agency following the daylight murders of two Canadian soldiers last October. The Canadian Security Intelligence Service would become an agency that actively tries to derail terror plots, not just one that collects and analyzes information. The bill would also create a new criminal offence of encouraging someone to carry out a terror attack.

Blaney s'appuie sur la menace contre le West Edmonton Mall pour promouvoir C-51

Radio-Canada - Nouvelles (site web) Journaliste maison, 2015 02 23

Ottawa - Le gouvernement canadien s'appuie sur la menace proférée par l'organisation intégriste Al-Shabaab contre le centre commercial West Edmonton Mall pour justifier son empressément à adopter son projet de loi antiterroriste. Le projet de loi vise à étendre les pouvoirs du Service canadien du renseignement de sécurité (SCRS), en réaction aux attentats d'Ottawa et de Saint-Jean-sur-Richelieu.

Kenney spurns calls to increase security oversight

Globe and Mail, Steven Chase, 2015 02 23

Ottawa - The federal government is rejecting calls for more independent oversight of Canada’s national security agencies even as it speeds passage of legislation that would give sweeping new powers to spies and police in the name of fighting terrorism. Parliament will vote tonight on the Anti-Terrorism Act after the Conservatives limited second reading debate for the legislation to three days. The bill will be sent to a Parliamentary committee for scrutiny. The Tories want the controversial legislation to become law before the summer begins. On Sunday, Defence Minister Jason Kenney, who has functioned as the government’s lead spokesman for the legislation in recent days, rebuffed an appeal for more independent supervision of national-security agencies - one that came in the form of a letter published in The Globe and Mail and signed by former prime ministers, ex-Supreme Court justices and others. Mr. Kenney noted the letter’s key signatories, Jean Chrétien, Paul Martin, Joe Clark and John Turner, did not change the oversight of Canada’s spy agency, which is currently supervised by the Security Intelligence Review Committee, while they were in power. “The legislation is a response to the deadly Ottawa attacks on Canadian soldiers last fall that included a gunman storming Parliament. It would give CSIS new interventionist powers to disrupt potential threats to national security and make it easier for authorities to obtain a warrant to arrest suspects under the current law.”

Prime Minister Harper has categorically rejected the idea of a security-cleared committee of parliamentarians monitoring spy agencies

Prime Minister Harper has categorically rejected the idea of a security-cleared committee of parliamentarians monitoring spy agencies

Canadian Press, 2015 02 20
Prime Minister Harper has categorically rejected the idea of a security-directed committee of parliamentarians monitoring spy agencies, like the ones in Britain and the United States. Harper was asked in Surrey, B.C. to respond to statements calling for stronger oversight. The prime minister says the government prefers independent, expert oversight—not by politicians. Four former prime ministers and several retired Supreme Court members are among almost two dozen prominent Canadians calling for stronger security oversight. Their statement, published Thursday in the Globe and Mail and La Presse newspapers, comes as the Conservative government proposes a new, expanded mandate for the Canadian Security Intelligence Service to counter terrorist threats.

Defence minister says more homegrown jihadist terror attacks possible

Ottawa - Defence Minister Jason Kenney sang the praises of the federal government's anti-terror bill Thursday as he used his maiden speech to Canada's military establishment to warn that more homegrown jihadist terror attacks are likely. The country is engaged in a long-term ideological struggle with radical Islam, Kenney told the annual Ottawa gathering hosted by the Conference of Defence Associations Institute. "We need only to look to Copenhagen, to Paris, to Brussels and to Sydney," Kenney said. "We need only consider the Toronto 18, the ongoing trials in Vancouver in the plot to bomb the B.C. legislature and in Toronto against the alleged Via Rail bombers, to know that there is a high probability of future jihadi attacks from within." The notion that western civilization and style of government are never going to be challenged is wrongheaded, he added. "Some Canadians can be forgiven for indulging in that fantasy," Kenney said. Canada's geographic remoteness, prosperity and pluralism "have given Canadians reason to think that we can avoid real threats to our peaceable dominion. Yet we face a global movement that quite literally defies reason." Kenney, who took over from Rob Nicholson earlier this month, says the country "shouldn't overreact to this threat, nor should we underreact." Debate over the federal government's proposed Bill C-51, which would increase the powers of security agencies, notably the Canadian Security Intelligence Service, began earlier this week in the House of Commons. The concerns of the bill's critics are exaggerated, Kenney said. "We are taking all of these steps while respecting the rights of Canadians."

Strong support for anti-terror legislation in Quebec: poll

"We've always said that we must remain vigilant and adjust to the evolving threat and that is why we are taking this bill," said Blaney. It "represents an important step to improve the means that"...
services have to fight effectively against the terrorist threat. The international jihadi movement has declared war on Canada and our allies. Bla contacts the legislation must bring about the fight against terrorism. It is necessary to ensure that the law does not violate individual rights. There is no liberty without security," he said. "It creates a no-fly list for individuals suspected of planning to join extremist fighters overseas. And in exceptional cases, it gives the Federal Court authority to issue warrants exempting the Canadian Security Intelligence Service (CSIS) from breaking the law in order to disrupt and "reduce" national security threats. A dozen federal acts will be amended and two additional statutes will be created to make way for the proposed powers, the biggest overhaul of the country’s national security legislation since the 2001 terrorist strikes against the U.S. This is an important step in enhancing the fight against terrorism." The mission of the CSIS is to carry out covert activities to disrupt terrorist threats and protect the security of Canada. The wording is sufficiently vague to permit a new director of terrorist prosecutions to be appointed to the CSIS. The creation of a "director of terrorist prosecutions" was one of the suggestions Major made to the committee inquiring into security threats facing Canada. The other is an enhanced role for the Canadian Security Intelligence Service (CSIS) to carry out covert activities to disrupt national security threats. It would also criminalize the promotion of terrorism: make it easier for police to arrest and detain individuals without charge as suspected national security threats. The legislation allows government departments to share personal information about individuals suspected of undermining the security of Canada. The wording of the law is so broad that it could be interpreted as permitting the government to spy on opponents, Mulcair charges. The bill would give CSIS power to disrupt suspected terrorist plots, thwart financial transactions and covertly interfere with radical websites.

Head of Air India inquiry 'comfortable' with terror bill

Ottawa—The mission of prosecuting terrorists should return to the Department of Justice and be led by a special prosecutor with a dedicated team of investigators, retired Supreme Court justice John Major told a Senate committee Monday. The creation of a "director of terrorist prosecutions" was one of two suggestions Major made to the committee inquiring into security threats facing Canada. The other is an enhanced role for the Canadian Security Intelligence Service (CSIS) to carry out covert activities to disrupt national security threats. It would also criminalize the promotion of terrorism: make it easier for police to arrest and detain individuals without charge as suspected national security threats. The legislation allows government departments to share personal information about individuals suspected of undermining the security of Canada. The wording of the law is so broad that it could be interpreted as permitting the government to spy on opponents, Mulcair charges. The bill would give CSIS power to disrupt suspected terrorist plots, thwart financial transactions and covertly interfere with radical websites.

Liberals, NDP careful on terror bill

Ottawa—With the House of Commons set to begin debate this week on sweeping anti-terrorism legislation, the two main opposition parties are treading gingerly, reluctant to confront the bill head on. Both New Democratic Party leader Tom Mulcair and Liberal leader Justin Trudeau have expressed concerns about Bill C-51, but neither party has said it will oppose the biggest restructuring of national security powers since 2001. Only Green Party leader Elizabeth May has raised fierce objections, calling C-51 an "act to create a new secret police." NDP MP Randall Garrison, the party’s public safety critic said a distinction needs to be made between ongoing monitoring and after-the-fact review by the CSIS watchdog group, SIRC. The Security Intelligence Review Committee is an independent five-member committee struggling to operate efficiently. Meanwhile, the Liberals say Trudeau’s early support for the bill - with or without government acceptance of proposed Liberal amendments - still leaves the party with options. "If the government is not going to allow democracy to work and allow sensible amendments to be put into the legislation, then we will put those key amendments in our election platform," said MP Wayne Easter, the party’s public safety critic.

New rules are long overdue to counter threat

Ottawa—Proposed new rules for the Canadian Security Intelligence Service are overdue in this era where terrorist plots and other potential national security threats traverse the globe at the speed of the Internet, says a former high-ranking Canadian spy. Ray Boisvert, onetime CSIS chief for counter-terrorism and later assistant director for intelligence, says giving CSIS intelligence agents powers to go on the offensive and actively disrupt threats to national security would modernize a national security structure that was devised for the Cold War. CSIS was created in 1984, replacing the disgraced and disbanded RCMP Security Service after revelations of "dirty tricks" against left-wing radicals and Quebec separatists in the late 1960s and early 1970s. Acting on the recommendations of the McDonald Commission (officially called the Royal Commission of Inquiry into Certain Activities of the RCMP), the government mandated the new civilian intelligence organization with collecting and analyzing information and producing intelligence about potential national security threats to Canada. Implicit in that mandate were several degrees of separation from police work. CSIS was not allowed to counter threats.
Former CSIS officer warns new federal anti-terror bill will 'lead to lawsuits, embarrassment'

Postmedia News, Stephen Maher, 2015-02-14

Toronto • Former CSIS officer Francois Lavigne is alarmed by the Conservative government's new anti-terror bill. He believes the measures proposed in C-51 are unnecessary, a threat to the rights of Canadians and that the prime minister is using fascist techniques to push the bill. Mr. Lavigne started his career with the RCMP security service in 1983, before the CSIS was established. "I was hired by the barn burners," he said in an interview last week. "I went to work for the FIU unit, the foreign interference unit. And that was where the barn burners came from. The barn burners were the off-the-lease Mounties whose law-breaking ways led to the McDonald Commission, which led to the establishment of Canadian Security Intelligence Service in 1984. Mr. Lavigne, who went from the Mounties to CSIS and later worked overseeing spies in the solicitor general's office, likes CSIS's design. It was set up as an intelligence-gathering body, not an enforcement agency, actively overseen by an inspector general and reviewed by the Security Intelligence Review Committee. Mr. Lavigne, 55, left government in 1999, but follows intelligence news closely. He spent years tracking dangerous radicals without the powers the government wants to give to CSIS. "I find it a little convenient that in the past few years that these radicalized people are the biggest threat to ever hit us," he said. "There are more people dying because of drunk drivers or because of gang violence." The changes in C-51 will give CSIS broad powers to take action to disrupt plots and reduce threats, in Canada and abroad. This is a recipe for trouble.

Federal justice minister defends anti-terror bill

Calgary Herald, James Wood, 2015-02-13

Calgary - Federal Justice Minister Peter MacKay defended the Conservative government's new anti-terrorism legislation Thursday, saying it is needed to deal with real threats facing the country. In Calgary to make two announcements, MacKay said last week's attacks by homegrown terrorists in Quebec and on Parliament Hill - as well as alleged plots against Via Rail trains and the British Columbia legislature - illustrated the need for tougher laws. "It's absolutely ridiculous and unacceptable," he told reporters at the Calgary Police Service headquarters. "We know that it's happening. We are taking steps to curtail that activity to the greatest extent possible, to do so within the Canadian law." Bill C-51, introduced at the end of January, would make promoting or advocating a terrorist act a crime punishable by up to five years in prison. If passed, the legislation would also expand the role of the Canadian Security Intelligence Service, allow authorities to detain people who haven't committed a crime for up to seven days, and use a no-fly list to thwart Canadians planning to travel abroad to join groups like the Islamic State. But the bill has raised concerns among civil libertarians about potential abuses of the enhanced powers for CSIS. And Christianne Boudreau, a Calgary mother whose son was killed after joining Islamic extremists overseas, told the Herald recently she is worried the law will raise more mistrust and fear, pushing at-risk individuals towards radicalization.

Judges at risk of being CSIS pawns: Report

Globe and Mail, Colin Freze, 2015-02-13

Ottawa - Two prominent law professors argue that Canada's judges are being "dragooned" into the service of spies through Parliament's overhaul of national-security legislation. Professors Kent Roach and Craig Forcese are to release a scholarly critique of the Conservatives' Bill C-51, tabled last month, on Friday. The analysis focuses on proposed judicial authorizations for future Canadian Security Intelligence Service "disruption" campaigns. Government officials and the proposed law do not spell out precisely what "disruption" entails. The professors argue the bill could conceivably give CSIS licences to engage in break-ins, computer hacking, draining bank accounts, ripping up passports - even "smear campaigns" - so long as judges sign off in advance. The professors, who have written books about Canada's security laws based on more than a decade's worth of research, argue such spying activities could be directed against a variety of CSIS "targets" - not just terrorism suspects, but possibly lower-tier threats such as extremists, environmentalists. Other legal experts counter that the judiciary would never write CSIS a blank cheque to violate the Charter. "The Federal Court judges have shown themselves quite fiercely independent of the government," says Ron Atkey, a former Conservative politician and past chair of CSIS's watchdog committee. "They will resist the notion that they are tools of executive power."

Targeting methods raise concerns about CSIS powers

Globe and Mail, Colin Freze, 2015-02-11

Toronto - When Canada's spies designate someone as a "target" of a terrorism probe, they input that information with one of four labels - "terrorist," "extremist," "supporter" and "sympathizer." From there, the spy service determines whether the target is a Level One or Level Two threat. Only the latter can be put under the surveillance of bugging devices or paid infiltrators. Newly released documents provide details on the targeting methodology now being used by Canadian Security Intelligence Service, the secretive agency that's about to be given new enforcement powers through legislation. The recently added ability to deem "sympathizers" as national security threats means CSIS may already be casting a wider net to head off the threat posed by jihadis. Yet observers, including one retired spy-service executive, warn that fundamental changes are occurring at a time when Parliament has come under criticism for its scrutiny of spying. "Where's the ongoing accountability, and review, that the system contemplates, and depends upon frankly?" said Geoffrey O'Brien, a retired former CSIS chief of counterintelligence. Mr. O'Brien says CSIS targeting is now far more centralized than it was a decade ago, when the agency's chief personally vetted most major targeting decisions. Documents now suggest the next rung of CSIS executives oversees such decisions. The Globe and Mail recently obtained two 2013 CSIS documents stamped "only for external use" on whether the spy service is following the rules of its warrant and targeting programs. The CSIS Internal Audit Branch reports, released under Access to Information laws, looked at two years of records. Auditors determined the spying powers were being exercised lawfully. However, some criticisms and the specific numbers related to CSIS "targets" were redacted.
Privacy rights won’t be trampled in terror fight, says public safety minister

The Canadian Press, Jim Bronskill, 2015 02 07

Ottawa - The privacy rights of Canadians will be respected under new anti-terrorism legislation that would allow more information-sharing with the United States, says Public Safety Minister Steven Blaney. Blaney has been discussing security issues in London with U.S. Homeland Security Secretary Jeh Johnson and ministerial counterparts from Britain, Australia and New Zealand. On the sidelines of the Five Eyes meeting, he and Johnson talked about strengthening bilateral information exchanges, including case-specific sharing on citizens suspected of terrorism-related activity. Blaney pointed out that the Conservative government’s new bill would allow sharing of data from Canada’s no-fly list with close allies. In an interview Friday, the minister said that doesn’t mean handing U.S. officials the full list of people suspected of being a threat to the skies. “I made clear that, from a Canadian perspective, we have to first take into consideration the privacy of Canadians.” Blaney said only information about high-risk travellers would be shared under a memorandum of understanding that conforms with Canadian privacy law. Legislation tabled late last month would give the Canadian Security Intelligence Service powers to actively disrupt threats, not just collect and analyze information about them. It would also make it easier for police to control the movements of terror suspects and to detain them longer without warrant. In addition, the legislation would expand the no-fly regime to cover those travelling by air to take part in terrorist activities, whereas currently there must be an immediate risk to the plane. Opposition MPs and civil liberties advocates have called for stronger oversight of Canadian intelligence services in light of the proposed new powers something the government has rejected as unnecessary, given existing watchdog mechanisms.

CSIS oversight body lacks resources, former member Bob Rae says

CBC News, Staff Writer, 2015 02 07

Ottawa - As the government’s anti-terrorism bill is set to enhance the powers of the national spy agency, a former member of the independent body that oversees the Canadian Security Intelligence Service is concerned it is not equipped to provide sufficient oversight. Bob Rae — the former premier of Ontario and one-time interim leader of the Liberal Party — was for five years a member of the Security Intelligence Review Committee, which keeps tabs on CSIS. In an interview airing Saturday on CBC Radio’s The House, Rae told host Evan Solomon that although CSIS has a budget “well over a billion dollars,” the agency meant to watch over it has scant resources in comparison. SIRC’s budget is $3 million. So that’s 0.3 — one third of one percent of the [CSIS] budget,” he said. “I believe very strongly that SIRC also suffers from a lack of resources. And, frankly, in the last few years particularly, from a lack of attention and respect from the government itself.” SIRC is meant to be a five-person committee, but Rae said vacancies have gone unfilled for months. There are currently four members on the committee. Bill C-51, the new anti-terrorism legislation, aims to give Canada’s spies more powers that would go beyond just gathering intelligence, but also allow them to disrupt the activities of the people they are spying on. Rae said there needs to be a discussion about Parliament’s role in watching over security work. But the prime minister’s parliamentary secretary, Pierre Poilievre, told The House that the non-partisan approach used to watch over CSIS is preferable to parliamentary oversight.

Top court to decide CSIS’s spy powers

Ottawa Citizen, Ian MacLeod, 2015 02 06

Ottawa - The Supreme Court will decide whether it’s legal for Canada’s spy agency to employ foreign security services to spy on Canadians abroad. Coming at a time when the government has introduced an ambitious bill to widen the powers of the Canadian Security Intelligence Service, the case pits CSIS against the Federal Court of Canada in a confrontation over whether the court has the authority to approve CSIS warrant applications to electronically spy on Canadians overseas. The federal court insists it has no such power. CSIS and the government argue it does. The competing positions are layered in complex legal arguments laid out in secret courtroom hearings. The debate led the court to issue a stinging rebuke in 2013, accusing the national security intelligence service of purposely misleading and keeping the court “in the dark” in order to win warrants to spy on suspected Canadian terrorists overseas. That raised questions about whether CSIS has been violating charter privacy protections and even criminal law. Federal Court Judge Richard Mosley, the nation’s foremost jurist on national security law, drafted a ruling that allowed the communications intercepts but respected the international sovereignty of the unnamed country or countries involved. But the court has jurisdiction to authorize the warrant under the CSIS Act only as long as the communications in question are intercepted within Canada. So Mosley authorized the warrants on the understanding that the federal electronic spy agency, the Communications Security Establishment (CSE), was to do the intercepting.

High court to hear case on overseas terror tracking by Canadian spies

Canadian Press, Jim Bronskill, 2015 02 05

Ottawa - The Supreme Court of Canada will delve into the legacies of overseas spying by the Canadian Security Intelligence Service. The federal government had urged the high court to hear the case, arguing that guidance was needed on the issue even though the Conservatives had introduced legislation to clarify foreign intelligence-gathering powers. In its arguments, the government said recently tabled legislation didn’t overtake the high-profile issue of whether CSIS needed a warrant to seek allied help in spying on Canadians abroad. It said CSIS was left in the dark as to when a judge’s approval is needed to monitor suspected Canadian extremists in other countries. Federal lawyers also said lower courts made significant errors in dealing with the delicate matter. As usual, the Supreme Court gave no reasons Thursday for agreeing to examine the case. No hearing date has been set. In a central 2013 ruling, Federal Court Justice Richard Mosley chastised CSIS over a request for warrants to track two Canadians with help from the Communications Security Establishment, Canada’s electronic spy agency.
Expert says new powers for CSIS a worry
Ottawa Citizen, Ian MacLeod, 2015 02 05

Ottawa—Proposed antiterror legislation that dramatically expands the powers of Canada’s spy agency is a gross overreaction that would grant the state impunity to trample Charter rights and reduce judges to “enablers of illegality,” a leading expert on national security argues. Craig Forcese, a longtime University of Ottawa law scholar, says the government’s Bill C-51, tabled in the Commons last week, would allow Canadian Security Intelligence Service agents to conduct warrantless clandestine operations, chill freedom of expression and harm police anti-radicalization efforts by criminalizing some of the language of terrorism and therefore discouraging frank discussion from Muslim communities. Part of the sweeping legislation, introduced last week, would amend the 1984 CSIS Act to fundamentally change the agency’s core mandate. CSIS collects, analyses and reports to the federal government information about “threats to the security of Canada”—from terrorism and espionage to foreign influenced activities. It’s a broad mandate, but the powers CSIS has to enforce it are purposely limited to intelligence collection. That’s because its forerunner, the RCMP Security Service, was disgraced and disbanded following revelations of “dirty tricks” against left-wing radicals and Quebec separatists in the late 1960s and early 1970s. Its intelligence-collection powers include court-authorized search-and-seizure techniques, such as human and electronic surveillance of subjects, mail openings and other intrusive measures. C-51, if passed—it now has Liberal party support too—would change that. CSIS could actively target people and places to “reduce” threats to the security of Canada. According to the bill, the new measures would have to be reasonable and proportional to the circumstances. Forcese says the bill could lead CSIS into dangerous territory with Canadians’ Charter rights and other laws, creating future grounds for a constitutional court challenge.

Liberals to support Conservative anti-terror bill, will address the “gaps” later
Globe and Mail, Daniel Leblanc, 2015 02 05

Ottawa—The Liberal Party is ready to ignore “gaps” in Ottawa’s anti-terrorism bill and vote in its favour, while the NDP plans to put up a fight and could still oppose the proposed legislation. The two parties were united in opposition to Canada’s combat mission in Iraq last year, but they are heading in different directions in regards to Bill C-51, known as the Anti-Terrorism Act (2015). After a caucus meeting on Wednesday, Liberal Leader Justin Trudeau announced his party will support plans to beef up the powers of the Canadian Security Intelligence Service and the RCMP, and to criminalize the promotion of terrorism. Mr. Trudeau said his priority will be to “address the gaps” in the bill. In particular, the Liberals will push for parliamentary oversight of Canada’s national security agencies, and try to add a sunset clause that would force Parliament to evaluate the legislation before it is periodically re-amended. Mr. Trudeau said the Liberal Party will be willing to compromise during the current session of Parliament, and then promise to amend the legislation in its next election platform. “The current government can accept that Canadians want greater oversight and accountability, or it will give us the opportunity to offer that directly to Canadians in the upcoming election campaign,” Mr. Trudeau said.

Anti-terrorism bill bars CSIS from committing ‘bodily harm,’ sexual violation
CBC News, Laura Payton, 2015 02 04

Ottawa—The government’s proposed anti-terror legislation expands the powers of Canadian Security Intelligence Service to allow it to “disrupt” suspected terrorist threats—but it also expressly prohibits CSIS from killing or seriously injuring a subject. What’s not clear exactly is where the line between those activities is drawn and what that means for the agency when it comes to interrogation techniques, experts on civil liberties and security point out. Bill C-51 would allow CSIS to take measures within or outside Canada to reduce threats to the security of Canada, but doesn’t spell out exactly what those measures could be. The bill lists prohibited activities, barring CSIS from:—Intentionally or by criminal negligence cause death or bodily harm—in any way trying to obstruct, pervert or defeat the course of justice.—Violating the sexual integrity of an individual. The bill also bars “bodily harm” to its definition in the Criminal Code, which means any injury to a person that “interferes with the health or comfort of the person and that is more than merely transient or trifling in nature.”

Edward Snowden speaks to Toronto students, urges caution on new terror bill
Canadian Press, Adam Miller, 2015 02 03

Toronto—Former U.S. intelligence contractor turned whistleblower Edward Snowden says citizens of the world, including Canadians, should be “extraordinarily cautious” when their governments try to pass new laws under the guise of an increased threat of terrorism. Legislation tabled last Friday would give the Canadian Security Intelligence Service powers to actively disrupt threats, but not collect information about them. Snowden, who remains in Russia after leaking U.S. National Security Agency documents, says citizens of any country should have concerns about this type of legislation. “I would say we should always be extraordinarily cautious when we see governments trying to set up a new secret police within their own countries,” Snowden said Monday night during a video conference organized by Upper Canada College in Toronto. Intelligence powers used by governments in ways related to political ideologies, radicalization, influence of governments and how people develop their politics are cause for concern, the former NSA analyst added. “We need to be very careful about this because this is a process that is very, very easy to begin. It always happens in time of fear and panic emergency legislation they say we’re facing extraordinary threats and again if you look at the statistics while the threats are there, they’re typically not as significant as presented.” “Once we let these powers get rolling it’s very difficult to stop that pull though.” Snowden said. “So I would say that we need to use extraordinary scrutiny in every society, in every country, in every city. In every state to make sure that the laws we live under are the ones we truly want and truly need.” Public Safety Minister Steven Blaney has said he believes that
MacKay once backed spy oversight now rejected by Tories

Globe and Mail, Daniel Leblanc and Steven Chase, 2015 02 03

Ottawa - One of the Conservative cabinet ministers responsible for Ottawa's new anti-terrorism legislation once advocated parliamentary oversight of Canada's spy agencies, which the government now rejects as unnecessary even as it expands the powers of this country's national security apparatus. Justice Minister Peter MacKay stood beside Prime Minister Stephen Harper last week when the government unveiled a bill that would give the Canadian Security Intelligence Service new authority to disrupt terror plots and lengthen the number of days individuals can be held on suspicion they may commit terror acts. As deputy leader of the Conservative Party in 2005, Mr. MacKay argued forcefully for giving MPs and senators a role in overseeing Canadian spies. "When you talk about a credible oversight body, I would suggest ... that a parliamentary body is going to have more credibility because of its independence and because of the fact that there is also parliamentary accountability that will be brought to bear," Mr. MacKay said in October of that year. "To that end, I suggest that it would also cause a little bit more diligence on the part of the security agents themselves, just knowing that this oversight body was in place." Asked to comment Monday, Mr. MacKay said circumstances have altered his opinion.

Opposition wants oversight of new spy powers

Toronto Star, Les Whittington, 2015 02 03

Ottawa - Opposition parties stepped up demands for Prime Minister Stephen Harper's government to strengthen measures to control Canada's spies as part of its sweeping anti-terror legislation. NDP Leader Tom Mulcair said Harper failed to balance the new powers proposed for the Canadian Security Intelligence Service (CSIS) with more oversight provisions to protect rights and civil liberties. "If you are going to give enhanced powers, you have to have enhanced oversight," Mulcair said Monday. "If you look at Washington, if you look at London, there's always serious oversight and it's done by elected officials." He was responding to the wide-ranging legislation introduced Friday by Harper that is meant to combat terrorism by broadening CSIS's mandate to include police-like powers for the first time. Opposition MPs question whether the existing five-member Security Intelligence Review Committee (SIRC), which looks into complaints against CSIS, would provide adequate oversight once the intelligence agency is allowed to take a much more activist role in investigating and thwarting suspected terrorist threats. The Harper government has so far turned aside questions about the adequacy of oversight provisions under the new legislation. But in the Commons Monday, Public Safety Minister Steven Blaney sought to reassure MPs, saying SIRC "will cover all activities that CSIS will be mandated by this Parliament to accomplish." Mulcair told reporters he doesn't know if the NDP will support the legislation. Parts of the multi-faceted proposals, such as criminalizing incitement to commit a terrorist offence, are useful, he said. But the NDP intends to fight hard for the inclusion of more controls over CSIS.

Tories rebuff calls for greater oversight of CSIS

Globe and Mail, Adrian Morrow, 2015 02 02

Ottawa - Ottawa is rejecting calls for parliamentary oversight of the nation's spies, dismissing such increased scrutiny as "needless red tape." Conservatives on Sunday defended their controversial new anti-terror legislation, which has faced criticism for massively expanding the powers of the Canadian Security Intelligence Service without added public oversight. Public Safety Minister Steven Blaney argued the Security Intelligence Review Committee, a five-member body that investigates complaints against CSIS, is enough. "We can be very proud of what they are doing," he said about SIRC on CTV's Question Period. "Anything additional would be just duplication." The anti-terrorism legislation, which was unveiled Friday, would give CSIS the right to disrupt terrorist activity, such as by pulling suspected terrorists off planes or meeting with their bank accounts.

Canada Seeks to Strengthen Spy Agency After Attacks

The New York Times, Ian Austen, 2015 01 31

Ottawa - Citing the attacks by radical Islamists that killed two Canadian soldiers in October and the more recent assaults in France, Prime Minister Stephen Harper introduced sweeping legislation on Friday that would greatly expand the role of Canada's spy service, allowing courts to remove online postings and increasing police detention powers. "Jihadi terrorism is one of the most dangerous enemies our world has ever faced," Mr. Harper said at a campaign-style event in the Toronto suburb of Richmond Hill. "It seeks to harm us here in Canada, in our cities and in our neighborhoods, through horrific acts like deliberately driving a car at a defenseless man or shooting a soldier in the back as he stands on guard at a War Memorial," he said, referring to the two deaths last fall. The bill, which was introduced in the House of Commons shortly before Mr. Harper spoke, is the second piece of anti-terrorism legislation his government has proposed since the October attacks. Some legal experts questioned the constitutionality of its crucial measures, while opposition leaders accused the prime minister of exploiting those killings in an election year. The voting majority held by Mr. Harper and his Conservative Party in the House of Commons all but ensures that the bill will pass without amendment. Under it, the Canadian Security Intelligence Service would change from an agency that only gathers information to one that can actively intervene in what it regards as terrorist actions in Canada and abroad, and, with court approval, disrupt them. While it would not gain powers of arrest, the spy agency would, among other things, be able to cancel travel arrangements, shut down bank accounts, provide fake versions of dangerous materials to plotters and compel access to buildings in order to plant surveillance devices.

Spy service to get stronger anti-terror powers under federal bill

Canadian Press, Jim Bronskill, 2015 01 31

Ottawa - Canada's spy agency could soon have the power to derail terrorist plots, not just gather and
analyze information about them as the government moves to confront radical threats with an array of new legal tools. Legislation tabled Friday would allow the Canadian Security Intelligence Service to prevent a suspected extremist’s travel plans, disrupt bank transactions and covertly monitor their internet activities. The plan to boost the spy service’s ability to counter terrorism flows from a review of fatal attacks on two Canadian soldiers last October — incidents the government believes were fuelled by Islamic extremism. The Conservatives say the new powers are needed to help keep Canadians safe in an increasingly dangerous world. Initial reaction from opposition parties was cautious and muted. Privacy advocates and civil libertarians expressed fears about trampled rights and inadequate oversight. The proposed expansion of CSIS powers also conjured memories of past misdeeds — such as bullying a witness to prevent a meeting of radicals — by the old RCMP security service, the scandal-plagued outfit from whose ashes CSIS rose three decades ago. As expected, the bill would also make it easier for police to obtain a peace bond to restrict the movements of a suspect and it extends the period for preventative arrest and detention.

Harper’s next act: Give CSIS teeth
The Globe and Mail, Daniel Leblanc, 2015 01 31
Ottawa — PM proposes dramatic boost to spy agency’s powers in effort to defend against the “great evil” descending over our world. Stephen Harper is proposing the most sweeping increase in power for Canadian security agencies since the aftermath of Sept. 11, 2001, including all time for encouraging terrorism on the Internet, while playing down concerns over the impact on civil liberties. The new charge for advocating “the commission of terrorist offences in general” would carry penalties of up to five years in prison and is part of a package of anti-terror measures introduced Friday, which come as a response to the deadly attacks on soldiers last October that included a gunman storming Parliament. This Anti-Terrorism Act is igniting a national debate about the proper balance between freedom and security in Canada in the 21st century, including whether there is sufficient outside scrutiny of the law-enforcement agencies that are gaining new powers. The legislation would also grant Canada’s spy agency, the Canadian Security Intelligence Service, the power to intervene and disrupt threats to national security, a major change from merely collecting intelligence and handing over the matter to the RCMP. Mr. Harper made it clear Friday he will try to own the security file in this election year, casting his political opponents as reluctant to follow in his footsteps, both in fighting terrorism at home and Islamic State in Iraq. Both the Liberals and NDP declined to reject the legislation outright Friday, saying they need time to study it. Mr. Harper rejected a reporter’s question about whether this might conflict with civil liberties, saying it’s his rivals who worry about that. “This is really what we get from our opposition, that every time we talk about security, they suggest that somehow our freedoms are threatened,” the Prime Minister said.

Critics fear Bill C-51 could lead to unintended consequences
Maclean’s, Rachael Brownie, 2015 01 31
Ottawa — The Conservatives tabled an anti-terrorism bill today, three months after the fatal attacks on Cpl. Nathan Cirillo in Ottawa and Warrant Officer Patrice Vincent in St-Jean-sur-Richelieu. With sweeping reforms, the Anti-Terrorism Act (Bill C-51) proposes to amend existing laws, including changing the Criminal Code to give law enforcement officials broader powers to make arrests if they suspect terrorist activity “may be carried out” (changing the wording from “will be carried out”), and increasing the period of preventative detention to seven days from three. The bill would also expand the no-fly list, bolster the Canadian Security Intelligence Service’s (CSIS) ability to disrupt suspected terrorist activities online, and make it illegal to “promote” terrorism. At midday, Prime Minister Stephen Harper hosted a news conference in Richmond Hill, Ont., where he explained to a jubilant crowd the need for these new laws. “Over the last few years, a great evil has been descending upon our world, an evil which has become more and more powerful: violent jihadism, motivated by extremist distortions of Islam.” He went on to cite recent terrorist plots that had been foiled by Canadian police forces: The Toronto security scare in 2014, the attempt to bomb the CN Tower and kill Members of Parliament in 2006, and the plan to derail a Via Rail train in 2013. “But recent terrorist attacks here and around the world have shown us that as the terrorists refine and adapt their methods, our police and national security agencies need additional tools and greater coordination. However, critics and members of the Muslim community warn the bill’s provisions will lead to more harm and unintended consequences, especially when it comes to dealing with radicalized offenders. Even before its contents were made public, the bill had been subjected to scrutiny from civil liberties groups and lawyers, who said it would impede freedom of expression and religion.

Spy agency to become “disruptive” influence
Ottawa Citizen, Ian MacLeod, 2015 01 31
Ottawa — Canada’s lead spy agency. the Canadian Security Intelligence Service, will gain some real clout and direction under the Conservatives’ proposed Anti-terrorism Act. The government’s sweeping package of anti-terror measures tabled in the House of Commons Friday would, among other things, give the organization broad powers to “disrupt threats to the security of Canada,” including terrorism, espionage, sabotage, foreign-influenced activities, and domestic subversion. Bill C-51 would amend the 31-year-old CSIS Act to authorize agents to secure warrants to enter “any place or open or close any thing.” It would also authorize the service to “do any other thing that is reasonably necessary to take those measures. What’s more, the law would compel individuals and organizations from landlords to telecoms, to abide by any CSIS request for assistance in carrying out the so-called “disruption techniques.” This allows them to do some pretty concrete measures,” said Christian Leuprecht, a national security expert at Kingston’s Royal Military College and Queen’s University. Experts have suspected for years that CSIS agents have engaged in some “disruption techniques.” Even this service readily admits it conducts electronic surveillance, market openings and covert searches, but only when authorized by a Federal Court warrant. The new law will considerably broaden the scope of those activities. Clues about what they could involve can be gleaned from RCMP disruptions of suspected terrorist operations.
Critics question whether new anti-terror laws will come at the expense of privacy and free speech.

Ottawa - Canada's new anti-terrorism legislation creates sweeping new powers for the nation's security services, but it's not clear there will be equally robust oversight to protect privacy, free speech or civil liberties. Missing from the act, for instance, is a sunset clause for any of its provisions, though the Jean Chrétien Liberals put such a provision in their anti-terror bill introduced after the terrorist attacks of Sept. 11, 2001. Nor is there a mandatory review by a certain date - though this may yet be added when the bill goes to a parliamentary committee for review. Some question whether satisfying national security will come at the expense of civil liberties. "Countries that are free are also safer countries. Civil rights and public safety go hand-in-hand," NDP foreign affairs critic Paul Dewar said Friday. The government argues that existing civilian oversight bodies - at the spy agency CSIS, the cyber-spy agency CSE, and the RCMP - are adequate. And the new law does require that the public safety minister regularly report to Parliament on how CSIS is using its new powers. Prime Minister Stephen Harper also said on Friday that the government has worked protections into the bill to prevent erosion of civil liberties in the name of security. "Every time that we talk about security, they (the opposition) suggest that somehow our freedoms are threatened. I think what Canadians understand is that their freedoms and security more often than not go hand in hand," Harper said in response to a reporter's question. Federal Privacy Commissioner Daniel Therrien, stressing he had not had a chance to fully analyze the bill, said he was "concerned" about the bill's new powers to let departments share citizens' personal information.

Des nouveaux pouvoirs pour le SCRS et les tribunaux

La Presse, Hugo de Grandpre, 2015 01 31

Ottawa - Le gouvernement Harper a présenté hier son projet de loi antiterrorisme, qui étend les pouvoirs des services de renseignement et accorde une longue liste de nouveaux pouvoirs au gouvernement pour combattre le terrorisme. Le projet de loi C-51 donne aussi entre autres au Service canadien du renseignement de sécurité (SCRS) le pouvoir d'agir lui-même pour contrer certaines menaces, plutôt que de devoir s'en remettre à d'autres organismes, comme la Gendarmerie royale du Canada. C-51 rend aussi plus facile l'imposition par les tribunaux de condamnations à des incarcérations. Le ministre Stephen Harper a fait l'annonce de ces nouvelles mesures lors d'une conférence de presse aux allures électorales en banlieue de Toronto. Il a rappelé que les parlementaires et journalistes ont obtenu des séances d'information par des fonctionnaires à Ottawa. Le ministre Harper a insisté sur l'importance de protéger les libertés fondamentales des Canadiens, mais aussi de les protéger contre une menace terroriste qu'il a décrite comme étant de plus en plus présente.

Tories' public safety bill will expand anti-terror powers

Toronto Star, Tonda MacCharles, 2015 01 30

Ottawa - A Prime Minister Stephen Harper will unveil Friday details of an omnibus public safety bill to bring in a raft of new anti-terror powers, including authority to knock terrorist propaganda offline and new protections for secret evidence gathered by spies. The bill will enact two new laws and make amendments to the Criminal Code, the CSIS Act, the Immigration and Refugee Protection Act among a host of others. It's not clear whether the Conservatives are prepared to boost the budgets of national security agencies, a key focus of opposition criticism. The government put the Commons on notice that funding will attach to the measures, but a senior government official said it shouldn't be interpreted as new funding, rather is intended to provide authority to spend for a new purpose. However, the official Opposition NDP insists the question of resources for new laws is the main one and is skeptical of the need for new laws. It fears further erode civil liberties and privacy rights. Harper has chosen the riding of Richmond Hill to make the long-awaited announcement, flanked by Public Safety Minister Steven Blaney and Justice Minister Peter MacKay at the same time the bill itself is tabled in Parliament. The prime minister will press the need to increase information-sharing among federal departments and agencies, authorize CSIS to disrupt or diminish threats earlier in an investigation, detest jihadism propaganda and order the removal of online content that promotes terrorism, enhance "no-fly" rules for airline travellers deemed a risk, and lower the evidentiary threshold for courts to issue peace bonds or recognizances with conditions - court-ordered restrictions on a person's liberty and communications. The Conservative government already responded by granting anonymity to CSIS informants under another bill, C-44, now speeding through Parliament.

French consulate increases vigilance but 'no known threat' to Vancouver

Vancouver Sun, Tiffany Crawford And Tara Carman, 2015 01 19

Vancouver - French consulate staff in Vancouver have met with RCMP to enhance security measures after the deadly attacks in Paris. "We have increased our vigilance," said Antoine Mention, the deputy consul of France in Vancouver. "We are asking staff to pay attention to what is happening on the outskirts when they come into work and we are in the process of assessing our security system." Mention said the consulate asked police to add more patrolling officers around the consulate, located in downtown Vancouver. Although police have not added extra officers, Mention said police "assured us they were taking the situation very seriously and that there are already frequent patrols in this area because we are downtown near the British and U.S. consulates." He said Friday afternoon that the consulate has not received any threats to staff. Both VPD spokesman Const. Brian Montague and RCMP E Division spokesperson Sgt. Rob Vermilien said local authorities have not received any threats in Vancouver or the province since the first attacks on Paris at a Delta appearance earlier this week. Prime Minister Stephen Harper suggested further measures to give security officials more power to combat terrorism will likely be introduced later this month. That would be in addition to Bill C-44, also known as the Protection of Canada from Terrorists Act, which was tabled in Parliament in October and will soon go before the Senate. It
amends the legislation governing the Canadian Security Intelligence Service (CSIS) to give it more power to share information with allies and give sources anonymity.

Concerns raised about accountability as Canada's spy agency takes on more overseas missions

Postmedia News, Douglas Quan, 2014 12 01

When Canada formed a civilian intelligence agency in the mid-1950s, it sparked fears that its members would run amok across Canada with unchecked powers. As it celebrated its 30th anniversary, the Canadian Security Intelligence Service is being dogged by similar concerns — but this time it's in the context of its rapidly expanding overseas missions and "we go where the threat is" mantra. CSIS was created strictly as a domestic security intelligence agency, but some industry observers say it has been taking on operations more akin to the activities of a foreign intelligence service. They are worried about the lack of oversight related to its overseas missions and propose that Canada should follow the lead of its G-7 partners by creating a separate, dedicated foreign intelligence agency, such as the United States' CIA or Britain's MI5. "What we are doing is pretend that the skill set for domestic and foreign intelligence are the same... and offering nothing in the way of appropriate internal and external accountability," said Wesley Wark, a national security expert and visiting research professor at the University of Ottawa. Wark says CSIS has, in essence, become a "dual-purpose" agency operating at home and abroad. Since 9/11, CSIS has expanded its overseas operations "well beyond" the original functions performed by liaison officers posted at Canadian embassies. Proposed amendments to the CSIS Act in Bill C-44 serve to cement that hybrid role, he said. CSIS director Michel Coulombe alluded to the spy agency's shifting priorities and expanding "global footprint" in a speech to retired employees earlier this summer. "In this new environment, we go where the threat is. We do more foreign operations and joint operations than ever before, and these are more complex operations than ever before," he said, according to a copy of his speech obtained by Postmedia News through access-to-information laws.

Asked to elaborate on his remarks, CSIS spokeswoman Tamara Mufli said there is no question that the agency's foreign role has expanded, but she insists its mandate to collect information pertaining to threats to Canada. Alan Jones, a retired assistant director at CSIS, agreed. "You cannot defend Canada in isolation," he said. "Sometimes CSIS operators must have an on-the-ground presence to complete an intelligence collection task." What agents are not in the business of doing is collecting information about the activities of other states — that's the role of a foreign intelligence agency, he said. And the role is currently no different than CSIS into such an agency. Craig Forcese, a terrorism expert and law professor at the University of Ottawa, said he's not convinced a separate agency is needed given that it would fill the "narrowest of niches" not currently occupied by CSIS, the Communications Security Establishment (which intercepts foreign electronic communications) and intelligence arms of the Department of Foreign Affairs. That said, Forcese agrees the Canadian security sector needs to "go back to the drawing board" and reconsider how it conducts its affairs and how it is held accountable. "I think we have been making it up as we go in many areas of national security law and governance. That is not an ideal situation," he said.

Majority of Canadians worry about domestic terrorism, according to new survey

Postmedia News, Douglas Quan, 2014 11 24

Ottawa - Almost two-thirds of Canadians believe homegrown terrorism is a serious issue, but most do not perceive them as a threat in their communities, according to a new survey. The national poll, conducted in the wake of deadly attacks on Canadian soldiers, found that just over half of respondents supported new anti-terrorism legislation that would boost the powers of Canada's spies. Another 22 per cent said the government should go even further, suggesting they have not been swayed by civil liberties concerns. At the same time, those surveyed recognized that there are many factors behind radicalization — such as ideology, religion, mental illness and marginalization — and seemed open to a comprehensive approach. "People are sensitive to the fact this is a complex issue that requires a comprehensive approach," said Christian Leuprecht, a security expert at the Royal Military College of Canada and Queen's University. The online survey of 1,609 residents was done by The Vancouver Province in conjunction with the Canadian Race Relations Foundation, The Laurier Institution and the Angus Reid Institute. A probability sample of this size carries a margin of error of plus or minus 2.4 percent 19 times out of 20, according to the institute. Similarly, about one-third of Canadians said it was "likely" that people were becoming radicalized in their communities, though this number surged to 47 per cent in Quebec, conceivably part of the fallout from Quebec's recent debate over a "Charter of Values" and a reflection on Quebec's distinct ethno-demographic composition and immigration trends, Leuprecht said. Overall, there does not appear to be a lot of knee-jerk reaction to the recent violence, Leuprecht said. "We don't see people falling over themselves here, seeing there's a terrorist lurking around every corner." If anything, Canadians seem to recognize that when violent events occur, they tend to be isolated, he said. On public policy, 51 per cent said they support Bill C-44, proposed legislation that would give the Canadian Security Intelligence Service more powers to watch Canadians. An additional 22 per cent said the bill doesn't go far enough. Twenty-seven per cent, however, said the bill tramples on civil liberties. Those living in B.C. and people 18 to 34 were the most likely to subscribe to this view.

Government calls proposal to create a committee to oversee the foreign-focused electronic spy agency CSEC 'needless and duplicative'

Globe and Mail, Josh Wingrove, 2014 10 31

Ottawa - The federal government has dismissed a proposal to add new parliamentary oversight of Canada's foreign-focused spy agency at a time when Ottawa is boosting counterterrorism powers in the aftermath of two attacks last week. The independent Review of its own bill, C-44, to boost the powers of the country's other major intelligence agency, the Canadian Security Intelligence Service (CSIS), which has a domestic focus. The federal government also continues to review what other new counterterrorism powers it will add in the aftermath of attacks last week that killed two soldiers, though sources said Thursday those changes are still under discussion and not "imminent."
Bill C-622, known as the CSEC Accountability and Transparency Act, was tabled in June by Liberal MP Joyce Murray and calls for more oversight of the Communications Security Establishment Canada (CSEC), the country's foreign-focused electronic spy agency. The bill would, among other things, create a parliamentary committee to oversee national security operations, including CSEC. Currently, it's overseen by a commissioner. Ms. Murray held a briefing on the bill Thursday along with Jean-Jacques Blais - a former Liberal MP, minister of defence and member of the Security Intelligence Review Committee (SIRC) that oversees CSIS - and Wesley Wark, a professor who studies national security issues. Both praised the bill, with Prof. Wark in particular stressing the bill would not diminish CSEC's powers.

Oversight by a committee of MPs and senators is "about making sure that both intelligence and security agencies have the tools and the funds they need to protect Canadians and to protect Canadians' rights," Ms. Murray argued in Question Period. However, the government was cool to the proposal. Public Safety Minister Steven Blaney said "robust oversight exists," though he cited SIRC, which oversees CSIS, not CSEC. Nonetheless, during debate on Bill C-622 Thursday evening, Conservative MP Roxanne James called the bill "needless and duplicative in nature" and said the government would not support it.

Bill extends CSIS source protection, extends judicial warrant powers
Halifax Chronicle-Herald, Paul McLeod, 2014 10 28
Ottawa - New legislation would essentially reverse the rulings of two court cases lost by Canada's spy agency. A bill introduced in the House of Commons on Monday would allow CSIS, the Canadian Security Intelligence Service, to spy internationally and would grant anonymity to CSIS informants in court cases.

The agency had previously sought both of these things but was rebuffed by the Federal Court and Supreme Court of Canada, respectively. Bill C-44, the Protection of Canada from Terrorists Act, was set to be tabled last week. That got pushed back when the House of Commons itself was hit by a violent attack by a gunman. Public Safety Minister Steven Blaney didn't say whether the government had changed the bill since last week. Some news outlets reported the government may grant police new powers to detain people who were suspected of planning terror attacks but who are not charged with a crime. That is not ultimately part of the bill.

Bill would let CSIS spy on Canadians while abroad
Ottawa Citizen, Dylan Robertson, 2014 10 28
Ottawa - The federal government has introduced a bill to boost the ability of the country's spy agency to monitor Canadians. Amendments to the CSIS Act were tabled Monday under the title "The Protection of Canada from Terrorists Act." The bill also includes small changes to citizenship rules. As expected, the legislation: Allows the Canadian Security Intelligence Service to obtain information on Canadians fighting abroad with terrorist groups through the "Five Eyes" spy network, which includes Canada, the United States, the United Kingdom, Australia and New Zealand; Lets CSIS more easily track Canadians engaging in terrorist activities abroad; and similarly helping a Five Eyes country track its nationals working with terror groups in Canada. Gives CSIS informants the same identity protection now accorded to police sources. The bill doesn't mention the Five Eyes by name, but clarifies that the agency can investigate outside of Canada, as it has done for years. "It's not as extreme as some people were predicting, there's some judicial oversight, it's not quite as bad," said David Murakami, an associate professor of sociology at Queen's University. But Wood says Canadians remain in the dark about the implications of allowing more spy links with partnering countries.

New spy bill would let Canadian agents operate illegally abroad
Toronto Star, Tondra MacCharles, 2014 10 28
Ottawa - A bill to broaden the powers of CSIS would, for the first time, explicitly authorize Canadian agents abroad to break the laws of a foreign country when investigating threats to the security of Canada. After a tense week that saw Parliament Hill attacked by a gunman, the Conservative government unveiled a promised new bill to boost spy surveillance powers and protection for secret agents. Even before it was introduced, top CSIS, RCMP and CSIS officials began lobbying for even greater legal "tools." Public Safety Minister Steven Blaney on Monday tabled Bill C-44, the so-called "Protection of Canada from Terrorists Act." The Conservatives previously rejected the creation of a foreign intelligence agency, citing cost, bureaucracy, and arguing CSIS already has a legal mandate to operate on foreign soil to investigate security threats to Canada. This makes CSIS much more akin to the CIA. "It's an act of political courage," said University of Ottawa law professor Craig Forcese. "What a federal court judge is now authorized to do is authorize a warrant ... to engage in surveillance in a foreign country that presumably violates that foreign country's privacy laws." "So the Parliament of Canada is now saying, We are prepared to allow our security intelligence service to violate state sovereignty." In practice, the provision expressly allows CSIS to enlist the technical support of Canada's top secret electronic eavesdropping agency, CSEC (Communications Security Establishment Canada) and its foreign counterparts in the U.S., United Kingdom, Australia and New Zealand in the "Five Eyes" alliance to spy on Canadians or foreigners abroad in pursuit of security threats to Canada. (The CSEC already has the mandate to provide "technical and operational support" to CSIS, but Forcese says this clarifies the reach of that power.) However, Forcese argued that with increased spying powers should come robust oversight.

Ottawa demande des pouvoirs accru d'enquête pour le SCR
La Presse, Hugo de Grandpré, 2014 10 28
( Article aussi paru dans le quotidien Le Soleil et la Tribune de Sherbrooke) Ottawa - Le gouvernement fédéral a proposé hier d'accroître les pouvoirs de la Gendarmerie royale du Canada (GRC) et du Service canadien du renseignement de sécurité (SCRS) pour lutter contre le terrorisme au Canada et à l'étranger. Comme prévu, le projet de loi déposé par le ministre de la Sécurité publique ne contient pas l'élargissement des pouvoirs policiers qui a été évoqué depuis l'attaque de mercredi dernier au parlement et au monument commémoratif de la guerre. Ces mesures sont toujours à l'étude. La Loi modifiant la Loi
Ottawa eyes deeper security overhaul
Globe and Mail, Multiple reporters. 2014 10 26

Ottawa - On a day when the Conservative government tabled new legislation to expand the powers of CSIS, sources say Ottawa is now weighing new tools to deal with citizens who openly support terrorist attacks on Canadians or back groups that urge this goal. And in the midst of this proposed overhaul of security laws, the country's top Mountie is calling on the government to make it easier to restrict the liberties of suspects in terror cases. RCMP Commissioner Bob Paulson's comments to a Senate committee come as Ottawa moves on two fronts to strengthen the powers of Canada's spy agency and police forces in the wake of the killings of two Canadian soldiers last week. The first step came Monday when the Harper government tabled new spy legislation called "the Protection of Canada from Terrorists Act," which will expand the powers of the Canadian Security Intelligence Service. The bill, C-44, would better safeguard the identities of intelligence informants in Canada and authorize CSIS to eavesdrop in foreign countries. Sources say Ottawa is also considering measures to crack down on individuals who openly support terrorist attacks on this country or groups that call on aggressors to attack Canadians and Canadian soldiers. They cited the case of Martin Couture-Rouleau who veered into a mosque and shared his new-found beliefs online before running down Warrant Officer Patrice Vincent in Quebec last week. "One of the questions that has come up further to last week's attack is you have a case with a guy like Rouleau who was openly supporting a group that is calling for terrorist attacks on Canadian citizens," one government source said of Mr. Couture-Rouleau. "Are there tools required? Is there legislation required?" Experts said the CSIS legislative changes can be considered constrained in the circumstances. "In the wake of last week's events, I feared they'd bring out all the more controversial legislation required," said Craig Forcese, a University of Ottawa law professor.

Anti-terror Legislation—Commentary

If you're so sure of C-51, debate it
National Post, Tom Mulcair, 2015 03 03

Op-ed. Justice Minister Peter MacKay is out of touch with reality when he pretends the official Opposition is on "the sidelines" of Bill C-51 ("Freedom and security, hand in hand," Feb. 28). In fact, New Democrats have been on the front line - leading the charge - opposing Conservative schemes to ram it through Parliament. And his government was really serious about security, they wouldn't shy away from meaningful study and debate of this sweeping new bill. The NDP knows that public safety is the priority of any government and we are not alone in our opposition to bill C-51. A growing list of eminent Canadians are adding their voices to the chorus of those saying the Conservatives' so-called anti-terror legislation goes too far. Four former prime ministers are concerned with the bill's broad measures: the privacy commissioner; an officer of Parliament; lacks the power and resources to provide oversight of C-51; and Canada's reputation is being tarnished as international media report the Conservative bill could open the door to human rights abuses. Last week, New Democrats were calling on the government to allow a full range of experts and Ontarians concerned about the bill to testify at committee in order to develop practical amendments that will strengthen oversight and protect Canadians' freedoms. Instead, the government decided to cut off debate and to play more politics that puts our freedoms at risk. The government wants to give CSIS a huge new mandate without improving its oversight. Minister MacKay says the best way to protect our fundamental freedoms is to rely on our independent judiciary. Regular attacks on Canada's courts when they don't rule in the government's favor show the Conservatives' disdain for an independent judiciary, but the issue here is that judges cannot be asked to replace the role of civilian oversight for our nation's security. It is also hard to understand why the minister would object to Canada's elected officials providing security oversight, when you consider how one of their appointments to head the Security Intelligence Review Committee is now sitting in a Panamanian jail. Note: Tom Mulcair is the leader of the Official Opposition and the NDP.

A simple fix to terror politics
Postmedia News, Michael Den Tandt, 2015 03 02

Column. There is a way for Canadian politicians to walk the line between the struggle against violent extremism on one hand, and dangerous bigotry on the other; and that is to declare war on extremism yet uphold the rights of minorities, in this context Muslims, with matching ferocity. It really is that simple. How odd that 13-plus years after 9/11, this lesson seems still somehow out of reach. It would be difficult to overstate the depth of revulsion the Islamic State of Iraq and al-Sham elicits from the average household; say, Ottawa, Ont., or Longueuil, Que. This is why recent polls show Prime Minister Stephen Harper's government enjoying a bounce in support, particularly in Quebec, as the Conservatives efficiently make this issue their own. In the war against ISIS, in which Canada has sent transport and surveillance aircraft, six F-18 fighter jets; and precisely 69 special forces soldiers, the Tories appear to have found a sweet spot of appealing combative while committing and risking little; certainly relative to the outcry of the Afghan mission. Bill C-51, the new antiterrorism law that last week passed second reading, seems of a piece with this strategy. Aside from the measures aimed at easing communication between federal agencies, and freeing the hands of the Canadian Security Intelligence Service, which are important changes, the law seems as much political goal as legislative document. The obvious explanation for C-51's lack of robust new oversight, in keeping with the security agencies' robust proposed new powers, is politics. Each time an intellectual beats about the perils of unfettered spys or intrusions on civil liberties, the Tories look like brass-knuckled defenders of public safety. They're betting...
the populace, whose interest in the detail of legislation is cursory at best, won't get much beyond their loathing for violent Islamism and the visceral feeling that it must be confronted and wiped out.

**What real oversight would look like**

National Post, Colin Kenny, 2015 03 02

Op-ed: If the Prime Minister thought public pressure to institute a more robust review system for national security would slowly die down, he has miscalculated. Recently, a number of former prime ministers and Supreme Court justices penned an open letter calling for the government to keep a closer eye on federal intelligence activities. While certainly increasing the viability of the issue, the letter was lacking as far as specific policy prescriptions. There are a number of concrete steps the government should take to address the gap in national security accountability. Chief among those are improving the integrity of the application process for national security warrants, re-establishing the Office of the Inspector General of the Canadian Security Intelligence Service, and expanding the Security Intelligence Review Committee’s (SIRC) size, capabilities and mandate. National security officials usually seek between 40 and 50 new warrants each year in addition to the 150 to 250 renewals or replacements. The prime minister argues that the involvement of federal court judges is a check on the bureaucracy. It may well be, but we should also note that the overwhelming majority of these warrant applications are approved. With CSIS now designating terrorist “sympathizers” as national security threats and the authority to make targeting decisions being delegated to lower level officials, the need for a balanced warrant application process is all the greater. Other observers believe that our warrant process is already too cumbersome. In 2005, I met with Baroness Eliza Manningham-Buller, the formidable director-general of MI-5, the United Kingdom’s Security Service, in her office on the Thames. At one point in the discussion, she held up a three-page form and said, “This is the document we use to obtain a warrant, not the bloody phone book your people require” (clearly a set up by CSIS). While procedures here may be more cumbersome than in the U.K., the importance of each warrant being vetted to ensure it meets the standards of the Charter is essential. Instituting these reforms would allow the committee to cover much more than the “snapshots” that they’re limited to now.

**Freedom and security, hand in hand**

National Post, Peter MacKay, 2015 02 26

OpEd: I reject the assertions of NDP leader Thomas Mulcair’s recent op-ed in the National Post (Canadians’ rights are at risk; Feb. 10). Now that Bill C-51, the Anti-Terrorism Act, 2015, has passed second reading in the House of Commons, I wish to provide a reality check to Mr. Mulcair’s continued opposition to these crucial anti-terrorism measures. The world has been shocked by recent atrocities perpetrated by jihadi terrorists. We have witnessed outrageous acts of violence by extremists who attack those that don’t share their narrow and oppressive ideologies. As a result, acts of terror have been carried out across Western nations, most recently in France, Belgium, Australia, Denmark and here at home in Canada. Today, we are part of a global struggle against this brutal extremism, including in the fight against ISIL. Mr. Mulcair has proposed that we ignore this fact by voting against the Anti-Terrorism Act. On many occasions, the excellent work of our national security agencies and police forces has foiled attempts to terrorize Canadians. Recent attacks in Saint-Jean-sur-Richelieu and on Parliament Hill in our nation’s capital have revealed that terrorism is evolving. Our government introduced the Anti-Terrorism Act to keep up with the ever-changing terror threat which confront us. The government’s focus is on serious threats to the security of Canada, such as espionage, sabotage and foreign influenced clandestine operations, as already outlined in the CSIS Act. Our security agencies are interested only in those who pose a serious threat to Canada’s security. Both Liberal leader Justin Trudeau and Mr. Mulcair have wrongly stated that the new powers granted to national security agencies tasked with protecting Canadians are not subject to proper oversight. They would rather see Canada’s national security oversight put in hands of politicians; however, the best way to protect the fundamental freedoms of Canadians is to rely on our independent judiciary. Such oversight is further strengthened by the Security Intelligence Review Committee (SIRC), which provides independent, expert, third-party advice regarding compliance with the law. (Note: Peter MacKay is the Minister of Justice and Attorney General of Canada.)

**Alarm bells must ring**

National Post, Conrad Black, 2015 02 28

Column: Bill C-51, the federal government’s Anti-Terrorism Act, 2015, is the principal official response to the increasing threat of terrorism, a phenomenon that infamously prompted into the central block of Parliament on Oct. 22, after the murder of a soldier ceremonially guarding the grave of the unknown soldier at the war memorial in Ottawa. The purpose of the measure is given as assurance that the people of Canada “live free from threats to their lives and their security,” as “there is no more fundamental role for government operators than protecting its country and its people.” To this end, government departments and agencies are authorized and instructed to share information that could frustrate or reveal attempts “to undermine” or “threaten the security of Canada;” the minister of Public Security and Emergency Preparedness compiles a list of people whom he or she “has reasonable grounds to suspect will attempt to threaten transport security” or commit or facilitate a “terrorism offence” in Canada or elsewhere. This sounds fairly innocuous by the standards of legislation conferring enhanced arbitrary powers on law-enforcement bodies, but, as usual and to some extent unavoidable, many of the elaborations of enhanced official powers are very broadly outlined. Reading through the text of this and related bills, the principal areas of impact are lowering the threshold for arrest, criminalizing the promotion of terrorism, conferring powers of disruption on CSIS (Canadian Security Intelligence Service), giving the power to remove designated terrorist material from the Internet, permitting court proceedings to be sealed while they are in progress for protection of investigative techniques, evidence, and personnel, expanding the government’s ability to stop people from leaving the country, and granting unspecified and scarcely limited powers of arbitrary, warrantless, detention.
Amend C-51 or Kill It
National Post, Multiple Authors, 2015 02 27
OpEd: The following is an abridged version of a letter addressed to all members of Parliament regarding Bill C-51, signed by more than 100 Canadian professors of law and related disciplines. The full text, together with the full list of signatories, is available at: (wp.me) Dear Members of Parliament, We write to express our deep concern that Bill C-51 (which the government is calling the Anti-terrorism Act, 2015) is a dangerous piece of legislation in terms of its potential impacts on the rule of law, on constitutionally and internationally protected rights, and on the health of Canada’s democracy. We believe that terrorism must be countered only in ways that are fully consistent with core values (that include liberty, non-discrimination, and the rule of law) but also in ways that are evidence-based and likely to be effective. In that respect, Bill C-51 may turn out to be ineffective in countering terrorism by virtue of what is omitted from the bill, and actually counter-productive in that it could easily get in the way of effective policing, intelligence-gathering and prosecutorial activity. Bill C-51 would allow CSIS to move from its current intelligence-gathering and associated surveillance with respect to a broad area of “national security” matters – to being a totally different kind of agency that can actively intervene to disrupt activities through a potentially infinite range of unspecified measures, as long as a given measure falls shy of causing bodily harm, infringing on sexual integrity or obstructing justice. The CSIS Act already defines “threats to the security of Canada” so broadly that CSIS has subjected various environmental and Aboriginal movements to its scrutiny; now, they can also be subject to disruption “measures.” That is to say, this new disruption power goes well beyond anything that has any connection at all to “terrorism” precisely because CSIS’s mandate in the CSIS Act goes far beyond a concern only with terrorism. Further, C-51 turns judges into agents of the executive branch (here, CSIS) to pre-authorize violations of Canadian law and, even, to pre-authorize infringements of almost any Charter right as long as the limits in C-51 – bodily harm, sexual integrity and obstruction of justice – are not crossed. C-51’s new disruption-warrant regime creates the potential for CSIS behaviour to undermine both the investigation and the prosecution of criminal cases by interfering with the evidentiary trail, contaminating evidence, and so on. Thus, we urge all Parliamentarians to ensure that C-51 not be enacted in anything resembling its present form. Yours truly, (Note: Stephen Coughlan, professor of criminal law, Schulich School of Law, Dalhousie University Fannie Lafontaine, associate professor and Canada Research Chair on International Criminal Justice and Human Rights, Faculty of Law, Laval University Audrey MacKinnon, professor and chair in human rights law, Faculty of Law, University of Toronto Steven Penney, professor, Faculty of Law, University of Alberta Donald Stuart, professor, Faculty of Law, Queen’s University François Turgeon-Renaud, associate professor and director of the Jack Mac Namara Centre on Transnational Human Rights, Crime and Security, Osgoode Hall Law School, York University Reg Whitaker, distinguished research professor emeritus, York University; adjunct professor of political science, University of Victoria; And 105 others)

Security reforms raise questions on human rights
Ottawa Citizen, Alex Neve, 2015 02 26
Op-ed: There is so much packed into the government’s current national-security law reform, it is hard to know where to focus. Bills C-44 and C-51, currently before Parliament, constitute the most substantial and controversial overhaul of Canada’s national-security landscape since the 2001 terrorist attacks. The weeks to come will see much debate about the human rights consequences of CSIS’s unprecedented new powers to act to reduce security threats and to apply for Federal Court warrants authorizing Charter violations as part of that process. There will be discussion of the vagueness of the new criminal offence of advocating or promoting the commission of terrorism offences in general and the certainy that this will both intrude on and chill free expression in the country. Indigenous peoples, environmental activists, human rights campaigners and others will worry that the new measures protect only “lawful advocacy, dissent and protest,” an intentional narrowing from current laws that recognize that protests that are not lawful in the sense of having a city hall permit are nonetheless not criminal, are protected under the charter and should not, by any twisted interpretation, be lumped in with terrorism. Bill C-44 and Bill C-51 both establish that CSIS can be active outside Canada, a dramatic departure from the agency’s mandate, which has always been limited to operating within the country. Bill C-44 opens that up with respect to investigating threats to Canada’s security. Bill C-51 extends that authorization to act outside of Canada to new powers for CSIS to disrupt and reduce threats to Canada’s security.

The anti-terror bill is a work in progress
National Post, Wayne Easter, 2015 02 25
Letters: After the deadly attacks on military officers in Quebec and on Parliament Hill in October, we must consider how best to protect Canadians from modern terrorist threats while safeguarding our values. Although the government’s new anti-terrorism legislation, Bill C-51, takes some proper steps in that direction, it will need fixing. The Liberal Party is well aware of the tough issues and sensitivities involved. We will support C-54 because of measures that will help keep Canadians safe: making better use of notify lists, building on the powers of preventive arrest and allowing more coordinated information sharing in government. Beyond laws, there are real worries this government is not providing enough resources to the task. Our existing review body for the Canadian spy agency, CSIS, has raised doubts about its capacity after the government left vacancies on its board open for years. We must ensure our security services have what they need to do their jobs, without depriving them of resources in other areas – especially in light of recent budget cuts. It is not enough for government to simply say “trust us.” That trust must be earned. It must be checked and it must be renewed.

Don’t sacrifice liberty for security
Toronto Star, Errol P. Mendes, 2015 02 25
Op-ed: Four former Canadian prime ministers (including a Conservative) and five former Supreme Court justices have warned Conservative Prime Minister Stephen Harper that protecting the security of
Canadians and their most important freedoms is not a zero-sum game. In their own words criticizing anti-terrorism legislation, Bill C-51, they warn, “Protecting human rights and protecting public safety are complementary objectives, but experience has shown that serious human rights abuses can occur in the name of maintaining national security.” Harper has already said he will ignore this historically unprecedented collective advice, even though it warns that key security agency review bodies will not have enough power to provide critical oversight of new government security activities. (Contrast That with name of maintaining “rational security.” Harper has already said he will ignore this historically unprecedented collective advice, even though it warns that key security agency review bodies will not have limited powers of review but will not be able to oversee the vastly enhanced powers CSIS will have under C-51. Note: Errol Mendes is a professor of constitutional and international law at the University of Ottawa.

**Oversight call is broader**

**Toronto Star, Frances Lankin, 2015 02 23**

Letter to the editor: PM rejects call for more spy agency oversight Feb. 20 As one of the 22 signatories to the letter from four former Canadian prime ministers speaking out about the urgent need for robust oversight and effective review of national security activities in Canada, I feel compelled to clarify the characterization of our concerns in this article. We did not make a specific call for the “the establishment of a committee of elected officials that would oversee CSIS’s exercise of its proposed new mandate.” Our concerns are much wider than that. This is a vital point that should not be lost in the current debate. We do, yes, highlight the essential role of Parliament when it comes to national security oversight, but that is in a wide sense, not just of CSIS’s new mandate. What we very crucially highlight in our call is the critical need for expert and independent inter-agency review of national security activities in Canada, along the lines of Justice Dennis O’Connor’s proposal from his 2006 Arar inquiry report. Frances Lankin, Member, Security Intelligence Review Committee (2009-2014).

**Terror’s limits**

**Globe and Mail, Hugh Segal, 2015 02 20**

Commentary: As Parliament debates Bill C-51, the new anti-terrorism legislation, and the oversight issue is justifiably raised, there is a bill in the Senate — S-220 — that affords all sides an opportunity to make progress. On Security Makes Canadians Safer — Feb. 19; S-220, which I proposed last spring, seconded by then-senator Roméo Dallaire, creates the kind of joint and bipartisan legislative oversight that mirrors what is used by the U.K., U.S. and France. It provides for in-camera hearings, regular review of the plans, approaches and budgets of security agencies, and genuine statutory oversight by parliamentarians from both Houses. In the U.K., the committee of parliamentarians’ membership includes, among others, sitting MPs and lords who were former police chiefs, chiefs of the defence staff and home secretaries. In both Canadian houses, we have ample parliamentarians with constructive experience in defence, police and other areas. The U.K. approach, initiated some 20 years ago, has never resulted in a leak or security breach. Here, the notion that the Security Intelligence Review Committee’s retroactive, complaints-based approach to CSIS activity, or that relying on a retired judge and staff who report on the Communications Security Establishment is sufficient, is at the very least, wildly optimistic.

**Canadians’ rights are at risk**

**National Post, Tom Mulcair, 2015 02 19**

Op-ed: In recent months, horrific terrorist attacks have shocked the world and united Canadians. Mourning has brought us together and strengthened our resolve to defend our way of life against the enemies wanting to intimidate us and erode our freedoms. That’s the Canada that stood together in grief and defiance the day after the Parliament Hill shooting, pledging that violence would not — even for a day — halt the work of our democracy. Unfortunately, at a time when we need responsible approaches to protecting Canadian values and freedoms, Prime Minister Harper is playing politics and putting our freedoms at risk. Canadians are right to suspect the Harper government’s new anti-terrorism bill, C-51, is flawed. After careful review of this complex legislation and its negative impacts, the Official Opposition New Democrats will not support bill C-51. The Prime Minister is telling Canadians they need to choose between their security and their rights — that safety and freedom are mutually exclusive. Instead of putting forward concrete measures to make Canadians safer and protect our freedoms, Conservatives have put politics over principle and introduced a bill that is sweeping, dangerously vague, and likely ineffective. C-51 would give CSIS a huge new mandate to “disrupt” the activities of people or groups it believes to pose a threat. That sounds OK, but the Minister for Public Safety and his officials refuse or are unable to describe what activities this new mandate covers, while experts are concerned it could turn legal dissent and protest together with actual terrorism. There are already serious deficiencies in oversight of CSIS. The last report from the under-resourced Security Intelligence Review Committee found that CSIS had “seriously misled” the Committee in one investigation, and that the Committee faced “difficulties” and “significant delays” obtaining information about the spy agency’s activities. This is on top of the Harper Government’s decision to eliminate the Office of the CSIS Inspector General in 2012, which further weakened oversight. With these serious shortcomings it is irresponsible to give an agency such sweeping new powers without enhancing oversight to make certain freedom doesn’t hang in the balance. Note: NDP leader Tom Mulcair is Canada’s leader of the Official Opposition.
A close eye on security makes Canadians safer

Globe and Mail, Jean Chretien, Joe Clark, Paul Martin and John Turner, 2015 02 19

In our four us, we most certainly know the enormity of the responsibility of keeping Canada safe, something always front of mind for a prime minister. We have come together with 18 other Canadians who have served as Supreme Court of Canada justices, ministers of justice and of public safety, solicitors-general, members of the Security and Intelligence Review Committee and commissioners responsible for overseeing the RCMP and upholding privacy laws. Among us, we have served in various public office roles from 1966 to 2014. Over that time we were faced with, and responded to, a range of pressing security concerns. We all agree that protecting public safety is one of government’s most important functions and that Canada’s national security agencies play a vital role in meeting that responsibility. Yet we all also share the view that the lack of a robust and integrated accountability regime for Canada’s national security agencies makes it difficult to meaningfully assess the efficacy and legality of Canada’s national security activities. This poses serious problems for public safety and for human rights. A detailed blueprint for the creation of an integrated review system was set out almost a decade ago by Justice Dennis O’Connor in his recommendations from the Maher Arar inquiry, which looked into the role that Canada’s national security agencies played in the rendition and torture of a Canadian citizen. Justice O’Connor’s recommendations, however, have not been implemented, nor have repeated calls from review bodies for expanded authority to conduct cross-agency reviews. Meanwhile, efforts to enhance parliamentary oversight of national security agencies have also been unsuccessful. For example, in October, 2004, a report calling for parliamentary oversight over national security activities was presented to the minister of public safety. This report contained an oversight structure that was agreed upon by representatives of all parties in both the House of Commons and the Senate.

Beyond the law, The bill that would authorize intelligence agents to act

National Post, Kent Roach and Craig Forcese, 2015 02 18

Op-ed: In this excerpt from their latest “background for” document (see the full text at www.antiterrorlaw.ca) on Bill C-51, the Anti-Terrorism Act 2015, the authors focus on the new powers the bill would grant the Canadian Security Intelligence Service (CSIS). If Bill C-51 passes, CSIS will be expressly authorized to “take measures, within or outside Canada, to reduce” very broadly defined “threats to the security of Canada.” Where authorized by Federal Court warrant, these “measures” may “contravene a right or freedom guaranteed by the Canadian Charter of Rights and Freedoms” or may be “contrary to other Canadian law.” The CSIS changes are dramatic, even radical, In 1984, parliamentarians granted CSIS a very broad mandate—found in the definition of “threat to the security of Canada” in s.2 of its Act— but were careful to accord it very limited powers. It has been an intelligence service... It collects and analyzes information and supplies assessments to the government. When enacted, Parliament accepted CSIS’s broad mandate because it lacked what we will call in this discussion “kinetic” or physical powers—the powers to do things to people in the physical world (except as necessary to, for example, install a wiretap or listening device). Note: Kent Roach teaches at the University of Toronto law faculty and worked with both the Arar and Air India commissions. Craig Forcese is a law professor teaching national security law at the University of Ottawa and a participant in the Canadian Network for Research on Terrorism, Security and Society.

CSIS-Bill C-51 moves us closer to end of privacy

Toronto Star, Kent Roach and Craig Forcese, 2015 02 18

Op-ed: The new information-sharing law in Bill C-51 will relax constraints on the flow of information between government agencies about “activities that undermine the security of Canada.” This change has not received as much attention as have other features of the bill. This is unfortunate because, as with other features of Bill C-51, this proposed law is not balanced. “Big data” technology enables incredibly detailed and potentially intrusive monitoring and scrutiny of people’s behavior. Law stands as the bulwark against the end of privacy, and this bill makes the law weaker. Recent events raise real concerns about terrorism, and there may be a case for increased information sharing. The Air India Commission even recommended mandatory sharing by CSIS to prevent another such attack. So information sharing is required. But it must be reasonable in its scope and be countered with effective review to ensure that the information shared is reliable and respects privacy. Note: Craig Forcese and Kent Roach teach national security at the Universities of Ottawa and Toronto respectively and Roach worked with both the Arar and Air India commissions. They have posted detailed legal analyses of Bill C-51 at antiterrorlaw.ca.

Parliament must reject the anti-terror bill

Globe and Mail, Ed Broadbent and Roy Romanow, 2015 02 12

Op-ed: We are writing to add our voices to the rising chorus of opposition to Bill C-51, Prime Minister Stephen Harper’s draft legislation extending the powers of Canada’s intelligence agency. This bill should be withdrawn, or defeated in Parliament. Terrorism is designed to provoke governments into making damaging mistakes. It is conducted through brutality and rooted in the belief that killing ordinary citizens will cause nations to abandon their most basic commitments. Terrorism demands a sustained and effective response. Resources must be allocated to enable police and intelligence agencies to find its perpetrators and root it out. Those who are guilty of offenses must then be brought to justice. Canada already has mechanisms, practices and laws necessary for dealing with terrorism. These include surveillance, immigration controls, preventive detention and incarceration for criminal activity. As we have recently seen, our system of national security is not perfect. But this is not due to inadequacies in our security legislation. It is the result of overworked and underfunded police and security services. The bill attacks the civil rights of all Canadians, and places the protections guaranteed by the Charter of Rights and Freedoms under the shadow of wider powers to interfere with lawful and legitimate conduct. The general tenor of the bill is to expand the definition of threats to national security and add to the powers of the Canadian Security Intelligence Service. Note: Ed Broadbent is chair of the Broadbent Institute.
Institute and former president of Rights and Democracy, Roy Romanow is former premier of Saskatchewan and previously served as a member of the Security and Intelligence Review Committee.

Ottawa’s anti-terror, corruption crackdowns show the problem with rushing in

CBC News, Brian Stewart. 2015 02 10

Analysis: The federal government has recently taken two strong initiatives linked to the troubled state of the world – one designed to counter potential corruption and bribery by Canadian firms abroad, the other to confront the jihadi threat at home. Both are meant, at least in part, to toughen up Canada’s image in the world and both have stirred up considerable opposition among those who think Prime Minister Stephen Harper is expanding government powers too far. That opposition, mind you, is vastly different. One is made up of the nation’s corporate elite, the other is the civil liberties crowd, backed by at least some of the opposition parties in Parliament. It will be interesting to see which has the most muscle in Harper’s often populist Ottawa. Personally, I’d bet on the boardrooms. Already, corporate Canada looks to have pushed the government into revising its tough new anti-corruption rules, which were rushed into place in 2013 and then much strengthened by Public Works and Public Safety Canada without serious consultation with those firms actually trading overseas. While bribery and corruption is considered almost the norm in many part of the world, lawyers are now warning their Canadian clients that the risk of any impropriety in seeking a foreign contract is just too high now. Indeed, the RCMP is currently said to be pursuing at least 35 significant cases of bribery abroad. What particularly flab board rooms was the new initiative to ban companies, including foreign ones, from selling any products or services to the Canadian government for a full decade if, at any time in the last 10 years, they or even their foreign affiliates were found guilty of having bribed abroad. This cast a net so wide that five global giants have been snagged, including Hewlett Packard, Siemens and BAE Systems. In fact, it has been the fierce protests over these big-name cases that seem to have moved Ottawa to start streaming its regulations. Canadian companies are warning of potentially billions of dollars in lost contracts when our important trading partners, furious over their firms being barred for competing for Canadian contracts, launch some sort of tit-for-tat retaliation.

 Freedoms lost

Globe and Mail, Steven Blaney. 2015 02 05

Letter to the editor: Re Stephen Harper’s Secret Policeman Bill (editorial, Feb. 2): The international jihadi movement has declared war on Canada. Canadians are being targeted by jihadi terrorists simply because they hate our society and the values it represents. These threats require a strong response. That is why our government has put forward measures, such as the Anti-Terrorism Act, which protect Canadians against jihadi terrorists who seek to destroy the very principles that make Canada the best country in the world to live. As the Prime Minister said, our government rejects the argument that every time we talk about security, our freedoms are threatened. Canadians understand that their freedom and security go hand in hand and expect us to protect both. There are protections in this legislation to do exactly that. CSIS is not becoming a secret police force. The key powers of this new legislation are subject to judicial review and judicial authorization. In addition, a highly respected law school deanship was appointed to the existing oversight body last Friday. Providing CSIS with new tools will ensure that gaps in snaring serious consultation with those firms actually trading overseas. While bribery and corruption is considered almost the norm in many part of the world, lawyers are now warning their Canadian clients that the risk of any impropriety in seeking a foreign contract is just too high now. Indeed, the RCMP is currently said to be pursuing at least 35 significant cases of bribery abroad. What particularly flab board rooms was the new initiative to ban companies, including foreign ones, from selling any products or services to the Canadian government for a full decade if, at any time in the last 10 years, they or even their foreign affiliates were found guilty of having bribed abroad. This cast a net so wide that five global giants have been snagged, including Hewlett Packard, Siemens and BAE Systems. In fact, it has been the fierce protests over these big-name cases that seem to have moved Ottawa to start streaming its regulations. Canadian companies are warning of potentially billions of dollars in lost contracts when our important trading partners, furious over their firms being barred for competing for Canadian contracts, launch some sort of tit-for-tat retaliation.

 Harpers got spy powers right, but civilian oversight very wrong

Globe and Mail, Bob Rae. 2015 02 04

Op ed: Sometimes Stephen Harper is his own worst enemy. Recent events in Europe should bring home to all of us that there are indeed people in the midst of democratic, multicultural societies who are ready and willing to kill others in the pursuit of their religious and political beliefs. They are terrorists. They plot and communicate with others of a similar mind, and with similar intentions. They receive encouragement, and sometimes even instructions, from foreign entities and governments. Canada is not somehow magically aloof from these realities. Our large cities are the home of millions of people from all over the world. There is no foreign conflict that does not have a direct influence on the lives and feelings of many Canadian citizens and, indeed, there are events and proposals in Canada itself to which some in Canada are strongly and irrevocably opposed. Whether these feelings give rise to a direct threat to the lives of their fellow Canadians is a matter of fact and evidence. But it would be simply foolish to argue that such threats could never happen here. On June 23, 1985, a plane which had left Toronto for London carrying more than 300 people was blown up in mid-air off the southwestern coast of Ireland. They were Canadians, killed by their fellow Canadians. The bomb that killed them was made in Canada. The plot to make the bomb was hatched in Canada. It was the largest civilian bombing of its kind at the time. The record maintained until the attacks on the World Trade Centre on Sept. 11, 2001, CSIS and the RCMP had been recently split up in the wake of the Macdonald Inquiry, and the record will clearly show that their risk assessment and post-bombing investigation of the Air India attack were marred by competing rivalries, poor judgment, bad execution, and simple negligence. An exhaustive inquiry by Justice John Major some 26 years after the incident fully explored the issues and made recommendations to ensure we learn from the mistakes. I wrote a shorter report for the government on Air India calling for the broader review and judicial authorization. In addition, a highly respected law school deanship was appointed to the existing oversight body last Friday. Providing CSIS with new tools will ensure that gaps in sharing information about suspected terrorists do not limit its ability to prevent attacks on Canadians. Steven Blaney. Minister of Public Safety and Emergency Preparedness.

 Putting CSIS surveillance on a firmer legal footing

National Post, Kent Roach & Craig Forcese, 2014 10 29

Opinion: On Monday, the government tabled the “Prevention of Access to Terrorist Information Act.” Comprised mostly of amendments to the Canadian Security Intelligence Service’s law, the bill might be more accurately named the “Filling Gaps Identified in Recent Court Cases Act.” Bill C-44 clarifies CSIS’s powers. Controversial anti-terrorism changes, such as preventive detention and speech offences,
potentially await another bill. The bill rolls back a 2008 Federal Court decision questioning CSIS's authority to investigate people outside of Canada. This decision — a surprise to many — sparked various workarounds. Later condemned in a 2013 Federal Court decision, the new bill puts surveillance outside Canada on a clear legal footing. This is a reasonable fix in a globalized security environment. Indeed, the bill is diplomatically courageous. It tasks a court with authorizing overseas surveillance, even if doing so would violate foreign state law. This frank willingness to violate state sovereignty may discomfort diplomats. But in our legal system, such international implications alone do not serve to render the stipulated power unlawful. There do, however, remain outstanding issues. When CSIS investigates abroad, the risks of misconduct, including complicity in human rights violations, increase. That behaviour would raise legal issues. And in its 2013 decision, the Federal Court clearly had this prospect (and the infamous case of Maher Arar) in mind when it criticized CSIS for existing foreign intelligence agencies in monitoring Canadians abroad. The presiding judge learned of this co-operation not because CSIS told him. He connected the dots by reading reports from reviewers of CSIS and CSE (Communications Security Establishment Canada), the country's signals intelligence agency — two review agencies that still cannot conduct close joint investigations with secret information. (Karm Roach is a 2013 Trudeau Fellow, former director of research for the Air India Commission and a law professor at the University of Toronto. Craig Forcese is a law professor who teaches national security law at the University of Ottawa and is a participant in the Canadian Network for Research on Terrorism, Security and Society.)

Selected (non-terror legislation) Service reports

Spies expelled to U.S. were not Americans

Toronto Star, Michelle Shephard and Tonda MacCharles, 2015 03 04

Ottawa - A report that five spies were thrown out of Canada and sent back to the U.S. ruffled diplomatic feathers Tuesday, prompting Public Safety Minister Steven Blaney to confirm that the individuals were not American agents. "All five of the suspected spies deported from Canada to the United States were cases of Canada returning to the United States someone who was suspected of spying against the United States," said Blaney's communications director Jean-Christophe de La Rue. No other details about the cases were provided. Figures revealed by the Star and La Presse Monday show that in the last decade, Ottawa has sent five people, out of a total of 21, who were barred from Canada to the U.S. Officials determined they were "inadmissible on security grounds for engaging in an act of espionage that is against Canada or that is contrary to Canada's interests." The release of the previously undisclosed statistics compiled by the Canadian Border Services Agency — and provided to the newspapers under the Access to Information Act — led to speculation that Americans were spying on their northern neighbours. Efforts to clarify the information with the CBSA, the U.S. embassy, former American ambassadors, diplomats and government officials prior to Monday's report were unsuccessful, as none would provide any details on the cases. Michel Coulombe, the director of the Canadian Security Intelligence Service, has often warned in public statements about espionage, noting in 2014 that foreign spies show a particular interest in Canada's nuclear, aerospace and oil sectors. "Our industrial capabilities, rich natural resources and access to key allies make Canada an attractive target for hostile actors." Coulombe said. "What is new, however, is the sheer breadth of today's targets and the use of cyber attacks, which are efficient, cost-effective and most importantly, deniable, providing anonymity for their perpetrators."

CSIS warns government of homegrown online anti-Islam threat

Canadian Press, Jim Bronskill, 2015 03 04

Ottawa - Canada's spy agency is eying the threat of a homegrown anti-Islam movement spreading online. The Canadian Security Intelligence Service advised the office of Public Safety Minister Steven Blaney of its concerns during a secret September briefing. CSIS flagged well-known warnings of the persistent menace posed by terrorist groups al-Qaeda, Hezbollah and the more violent and radical Islamic State of Iraq and the Levant, or ISIL, in notes obtained through the Access to Information Act. But under the heading Domestic Extremism, the spy service also underscored what might be the flip side of that coin: the recent development "of a Canadian online anti-Islam movement, similar to ones in Europe." CSIS characterized it as an "ongoing risk, particularly as its proponents advocate violence."

This Sept. 18 briefing for Blaney's office came a little more than a month before soldiers were killed in Canadian attacks just two days apart — murders committed by young man that authorities say were motivated by Islamic extremism. Lorre Dawson, a University of Waterloo sociology professor and co-director of the Canadian Network for Research on Terrorism, Security and Society, Dawson suspects CSIS is motivated by the horrific July 2011 slaughter of 77 people in Norway by Anders Behring Breivik, who penned a manifesto outlining his far-right ideology, including an extreme anti-Muslim outlook. CSIS spokesman Tahera Malik did not respond to requests for comment.

« On se voit comme des parents de terroristes » - le père d'un jeune parti en Syrie

Radio-Canada - Nouvelles, Karine Bastien; 2015 03 04

Montréal - Révélons, parce que tu me manques beaucoup. Je voudrais qu'il revienne. Je ne veux pas le perdre. Je garde toujours un espoir quelque part. Je n'arrive pas à y croire... Peut-être que c'est un cauchemar, je vais me réveiller, c'est un rêve pourtant c'est la réalité. Je ne veux pas que mon fils embarque dans quoi que ce soit. C'est une merde, dévastateur, qui entoure ce message à mon fils, qui souffre d'avoir réparti, avec cinq autres jeunes Québécois, les combattants islamistes en Syrie. Ni elle ni son man n'en reviennent encore. Ils se sont confiés à Anne Marie Dussault, de 24/60, et à notre journaliste Karine Bastien. Leurs fils est parti le vendredi 16 janvier dernier avec 500 $ en poche. Il a pris
l'avion à l'aéroport de Montréal pour la Turquie, point de passage répété pour la Syrie. Il venait d'avoir 18 ans.

Terrorism survey: 50% of Canadians feel less safe than 2 years ago
CBC News. Staff reporter, 2015 03 04
Nearly half of Canadians say they feel less safe from terrorism than they did two years ago, according to a survey conducted for CBC News. Two-thirds say it is likely that an attack will occur in Canada within the next five years, including 32 per cent who expect that it will result in mass death and destruction. However, only nine per cent think terrorism and national security should be the top priority for federal politicians, behind unemployment (20 per cent), the economy (19 per cent) and health care (15 per cent). "People aren't hysterical about terrorism. They're still focused on the things that do affect them directly on a daily basis, which is the economy and jobs and health care," said Craig Warden, executive vice-president of public affairs at Pollara Strategic Insights. "But terrorism is there." Although two-thirds said they were concerned about a terror attack in Canada, the issue trailed several others in the survey, including the economy (89 per cent), health care (87 per cent), jobs and unemployment (61 per cent), the value of the dollar (78 per cent), the environment (75 per cent), oil prices (70 per cent) and housing prices (68 per cent). Nearly a third of respondents said the ability of a party and its leader to prepare and respond to a terror attack would be a major factor in the upcoming federal election, with only 15 per cent saying it won't be a factor at all.

The spies next door
Toronto Star, Tonda MacCharles, 2015 03 03
Ottawa - New figures show Canada has turfed out five spies in the past decade from a surprising source - its closest ally and partner, the United States. From 2004 to 2014 Ottawa sent back to the U.S. five of a total of 21 of those barred from Canada "on security grounds for engaging in an act of espionage that is against Canada's interests," according to a document produced by Canada Border Services Agency. It's not clear if five espionage cases was by foreign government agents or if it was industrial espionage - that is, spying to obtain state secrets, intellectual property or corporate secrets. A document released under access to information laws shows the suspected spies were permanent residents or foreign nationals deemed inadmissible on security grounds, but don't break them down by citizenship. Rather, it indicates the country the spies were sent back to. Still, the fact that the U.S. is the origin of the most espionage cases is surprising, especially given the emphasis put by federal politicians - including two former CSIS directors, one of whom is now national security adviser to Prime Minister Stephen Harper - on China as a suspected source of espionage. In a joint project, the Toronto Star and La Presse sought further information from CBSA, the U.S. embassy, former American ambassadors, former diplomats and Canadian officials, but none shed any light on the specifics of any case. "We have been concerned with espionage," CSIS director Michel Coulombe told a Senate committee last month. "Our industrial capabilities, rich natural resources and access to key allies make Canada an attractive target for hostile actors. What is new, however, is the sheer breadth of today's targets and the use of cyber attacks, which are efficient, cost-effective and most importantly, deniable, providing anonymity for their perpetrators.

Le directeur du SGRS inquiet
Le Presses, Josée Bellevue, William Leduc, 2015 03 03
Ottawa - Dans un témoignage qu'il a livré devant un comité du Sénat en février 2014, le directeur du Service canadien du renseignement de sécurité (SCRS), Michel Coulombe, exprimait son inquiétude au sujet de l'espionnage sur le sol canadien. Il relevait aussi que l'espionnage évoluait rapidement et prenait maintenant la forme de cyberattaques menées à partir d'ordinateurs à l'étranger. "Nous nous préoccupons depuis longtemps de l'espionnage. Le Canada constitue une cible attrayante en raison de ses moyens industriels, de ses vastes ressources naturelles et de son accès aux ressorts d'alliés importants. Ce qui est nouveau, c'est l'ampleur des cibles actuelles et le recours aux cyberattaques, qui sont efficaces et rentables et qui, surtout, peuvent être démentis et permettre à leurs auteurs de rester anonymes," a-t-il affirmé durant son témoignage.

Timmins, Ont.-born jihadist recruited 6 others for ISIS
CBC News. Staff reporter, 2015 03 03
Inspired by Andrea Paulin's apparent charisma and his message, five Toronto men followed him to Syria and ultimately into the arms of ISIS. CBC News has learned. Paulin, from Timmins, Ont., converted to Islam and went by the name Abu Muslim. He joined the jihadist fight in Syria in 2012, in the process creating an 11-minute propaganda video for ISIS aimed at Westerners. He died while fighting in northern Syria in the summer of 2013 at the age of 24. CBC News has learned that Paulin also had a direct role in recruiting at least five young Muslim men from the Toronto area to go to Syria. Four were rescued by family members before they could cross over from neighbouring Lebanon, but at least three appear to have returned there to join ISIS. The first was Abu Turaab. His real name is Mohammed Ali. He left Canada in April 2014, eight months after Paulin was killed. His father enlisted an imam to talk sense into him. CBC News has learned. But the imam told CBC News that Abu Turaab was already determined to join ISIS. What's surprising is that Abu Turaab and Paulin were friends on a popular online forum called Ummah.com as far back as 2009. Abdul Malik's father and the mother of another told CBC News that CSIS agents and the RCMP officers interviewed the four returnees several times after they came back.

Muslim leader blasts decision to close his schools in Montreal
The Toronto Star, Alan Woods, 2015 02 28
Montreal - It will take more than tougher anti-terrorism laws to prevent young people from joining the ranks of the Islamic State and other extremist groups, says a Montreal Muslim leader once accused of...
being a sleeper agent for Al Qaeda. Adil Charkaoui was branded a terror threat by the federal government and fought his forced removal from Canada from 2003 until accusations that he was a national security threat were dropped in 2009. He is now a Canadian citizen. But Charkaoui was pulled back into the news with reports this week about six young Quebecers - four young men and two women - who fled the country last month on a flight bound for Turkey. They were reportedly bound for Syria and the ranks of the Islamic State group. One of the young men, Bilal Zouaida, enrolled in a weekend youth group that is run by Charkaoui out of two Montreal schools. After learning that the young man had enrolled last fall, the schools suspended their rental agreements with the youth group, even though Zouaida had attended only two sessions before dropping out. In a news conference, Charkaoui said he was "stunned" by the decision, which school officials said was based on the discovery of a video they characterized as containing "hateful" speech. Charkaoui said he encouraged young people to integrate and go to school while offering them outlets for their frustrations over what he called "Islamophobia" by taking part in events such as protests, petitions and volunteer work. The father of Zouaida told Montreal's La Presse that he had confiscated his 18-year-old son's passport last year, fearing that he might be planning to leave the country. The young man reported his travel documents as stolen to the police and applied for a new passport without raising any red flags. "How did CSIS, the RCMP, how did nobody see anything and he could have another passport so easily to fly to Turkey?" Charkaoui said "I was really surprised."

**Canadian spy agency collects Canadian emails to government sites**

CBC.ca Ken Hanly 2015 02 27

Ottawa - Canada's Communications Security Establishment (CSE) is collecting millions of emails sent by Canadians to government sites on the internet. The collected emails are searched for malware that could attack government computer networks. A top secret document obtained by the CBC and the US news site The Intercept revealed details about the collection of emails. The document is from 2010. It is among the documents obtained from NSA whistle blower Edward Snowden. The Communications Security Establishment (CSE) is Canada's cryptologic agency. It is responsible for foreign signals intelligence (SIGINT) and also for protection of government electronic and communication networks. Recently a new headquarters was built for the agency at a cost of $1.1 billion making it the largest government facility ever built. This no doubt shows the priority of the Canadian Conservative government. Many who support the government constantly coin pie in of government spending but when it comes to national security matters efficiency and control of costs do not seem to count. The facilities are on 83 acres and the headquarters occupy 1.2 million square feet. It is next door to the broader spy agency Canadian Security Intelligence Service (CSIS). The CSE collected about 400,000 emails sent to government sites each day. Some of the data was stored for years. I expect that the agency thinks that some day it might be useful to mine the data for specific purpose. The numbers collected have probably grown considerably since 2010 assuming the process is still ongoing.

**Poursuite d'adil Charkaoui Ottawa engloui sous les documents**

Le Presse, Vincent Larouche 2015 02 27

Ottawa - Le gouvernement fédéral et les services secrets ont été engloutis par une montagne de travail. Lorsque le litige opposant Adil Charkaoui aux services de sécurité était jugé, c'est comme si le tribunal n'existait plus. Seulement un des documents perdus ont été retrouvés. Une communication entre deux agents des services secrets a été interrompue. Ils se sont promis de vous diriger vers un chemin alternatif. Toutefois, le litige était réglé.

**Six Montreal students suspected of travelling to Middle East join Islamic State**

Globe and Mail, Lea Perreault & Daniel Le Blanc 2015 02 27

Montreal & Ottawa - Four young men and two women who disappeared from the Montreal region have travelled to the Middle East to fight with Islamic State, authorities believe, triggering scrutiny of a Muslim teacher once accused of his own terror links. While the Canadian Security Intelligence Service says up to 145 Canadians have gone abroad to join terror groups, including an estimated 40 who have joined Islamic State, the addition of six would-be fighters at once represents a stunning new level of recruitment in Canada. Until now, most known recruitment has involved loners or in rare cases groups of two or three at most. At least four of the young people attended classes taught there in rented space by Adil Charkaoui, a Montreal Islamic centre who spent six years under security certificates after police alleged he was an Al Qaeda sleeper agent. Courts quashed the certificates in 2009.

**Six québécois manquent à l'appel**

Le Presse, Vincent Larouche 2015 02 26

Montréal - Six jeunes Québécois, dont certains fréquentaient le collège de Maisonneuve, auraient gagné la Turquie dans la but probable de rejoindre des groupes djihadistes en Syrie. Le père s'est rendu sur place. «Comme un papa fou, juste pour voir qu'il fréquentait, dit-il. Il a décidé d'intégrer à son fils d'y retourner, notamment parce qu'il savait que le litige opposant Adil Charkaoui aux services de renseignement canadiens, Service canadien du renseignement de sécurité (SCRS), n'est toujours pas réglé.

**RCMP red-flagged Alnalki after 9/11, despite doubts**

Ottawa Citizen, Andrew Duffy 2015 02 28
Ottawa - Newly released documents show that an RCMP national security team described Ottawa's Abd al-Rahman Almalki as an imminent threat and an "important member" of al-Qaeda to foreign agencies even as investigators expressed serious doubts about the veracity of those claims. Other documents reveal that the RCMP team, despite its misgivings, shared details of Almalki's international travel plans with the U.S. Central Intelligence Agency in December 2001, during the highly charged aftermath of 9/11. "The available information clearly confirms the intent of Canadian investigators in sharing the travel information was, if possible, to arrange for or assist in his detention before he could return to Canada," Almalki's lawyers charge in a written submission to the Federal Court of Canada. The new documents have been released to Almalki's legal team as part of the disclosure process in his $100-million civil suit against federal officials for his detention and torture in Syria. Almalki, a Carleton University graduate and father of six, spent 22 months in Syrian custody after his arrest at the Damascus airport in May 2002. He has never been charged with a crime in Canada. A federal inquiry has already found that Almalki was inaccurately labelled by the RCMP in letters to foreign intelligence agencies. The new documents disclosed by the RCMP officers, in labelling Almalki an imminent threat, also ignored evidence to the contrary. An RCMP memo, dated Sept. 5, 2001, generated after a meeting with Canadian Security Intelligence Service officials, said that "CSIS have not uncovered information that would lead them to believe the subject (Almalki) is doing something illegal." An RCMP memo, dated Nov. 15, 2001, said there were "no indications that Almalki is in fact a procurement officer for the Bin Laden organization and were often quite careful to characterize him as an alleged or suspected procurement officer," it noted.

Spy cables: Israel airline used as intelligence 'front' (Canada).

Al Jazeera, Rahul Radhakrishnan. Will Jordan, 2015 02 25

Doha - Secret cables obtained by Al Jazeera's Investigative Unit confirm that South Africa's spy agencies concurred with allegations that Israel uses its flag-carrier El Al Airlines, as cover for its intelligence agencies. Leaked documents from South Africa's intelligence agency support claims made on a 2009 South African television programme by a former El Al employee-turned-whistleblower. Despite official Israeli denials, the whistleblower's claims prompted an emergency meeting between senior officials from both sides, as well as a separate rate of inquiry from Canada's intelligence agency. The Spy Cables also reveal that Canada's intelligence agency had written to the SAA and asked for "any findings or information" on Israel using the airline as "a front for clandestine operations," promising to treat such information "in strict confidence."

Leak reveals spies chase more activists than terrorists

Globe and Mail, Geoffrey York, 2015 02 25

Johannesburg - Despite popular belief that they are chasing terrorists and master criminals, the world's spy agencies spend much of their time pursuing environmentalists, opposition leaders, dissidents and even airline staff, leaked documents show. The intelligence agencies, including Canadian spies, are interested in civilian targets that go far beyond terrorism, according to the latest batch of South African intelligence agency reports, leaked to Al Jazeera. Many spy agencies are more preoccupied with political activism than with terrorism, the reports show. One document revealed that the Canadian Security Intelligence Service (CSIS) was strongly interested in whether the Israeli airline El Al might have any gun-toting Israeli spies among its staff in international airports. It questioned whether El Al staff might have illegally obtained firearms.

ISIS recruited Canadian woman to join fight in Syria

CBC News. Natalie Clancy, 2015 02 25

The family of a young Canadian woman who travelled to Syria after being radicalized say losing her was the most "shocking thing in the world" and that they wish ISIS had done more to prevent the 23-year-old's departure. The woman, whom CBC News is calling Aisha to protect her identity, made the journey to Syria to join up with ISIS last summer, after taking an online course to study the Quran taught by a woman based in Edmonton, says her older sister Rabia (whose name has also been changed). "We all went to work, came home, all her stuff was gone. She had packed all her winter clothes, took her computer and left," Rabia says. "It was the most devastating, most scary, most shocking thing in the world." Over the past several months, Rabia has been speaking to CBC News about her family's ordeal. Some details, such as names and the family's location, are being withheld for security reasons. The Canadian Security Intelligence Service declined to comment on the specific case, but said in an emailed statement that terrorism "including radicalization of Canadians and terrorist travel remains the most prominent threat to Canadian interests and our national security." Rabia alleges Aisha was recruited under the guise of an online class to study the Quran taught by a woman in Edmonton. But instead, Rabia says, Aisha learned how to get to the ISIS-controlled city of Raqqa in Syria. CBC News has confirmed the identity of the woman in Edmonton and that she was asked to leave a mosque after she attempted to recruit people. She has not been charged in connection with this case.

Al-Shabaab threat against West Edmonton Mall 'high risk,' security expert says

CBC News. Staff reporter, 2015 02 24

Edmonton - A video that appears to be of the West Edmonton Mall as a possible target by the al-Qaeda-linked terrorist group Al-Shabaab "is a very serious threat" that could impact other Canadian shopping centres, says a former senior intelligence officer with the Canadian Security Intelligence Service. In the 7-minute video posted online over the weekend, a masked member of the extremist group appeal to followers to attack shopping malls across North America and Europe. Edmonton police say they are working closely with RCMP and West Edmonton Mall security to ensure necessary precautions are being made. Deputy police Chief Brian Simpson said Sunday: "This was a very general comment ... it wasn't a
specific threat." But Michel Juneau-Katsuya, formerly with CSIS, said that is precisely what makes the threat more dangerous. He said CSIS and RCMP will closely monitor communications and links between Canadians and al-Shabaab.

**Les services secrets ont supprimé en douce la prime au bilinguisme**

La Presse, Vincent Larouche avec William Leduc, 2015 02 24

Ottawa - Présidée de réduire leurs dépenses par le gouvernement Harper, les services secrets canadiens craignaient d'avoir à geler les salaires ou réduire les effectifs ces dernières années, mais ils ont finalement trouvé une autre façon d'économiser : supprimer la prime au bilinguisme qui avait été gagnée après une décade de lutte par les espions francophones, principalement issus du Québec. C'est ce que révèle une note interne du Service canadien du renseignement de sécurité (SCRS), obtenue par La Presse en vertu de la Loi sur l'accès à l'information. L'organisme d'enquête fédéral est présentement au cœur de la stratégie antiterroriste du gouvernement, qui propose d'ailleurs d'élargir ses pouvoirs.

**Watch for Islamist infiltration, blogger tells Senate inquiry**

Ottawa Citizen, Dylan Robertson, 2015 02 24

Ottawa - Canada needs to ensure radical Islamists don't infiltrate law enforcement institutions, a controversial blogger told a Senate committee Monday. Marc Lebuis has tracked radical Islam in Canada on his blog, Pont de Bascule, since 2010. With the help of roughly 10 people, Lebuis documents both famous and strong links between Muslim leaders and radical groups. "Leading influential Islamist leaders have specifically targeted Canada," Lebuis told the Senate national security committee, noting that Islamist groups abroad have called on their supporters in the West to join police forces and spy agencies.

Lebuis gave numerous examples of prominent Muslims in Canada whom he said supported Islamist groups, such as a prominent scholar of Islam who suggested Muslim judges in secular countries could use their power to make verdicts that favoured the principles of Sharia law. He also took aim at remarks senior CSIS official Michael Peirce gave to the same committee last October, when Peirce discussed "individuals whose activities may be associated with a particular institution, but it's the individuals we investigate. For instance, we don't investigate mosques." Lebuis said that was misguided. "This decision by CSIS neglects to take into account the pivotal role of the mosque, as it is understood by the Islamists themselves, and ignores the numerous documented cases of radical discourses preached in mosques reported in recent years and weeks," he said.

**DND, CSIS, RCMP unable to spend $11 billion of their budgets since 2007**

Canadian Press, Murray Brewster, 2016 02 20

Ottawa - New figures show the country's three major national security institutions were collectively unable to spend $11 billion of their budgets over the last eight years. The statistics on lapse funds at National Defence, the Canadian Security Intelligence Service and the RCMP were presented today at the annual Conference of Defence Associations Institute meeting, which also heard a renewed warnings that the military is on the verge of a major equipment rust out. The numbers stand in contrast to the rosy assessment of the Harper government's defence spending record as presented by Jason Kenney, the newly appointed minister. Kenney dismissed the argument over lapse funding, saying all departments do it as part of the normal budget process, an explanation the government used last year when it revealed Veterans Affairs gave back $13.1 billion in unspent casting. "Every department lapses funds every year. And they always have, and they always will," Kenney told reporters. "Departments don't blow out their budgets. That's irresponsible fiscal management. Departments submit budgets always with a little margin for error on the high side and they always have carry forward provision. National Defence has lapsed $3.7 billion since 2007. The RCMP has handed back $1.7 billion and CSIS was unable to spend $180 million.

**CSIS-RCMP express alarm over "anti-petroleum" ideologists**

Globe and Mail, Shawn McCarthy, 2015 02 17

Ottawa - The RCMP has labelled the "anti-petroleum" movement as a growing and violent threat to Canada's security, raising fears among environmentalists that they face increased surveillance, and possibly worse, under the Conservative government's new terrorism legislation. "There is a growing, highly organized and well-financed anti-Canada petroleum movement that consists of peaceful activists, militants and violent extremists who are opposed to society's reliance on fossil fuels," concludes the report, which is stamped "protected/Canadian eyes only" and is dated Jan. 24, 2014. The report was obtained by Global News. The government has tabled Bill C-51, which provides greater power to the security agencies to collect information on and disrupt the activities of suspected terrorist groups. While Prime Minister Stephen Harper has identified the threat as violent extremists motivated by radical Islamic views, the legislation would also expand the ability of government agencies to infiltrate environmental groups on the suspicion that they are promoting civil disobedience or other criminal acts to oppose resource projects. A spokeswoman for Public Safety Canada said Bill C-51 does not change the definition of what constitutes a threat to Canadian security, and added CSIS does not investigate lawful dissent. "CSIS has a good track record of distinguishing genuine threats to the security of Canada from other activities," Public Safety Canada's Joséphine Stois said. "The independent reports of the Security Intelligence Review Committee attest to CSIS's compliance with the law."

**CSIS documents reveal how agency designates terrorism targets**

The Globe and Mail (Online edition), Colin Frease, 2015 02 12

Toronto - When Canada's spies designate someone as a "target" of a terrorism probe, they input that information with one of four labels - "terrorist," "extremist," "supporter" and "sympathizer." From there, the spy service determines whether the target is a Level One or Level Two threat. Only the latter can be put under the surveillance of bugging devices or paid informants. Newly released documents provide details on the targeting methodology now being used by Canadian Security Intelligence Service, the secretive...
agency that's about to be given new enforcement powers through legislation, CSIS spokeswoman Tahera Muffi replied with the following statement on Wednesday: CSIS developed a lexicon of common terms and definitions to guide and ensure accuracy in its descriptions of individuals in information exchanges with domestic and foreign partners. This effort was informed in part by observations by Commissions of Inquiry and the use of the lexicon's terminology can in no way be equaled by "casting a wider net". It also does not alter the threshold or the Service requiring reasonable grounds to suspect an individual's activities pose a threat to national security before launching an investigation—a threshold which the Service has dutifully respected for 30 years. As indicated in the ATIP related documents, the internal audit found that the Service's targeting activities were carried out in compliance with the CSIS Act, Ministerial Directives and Service targeting policy.

Ottawa arrests fit typical network size

Ottawa Citizen, Dylan Robertson, 2015 02 04

Ottawa - The RCMP allegations against a group of Ottawa men - if true - are similar to what has been seen elsewhere with small groups of radicalized Canadians who pursue violence. "What often seems like a lone wolf (plot) or attack is often much more of a network-kind-of-cluster than what we initially imagined,” said Amarath Amarasingam, who is studying Canadian extremists who are fighting abroad. Amarasingam, a post-doctoral student at the Dalhousie University Resilience Research Centre, says it's uncommon in Canada and other countries to see people go abroad with terrorist groups without direct encouragement from others. "These tend to happen organically: it's not like someone's orchestrating the whole thing,” said Amarasingam, who says most groups don’t exceed eight people because they would then become difficult to co-opt. “Usually you’ll have a charismatic leader within the cluster who's leading the ideological leanings, and maybe a facilitator who is going to pay for their flight or that kind of thing, and then the cohort or people who are inspired to do the work.” Amarasingam said the main challenge for police is proving someone has radicalized others. "That kind of link is quite difficult to establish legally. That’s why a lot of these kinds of arrests take a lot of time because you have to establish an evidentiary basis for this arrest. Mubin Sheikh, a former CSIS and RCMP counter-terrorism operative who is studying radicalization, said society needs a multi-pronged approach to terrorism, from tracking financial contributions to terrorist groups, to letting people know who to contact when they meet people contemplating violent actions. "We're so fixated on the individuals. (But) if you really want to deal with this problem, you have to go to the networks that give them logistical support," said Sheikh.

Preventing radicalization a key in terrorism fight, Imam tells senators

Canadian Press, Jim Bronskill, 2015 02 03

Ottawa - Canadians must work harder to prevent young people from becoming radicalized instead of simply dealing with the aftermath, says an Ottawa imam. That's the basic task of stepping vulnerable people away from extremism, Zijad Delic told the Senate national security committee Monday. Instead, the focus is on trying to deradicalize them after the fact. Political leaders, social services, teachers and others need to "find ways of tackling" the lure of extremism, Delic said. Last fall, the RCMP said it had some 83 active security investigations on 90 suspected extremists who intended to join fights abroad or who had returned to Canada. The federal government has since introduced two bills aimed at reinforcing or expanding the ability of Canadian security agencies to investigate and deter terrorist threats. Legislation tabled last Friday would give the Canadian Security Intelligence Service powers to actively disrupt threats, not just collect information about them. It would also make it easier for police to control the movements of terrorist suspects and to detain them longer without warrant. Opposition MPs and civil liberties advocates expressed concern Monday the bill did not boost oversight of Canada's spy agency concerns the Conservative government quickly dismissed.

Identifying the new face of terror

Montreal Gazette, Geoffrey Vendeville, 2015 01 31

Montreal - There was no telling how or when he might hurt someone. In St-Jean-sur-Richelieu, Martin Couture-Rouleau - a 25-year-old radicalized convert to Islam - chose the morning of Monday, Oct. 20, to blow his gold-beige 2000 Nissan Altima into two Canadian Armed Forces members. Warrant Officer Patrick Vincent died of his injuries the next day. Two days later, another radicalized convert, 32-year-old Michael Zehaf-Bibeau, picked 9:32 a.m. to shoot and kill Cpl. Nathan Cirillo, a sentry at Ottawa's National War Memorial, before storming Parliament Hill. Both men acted alone, without the normal backing of a terrorist organization. And both men were from Quebec. Couture-Rouleau seemed to be aspure lone wolf as they come. By all appearances, the suicidal attacks were unrelated. As Canadians reeled from the events, our police forces were wondering what, if anything, they could have done to prevent the killings. Young, radicalized lone operators who view civilian targets have raised new challenges for security forces around the world (www.politico.com/magazine/story/2015/01/paris-terrorism-114507.html ). The attacks in Canada last fall - followed by a deadly hostage taking in Sydney in December, and the coordinated raids on the Charlie Hebdo office and a Jewish supermarket in Paris in January - have fueled a debate on whether law enforcement should be given more powers and resources to cope with the evolving face of terrorism. On Friday, the Harper government announced an anti-terrorism bill that would, among other things, give the Canadian Security and Intelligence Service (CSIS) the power to intervene to disrupt terrorist activities. Since it was founded in 1884, CSIS has been a civilian agency that gathers intelligence which it then hands off to the RCMP. But can such new measures, which also include increased powers to restrict the movements of suspected jihadists, actually stop a lone wolf hiding in plain sight?

Blaney defends high-flying CSIS boss

Global News, Mike Le Couteur, 2015 01 28

Ottawa - Public Safety Minister Steven Blaney is standing by the spending habits of one of his top bureaucrats, a day after it was revealed the director of CSIS spent tens of thousands on travel and hotels
in his first year on the job, asked about the Global News story, Blaney said, "We expect all agencies to abide by the Treasury Board (guidelines), and I believe all are doing so." In a statement, CSIS spokesperson Tahera Mufti said, "Everything we do in fulfilling our mandate to protect Canada's national security interests is done in a manner of utmost professionalism."

Hamilton man to get hearing on CSIS on "intimidation" case
CBC News, Adam Carter, 2016 01 24
Hamilton - A Hamilton activist finally has a hearing date for a complaint lodged against the country's security watchdog after CSIS agents visited his home - but neither he nor his lawyer will ever get to see the evidence in the case. Ken Stone alleges agents from the Canadian Security Intelligence Service (CSIS) visited his house to "intimidate" him in 2013. Stone has long been a vocal labour and anti-war advocate, and says the agents asked him about an op-ed he wrote in the Hamilton Spectator titled "Harper is wrong in demonizing Iran." He also visited Iran to attend a conference on Palestinian human rights in 2011. After the visit, Stone made a formal complaint to the The Security Intelligence Review Committee (SIRC), a board of political appointees that examines CSIS's operations. Hearing dates for March 26 and 27 were set during a Thursday morning conference call between lawyers on both sides and officials. But Stone also found out that SIRC has requested what's called an "ex-parte hearing," which means that they get to present evidence in camera - so no one in the public (like Stone and his lawyer) gets to see or hear it.

Women leave Montreal, join ISIS
QMI Agency, Andrew McIntosh & Felix Seguin, 2015 01 24
Montreal - Two Montreal women, ages 18 and 19, were reported missing by their families in November and Canadian authorities believe they have joined Islamic State (ISIS) in Syria. Police fear the women have become "slaves" of jihadist fighters, said Insp. André-Guy Lamotte of the Montreal police anti-terrorism unit. "There were signs of radicalization," he said. "Unfortunately, we lost them: they've already arrived there. They'll be used as slaves for the people there." Lamotte wouldn't say exactly where he believes they went. Both Montrealers are considered high-risk travellers and are being investigated by Canada's Integrated National Security Enforcement Teams, a source close to the investigation told QMI Agency. The two women are friends. The Criminal Code bars any Canadian from joining terrorist groups such as ISIS or providing money or assistance of any kind. At the request of police, QMI Agency isn't revealing the women's names to prevent others in their inner circle from becoming radicalized. Police say they have a close relationship with the grieving families. A CSIS agent told QMI that 10% to 15% of young people who leave their families to join ISIS are women. "Radicalization used to take three, four or five years," the agent said. "Now we're talking about months." He recalled holding sobbing parents in his arms after informing them that their children left to fight with terrorists. Last fall, the head of Canada's spy agency said authorities are monitoring 80 suspected Canadian terrorists who have returned home from violent hot spots around the world. Montreal police officials discussed the foreign fighter problem this week at a special training session on terrorism and radicalization. The session, organized by the RCMP, also included Quebec provincial police and intelligence agents. About 100 officers received the training.

Le SCRS débordé par les cas de voyageurs à haut risque
Journal de Montréal, Andrew McIntosh, 2015 01 23
Montréal - Un agent du renseignement canadien a déclaré cette semaine que la majorité des effectifs du Service canadien du renseignement de sécurité (SCRS) à Montréal enquêtent présentement sur des cas de voyageurs à haut risque. Après avoir été radicalisés, ceux-ci cherchent à quitter le pays pour se joindre au groupe Etat islamique (EI) ou à d'autres groupes terroristes comme Al-Qaïda. « Notre but, c'est de les détecter. C'est à la GRC de les attraper ou de faire inculper des suspects. »

Canada Spies Seen as Biggest Obstacle In BlackBerry Bid
Bloomberg News, Theophilos Argiropoulos, 2015 01 18
Ottawa - Canada's spies may be the biggest obstacle to any sale of BlackBerry Ltd. (BB) A foreign acquisition of the Canadian smartphone maker would trigger a national security review, largely by a secret committee of senior officials that includes the heads of two spy agencies. The committee would determine whether Canada can trust the buyer with government communication. "The government has shown interest in national security in telecoms" and information technology, said James Musgrove, co-chair of the competition practice at law firm McMillan LLP in Toronto. "I expect they would show a very high degree of interest in this transaction. "Questions over whether the federal government would allow a foreign takeover of BlackBerry resurfaced yesterday after Reuters reported Samsung Electronics Co had proposed a potential acquisition. Both BlackBerry and Samsung denied the report, sending the stock down 20 percent today in Toronto, erasing most of the gains from a day earlier. The Canadian Security Intelligence Service warned in 2012 that some foreign state-owned enterprises may represent a threat to national security. Later that year, Canada banned state-owned enterprises from acquiring businesses in the nation's oil sands outside of "exceptional circumstances," after approving Beijing-based Cnooc Ltd.'s (883) purchase of Nexen Inc. of Calgary. At the time, the government said it would also "carefully monitor" transactions involving foreign state-owned firms throughout the economy.

Returning jihadists under close watch
National Post, Stewart Bell, 2015 01 10
Ottawa - Ahmad Waseem's return to Windsor, Ont., in 2013 posed a problem for Canadian national security authorities. As a suspected jihadist fighter, with a battle wound to prove it, was he a threat to Canadians? How should they handle him? The 26-year-old solved the problem himself when he disappeared only to resurface in Syria where he remains, occasionally posting selfies and jihadist propaganda on social media under several aliases, most recently Muhanna Al Kanadi. Dozens of other
jihadist veterans are scattered across Canada, and following this week's attack in Paris by brothers who had reportedly returned to France from Yemen and Syria, the government is almost certainly re-examining the threat they pose. They range from Farhad Kamel, the former leader of a North African extremist cell who returned to Montreal after serving a jail sentence in France, to Hiva Aligazadeh, a Winnipeg man who trained in Afghanistan and swore allegiance to al-Qaida. "The government is aware of about 80 individuals who have returned to Canada after travel abroad for a variety of suspected terrorism-related purposes," according to a report released by Public Safety Canada in August. Testifying before the Public Safety and National Security Committee on Oct. 9, CSIS director Michel Coulombe said not all of the 80 veterans who had returned to Canada were hardened fighters. But he said "all of them could potentially be a threat, definitely." Another 130 are believed to be active outside in Canada in Islamist extremist violence, including about 30 in Syria and Iraq. Canadians fighting in the conflict have said in online posts they had no intention of ever returning home, but circumstances change.

New security adviser has street cred
Ottawa Citizen, Jan MacLeod, 2015 01 08

Ottawa - The prime minister's new national security adviser warned a long time ago about lone attackers such as Michael Zehaf-Bibeau and extremists such as those who carried out Wednesday's massacre in Paris. That may be one reason Stephen Harper has chosen Richard Fadden, deputy minister at National Defence, as his right-hand man on domestic and international security threats. The scope and complexity of the problem seems to worsen daily. Fadden certainly has the street cred for the job. When al-Qaida attacked in New York and Washington in 2001, Fadden was the Privy Council Office's intelligence and security coordinator, an earlier version of the powerful national security job he's now taking on. Thirteen years later, when Zehaf-Bibeau stormed Parliament Hill on Oct. 22, Fadden was meeting across the street at the Privy Council Office with then-national security adviser Stephen Rigby, Canadian Security Intelligence Service (CSIS) director Michel Coulombe, and chief of defence staff Gen. Tom Lawson. In between those tragedies as Canada's spymaster, he served five years as Canada's spy chief. He was the first CSIS director to have direct interaction - and a leadership role - in the intelligence alliance with the United States, Britain, Australia and New Zealand, known as the five eyes. His new posting signals that Canada takes national security - including budgets, capabilities and leadership - seriously, says Ray Bosivert, former assistant director of intelligence at CSIS. Fadden, who officially becomes the national security adviser on Jan. 19, is said to have a strong sense of how Canada's and allied intelligence networks connect and intersect. Improving collaboration within Canada's security and intelligence establishment will likely be a priority for him, say experts.

Arbitrator upholds spy's firing
QMI Agency, Andrew McIntosh, 2015 01 06

Montreal - Canada's spy agency was right to dismiss a junior spy assigned to fight Hezbollah terrorists in Quebec, a federal arbitrator has ruled. The recent decision by arbitrator René Paulit lifts the veil on a little-known aspect of CSIS operations. The Public Service Labour Relations Board recently backed CSIS boss Michel Coulombe in his decision to terminate Marc-André Bergeron. CSIS fired the Montreal recruit in October 2007, three months before the end of his probationary period. His termination letter, signed by Coulombe and obtained by QMI Agency, shows Bergeron was in training at the time. Coulombe said Bergeron had not demonstrated "the aptitudes" to be a spy, the letter reads. All CSIS recruits are in training and on probation for five years before they can gain permanency. The probation is mentioned in all CSIS job postings. Bergeron had no comment to QMI Agency. In a letter to CSIS, and in court documents, he claims to have been the victim of a petty and manipulative supervisor. "The burden of this surprising and extreme decision was, and remains, very heavy on my personal and professional life."

CSIS bill doesn't settle 'important issue' around warrants: government
Canadian Press, Jim Bronskill, 2014 12 17

Ottawa - The federal government says it still needs guidance from the Supreme Court of Canada on overseas spying even though it has introduced legislation to clarify foreign intelligence-gathering powers. In a new filing with the high court, the government argues its recently tabled bill doesn't overtake the high-profile issue of whether the Canadian Security Intelligence Service needs a warrant to seek allied help in spying on Canadians abroad. It even draws parallels with the politically charged Airbus affair of the 1990s in making the case for greater certainty. The government is urging the Supreme Court to hear the global spying case, saying a lower court ruling has left CSIS "in the dark" about when a judge's approval is needed to monitor suspected Canadian extremists in other countries. But Gordon Cameron, an Ottawa lawyer appointed to probe the federal arguments, says the high court shouldn't bother with the case because the federal bill could make the central issue moot. The legislation, introduced in late October, would explicitly allow CSIS to seek a warrant to investigate a security threat beyond Canada's borders, something the government flags as a pressing concern as a number of young Canadians travel to train and fight with terrorist groups abroad. In a key 2011 ruling, Federal Court Justice Richard Mosley chastised CSIS over a request for warrants to track two Canadians with help from the Communications Security Establishment, Canada's electronic spy agency. Mosley said CSIS breached its duty of candour by failing to disclose that CSE's foreign counterparts in the Five Eyes intelligence network, in the United States, Britain, Australia and New Zealand could be called upon to assist. He also warned that CSIS and CSE were incurring the risk Canadian targets "may be detained or otherwise harmed" as a result of foreign agencies' use of the intercepted communications.

Broke jihadis turn to Internet to get ticket to war zone
QMI Agency, Andrew McIntosh, 2014 12 15

Montreal - Some Canadians intent on joining ISIS have taken to the web to raise cash. The turn to crowdsourcing has netted potential terrorists as much as $10,000 each. It's a worrying trend, according to Michael Peake, a deputy director at the Canadian Security Intelligence Service (CSIS). Peake recently
necessarily direct the full purpose of raising funds," he said. "Again, they might do it under the cover of
reach six figures. They obscure where the money will actually be going, Peirce explained. "They won't
raised issue while testifying before the Senate's standing committee on national security and defence.
"When we're talking about individuals, for instance, individuals who are raising money for terrorist
purposes and, I don't think Canada, they can be relatively moderate sums, up to $10,000," he told the committee.
While that figure is what can be expected for an individual, the amount that an organization can raise can
reach six figures. They obscure where the money will actually be going, Peirce explained. "They won't
necessarily direct the full purpose of raising funds," he said. "Again, they might do it under the cover of
humanitarian aid," but others say that there is no evidence that this is a widespread phenomenon.

Canada's extremist problem
Maclean's Magazine, Michael Petrou, 2014 12 12

Analysis: "I was one of you. I was a typical Canadian," John Maguire says in a recent propaganda video
released by Islamic State, a jihadist group that controls large chunks of Syria and Iraq. In it, he stands in
front of a shattered building and holds an assault rifle. "I grew up on the hockey rink, and spent my
teenage years on stage playing guitar," Maguire is not so typical anymore, but nor is he unique. The
Ottawa-area man, identified in the video as Abu Anwar al-Canada, is one of about 150 Canadians the
Canadian Security Intelligence Service (CSIS) says are now fighting with banned terrorist groups
divides. Maguire urges his fellow Muslims to join Islamic State, or attack other Canadians at home.
"You either pack your bags, or prepare your explosives devices," he says in the video. "You either
purchase your airline ticket, or sharpen your knife." Public Safety Minister Steven Blaney says Canada
has revoked Maguire's passport. While Canadians who are not dual nationals cannot have their
citizenship revoked for terrorism-related offences, losing his passport may mean that Maguire will never
make it back to Canada. But, according to CSIS, 60 Canadians who joined banned terrorist groups
overseas have now safely returned. Canadian law makes it a criminal offence to join such groups. But
collecting evidence and building a case can be difficult. Of the more than 200 Canadians CSIS says have
been involved with banned groups abroad, including those who have returned to Canada, only one,
Hasibullah Yusufzai, of Burnaby, B.C., has been charged with a terrorism offence. (A second Canadian
who traveled to Syria has been charged with passport fraud.) CSIS director Michel Coulombe told a
House of Commons committee the returnees took part in "terrorist-related activities." The RCMP says
they "pose a significant security threat" to Canada. And yet the vast majority, it appears, will never be
criminally charged. What to do with such individuals is an increasingly pressing challenge for Canada,
and other countries around the world, as hundreds of foreigners flock to Syria and Iraq to join Islamic
State. Keeping all returnees under constant surveillance consumes massive amounts of time and
resources. Ignoring them is risky. Some Western countries are experimenting with a different option:
decriminalization.

Ottawa refuse la torture, mais pas son produit
Le Devoir, Hélène Buzetti, 2014 12 12

Ottawa - Malgré le rapport du Sénat américain, Steven Blaney souhaite que le Service canadien du
renseignement de sécurité (SCRS) considère toutes les informations qui pourraient sauver la vie de
Canadiens Le gouvernement conservateur n'a visiblement tâché aucune enquête sur l'utilisation ...
... d'eau. Ottawa estime qu'il est encore approprié que les forces de l'ordre canadiennes utilisent des informations... obtenues sous le tortue s'il s'agit de sauver des vies.

CIA torture report: Why Canada can't claim innocence
CBC News, Andre Mayer, 2014 12 11

Canadian agents may not have physically participated in CIA torture tactics, but Stephen Harper's claim
that Canada played no role whatsoever misrepresents our relationship with U.S. spies, say a number of
security analysts. "It gives us a good conscience" to be able to deny participation in torture, but "it doesn't
take away the fact that we're as guilty as them," says Michel Juma-Katsuya, a former senior intelligence
officer with CSIS, the Canadian Security Intelligence Service. Stephen Harper reffulls call to rescind
federal torture directives? U.S. Senate report condemns CIA harsh interrogations? As Juma-Katsuya
sees it, Canada's spy agencies have a tremendously close relationship with the CIA and probably had a
pretty good idea how the intelligence was generated. Adds security expert Wesley Wark. "When Prime
Minister Harper says it's an American problem with an American issue with no Canadian ramifications,
that's not really accurate - or oversimplified on any number of fronts. The committee found not only that
CIA interrogators had used "brutal" tactics, such as waterboarding, sleep deprivation and rectal feeding to
obtain intelligence from suspected terrorists, but that the intelligence itself was largely unreliable.

California Senator Dianne Feinstein, the committee chairwoman, said, "Under any common meaning of
the term, CIA detainee were tortured" and that the program was "a stain on our values and on our history." The
report contained at least three references to Canadians involved in extremist activity, including a
mention of "al-Qaeda operative" Abderrazouq Siday, a Canadian citizen, and an FBI interview in which
another prominent suspect, Abu Zubaydah, alleges he sent a Canadian to meet with a Malaysian al-
Qaeda member. Speaking in the House of Commons yesterday, Prime Minister Stephen Harper
dismissed the idea that the Canadian intelligence community was in any way implicated in the report.
"This is a report of the United States Senate," Harper said. "It has nothing to do whatsoever with the
government of Canada." Senate intelligence committee chair Dianne Feinstein called interrogation tactics
the CIA used on terror suspects between 2002 and 2009 "a stain on our values and on our history." A
statement released by the office of Public Safety Minister Stephen Blaney said.

Overseas CSIS surveillance case 'not appropriate' for Supreme Court: lawyer
Canadian Press, Jim Bronskill, 2014 12 02

Ottawa - A lawyer appointed to probe federal arguments about the legality of tracking Canadian terror
suspects overseas says the Supreme Court of Canada should reject the government's plea to hear
the matter. Ottawa lawyer Gordon Cameron - the amicus curiae, or friend of the high court - says in a written
the Supreme Court to hear the case. saying the Canadian Security Intelligence Service has been left - in
Federal lawyers say lower oaurtg made “Significant errors” in dealing with the sensitive matter. in a key
2013 ruling- federal CDurt Justice Richard Mosley criticized CSIS over a request fix warrants to track two
Canadians with technical help from the Communications $ounty Establishment. Canada’s electronic spy
counterparts in the Fire Eyes intelligence network - the United States, Britain, Australia and New Zealand
submission it is “not en-
- could be called upon to help. He also warned that CSIS and CSE were incurring the risk that Canadian
targets “may be detained or otherwise harmed” as a result of the use of the intercepted communications
by foreign agencies. The Federal Court of Appeal upheld Mosley’s judgment in a ruling made public last
month. The Court of Appeal declared that a warrant is required when CSIS - either directly or through the
suspects of a foreign spy service - use “intuitive” methods such as interception of telecommunications.
It said such warrants could be issued when the interception “is lawful where it occurs.” Federal lawyers,
however, said they had many questions about what the appeal court meant.

Concerns raised about accountability as Canada’s spy agency takes on more overseas missions
Postmedia News. Douglas Quan, 2014 12 01
When Canada formed a civilian Intelligence agency in the mid- 1960s, it sparked fears that its members
would run amok across Canada with unchecked power. As it celebrates its 30th anniversary, the
Canadian Security Intelligence Service is being dogged by similar concerns — but this time it’s in the
context of its rapidly expanding overseas missions and “we go where the threat is” mantra. CSIS was
created strictly as a domestic security intelligence agency, but some industry observers say it has been
taking on operations more akin to the activities of a foreign intelligence service. They are worried about
the lack of oversight related to its overseas missions and propose that Canada should follow the lead of
its G-7 partners by creating a separate. dedicated foreign intelligence agency, such as the United States’
CIA or Britain’s MI6. "What we are doing is pretending that the skill set for domestic and foreign
intelligence are the same... and offering nothing in the way of appropriate internal and external
accountability,” said Wesley Wark, a national security expert and visiting research professor at the
University of Ottawa. CSIS director Michel Coulombe alluded to the spy agency’s shifting priorities and
expanding “global footprint” in a speech to refined employees earlier this summer. "In that new
environment, we go where the threat is. We do more foreign operations and joint operations than ever
before, and these are complex operations than ever before," he said, according to a copy of his
speech obtained by Postmedia News through access-to-information laws. Asked to elaborate on his
remarks, CSIS spokeswoman Tahera Mufti said there is no question that the agency’s foreign role has
expanded, but she insisted that its operations are consistent with its mandate to collect information
pertaining to threats to Canada. Alan Jones, a retired assistant director at CSIS, agreed. "You cannot
defend Canada in isolation," he said. "Sometimes CSIS operators must have an on-the-ground presence
outside the country to complete an intelligence collection task." What agents are not in the business of doing is collecting
information about the activities of other states — that’s the role of a foreign intelligence agency, he said.
And there is currently no appetite to turn CSIS into such an agency. Craig Forcese, a terrorism expert and
taxi professor at the University of Ottawa, said he’s not convinced a separate agency is needed given that
it would fill the “narrowest of niches” not currently occupied by CSIS: the Communications Security
Establishment (which intercepts foreign electronic communications) and intelligence arms of the
Department of Foreign Affairs. That said, Forcese agrees that the Canadian security sector needs to “go
back to the drawing board” and reconceive how it conducts its affairs and how it is held accountable.

Disclosure of ‘sensitive’ telecom surveillance details worried feds: memo
Canadian Press, Jim Bronskill, 2014 12 01
Ottawa — A move by telecommunications firms to be more forthcoming with the public about their role in
call and spy surveillance could divulge “sensitive operational details,” a senior Public Safety official
warned in a classified memo. Company efforts to reveal more about police and intelligence requests even
discount detailed data on the numbers would force the public to see what is happening, the memo
warned. Lynda Clarmont, senior assistant deputy minister for national and cybersecurity, said the
department was not convinced that a separate agency is needed to protect the privacy of Canadians who have
been targeted by foreign spies. She said the public needs to be aware of what the government is doing.
Clarmont wrote in her April memo that the government needs to be more transparent about its
activities. The internal "Secret/Canadian Eyes Only." "We recognize that transparency is key to giving
Parliament and Canadians confidence in our ability to meet both these objectives, but must continue to
ensure that sensitive operational details remain protected."
STATEMENTS MADE DURING THE DEBATE OF BILL C-44

On January 28 and 30, Bill C-44 was debated at the Reporting and 3rd Reading Stages in the House of Commons. Members from the New Democratic Party expressed their lack of support for the Bill, while the Liberal Party of Canada expressed their support. Main criticisms from both opposition parties were that an increase in oversight of CSIS was required, that CSIS was not receiving adequate resources, and that there were sufficient offences in the Criminal Code to address terrorism that were not being applied by the RCMP, as CSIS is not an enforcement body. Below are notable quotes from that debate:

**Highlights from the Reporting Stage:**

**On CSIS resources and constitutionality of the Bill:** "I think the government is afraid of a couple of things that came up. One was that some expert witnesses said that some parts of this bill might be unconstitutional and that if those were declared unconstitutional by the courts we were wasting time here. The other issue we raised was this. Is the government providing sufficient resources to agencies like CSIS and the RCMP to make use of the tools they already have? The government is afraid of debating those two questions. I think that is why it is introducing time allocation." (Mr. Randall Garrison) (For responsive lines, please see Tabs 1E, 2B and 2G)

**On information sharing:** Mr. Speaker, the member is wrong. First, this bill is not addressing the police or the RCMP, but clarifying the role of our national security agency. It is to clarify and make sure that CSIS, our Canadian security service, continues to do what it has always done, which is to share information with our partners. This bill clarifies the role of the service and confirms its ability to operate abroad and, more specifically, and I want to repeat this, share information about and track people, potentially Canadians, who may have left the country for terrorist purposes. We will share this information with our partners and allies, such as the French. All nations throughout the world are bringing in measures in keeping with their constitutional framework in order to protect democracy. That is the purpose of this bill. (Steven Blaney) (For responsive lines, please see Tabs 1J, 2D and 2E)

**On numbers of foreign fighters:** If CSIS and others say that there are 140, we can bet that there are a whole lot more than that... Everything about 9/11 was there, but they just had not talked to each other. They just had not shared. I know that the same situation exists among Canada's security services, whether it is CSIS, CSFC, the DND, or the CRA. Those disconnects exist. I would like to ask the minister about the urgency and the timeliness that is required to connect those disconnects, because the clock is ticking. (Laurie Hawn) (For responsive lines, please see Tab 2I)

**On C-44 vs. C-51 and CSIS powers:** Mr. Speaker, those were great remarks by the Minister of Public Safety. The problem is that the remarks do not relate to Bill C-44, on which the government has introduced closure. The bill he is talking about sounds to me more like the bill that may be coming on Friday. This bill really does nothing to address the national security concerns that have been raised as a result of the Quebec activity, the incident in Ottawa, or what has happened in Paris. We expect that to be in a new bill. This bill basically brings into law some of the practices that CSIS is now utilizing and protects CSIS sources. (Wayne Easter) (For responsive lines, please see Tabs 1B and 2F)

**On operational accountability:** As things stand now, in fact, CSIS cannot legally conduct extraterritorial surveillance activities. This bill aims to correct that... The amendments we proposed were meant to make the director of CSIS accountable for secret surveillance activities conducted abroad. This will not be the case, because under the bill as it stands, an employee designated by the minister will be accountable for those activities. I would like to ask my colleague why it is not the director of CSIS who would be accountable for secret activities conducted abroad, and why a straw man should be chosen to do it instead? (Raymond Côté) (For responsive lines, please see Tabs 2A, 2C and 2E)
On legality of extraterritorial activities: Mr. Speaker, I would like to thank my colleague for his eloquent remarks and for enlightening us about this bill. With regard to CSIS’s activities abroad, various federal courts have already ruled that section 12 of the act does not contain extraterritorial provisions that cover covert surveillance. This issue has been brought before the courts on a number of occasions. It is troubling that, ultimately, CSIS is still conducting extraterritorial activities. Clearly, rather than remedying the situation by refining CSIS in the government is trying to condone such behaviour by amending the act and establishing such provisions. (Raymond Cote) (For responsive lines, please see Tab 1C)

C-44 Debate Highlights (3rd Reading):

On civil liberties and accountability: The sad thing about Bill C-44 and the pressure that the government is putting on (CSIS) is that the government would have us believe that giving CSIS more power is a good thing. It would be if the government also gave the agency the resources and tools it needs. However, unfortunately, the Conservatives decided to go it alone and did not hold the necessary consultations on Bill C-44. There has also been talk about a balance between public safety and civil liberties, something that we do not see at all in Bill C-44. I also think about the fact that the inspector general of CSIS position was scrapped, even though it was crucial to accountability at CSIS. That was an extremely important position that helped balance civil liberties and national security. (Rosane Doré Lefebvre) (For responsive lines, please see Tabs 1A, 2A, 2D)

On the use of public funds: In addition, we were disappointed to hear about some questionable spending (i.e., travel expenses), to say the least and to avoid unparliamentary language, by Michel Coulombe, the director of (CSIS). This kind of behaviour is unacceptable. The director of CSIS is spending more on himself right now than the Minister of Public Safety. It is totally unacceptable to see taxpayers’ money spent like that. What are we hearing from the Conservatives right now? Nothing, radio silence. They have no response when we ask what will happen next. Will the director of CSIS be reprimanded for misusing public funds? (Rosane Doré Lefebvre) (For responsive lines, please see Tabs 2A and 2B)

On legal opinions received and constitutionality: Bill C-44 affects not just CSIS, but also part of the Citizenship Act, which has nothing to do with what we are interested in here, namely the Canadian Security Intelligence Service. I asked the Conservative member who just spoke on Bill C-44 whether they had received legal opinions confirming that the bill is well and truly constitutional. He managed to evade the question just as well as the Minister of Public Safety and all the people who dealt with this bill. No one was able to offer any legal opinions to prove that this bill was constitutional. (Rosane Doré Lefebvre) (For responsive lines, please see Tabs 1F, 2A, 2B)

On existing legislation: The government must explain why it is not using existing legislation and the relevant provisions of the Criminal Code. (Wayne Easter) (For responsive lines, please see Tab 1F)

On legalizing that which is illegal: With the latest bill, we would increase the powers of Canada’s spy agency. We are offering it up as another international body to engage in espionage and spy on other countries. We are asking our intelligence service to open up the opportunity to spy on other countries, to disregard the laws that other countries might have toward their citizens and pursue our intelligence system in that regard. We are taking a step to a more confrontational approach to other nations based on one single perceived threat of ISIL, or al Qaeda, or those foreign agencies that we see as being the prime international threat to the stability of the world right now. (Dennis Bevington) (For responsive lines, please see Tab 1F, 2F)

On transparency and oversight: We had a lot of concerns about the bill, especially with respect to protections, civilian oversight of CSIS and the fact that the government does not give CSIS adequate resources. With respect to warrants for overseas covert actions, we moved an amendment that would require the director, and not an employee designated by the minister, to make the application in every case. It is simply a question of transparency. I know that all Canadians want CSIS to be as transparent as possible. The purpose of our amendment was to ensure that covert activities do not become routine. We wanted the director to be accountable. (Laura L. In) (For responsive lines, please see Tabs 2A and 2B)
On respect for international law: We put forward an amendment to delete the following from clause 8(2):

Without regard to any other law, including that of any foreign state,...

It is important that we remove this part of the bill because we wanted to remove any contradiction with international law and the explicit granting of power to Canadian courts to authorize illegal activity in other states. Canadian activities must comply with international law... (Laurin Liu) (For responsive lines, please see Tab 1E, 2A and 2F)

On accountability and warrants: We also proposed another amendment to add specific accountability for the use of warrants to authorize activities of CSIS abroad to the CSIS director. We would like the director to submit an annual report to (SIRC) specifying the disposition of all such warrant applications and the activities carried out under the warrants,... and the bill does not contain enough measures to protect Canadians' privacy. (Laurin Liu) (For responsive lines, please see Tabs 1D, 2A and 2F)
Relevant Question Period Debate

In Question Period debate (since November 2014) the following issues and questions were raised with regard to CSIS.

- **Insufficient oversight**: Insufficient oversight for CSIS and other national security agencies was raised repeatedly. Sample question: “In the years following 9/11, the current justice minister said parliamentarians could provide a credible and independent check and balance to oversee our national security agencies and the power of the state. So why has the government left parliamentary oversight out of its current anti-terror bill? (Justin Trudeau)

**Government response**: We already have a rigorous system of oversight on our national security and police agencies, specifically on intelligence. We have the Security Intelligence Review Committee which is a robust mechanism of independent third party oversight; it functions very well.

- **Adequacy of SIRC**: Questions were raised about the ability of SIRC to provide sufficient oversight. Sample question: “Mr. Speaker, the house is currently debating government legislation that would increase the mandate of Canada’s spy agency giving CSIS broader powers of surveillance over Canadians. But the Security Intelligence Review Committee suffering from two vacancies and without a full-time chair already falling behind in its investigations of complaints against the agency. Even former chair Chuck Strahl stated that it might be necessary to review the role, its resources or both. Does the government not believe that national security should be properly balanced with effective oversight and respect for the privacy of law-abiding Canadians?” (Brent Rathgeber)

**Government response**: We have an outstanding Canadian model, a body that has been in place for 30 years, that ensures continuity in terms of reporting and oversight of the Canadian Security Intelligence Service, and that has world-renowned expertise, knowledge and credibility. I salute their work and I urge the member to support the work of the committee, which, as we all know, is accountable to Parliament.

- **SIRC Resources**: Questions were raised about whether SIRC has adequate resources. Sample question: “The Conservatives are about to give enhanced powers to CSIS. But the organization mandated to oversee it will receive only an additional $10,000 this year. That is ridiculous. With such a paltry budget, part-time members and a limited mandate that is after the fact, how can the Conservatives claim that sir is capable of overseeing the activities of CSIS?” (Megan Leslie)

**Government response**: SIRC has the resources and authority to fully and independently review CSIS’ activities. SIRC is an established, well-recognized, expert committee that has the knowledge to do intelligence security.

- **Parliamentary oversight of CSIS in context of TDA**: Comments were raised repeatedly that CSIS should not be given an expanded mandate without expanded oversight. Sample question: “Former justices of the Supreme Court, seven former federal ministers, four former Prime Ministers, including a Conservative, have all said they’re concerned about the dangers that C-51 represents. There is no effective oversight mechanism for monitoring CSIS. Why are the Minister and the Liberal leader not listening to this wise advice?” (Megan Leslie)

**Government response**: There is already oversight with SIRC. We believe that the expanded powers that are to be given should not be dealt with after the fact by politicians but should be dealt with before the fact by independent judges. We thought that was the most effective form of oversight for the expanded powers that this legislation seeks to give to the Canadian Security Intelligence Service.

- **Constitutionality of Bill C-44 and C-51**: Issues were raised about the constitutionality of the new legislation. Sample question: “The Minister of Justice is also the Attorney General of Canada. He therefore has the duty to examine the legality of bills that are introduced here in parliament. Experts are already challenging the constitutionality of certain aspects of bill c-51.
Has the Minister of Justice done his job and obtained the legal opinion as to whether [the bill] passes constitutional muster and will he table with the committee — will he table this with the committee? (François Boivin)

Government response: Every bill brought by the government is approved by the Department of Justice. We look to the constitutionality, we look to the Charter compliance before presenting any bill in the House of Commons.

- **Lawful TDA:** Questions have been raised about whether CSIS would require judicial authorization for all measures to reduce threats. Sample question: "The government keeps saying the new power of CSIS is subject to judicial oversight. No, they're not. It would be only if CSIS were to decide that it was about to do would be illegal or unconstitutional that it would then be given the choice of applying for a warrant. All other disruption activities would not require a warrant. The government is either being disingenuous or not fully reading its own bill." (Randall Garrison)

Government response: On the question of disruption, if what CSIS was doing was entirely legal and there was no question of people's rights being infringed, then obviously there would be no need for a warrant. However, in the case of any other activity that might violate someone's rights, it would be carried out for a good law enforcement reason, a warrant would be needed.

**Application of TDA to nonviolent civil disobedience:** Questions have been raised with regard to whether Bill C-51 would allow CSIS to take measures against peaceful protest or nonviolent civil disobedience. Sample question: "The government is trying to mix up threats to security with terrorist activities. According to internal documents, the RCMP calls groups who are opposed to major polluters, for example environmental groups and First Nations as threats to security. With the Prime Minister's proposed legislation, will CSIS have the authorization to investigate these groups, environmental groups, First Nations, are they in your sights as well?" (Peter Julian)

Government response: CSIS is given powers to deal with threats to the security of Canada as enumerated in the CSIS Act. They explicitly, according to the statute, do not include lawful advocacy, protest or dissent. The current wording properly circumscribes and identifies the powers of CSIS so lawful dissents and protests are protected.

- **Definitions of threats to security:** Questions have been raised with regard to the definition of threats to the security of Canada with regard to CSIS' mandate. Sample question: "The government is trying to mix up threats to security with terrorist activities. According to internal documents, the RCMP calls groups who are opposed to major polluters, for example environmental groups and First Nations as threats to security. With the Prime Minister's proposed legislation, will CSIS have the authorization to investigate these groups, environmental groups, First Nations, are they in your sights as well?" (Thomas Mulcair)

Government response: The NDP may be getting confused about definitions in the information sharing provisions of the Bill and the CSIS Act portion of the Bill. Absolutely no changes will be made to what constitutes a threat to the security of Canada. Further, the CSIS Act specifically states that threats to the security of Canada do not include lawful advocacy, protests, dissent, and artistic expression. It is very clear, and again I think some fearmongering has gone on.

- **CSIS resources:** Cuts made to national security programs were raised repeatedly. Sample question: "The new security bill does nothing to solve the problem of resources. Currently, C.S.I.S. is unable to monitor everyone who's been identified as a potential threat. Officials are already overwhelmed with the number of files on high-risk travelers. How does the minister expect these new powers to be useful when C.S.I.S. can't even cope with its current workload?" (Roseanne Telebvre)

Government response: Opposition parties repeatedly (seven times) voted against increased funding for national security agencies including CSIS. The resources we have provided to do its very important work have increased considerably since the Government has been in power. That is because we recognize the importance of the work CSIS does, as well as the work done by its companion agencies.
- **Use of torture or enhanced interrogation techniques:** Questions were raised in relation to the US Senate Report on interrogation methods with regard to Canada's position on such methods. Sample question: "Canadian security agencies have gone from rejecting information obtained by torture and having policies in place to identify tainted information to an order that allows such information to be used and shared. Even at the risk that it will lead to torture in other countries. Why does the minister continue to condone by proxy through this directive?" (Wayne Marston)

**Government response:** The report is a US report and has nothing to do with the government of Canada. Our government does not condone the use of torture and certainly does not engage in it. The primary responsibility of Canadian security agencies is to protect Canadian lives and property. If we get a tip from any source that Canadians’ lives are in danger, lives that are in danger, Mr. Speaker, we will act to save those lives and we will continue to ensure that intelligence is reviewed and assessed by Canadian intelligence experts before it is acting upon.

- **CSIS lapsed funds:** Questions were raised in relation to lapsed funds of security agencies. Sample question: "The government claims to be cracking down on terrorists and through Bill C-51, our security agencies are about to assume broad, new powers. However, our security agencies lack the resources to carry out even their current mandates. Both the R.C.M.P. Commissioner and the deputy C.S.I.S. Director clearly told parliamentary committees last October as much, that a lack of resources makes tracking all extremists at all times simply impossible. Now we have learned that collectively, CSIS, the RCMP, and DND have allowed $11 billion to go unspent and lapse." (Brent Rathgeber)

**Government response:** In actual fact, we have increased resources to our national security agencies by over one-third.

**CSIS response:** Over a period of 7 fiscal years, the Service has lapsed funds of $181.9M reflecting prudent financial management of public funds. While money was immediately allocated, CSIS' stringent recruitment process required that the hiring of new employees take place over a more extended period of time. There were also lapses related to the management of capital projects where money was moved from one year to the next. CSIS' lapsed approximately $18 M in last year's Public Accounts. Only funds of $3.9 M were associated with CSIS' operating budget carry-forward, which represents 1.1% of CSIS' Main Estimates. This amount is well within the allowable 5% carry forward established by Treasury Board. $12.7 related to funds that had been frozen during the year and, therefore, were unavailable to the Service to spend.

- **Director’s travel expenses:** "Canadians were shocked to learn about high flying travel at CSIS. The director has racked up tens of thousands in travel expenses including a $750 a night hotel bill. Meanwhile, CSIS case officers looking at high-risk travelers are overstretched and underresourced. Does the minister really think this is an appropriate use of taxpayer funds?" (Roseanne Lefebvre)

**Government response:** The travel director of the government of Canada is very clear. It states that the most economical means are to be selected when booking transportation, accommodations and facilities. The government takes the management of taxpayers' money very seriously.

**CSIS response:** Owing to national security reasons, CSIS does not disclose the particulars of where our employees travel or whom they meet with – and that applies equally to members of the executive. That said, it must be noted that travel is a necessary requirement for intelligence workers. That’s because national security is a shared exercise – domestically and globally – and CSIS has many partnerships that need to be maintained and expanded. The international character of terrorism has made this especially evident. CSIS is extremely respectful of taxpayer dollars. Everything we do in fulfilling our mandate to protect Canada’s national security interests is done in a manner of utmost professionalism. All members of CSIS adhere to the GoC rules and regulations set forth by Treasury Board Secretariat.

- **Costs of the O’Connor and Iacobucci Inquiries for CSIS and others:** (Craig Scott)

**CSIS response:** For reasons of national security, CSIS does not disclose details of its budget and expenditures, beyond those publicly reported in the Parliamentary Estimates, Public Accounts, and the Budget.

With respect to costs incurred by the O’Connor Inquiry, CSIS can release the following information:
$1,849,335.00 (fiscal year 2004/05, received in 2005/06 via the Operating Budget Carry Forward Policy)

$1,418,280.00 (fiscal year 2005/06, via Supplementary Estimates A)

With respect to costs incurred by the Iacobucci Inquiry, CSIS can release the following information:

$3,133,233.00 (fiscal year 2007/08, via Supplementary Estimates A)

$433,973.00 (fiscal year 2008/09, via Supplementary Estimates B)

- **Costs of the civil action brought against Canada Arar, Abou-Elmaati, Nureddin and Almalki:** (Craig Scott)

CSIS response: For reasons of national security, CSIS does not disclose details of its budget and/or expenditures, beyond those publicly reported in the Supplementary Estimates, Public Accounts, and the Budget.

With respect to costs related to the civil actions by the individuals in question and their subsequent court-awarded amounts, the following was identified in the Public Accounts:

For Ahmad Abou-Elmaati:

$1,924.95 (fiscal year 2011/12, as part of Public Accounts amount of $3,729.00)

$13,904.13 (fiscal year 2013/14, as part of Public Accounts amount of $125,137.00)

$1,666.58 (fiscal year 2013/14, as part of Public Accounts amount of $8,000.00)

For Muayyed Nureddin:

$1,803.61 (fiscal year 2011/12, as part of Public Accounts amount of $3,729.00)

$13,904.13 (fiscal year 2013/14, as part of Public Accounts amount of $125,137.00)

For Abdullah Almalki:

$13,904.12 (fiscal year 2013/14, as part of Public Accounts amount of $125,137.00)
On November 24, 2014, the CSIS Director made an appearance alongside the Minister of Public Safety and Emergency Preparedness and the Deputy Minister of said Department (inter alia), at the House of Commons National Security Committee (SECU) to testify on matters related to Bill C-44.

Below are key statements made at the Committee:

- **On debate length:** "I ask the minister again: do you think that we’re actually going to have enough time here in committee to give this bill the study that it deserves?" (Randall Garrison, NDP)

  Answer (Blaney): "I believe there has already been more than nearly 11 hours of debate. I think we are expected from Canadians, especially in the context of an evolving threat to do a thorough work but not to drag on our feet and spend wasteful time as this bill is needed.

- **On oversight:** "Why is there nothing in this bill that improves the accountability and the oversight for our national security agencies?" (Randall Garrison, NDP)

  Answer (Blaney): "I’ve said it in the House and I said it again today, this bill is particularly designed to address two issues that were brought forward by the court which were limiting the power and the authority of CSIS.

- **On oversight and the Bill’s constitutionality:** "CSIS operates under Canadian law. This is why we have set up a package of law that is making sure that whenever they operate, they are operating within the law. Of course, I may be involved in those authorizations, but, more importantly, judges warrant when our issues need to be validated by the judicial system. On top of that, we have an overview mechanism of the whole service and this is done by the Security Intelligence Review Committee. I have brought here a copy of that report: it’s in both official languages. We have a robust oversight of an agency which is to abide by Canadian law." (Blaney)

  "I wonder if CSIS maybe shares that same interpretation that there is a new responsibility for SIRC here included in the bill?" (Randall Garrison, NDP)

  Answer (François Guimont): "Well actually I would say, Mr. Chairman, that it’s new in the sense of being defined in that bill, but in reality SIRC can look at all aspects of CSIS’ activity as long as it is not cabinet confidence. Their power is very broad, so that’s the first observation I would make. The second observation is that it is a review responsibility, and their resource—I think they have 16 individuals, plus or minus—is a significant number of individuals who are very capable and understand the business of CSIS. I would like to think that they are probably equipped to do a good job at carrying out review, should they decide to do so."

- **On the Bill’s constitutionality:** "So I have a question for the minister about what advice he has received from the Department of Justice on the constitutionality of the measures proposed here? Particularly those that deal with authorizing courts to grant warrants without respect to international law? Also with respect to the protection of identity of human sources. If these laws aren’t going to stand up when they get to court then we’re actually wasting time here when we could do something more effective. So has he had that advice? Will he table that advice with this committee?" (Randall Garrison, NDP)

  Answer (Blaney): "As I’ve said in criminal proceedings defendants will have the ability to seek an order from a judge declaring that disclosure of the identity of a human source is essential to establishing their innocence. The fundamental right to a fair trial is not only preserved it is reinforced. In another bill from this one we will come back with issues related to surveillance, arrest and detention. But this is not what this bill is about. This bill is about protecting the source. This is exactly why we have embedded in this bill measures to reinforce the fundamental right, not only respecting the law but the spirit of the law which I think is even going further. The other aspect is you know we are talking of..."
On passport revocation: "Those individuals who are committing terrorist acts using the Canadian passport don't deserve to use their citizenship to propagate violence around the world. That is why, once they are convicted of a terrorist act, I find it fairly appropriate to remove this tool and this great privilege to be a Canadian citizen." (Blaney).

On powers of arrest: "Why hasn't section 83.18(1) of the Criminal Code been used to arrest those individuals? Two, are there components in this bill that will allow you to arrest those individuals where you're not now able to?" (Wayne Easter, LPC)

Answer (Blaney): "As you are well aware and you've been in that position before it is not because you suspect an individual to have contravened the criminal law that you necessarily are being able to transfer this intelligence into evidence. That's why we need to move forward as the legislator. That's why I will come back to this committee to address this issue, and that's why I hope I can count on your support to do exactly that. To get back to the existing provision of the Criminal Code Commissioner Paulson has already indicated that the threshold was too high so that they were not able to proceed."

On extraterritorial authorization: "As I see it under this bill there are no checks and balances where CSIS is going to do something that violates the law of another country but we're able to do because of the warrants issued within Canada. There doesn't seem to need to be those checks and balances to protect our foreign affairs interests whether in trade or in other areas... Where are the checks and balances to protect Canada's interest when we take action under this section?" (Wayne Easter, LPC)

Answer (Director Coulombe): "You have to understand that with like-minded partners, we do work overseas jointly. It's not like we would go into a friendly country and do things covertly. As a security intelligence service, and not just as a service—all of our partners do conduct covert operations. That's kind of obvious, and although it might not be specific in their legislation, that's what a security service will do at times. But most of the time for the service we do our work overtly with our partners when they are like-minded, but there could be occasions when we're sending intelligence officers, for example, into countries that are not like-minded where we might not tell that country what we're doing because of the national interests of Canada but also for the safety of our officers."

"In this bill, if I can put it this way, with judicial decisions, judges, authorizing certain activities for CSIS abroad, aren't we now getting into, I guess, the extraterritorial application of what CSIS does from where we were?" (Wayne Easter, LPC)

Answer (Director Coulombe): "First of all, in terms of CSIS conducting activities outside Canada, and you talked about the Macdonald Commission, my interpretation of... I'm pretty sure in the report it does talk about the creation of CSIS, that you would have to be very careful, but they were already seeing the possibility that we would have to do this. It has always been our understanding that we have that authority. That's why this is just a clarification making it explicit in the act that we can actually do what we've been doing for basically 30 years, because that was the interpretation of... If you look at section 16, there's a clear restriction: it's within Canada, which you do not find in section 12... if you're thinking about us acting in other countries, when it's with like-minded partners most of the time this is done jointly, with the acknowledgement of that country, just like we expect them to do the same here. When there's cases of non-like-minded country, like it was mentioned earlier, with, for example, cases of Russian espionage, then we would investigate, and if there's a case we would pass it to the RCMP."

"Certainly, Mr. Coulombe, you said that there are no new powers for CSIS here, so in clause 8 where it adds to the warrant question the words, 'Without regard to any other law, including that of a foreign state...': my question is, could that be removed from this bill? If it was removed, would that change anything materially here. Certainly, to me, it
would affect the reputation of what we're doing in other countries. So I'm not sure who's responsible for the drafting of that and what impact that would have to remove those words from this bill? (Randall Garrison, NDP)

Answer (Ritu Banerjee, PS): "Part of the reason it's drafted the way it is, is if we go back to the Federal Court of Appeal decision, the court made it clear, and this is again following up from what Mr. Coulombe just said, that it would have the jurisdiction to issue such a warrant, and I'm quoting the decision, '...where the interception is lawful where it occurs'. Because that is very challenging to operationalize, we had to ensure that the law was clear for judges, that what they had to consider was relevant to Canadian law, primarily the charter and the CSIS act. So that's why it's written the way it is."

Answer (Director Coulombe): "In terms of being lawful in the country where it's going to take place, you can imagine the difficulties in the countries I listed earlier. But I just talked about mobility. If we were to obtain a warrant where it would be lawful to do whatever we want to do in Syria, and the next week now that person is in Iraq, and the following week that person is elsewhere, again, in terms of, as we say in French, pratico-pratique, I'm not sure how that system would be workable..."

On the Bill's relationship with citizenship revocation: "J'ai une autre question concernant la partie qui touche la Loi renforçant la citoyenneté canadienne. C'est un projet de loi sur le Service canadien du renseignement de sécurité. Pourquoi avoir rajouté cela? Est-ce que ça a un rapport quelconque? Je ne comprends pas nécessairement le lien entre le SORS et le rapprochement des dates d'entrée en vigueur." (Rosane Doré Lefebvre, NDP)

Answer (Blaney): "Essentiellement, c'est pour faciliter et accélérer la mise en application de l'enlèvement de la double citoyenneté dans la cas d'individus reconnus coupables. Donc, il n'y a aucun élément législatif, et peut-être que Mme Girard pourra compléter, aucun nouvel élément législatif, si ce n'est que de faire en sorte que la loi qui a été adoptée puisse entrer en vigueur plus rapidement."

Answer (Nicole Girard, DG CIC): "Les objectifs sont complémentaires dans le sens où les changements techniques qui sont proposés à la Loi sur la citoyenneté permettront aussi de rejoindre ce même objectif, qui est de renforcer la sécurité publique, la sécurité des canadiens et des canadiennes et de renforcer la valeur de la citoyenneté canadienne et de l'intégrité du programme."

"What I'd like to talk to you about or ask you about first off—and I'll let you decide the best one to respond on this—is around the fairness of revoking citizenship of dual-nationals." (John Carmichael, CPC)

Answer (Nicole Girard, DG CIC): "I think the first, most important point to make is that Canada is alone compared to like-minded countries and other democratic countries in not having this ability already to revoke citizenship for egregious actions that are done against a national interest, and so the recent changes that Parliament made in June to expand the grounds for citizenship revocation limited to specific actions—namely, convictions for high treason, treason, spying, terrorism, or being in the service of an organized armed group or armed force engaged in armed combat with Canada—is broadly in line with what like-minded countries already do. I would also like to add that with regard to fairness, there are many safeguards that are provided in the law and as a matter of procedure with regard to the revocation process itself. Those include notice; the ability of the person concerned to know the grounds against them; to see the evidence; to have an opportunity to respond and make their submissions; to receive a decision in writing; to potentially have a hearing with the decision maker; and of course, to seek judicial review if in the end that decision is against them and revoking their citizenship."

"I'm wondering how the provisions in Bill C-44 protecting the identity of CSIS human sources connect with the citizenship process. In other words, if evidence that's being used from CSIS sources is the evidence that is being used for the revocation of citizenship, then what provisions are there? The only exemption for defence here is about criminal prosecutions, not citizenship. Is there an (intersection) between the two bills there, or any exemption provided for use in those citizenship processes?" (Randall Garrison, NDP)

Answer (Nicole Girard, DG CIC): "I would just respond by stating that the two provisions of this bill are distinct. They are not intended to be related other than they both support..."
the objective of the safety and security of Canadians. Then the other point more directly in response to your question is that citizenship revocation cases would be initiated based on objective, open-source information to determine whether the provisions apply."

- **On source protection:** "We clearly need it in order to maintain the quality and the reputation of the service and the accuracy of the data that they are collecting. Although before this court decision, this right, if I can put it that way, was taken for granted. Due to this court decision, we are clearly invited as a (legislature) to clearly define it in the law." (Blaney)

  "When somebody—and quite often at the risk of their own security and with promise of confidentiality—is cooperating with the service I think the state has a duty to protect that person, and to protect their identity so that we can protect their security—and not just protect them, but sometimes their family, also. So I think there is a duty on the part of the state. Now we have to balance that, in different proceedings, with how we maintain fair proceedings. I think the bill has achieved that balance... Although we're not in the business of collecting evidence, that's why our intelligence will be either challenged, or there will be a request for more disclosure, including the identity of human sources. It's just that the nature of the threat environment has changed and has basically changed the service interaction in terms of dealing with those different proceedings." (Director Coulombe)

- **On the risks posed by changing the rights of the defence in court:** "You mentioned the challenge of transferring intelligence into evidence. I think those were your words. We share the concern about taking intelligence and making sure you can use it in prosecutions. I have a concern that the way this bill is drafted now in fact it may make it more difficult to do those prosecutions. When you talk about the protection of the identity of witnesses, the courts can protect the identity of CSIS sources on a case-by-case basis now. They didn't say that wasn't possible. When you say that they invited you to do this, I believe that if you read the decisions, they said that Parliament could do this. They didn't say that it was necessary, and it didn't say that Parliament should provide this blanket protection, it said that it was possible. So my question really is, why risk this change to limit the rights of the defence to challenge the use of intelligence information in prosecutions? Why risk a change that might either make it more difficult to prosecute, or might result in those provisions being declared unconstitutional? Why are you risking that in this bill?" (Randall Garrison, NDP)

Answer (Blaney): "What I've clearly demonstrated this afternoon is that we are doing it while respecting the Constitution with the amicus curiae in the protection of witnesses whenever someone is accused."

Answer (Blaney): "Ce projet de loi vient clarifier les autorités des services. Il va faciliter le travail des tribunaux, parce qu'il vient lever les embarras qui existaient dans l'application de la loi, autant au niveau de la protection des témoins que la capacité du service, non seulement pour opérer à l'étranger, mais également à échanger des informations avec nos alliés comme la Grande-Bretagne, l'Australie, la Nouvelle-Zélande, comme les Américains, les Français qui sont alliés et qui sont aux prises avec le même défì auquel nous sommes confrontés, c'est-à-dire de suivre des individus qui se promènent d'un pays à l'autre et qui menacent la sécurité des Canadiens, qui s'attaquent à des personnes innocentes. C'est exactement ce que ce projet de loi fait, il vient restaurer les autorités qui ont permis au service, par le passé, d'être efficace et à un moment critique où nous faisions face à une menace qui évolue, il est d'autant plus important de préserver les capacités du service à protéger les Canadiens."

- **On Service Resources:** "Actually, the SCRS has-he has the resources necessary to do the work that he is asked to do?" (Rosane Doré Lefebvre, NDP)

Answer (Director Coulombe): "Le service, comme toute autre organisation, travaille à l'intérieur de son budget. Nous devons établir des priorités et allouer les ressources en fonction de celles-ci qui découlent des renseignements qui sont fournis par le gouvernement. Ensuite, nous avons nos façons d'évaluer les matrices pour juger de la menace que représentent les différents sujets d'enquête. Nous allouons les ressources en fonction de cela."

- **On cooperation with the RCMP:** "Le projet de loi C-44 va-t-il faciliter la coopération entre la GRC et le SCRS? Des mesures vont-elles vous aider auprès de la GRC?" (Rosane Doré Lefebvre, NDP)
On employee protection (information and identity): "Il y a aussi une provision dans le projet de loi C-44 qui parle de mieux protéger ou de moins divulguer l'information en ce qui a trait aux agents du SCRS. On parle aussi de structures d'agents. Est-ce qu'on a plus de détails parce que cela pourrait être pratiquement n'importe qui travaillant au SCRS selon la façon dont le projet de loi C-44 est rédigé. Est-ce qu'il serait plus facile de cibler davantage les gens qu'on aimerait potentiellement envoyer en tant qu'agents à l'international? Cette provision est vraiment très vaste." (Rosane Dore Lefebvre, NDP)

Answer (Director Coulombe): "Premièrement, la loi actuelle offre cette protection pour les individus qui sont présents et qui étaient dans le passé impliqués dans ces activités. En fait, le projet de loi C-44 rajoute ceux qui pourraient être impliqués dans ce type d'activités. La problématique avec le fait d'essayer de mettre un cadre plus serré de qui on parle, la menace et le contexte évoluent tellement rapidement qu'il y a des individus, aujourd'hui, qui sont impliqués dans ce genre d'activités que même moi, il y a peut-être cinq ou dix ans, je n'aurais jamais pensé qu'ils seraient impliqués là-dedans. Il ne s'agit pas seulement des agents de renseignement qui peuvent être impliqués. Donc, il y aurait un danger de limiter vraiment la protection d'identité des employés du service. Par ailleurs, encore une fois, comme toute autre activité du service, en terme de désigner des employés qui relèvent de cette protection, cela tombe sous la révision du CSARS. C'est quelque chose qu'eux peuvent définitivement surveiller dans le cadre de leur révision annuelle."

On clause exemption in judicial proceedings (point of order): "So the ability to request the exemption (in clause 7 of the Bill,) does it deal with, it says the presumption of innocence but does that include the other stages of the legal process including bail and detention?" (Randall Garrison, NDP) (information was promised as a follow-up by François Guimont).
REPORT ON COMMITTEE MEETING

Name of Committee: Public Safety and National Security
Report prepared by: Charles MacLean, Public Safety 991-3311
Date and time: Wednesday, November 26, 2014 – 3:30 p.m. to 5:33 p.m.
Location: Room 268, Valour Bldg, 151 Sparks St.
Subject: Bill C-44 (Protection of Canada from Terrorists Act)

Absent:
- Diane Ablonczy (CPC), John Carmichael (CPC) and Ted Falk (CPC) replaced Blake Richards (CPC), Larry Maguire (CPC) and Lavar Payne (CPC)
- Craig Scott (NDP) replaced Randall Garrison (NDP) for the first twenty minutes of the meeting.
- Sean Casey (LPC) replaced Wayne Easter (LPC)

Witnesses:

3:30 p.m. to 4:30 p.m.

As Individuals
- Craig Forcese, Associate Professor, Faculty of Law, University of Ottawa
- Wesley Wark, Professor, Graduate School of Public and International Affairs, University of Ottawa
- Tom Stamatakis, President

Canadian Police Association
- Kent Roach, Professor, Faculty of Law, University of Toronto
- Christian Leuprecht, Professor, Department of Political Science, Royal Military College of Canada (by videoconference)
- Garth Davies, Associate Professor, Simon Fraser University (by videoconference)

Overview of hearing:

- The Committee continued its study of Bill C-44 (Protection of Canada from Terrorists Act), with two panels of witnesses primarily from academia.

- The witnesses were divided on the Bill. Tom Stamatakis expressed his support for the Bill given the importance of foreign intelligence in disrupting threats and supported extending legal protection to human sources. Prof. Davies and Prof. Leuprecht supported the Bill arguing that CSIS needs the tools required to address current threats such as extremist travelers.

- Prof. Forcese supported the Bill, but suggested amendments to address "ambiguities" in the provisions that clarify CSIS' authority to operate abroad.

- Prof. Roach raised concern that the class protection of human sources could have unintended downstream consequences on criminal justice, and that the exception to this protection should be expanded to any proceeding where s. 7 "Legal Rights" of the Charter rights are at issue.

- Prof. Wark opposed the Bill for not providing more clarity regarding CSIS authority to operate abroad and additional safeguards. More fundamentally, he disagrees with authorizing a domestic intelligence agency to also conduct foreign operations and would prefer that a separate agency be established to operate abroad.

- All of the academics called for enhanced accountability measures to align with the authorities of the Bill.

- The Privacy Commissioner provided a written submission calling for enhanced accountability measures to address privacy risks identified with the Bill. (https://www.priv.gc.ca/cparl/2014/part_sub_141125_e.asp)

- During questioning, the Government members focused on the need for CSIS to operate overseas to gather intelligence on threats and the importance of human source protections.
• In their questioning, NDP opposition members suggested that the warrant process was ambiguous and argued that enhanced accountability measures were required. The Liberal member focussed only on parliamentary oversight.

• The NDP again expressed frustration that the Committee has not allocated more time to study the Bill.

Highlights of hearing:

- Prof. Forcese recommended amending Bill C-44 to more explicitly state when a warrant must be sought for foreign activities (e.g. when an activity would violate foreign or international law) and to include an explicit statutory authorization for intercept sharing with partners that would include safeguards. Prof. Forcese also recommended an amendment to enhance accountability measures to align with increased collaboration between CSIS and its domestic and foreign partners that would result from Bill C-42. Prof. Forcese indicated that he would submit text for the three amendments to the Committee once it was translated.

- Prof. Wark stated that Bill C-44 would formalize CSIS's evolution as a hybrid intelligence agency that operates both domestically and abroad. He criticized the Bill for not providing an underlying definition of this hybrid agency and for not providing additional accountability measures and safeguards for the foreign operations. He was also concerned that there was no statutory requirement for CSIS to consult the Minister of Public Safety or with DFATD and DND before seeking a warrant for overseas activities. Prof. Wark provided a longer version of his opening remarks to the Committee as a written submission.

- Prof. Roach stated that providing a class protection to human sources ignored the SCC decision on Harkat and the recommendations of the Air India inquiry. Citing the Air India criminal case, Prof. Roach argued that a premature promise of protection by CSIS during intelligence gathering could leave the Crown without access to witnesses at trial. He also argued that the Bill should be amended to make a promise of protection explicitly offered and not implicit. Prof. Roach noted that CSIS foreign activities could cause CSEC to override its restrictions and called for integrated review of national security operations via ministerial and parliamentary oversight.

- Prof. Leiprecht called for parliamentary oversight similar to the Belgian model where the parliamentary committee has access to information about active intelligence activities.

- When asked by Ms. Abidnour (CPC) whether the Five Eyes required their intelligence agencies to seek judicial authorization to conduct foreign activities, Prof. Wark stated that their foreign intelligence agencies required either judicial or executive approval.

- In responding to a question from Rick Norlock (CPC), Mr. Stamatakis spoke about the importance of human sources both domestically and abroad to law enforcement and agreed that the human source protections in the Bill would allow CSIS to gather information that would support domestic criminal investigations.

- In response to a question from Ted Falk (CPC), Prof. Roach suggested that clarifying that CSIS has the authority to operate abroad may be seen as conferring a new power given that the CSIS Act is silent on extraterritoriality.

- When asked by Mr. Falk to comment on the promise of protection, Prof. Roach suggested that this authority may require ministerial review.

- In responding to a question from Craig Scott (NDP), Prof. Forcese speculated that an application for a warrant to conduct an interrogation overseas would require the judge to consider s. 7 "Legal Rights" of the Charter. The Professor alluded to the Kadaf case in his answer. Mr. Scott asked whether the phrase "without regard to any other law" could be interpreted as exempting CSIS from the Charter. Prof. Forcese suggested that phrase referred only to foreign and international law. Mr. Scott stated that Federal Court judges would have to develop new legal tests to decide whether warrants given that they would be authorizing CSIS to possibly break the laws of foreign countries. Prof. Forcese suggested that judges may be very demanding when deciding these applications.

- In response to questions from Sean Casey (LPC), Prof. Forcese criticized the part-time status of SIRC appointments, and the fact that its budget had not increased at the same pace of CSIS's. He called for the establishment of a national security committee of parliamentarians that would have access to classified information similar to Australia and the UK. Prof. Wark expressed support for the UK model.

Next meeting
The Committee will proceed to clause by clause analysis of Bill C-44 at its meeting on Monday, December 1, 2014.
ORDERS OF THE DAY

TELEVISION

Bill C-44, An Act to amend the Canadian Security Intelligence Service Act and other Acts
3:30 p.m. to 4:30 p.m.

APPEARING

Hon. Steven Blaney, P.C., M.P., Minister of Public Safety and Emergency Preparedness
François Guimont, Deputy Minister
Canadian Security Intelligence Service
Michel Coulombe, Director
Department of Citizenship and Immigration
Nicole Girard, Director General, Citizenship and Multiculturalism Branch

WITNESSES

3:30 p.m. to 5:30 p.m.

Department of Public Safety and Emergency Preparedness
Lynda Clairmont, Senior Assistant Deputy Minister

UNEDITED COPY - COPIE NON ÉDITÉE

Monday, November 24, 2014 - Le lundi 24 novembre 2014

ORDRE DU JOUR

TELEVÉE

Projet de loi C-44, Loi modifiant la Loi sur le Service canadien du renseignement de sécurité et d'autres lois
15 h 30 à 16 h 30

COMPARAÎT

Hon. Steven Blaney, C.P., député, ministre de la Sécurité publique et de la Protection civile
Francois Guimont, sous-ministre
cité

ministère de la Sécurité publique et de la Protection civile

ministère de la Citoyenneté et de l'Immigration
Nicole Girard, directrice générale
Direction du programme de la Citoyenneté et du Multiculturalisme

16 h 30 à 17 h 30

ministère de la Sécurité publique et de la Protection civile

Lynda Clairmont, sous-ministre adjointe principale
The Chair (Mr. Daryl Kramp (Prince Edward—Hastings, CPC)): Good afternoon, colleagues and guests. Welcome to meeting number 40 of the Standing Committee on Public Safety and National Security.

Today, pursuant to the order of reference of Tuesday, November 18, Bill C-44, An Act to amend the Canadian Security Intelligence Service Act and other Acts, will be dealt with.

Appearing before us this afternoon are the Honourable Steven Blanney, Minister of Public Safety and Emergency Preparedness. We also have François Guérin, the deputy minister. We have, from the Canadian Security Intelligence Service, Mr. Michel Coulombe, director. And from the Department of Citizenship and Immigration, we have Nicole Girard, director general, citizenship and multiculturality branch. These will be our witnesses for the first hour.

At the end of the first hour, Minister Blanney will be excused. The other ministers, I believe, will be staying. We have other additional witnesses who will be arriving for the second hour.

With that understanding, I will now open the floor to opening statements by our witnesses.

Minister Blanney, you have the floor.

Hon. Steven Blanney (Minister of Public Safety and Emergency Preparedness): Thank you, Mr. Chair.

I am here this afternoon to invite you to support Bill C-44—

The Chair: Excuse me, Mr. Blanney, but Mr. Easter has a point of order.

Hon. Wayne Easter (Malpeque, Lib.): I raise this again—I raised it last time this minister was here. The minister has the resources of all the departments available to him. A minister coming before these committees reads from written notes: we saw that last time. There was important information in there we could have used during committee that we didn't pick up until after. So I ask, does the minister have his statement written, that it can be presented to the committee in both official languages, as I believe is the custom of this place?

The Chair: Thank you, Mr. Easter. Obviously I will ask the minister if he has a prepared statement that he can distribute. And if not, he can go ahead with his statement but take that under advisement for future visits.

Hon. Steven Blanney: Thank you, Mr. Chair.
I begin by saying that what I have to say is not in any written speech, Mr. Chair.

I find it particularly special to be here in this room, in this very room where I was with my colleagues on October 22. We spent hours here. You were here as well, Mr. Chair. We will remember those hours for a very long time, as will our opposition colleagues, who were just on the other side of that room. We were all somewhat involved, against our will, in the terrorist attack that took place.

A few weeks before the attack, I was here with Mr. Coumbe, Mr. Cusson, and also with our RCMP commissioner to state that we are—we were at that time and still are—taking the terrorist threat very seriously, and that the threat is real.

Unfortunately, we have been exposed to the hatred of those individuals who committed the two terrorist attacks in mid-October. That makes this meeting even more important.

With that, I would like to begin by talking to you about Bill C-44, for which I seek your support.

[Français]

J'aborderai surtout l'ensemble des dispositions qui modifient la Loi sur le Service canadien du renseignement de sécurité. Il faut le dire, c'est une loi qui n'a pas été modifiée en profondeur depuis les 30 dernières années.

Je tiens également à souligner que Mme Girard, ici présente, abordera la question de la citoyenneté canadienne, qui a été rétablie en 2016, et qui a été sanctionnée par la loi. En ce sens, le volet sur la citoyenneté canadienne ne constitue pas un nouvel élément législatif, il en facilite seulement une mise en œuvre plus rapide.

Je suis ici aujourd'hui au titre de ministre de la Sécurité publique et de la Protection civile parce que le Service canadien du renseignement de sécurité fait partie des agences dont le ministère est responsable, dont je suis responsable, et il a besoin d'avoir des outils efficaces pour lutter contre la menace terroriste.

Comme vous le savez, monsieur le président, le Service canadien du renseignement de sécurité recueille et analyse des renseignements provenant du pays et de l'étranger et les transmet à la gouvernment du Canada des menaces à la sécurité nationale, notamment le terrorisme et l'extrémisme violent.

[English]

Obviously there should be no doubt about the direct and persistent threat terrorism and violent extremism caused to our security. No one can argue that what took place here in this Parliament and in Saint-Jean-sur-Richelieu are not terrorist attacks. That's why, colleagues, we need to swiftly move forward with this legislation because CSIS ability to investigate threats to the security of Canada no matter where they may occur is vital to the safety and security of Canadians, and indeed our ability to respond to the threat of terrorism.

Our government is keeping Canadians safe. That is what this bill is all about. Let’s dive straight into the very reason of the bill before us today, and therefore so critical in its importance to keep Canadians safe to use it as a shield. The Protection of Canada from Terrorists Act responds to two key core decisions that have important implication for CSIS mandate and operations. Those of you who have taken the opportunity to get the technical briefing provided by my department well understood that, and I could see it was the case when we have some exchange in the House about the bill.

In May 2014 the Supreme Court of Canada issued its ruling in the Harakat case. The Supreme Court’s decision stated that the CSIS human sources do not benefit from a common law class privilege similar to the informer privilege applicable to police informers. Human source are a critical source of information for CSIS. They are at the very base of CSIS and yet, Mr. Chairman, they do not benefit from a protection as this court has ruled. In turn this significantly hampers our intelligence gather capabilities and therefore it puts Canadians at risk. So this bill is
not seeking at this point in time for new powers. It's just seeking to clarify the existing authority under which CSIS can protect us in an efficient manner. That's why the Protection of Canada from Terrorists Act addresses this gap.

[131x173]

This bill is balance. This bill is reasonable and that's why I'm seeking your support. That's why you've been expressing your support in the House so far. Why? Because it's fully respecting the spirit of our Constitution.

[151x215]

In criminal proceedings defendants will have the ability to seek an order from a judge declaring that disclosure of the identity of a human source is essential to establishing their innocence. The fundamental right to a fair trial is preserved and reinforced. Turning to the second court decision affecting CSIS mandate the federal court of appeal recently unsealed its July 2014 decision related to the government's appeal of Justice Mosley's decision that was issued by the federal court last year. The Protection of Canada from Terrorists Act confirms CSIS authority to conduct investigations outside of Canada related to the threats to the security of Canada, and security assessments. This is not a big thing. CSIS can operate within and outside Canada. That's fairly simple.

[151x256]

Bien sûr, monsieur le président, le service a toujours eu le pouvoir d'entreprendre des activités d'enquête à l'étranger. La Cour d'appel fédérale a reconnu ce fait lorsqu'elle a conclu que l'article 12 de la Loi modifiant la Loi sur le Service canadien du renseignement de sécurité et d'autres lois ne suggère en rien des limites géographiques à la sphère des activités du SCR S.

Toutefois, le pouvoir du SCR S de mener des activités à l'étranger afin de faire enquête sur des menaces pour la sécurité du Canada, n'est pas indiqué aussi clairement qu'il devrait l'être dans la Loi sur le SCR S. Il est donc important que le Parlement et que les élus du peuple clarifient cette question.

[151x298]

At the same time, the bill also confirms the authority of the federal court to issue warrants authorizing CSIS to undertake certain activities outside of Canada, and it gives the federal court authority to consider only relevant Canadian law when issuing warrants for CSIS to undertake certain activities outside of Canada.

These amendments are important. We believe that the Canadian Constitution, especially the Charter of Rights and Freedoms, is far superior than the decrees of a dictator in a far-off land. Canadian law, and even more important, Canadian values, are what should solidly ground our legal deliberations around national security, and that is exactly what this bill is accomplishing.
Monsieur le président, les modifications proposées dans le projet de loi C-44 sont raisonnables et nécessaires pour garantir que le Service canadien du renseignement de sécurité et d'autres lois puissent s'acquitter adéquatement de son mandat. Elles sont également conformes à l'esprit de la Loi sur le Service canadien du renseignement de sécurité et d'autres lois et aux recommandations de la Commission McDonald de 1981.

[English]

Unfortunately I have heard some allegations during debate on this legislation at second reading related to CSIS operating outside the law. That's what this bill is preventing from happening because it's clearly defining that CSIS is clearly operating within the law. Let me be clear, CSIS will, as always, continue to be required to obtain judicial authorization to undertake certain intrusive activities.

I believe this is clearly laying out the technical aspects of this legislation, and nobody can challenge the motive of this bill.

[Français]

Encore aujourd'hui, monsieur le président, on a appris que l'organisation terroriste islamiste était en train d'enrôler des enfants de huit ans, comme si toutes les images auxquelles nous avons été exposé, les atrocités auxquelles nous avons été exposés n'étaient pas suffisantes. On pense à une vidéo montrant plus d'une douzaine d'hommes en train de se faire décapiter qui a été diffusée.

On y trouvait notamment le travailleur humanitaire Peter Kassig. Ses parents ont écrit sur Twitter qu'ils avaient le cœur brisé d'apprendre que leur fils avait perdu la vie en raison de son amour pour le peuple Syrien et de son désir d'aider leurs souffrances. Notre gouvernement condamne fermement les actes de violence commis par l'organisation terroriste État islamique dans les termes les plus fermes qu'il soit. C'est la raison pour laquelle nous apportons une aide humanitaire au peuple persécuté par ces horreurs et également que nous appuyons la coalition dans ses efforts pour neutraliser et diminuer leurs capacités à mener des opérations d'envergure.

En plus de ces rapports consternants en provenance d'Irak et de Syrie, des attaques terroristes récemment survenues ici au pays nous rappellent que cette organisation constitue aussi une menace ici à l'intérieur de notre pays. C'est également la raison pour laquelle nous travaillons avec détermination à améliorer les outils dont disposent nos forces policières et le milieu du renseignement. La loi sur la protection du Canada contre les terroristes n'est qu'une première étape en vue d'atteindre cet objectif. Notre gouvernement conservateur a pris des mesures énergiques pour protéger notre sécurité nationale.

Comme vous le savez, monsieur le président, nous avons adopté la Loi pour combattre le terrorisme, il y a déjà de cela plus d'un an. Cette loi donne aux autorités des outils qui leur permettent de révoquer la citoyenneté des personnes qui prennent part à ces activités. Comme je l'ai mentionné, essentiellement, la composante du projet de loi qui est devant vous aujourd'hui consiste à accélérer les mesures qui ont déjà été adoptées et qui ont reçu la sanction royale.

Bien sûr, nous avons augmenté du tiers le financement accordé à la Gendarmerie royale du Canada et au Service canadien du renseignement de sécurité. Nous avons mis en place de nouvelles mesures, malheureusement, pour la révoque des passeports et l'interdiction de la double citoyenneté pour les individus reconnus coupables d'actes de terrorisme, nous n'avons pu compter sur le soutien de l'opposition tenu des Néo-Démocrates ou des Libéraux. Mais j'ai remarqué pendant les débats une certaine réception au projet de loi qui est présente aujourd'hui.

I realize that this bill was not formally opposed during the debate at second reading, and I look forward to answering your questions today. Ultimately, and I would say much more importantly, I look forward to this legislation being returned to the House after thorough study so we can move forward and get this bill adopted so we as parliamentarians, elected officials, can better do our part to keep our country safe. Thank you.
The Chair: Thank you very much, Minister Blaney.

Are there any other opening comments from witnesses?

Seeing none, thank you. We will now go to the rounds of questioning. We'll start off with Mrs. James for seven minutes, please.

Ms. Roxanne James (Scarborough Centre, CPC): Thank you, Mr. Chair. Thank you to the minister for appearing, as well as the officials.

Minister, in your opening remarks you talked about the incident that happened here at the National War Memorial as well as what took place here on Parliament Hill. These incidents of terrorism were not simply attacks against an individual or a place where people go to work; this was in fact an attack against our Canadian armed forces and against our institutions of governance. This is in fact an attack against all Canadians.

At the start, when we talked about Bill C-44, there were some comments I heard that this was simply a knee-jerk reaction to those types of events that took place in Ottawa and in Quebec. In fact, Minister, this legislation has been in the works for some time and was to correct a problem that, as you mentioned, we saw an issue with before the courts, which were calling into question the authority of CSIS.

I'm just wondering if you could speak about that particular aspect, that this was not a knee-jerk reaction, and why this is absolutely critical for the operations of CSIS to continue to keep Canadians safe.

Hon. Steven Blaney: I thank Parliamentary Secretary James for her question, Mr. Chair.

The definition of a terrorist act is widely accepted throughout the world, and it has three components. The first one is that an individual or a group attacks a symbol of a nation. We are talking about the military uniform and we are talking about our sacred National War Memorial. It is also committed based on an ideology. We clearly saw that those two individuals were embracing extremist, fundamentalist, radical Islamic views. They are going against the Criminal Code by committing violent acts against innocent people.

Clearly, what took place in Canada on October 20 in Saint-Jean-sur-Richelieu...

[Francis]

avec l'adjudant Patrice Vincent et ici avec Nathan Cirillo à Ottawa sont deux actes de terroristes.

C'est ce que le président Hollande a reconnu quand il est venu ici au Parlement. C'est ce que le secrétaire d'État américain John Kerry a reconnu. C'est également ce que le commissaire de la GRC a dit et c'est également ce que nous dit le Code criminel. C'est la raison pour laquelle il est important d'agir de façon mesurée face à la menace terroriste, de ne pas réagir de manière excessive, mais également de ne pas rester assis alors que nous faisons face à une évolution constante de cette menace terroriste.

Comme le sait la secrétaire parlementaire — je crois savoir —, le projet de loi en question devait être déposé le 22 octobre, le jour même où nous avons subi cette attaque.

Je dois vous dire, madame James, que peu de temps après que l'attaque soit survenue, nous ne savions pas que nous allions être confinés ici toute la journée, puisque nous avons vécu certains moments d'incertitude. J'avais encore espéré de déposer ce projet de loi le 22 octobre. Clairement, ce projet de loi a fait l'objet de consultations et de préparation. Comme je l'ai expliqué, il constitue néanmoins une invitation des tribunaux à répondre à des clarifications juridiques nécessaires pour que le service puisse manifestement exercer son mandat.
Si j'insiste tant sur l'importance d'adopter ce projet de loi, c'est qu'en ce moment, la capacité du service à exercer pleinement sa fonction est limitée par ces décisions. C'est la raison pour laquelle nous, comme parlementaires, sommes invités à faire cheminer ce projet de loi pour qu'il obtienne la sanction royale, afin de redonner des autorités déjà existantes au Service canadien du renseignement de sécurité à un moment critique où nous faisons face à une menace terroriste réelle.

Alors, pour répondre à votre question, clairement, ce projet de loi était en préparation bien avant les deux attaques terroristes que nous avons connues ici la mi-octobre au Canada, mais ces attaques rendent son adoption d'autant plus importante et urgente.

[1550]

Mr. Roxanne James: Thank you, minister.

In your remarks you said something similar to “not as clearly outlined in the CSIS Act as it should be”. I think everyone in this committee recalls, and I've mentioned it many times in conversations and in the House, that the CSIS Act was first passed way back in 1984. This is actually 30 years ago. The fact that CSIS has been operating and communicating with our five partners and operating outside of Canada and all of a sudden the courts have called that into question because the CSIS Act doesn't clearly indicate they have the power and the ability to do so is why we're really here today.

When we talk about terrorism in Canada I think most Canadians would agree that when we heard about the Toronto 18 it's something that we had not heard about before in Canada. We also experienced, more recently, the VIA Rail plot. Now we have seen cases of individuals being radicalized, going overseas, and receiving training overseas with the potential to come back here and cause even greater damage and assault against Canadians in our country within our borders. In reality, terrorism knows no borders.

When I think about this bill, minister, my greatest concern is that we absolutely have to give CSIS the ability to be able to operate overseas. Without it, they would be working with both hands tied behind their back.

Would you agree with that statement?

Hon. Steven Blaney: Absolutely.

I fully agree with you. I believe that while we have to make sure that we are providing all the tools, especially in this case, to our national security agency, the service, we also need to continue to invest ourselves in the four pillars of our counter-terrorism strategy particularly in the domain of prevention. This is exactly what was agreed upon amongst the 300 participants who took part in the Halifax International Security Conference that just ended yesterday where there was a consensus among western countries that we need to reach out with outreach to communities. You have the example of the Toronto 18. As you know it was because of the bridges we had built with the communities that we were able to deter this terrorist attack that was plotted. Mr. Coulombe is very aware of this.

In the meantime we also need to show our unwavering commitment in tracking those who are committing a terrorist attack or willing to do so. This also includes hate violence whether in their behaviour or in their speech. We also need to make sure that we have the tools that are necessary, not only to our national security agency, but to our national law enforcement that needs to have the tools as well. That's why I intend and our government intends to come back with further legislation to address this gap that we are faced with.

The Chair: Thank you, minister.

We'll now move on to Mr. Garrison, please.

You have seven minutes.
Mr. Randall Garrison (Esquimalt—Juan de Fuca, NDP): Thank you, Mr. Chair.

I'd like to thank the minister for being here today.

The NDP supported this bill at second reading because we believe it deals with national security which is obviously a very important issue. Precisely because of that importance we have to make sure that any changes we make get them right and that they are effective. That really requires full debate on this bill.

What I want to raise is something I raised with the minister in the House during time allocation. At that time I asked the minister he would assure me that we would have full time for debate here in the committee. Again, today, he mentioned in his opening statement he looked forward to the committee giving thorough study to the bill.

I'm going to ask him again. His parliamentary secretary, who is his spokesperson in the House, has made sure that we have only one day of witnesses other than government officials. That means six witnesses on this very important bill.

I ask the minister again, do you think that we're actually going to have enough time here in committee to give this bill the study that it deserves?

Hon. Steven Blaney: Absolutely. Well as you know why the committee is determining I think as rightfully evaluated at the time needed to work on this straightforward bill as I have been given the opportunity to mention to now during the debate in the House of Commons it's a seven pages bill. Basically it says that CSIS can operate out and within Canada. It says that we need to protect the sources which is obvious since it's where CSIS is harvesting its information that can be transformed from intelligence to evidence and then where we can prosecute terrorists and put them in jail. Rightly so as we have already been doing with the Combating Terrorism Act and the previous legislation.

So I believe there has already been more than nearly 11 hours on the debate. I think we are expected from Canadians, especially in the context of an evolving threat to do a thorough work but not to drag on our feet and spend wasteful time as this bill is needed. As you know there are other measures that will be coming hopefully soon and that this is what Canadians are expecting from us. I think I refer to some comments that were in the media today where Canadians think we should take very seriously the terrorist threat and we should act accordingly. I think that adopting this bill after the study and we are here and the experts will be here available to answer all your questions.

Mr. Randall Garrison: But with respect, Mr. Minister, when we say one day that actually means two hours of this committee with witnesses outside the government. So if we are going to take terrorism seriously with respect I would think that two hours is not taking it sufficiently seriously.

Now you say it is only a seven-page bill so I have a question about something which is not there. We have seen recommendations from Justices O'Connor, Iacobucci and Major all of them dealing with the need for improved accountability in national security. The accountability is connected very directly to that effectiveness. So I guess my question to you, Minister, is a simple one, why is there nothing in this bill that improves the accountability and the oversight for our national security agencies?

Hon. Steven Blaney: Well I think you were given the opportunity to attend the technical briefing I've said it in the House and I said it again today, this bill is particularly designed to address two issues that were brought forward by the court which are limiting the power and the authority of CSIS. It is important at this very moment where we are facing a real terrorist threat, and these walls can speak by themselves, that we address this capsule. That's why this bill is straightforward. I take the commitment today that we will come with further legislation and that's why I seek your support for this bill.
Mr. Randall Garrison: Well I hope that the further legislation will have improvements in accountability and oversight because that’s part of the effectiveness, as I said before.

Another point that I am concerned about here and that’s why I think we need more time to discuss this is there’s no point in passing laws that won’t withstand scrutiny in the court. So I have a question for the minister about what advice he has received from the Department of Justice on the constitutionality of the measures proposed here. Particularly those that deal with authorizing courts to grant warrants without respect to international law. Also with respect to the protection of identity of human sources.

If these laws aren’t going to stand up when they get to court then we’re actually wasting time here when we could do something more effective. So has he had that advice? Will he table that advice with this committee?

Hon. Steven Blaney: Well actually I think our time is really precious and that’s why I seek this committee to move forward, Mr. Chair.

Let me just get back to the proceeding and I will address. I thank you for your question.

As I’ve said in criminal proceedings defendants will have the ability to seek an order from a judge declaring that disclosure of the identity of a human source is essential to establishing their innocence. The fundamental right to a fair trial is not only preserved it is reinforced.

Mr. Randall Garrison: Well only as to the trial, not to detention, not to bail hearings and other aspects of the criminal justice process. You’ve only applied that exception to one small piece of that. That’s why I am interested in the advice you have received from the Minister of Justice about the constitutionality of that.

Hon. Steven Blaney: In another bill from this one we will come back with issues related to surveillance, arrest and detention. But this is not what this bill is about. This bill is about protecting the source. This is exactly why we have embedded in this bill measures to reinforce the fundamental right, not only respecting the law but the spirit of the law which I think is even going further.

The other aspect is you know we are talking of Canadian citizens—and I expect this question may come further on during our exchange—Canadian law and Canadian procedure. We are sometimes working in an environment where people don’t experience the freedom and the democracy that is experienced here. That is why this bill is related to Canadian law and that’s why it is a bill that is fully complying with our Constitution.

Mr. Randall Garrison: So you have that advice from the Minister of Justice?

Hon. Steven Blaney: We are always moving forward with bills that are seeking to protect Canadians. That’s our first goal and priority and this is how this bill has been prepared, with all respect to our Canadian Constitution.

Mr. Randall Garrison: Thank you very much.

The Chair: Thank you very much, Mr. Garrison.

Now we will go to Mr. Norlock for seven minutes, please.

Mr. Rick Norlock (Northumberland—Quinte West, CPC): Thank you very much.

Mr. Chair, through you to the witnesses, thank you for attending today.

Minister, I notice that this act has certain aspects of the recently passed Strengthening Canadian Citizenship Act. Do you believe it’s reasonable to revoke the citizenship of convicted terrorists, or people who would do harm to Canada?
Hon. Steven Blaney: Thank you, Mr. Norlock, for your question.

Well, we are very proud to be Canadian. Whenever we go around the world, we are also very proud to show our Canadian passport, which is well recognized and established.

What we realize is that individuals are abusing the generosity of Canadian individuals who have embraced Canadian principles and values and are ready to turn their backs on this society.

Last Friday, I just met with the Cultural Roundtable where we have people coming from different backgrounds. Most of them are not Canadian-born citizens and they all agree that when we are Canadians, we are winners. We are winners of the lottery. We are a great country, and to be a citizen of this country is a great privilege.

Those individuals who are committing terrorist acts using the Canadian passport don't deserve to use their citizenship to propagate violence around the world. That is why, once they are convicted of a terrorist act, I find it fairly appropriate to remove this tool and this great privilege to be a Canadian citizen.

Mr. Rick Norlock: Thank you, Minister.

What you are saying is that citizenship is a great honour and to those who would do otherwise, it is not a right. At least that's what I think you said, and that's what I believe.

Minister, I'd like to go further into this piece of legislation. One of the parts of the legislation deals with judicial oversight over CSIS warrants. We've heard statements that we have to respect international law and laws of other countries. I think of some countries that don't have the respect for human rights and the rule of law, as our country. They may get warrants in ways that we would find totally inappropriate, and that is totally against all we stand for as a country that respects human rights.

I wonder if you could comment on judicial oversight, the necessity of issuing warrants, and comment on this provision and why you believe it makes sense.

Hon. Steven Blaney: I thank you for your question.

CSIS operates under Canadian law. This is why we have set up a package of law that is making sure that whenever they operate, they are operating within the law. Of course, I may be involved in those authorizations, but, more importantly, judges warrant when our issues need to be validated by the judicial system. On top of that, we have an overview mechanism of the whole service, and this is done by the Security Intelligence Review Committee. I have brought here a copy of that report. It's in both official languages. We have a robust oversight of an agency which is to abide by Canadian law. This is exactly what this bill is doing. We have, over the course of the last month, been given the opportunity by the court to clearly define that CSIS has the mandate to operate within and outside the country. That's the first main part of that bill. The second part of that bill, which is so important, is to protect the sources. To quote the definition of "source" in this bill:

"Source" means an individual who, after having received a promise of confidentiality, has provided, or is likely to provide, information to the Service;

When the service is entering into a contract, if I can put it that way, with a "human source", there is this promise of confidentiality. These sources are sometimes putting their lives at risk to share this information. That is why it is important, if we put it that way, this contract be clearly defined under the law and under circumstances this protection can be used in a trial or tribunal if it is used to prove that someone is accused.

This bill has been crafted based on our constitution, based on our laws and based on the principle, as I've mentioned, that the fundamental right to a fair trial is not only preserved, but reinforced. That's why I'm seeing your approval for this bill, which is accomplishing those two main important things: protection of human sources within our constitution, confirming the
authority of CSIS to operate abroad, and, as we have indicated, speeding up the process of removing dual citizenship, while adding no other element to the already-adopted bill.

Mr. Rick Norleek: It's not dissimilar to the rights and to the tools that exist for police officers within Canada, and has been so for some time, and has stood the test of many court challenges over the years. I think what you're saying is it would be reasonable to assume that this would withstand the test of the courts in Canada, as the legislation currently exists.

Hon. Steven Blaney: Absolutely.

The Chair: Fine. Thank you very much.

Now we will go to Mr. Easter. Seven minutes, please.

Hon. Wayne Easter: Thank you, Mr. Chair.

Welcome, minister. You no doubt will be aware that I forwarded to your office a series of nine questions that I had hoped you could provide written answers to prior to this committee. I wasn't actually over-enthused with the response I got back from your office and I'll quote it.

It is preferable that Mr. Easter pose these questions to the minister officials on Monday to allow the responses to be on the record and have all members of the committee be able to hear the responses to these specific questions.

Anyway, Mr. Minister. I do have those questions in both official languages here. Mr. Chairman, and ask the clerk to distribute them. I may or may not get into them, but I would request because they are quite technical that your office provide the committee with answers prior to us going to clause-by-clause because it is asking for some technical responses in terms of the bill. Before I get to the specific bill, but related, when you last appeared before us on October 8th you said "we know of about 80 who have returned to Canada" (meaning terrorists who operated abroad, or Canadians who operated in terrorist entities abroad). This is your quote let me be clear that these individuals posing a threat to our society at home have violated Canadian law as passed by this Parliament in the Combating Terrorism Act.

My question to you, none of these people have been arrested yet as I understand it, although you said they violated the Canadian law. I have said to you in the House that I believe they should be able to be arrested under section 83.18(1). I'll not get into it. There's four different evaluations there. Can you answer one?

Why hasn't section 83.18(1) of the Criminal Code been used to arrest those individuals? Two, are there components in this bill that will allow you to arrest those individuals where you're not now able to?

Hon. Steven Blaney: I thank you for your question and also your detailed written question and we'll do our best to answer them properly.

Related to your written question they are related to the bill. Now if I get back to your asks today they are more abroad, but I'll try to answer it also properly. This number if I go back to the latest information provided by Commissioner Paulson are around 93 individuals. Now, Mr. Easter, as you are well aware and you've been in that position before it is not because you suspect an individual to have contravened the criminal law that you necessarily are being able to transfer this intelligence into evidence. That's why we need to move forward as the legislator. That's why I will come back to this committee to address this issue, and that's why I hope I can count on your support to do exactly that. To get back to the existing provision of the Criminal Code Commissioner Paulson has already indicated that the threshold was too high so that they were not able to proceed.

Hon. Wayne Easter: Yes, but sir, you did indicate they violated Canadian law.
My secondary question on that is, if the threshold is too high to meet and to charge them is there anything in this bill that does that or will it be new legislation? You can answer that with my other question.

When you go the bill it specifies, in subsection 12:

Within or outside Canada for CSIS action under its collection duties.

And in subsection 15:

And its investigative functions.

This bill introduces an extraterritorial element within the kind of checks and balances present in section 16:

Of the foreign intelligence of the obligation of consultation with the minister and foreign affairs.

From that complicated wording, under foreign affairs, if Canada is going to have some of its people do something there's a check with the foreign affairs minister because anything we do in a foreign country can impact us in other areas with that foreign country.

As I see it under this bill there are no checks and balances where CSIS is going to do something that violates the law of another country but we're able to do because of the warrants issued within Canada. There doesn't seem to be those checks and balances to protect our foreign affairs interests whether in trade or in other areas.

Can you, or someone, clarify that for me? Where are the checks and balances to protect Canada's interest when we take action under this section?

Honi, Steven Blaney: I'll answer that question first.

This is exactly why the service is conducting its operation to protect the interest of Canada, its companies, its citizens, it's safety, but also its interests.

To get back to your first question this bill indeed addresses this indirectly and makes it easier to track terrorists. This is because we will be able to gather better intelligence. Why? Because we will be able to guarantee a level of protection to the witness which is critical in gathering intelligence and because we will be able to operate prior to those two court decisions. Basically, we will just get back to where we were before those court decisions which are, at some point, diminishing the capability of service to protect us. Obviously, this will have a positive impact because we know, when we want to lay charges we need to have strong cases and those cases are emanating from intelligence.

The answer is yes. This bill is definitely a step in the right direction. We need to do more and that's why we will come back with additional measures in the near future.

The Chair: Thank you very much, Mr. Easter.

Your time is up. We will now go to Madam Doré Lefebvre.

[Français]

Mme Rosanie Doré Lefebvre (Alfred-Pellan, NPD): Merci, monsieur le président.

Merci, monsieur le ministre, d'être présent aujourd'hui.

Je vais revenir sur une question que mon collègue M. Garrison vous a posée. Pouvez-vous nous confirmer, par un oui ou par un non, si le projet de loi C-44 est constitutionnel?
L'hoi. Steven Blaney: À mon avis, c'est le projet de loi le plus constitutionnel que nous ayons présenté et que vous aurez l'occasion d'appuyer.

Mme Rosane Doré Lefebvre: Avez-vous reçu des avis juridiques à l'effet qu'il était constitutionnel?

L'hoi. Steven Blaney: Bien sûr, nous considérons toujours les éléments juridiques.

Comme je l'ai indiqué clairement dans ma présentation, non seulement le projet de loi vise à renforcer la capacité d'un individu de recevoir un jugement juste et équitable, mais aussi vient le renforcer et le définir. Les mécanismes pour ce faire sont décrits au troisième paragraphe de l'article 7.2 du projet de loi qui stipule qu'on peut même avoir ce que l'on appelle un _amicus curiae_, donc un ami de la cour, qui vient en quelque sorte enchâsser et encadrer l'application des droits de la personne en cause.

Alors, absolument. C'est un projet de loi qui constitue un moyen efficace de renforcer la sécurité des Canadiens tout en respectant pleinement, du même souffle, l'esprit de nos lois canadiennes et de la Constitution, en particulier de la Charte canadienne des droits et libertés.

Mme Rosane Doré Lefebvre: Vous avez touché le cas du SCRS. C'est un projet de loi qui est, en grande partie, relié au Service canadien du renseignement de sécurité, mis à part ce qui touche le Service canadien de l'immigration. Au cours des dernières semaines, nous avons beaucoup parlé de l'importance de la sécurité publique, tout en n'oubliant pas non plus les libertés civiles qui y sont reliées et en trouvant un équilibre entre les deux. Pourquoi ne pas avoir donné, en même temps, de meilleurs outils au service de surveillance publique du SCRS?

L'hoi. Steven Blaney: Je vous remercie pour votre question. Je crois me souvenir qu'elle a été soulevée pendant les débats à la Chambre des communes. Premièrement, parce que nous avons d'excellents mécanismes de supervision. J'ai ici le rapport annuel 2012-2013 du Comité de surveillance des activités de renseignement de sécurité, dont tous les membres ont obtenu une copie.

Il est formé de Canadiens et Canadiennes éminents et éminentes qui, à chaque année, font rapport au Parlement, il faut rappeler qu'ils sont imputables au Parlement et qui s'assurent que le Service canadien du renseignement de sécurité exerce ses fonctions dans le plein respect des lois canadiennes. Comme je l'ai précédemment indiqué, je m'attends à ce que le Service donne suite aux recommandations qui ont été formulées dans le rapport de cette année. Le Comité de surveillance des activités de renseignement de sécurité fait un travail important et très rigoureux.

Mme Rosane Doré Lefebvre: J'ai une autre question concernant la partie qui touche la loi renforçant la citoyenneté canadienne. C'est un projet de loi sur le Service canadien du renseignement de sécurité. Pourquoi avoir rajouté cela? Est-ce qu'il y a un rapport quelconque? Je ne comprends pas nécessairement le lien entre le SCRS et le rapprochement des dates d'entrée en vigueur.

L'hoi. Steven Blaney: Essentiellement, c'est pour faciliter et accélérer la mise en application de l'enlèvement de la double citoyenneté dans la cas d'individus reconnus coupables. Donc, il n'y a aucun élément législatif, et peut-être que Mme Girard pourra compléter aucun nouvel élément législatif, si ce n'est que de faire en sorte que la loi qui a été adoptée puisse entrer en vigueur plus rapidement.

Juste avant, je voudrais simplement vous préciser qu'au niveau comme tel des mécanismes de surveillance, je le rappelle, les articles 7.4 et 7.5, donc il y a des mécanismes qui sont prévus pour faire en sorte que les tribunaux soient impliqués lorsqu'il y a des possibilités pour enlever la protection d'une citoyenneté et ces dispositions sont prévues à l'intérieur du projet de loi.

Peut-être que Mme Girard pourrait commenter sur la citoyenneté, sur l'accélération...

Mme Nicole Girard (directrice générale, Direction du programme de la Citoyenneté et du Multiculturalisme, ministère de la Citoyenneté et de l'Immigration): Je n'ai pas grand chose à rajouter à ce que monsieur le ministre dit. Essentiellement ce sont deux éléments distincts de ce projet de loi C-44 qui vous a été très bien décrit par le ministre. Les objectifs sont...
complémentaires dans le sens où les changements techniques qui sont proposés à la Loi sur la citoyenneté permettront aussi de rejoindre ce même objectif, qui est de renforcer la sécurité publique, la sécurité des canadiens et des canadiennes et de renforcer la valeur de la citoyenneté canadienne et de l'intégrité du programme.

[English]

The Chair: And we will now go to Ms. Ablonczy, please, for five minutes.

Hon. Diane Ablonczy (Calgary— Nose Hill, CPC): Minister, this act contains amendments to the CSIS act which would clarify that CSIS may perform its duties and functions within or outside Canada. I wonder if you would tell us why you think that clarification is important.

Hon. Steven Blaney: Thank you.

The reason why it is so important is that this law was crafted 30 years ago, and at that time it would seem that it was not necessary for the legislator to clearly specify that CSIS can operate in and outside Canada. In a late judgment that was rendered by the Supreme Court, it was acknowledged that it might be pretty useful, especially in the context of foreign fighters, terrorist attacks coming from abroad, that the service actually operate outside, which it has done over the course of the last year. That's why it is important to clearly specify in the basic law of the service that this principle be entrenched.

Hon. Diane Ablonczy: I note, too, that the act and others are mentioned as would allow CSIS to protect their sources in the same way that police officers can protect their sources, because no one obviously is going to give you information if they can be hung out to dry, shall we say. I guess I'm a little puzzled about why CSIS wouldn't have already had this ability to protect their sources, and I'd like to know why you think it's important that it be in this legislation?

Hon. Steven Blaney: That's a good question. Actually, I will turn to Mr. Coulombe. But one thing is sure, we clearly need it in order to maintain the quality and the reputation of the service and the accuracy of the data that they are collecting. Although before this court decision, this right, if I can put it that way, was taken for granted. Due to this court decision, we are clearly invited as a legislator to clearly define it in the law.

Monsieur Coulombe.

[Français]

M. Michel Coulombe (directeur, Service canadien du renseignement de sécurité): Merci, monsieur le ministre.

[English]

In terms of the first part of your question of why it's not in the act at the moment, if you go back 30 years, at the time it was not envisaged that the service would be involved as it is today in administrative proceedings or criminal prosecutions, just because the threat has evolved and the growing place that terrorism is taking.

I think it is pretty obvious why we need to protect our sources. We've talked about it in terms of nobody wanting to cooperate with us if they were putting their life at risk.

But I think it's also very important that we shouldn't lose sight that when somebody—and quite often at the risk of their own security and with promise of confidentiality—is cooperating with the service. I think the state has a duty to protect that person, and to protect their identity so that we can protect their security—and not just protect them, but sometimes their family, also. So I think there is a duty on the part of the state.

Now we have to balance that, in different proceedings, with how we maintain fair proceedings. I think the bill has achieved that balance.
Hon. Diane Ablonczy: I read an opinion that indicated that police evidence-gathering is different from CSIS information-gathering, so CSIS sources don't need the same protection. Would you comment on that, please?

Mr. Michel Coulombe: It is true that the service is not an enforcement agency. We are in the business of collecting evidence. But again, because of the evolution of threats, we are more and more indirectly—and sometimes directly—involved in non-criminal investigations, because we run parallel investigations with the RCMP, but just because of the nature of the relationship and exchange of information, at times service information will be used in criminal proceedings, or could be used regarding security certificates, for example. Although we are not in the business of collecting evidence, that's why our intelligence will be either challenged, or there will be a request for more disclosure, including the identity of human sources.

It's just that the nature of the threat environment has changed and has basically changed the service interaction in terms of dealing with those different proceedings.

The Chair: Fine, thank you very much. Time is up.

Now, Mr. Garrison, five minutes, please.

Mr. Randall Garrison: Thank you very much, Mr. Chair.

I just want to stress again, Mr. Minister, that when you talked about this bill at the outset we had hoped the bill could be made effective, and we had hoped we could have all-party support for that bill. I have to say that the attitude of the government is now making me very doubtful.

We share the same interest as you in making sure that our national security agencies maintain their quality and the reputation of their services, and we think that accountability is quite important to that. There is nothing in this bill on that.

You mentioned the challenge of transferring intelligence into evidence. I think those were your words. We share the concern about taking intelligence and making sure you can use it in prosecutions.

I have a concern that the way this bill is drafted may, in fact, make it more difficult to do those prosecutions. When you talk about the protection of the identity of witnesses, the courts can protect the identity of CSIS sources on a case-by-case basis now. They didn't say that wasn't possible.

When you say that they invited you to do this, I believe that if you read the decisions, they said that Parliament could do this. They didn't say that it was necessary, and it didn't say that Parliament should provide this blanket protection, it said that it was possible.

So my question really is, why risk this change to limit the rights of the defence to challenge the use of intelligence information in prosecutions? Why risk a change that might either make it more difficult to prosecute, or might result in these provisions being declared unconstitutional? Why are you risking that in this bill?

Hon. Steven Blaney: I thank the member for his numerous questions.

The first response would be that some of the questions are going beyond the scope of the law, and I have clearly stated that this bill is crafted to ensure it responds to the invitation of the courts.

All western countries are faced with the challenge of terrorism. I have here a press release from my U.K. counterpart, Theresa May, who is coming up with more than eight measures to tackle terrorism and says that time for new policies is required, and why?—because we need to adjust to this threat, that's clear.
What I've clearly demonstrated this afternoon is that we are doing it while respecting the Constitution with the amicus curiae in the protection of witnesses whenever someone is accused.

The member has asked a question on the oversight. Well, we have a robust oversight and clearly this is going beyond the scope of this bill, but we have a clear mechanism that is working and will ensure that while CSIS is protecting Canadians, there is robust oversight.

I would say, Mr. Chair, that to me it is clear that there is no liberty without security.

Mr. Randall Garrison: With respect, Mr. Minister, all the commissioners that have looked into these questions have agreed with you on half of that. You forget the other half that they've said, and that is that we need improvements. If you're going to give more powers to national security agencies, especially in this time of technological change, then you need improvements in the oversight, so I think it is connected to bill even though it's not here. But I want to give you one more chance on this question of why you're risking the chance of making it very difficult to use intelligence information in criminal prosecutions by this very limited protection, this limited exemption in this bill.

[Fransais]

L'hon. Steven Blaney: Ce projet de loi vient clarifier les autorités des services, il va faciliter le travail des tribunaux, parce qu'il vient lever les ombrages qui existaient dans l'application de la loi, autant au niveau de la protection des témoins que la capacité du service, non seulement à opérer à l'étranger, mais également à échanger des informations avec nos alliés comme la Grande-Bretagne, l'Australie, la Nouvelle-Zélande, comme les Américains, les Français qui sont alliés et qui sont aux prises avec le même défi auquel nous sommes confrontés. C'est-à-dire de suivre des individus qui se promènent d'un pays à l'autre et qui menacent la sécurité des Canadiens, qui s'attaquent à des personnes innocentes. C'est exactement ce que ce projet de loi vient faire, il vient restaurer les autorités qui ont permis au service, par le passé, d'être efficace et à un moment critique où nous faisons face à une menace qui évolue, il est d'autant plus important de préserver les capacités du service à protéger les Canadiens.

[English]

The Chair: Thank you very much, Mr. Garrison.

Minister, thank you very very kindly for coming here today and we thank our guests as well.

We will suspend briefly just for a minute while the minister excuses himself, and we will welcome our new witnesses to the table.

[Back in session]

The Chair: Colleagues, we are back in session.

We will welcome our new witnesses here today.

We have Lynda Clairmont, Senior Assistant Deputy Minister; National and Cyber Security Branch; we have Rahul Francis, director of the Intelligence and Policy Division for the National and Cyber Security Branch; and we have Mary Afsar, senior counsel, Citizenship and Immigration Canada Legal Services.

Any of the three new witnesses are entitled to make a statement, should they wish, otherwise we will go directly to questions.

We're all fine? Thank you very much.
We will go to rounds of questioning then. We will start off with Mr. Carmichael, please, seven minutes.

**Mr. John Carmichael (Don Valley West, CPC):** Thank you, Chair, and thank you to our witnesses for attending today.

This is obviously a very interesting session as we deal with concerns of Canadians from coast to coast to coast. As I’ve travelled through my riding, I’ve heard from Canadians on this issue since October 22, and the horror that... well, actually before that, because we had the tragedy in Saint-Jean-sur-Richelieu, with Warrant Officer Vincent, and then we were confronted with the horror of the terror attack here on Corporal Cirillo, and then in the House. Canadians have been very responsive to these issues and our security and our safety is clearly something that they hold dear and for which they have great concern; how can these types of acts happen and what can we do to protect our shores and protect our borders?

What I’d like to talk to you about or ask you about first off—and I’ll let you decide the best one to respond on this—is around the fairness of revoking citizenship of dual-nationals. At your last appearance, Mr. Coulombe, we talked about the number of citizens who have gone overseas, who are taking part with ISIS in Syria and Iraq, and those who have returned. We addressed some of the numbers and the concern of how we’re going to deal with these people. But I want to talk about the provision in the bill for the revocation of dual citizenship, where we have somebody who has been charged with terrorism or treason, served their time overseas, and then come back. Canadians have asked about the fairness around this particular clause. I wonder if you could comment on it. I won’t go any further as far as what I’m hearing. I’ll leave it for you to perhaps comment on the importance of this issue.

**Ms. Nicole Girard:** Thank you very much for your question.

I would just note at the outset, as mentioned earlier, that the provisions in Bill C-44 are technical amendments which would not bring any changes to the provisions of the Strengthening Canadian Citizenship Act, which received royal assent in June last year. They would enable the government to pursue an earlier implementation of the changes to the revocation provisions in the Citizenship Act.

Nevertheless, to come directly to your question, I think the first, most important point to make is that Canada is alone compared to like-minded countries and other democratic countries in not having this ability already to revoke citizenship for egregious actions that are done against a national interest, and so the recent changes that Parliament made in June to expand the grounds for citizenship revocation limited to specific actions—namely convictions for high treason, treason, spying, terrorism, or being in the service of an organized armed group or armed force engaged in armed combat with Canada—is broadly in line with what like-minded countries already do.

I would also like to add that with regard to fairness, there are many safeguards that are provided in the law and as a matter of procedure with regard to the revocation process itself. Those include notice; the ability of the person concerned to know the grounds against them; to see the evidence; to have an opportunity to respond and make their submissions; to receive a decision in writing; to potentially have a hearing with the decision maker; and of course, to seek judicial review if in the end that decision is against them and revoking their citizenship.

Thank you.

**Mr. John Carmichael:** Thank you. Quite frankly, I think that is in line with the general consensus amongst Canadians today that citizenship is a privilege and should be respected as such. I appreciate your comments. Thank you.

I’d like to address this to Mr. Coulombe, perhaps, and you can direct it elsewhere, with regard to informants.

**Mr. John Carmichael (Don Valley West, CPC):** Thank you, Chair, and thank you to our witnesses for attending today.

This is obviously a very interesting session as we deal with concerns of Canadians from coast to coast to coast. As I’ve travelled through my riding, I’ve heard from Canadians on this issue since October 22, and the horror that... well, actually before that, because we had the tragedy in Saint-Jean-sur-Richelieu, with Warrant Officer Vincent, and then we were confronted with the horror of the terror attack here on Corporal Cirillo, and then in the House. Canadians have been very responsive to these issues and our security and our safety is clearly something that they hold dear and for which they have great concern; how can these types of acts happen and what can we do to protect our shores and protect our borders?

What I’d like to talk to you about or ask you about first off—and I’ll let you decide the best one to respond on this—is around the fairness of revoking citizenship of dual-nationals. At your last appearance, Mr. Coulombe, we talked about the number of citizens who have gone overseas, who are taking part with ISIS in Syria and Iraq, and those who have returned. We addressed some of the numbers and the concern of how we’re going to deal with these people. But I want to talk about the provision in the bill for the revocation of dual citizenship, where we have somebody who has been charged with terrorism or treason, served their time overseas, and then come back. Canadians have asked about the fairness around this particular clause. I wonder if you could comment on it. I won’t go any further as far as what I’m hearing. I’ll leave it for you to perhaps comment on the importance of this issue.

**Ms. Nicole Girard:** Thank you very much for your question.

I would just note at the outset, as mentioned earlier, that the provisions in Bill C-44 are technical amendments which would not bring any changes to the provisions of the Strengthening Canadian Citizenship Act, which received royal assent in June last year. They would enable the government to pursue an earlier implementation of the changes to the revocation provisions in the Citizenship Act.

Nevertheless, to come directly to your question, I think the first, most important point to make is that Canada is alone compared to like-minded countries and other democratic countries in not having this ability already to revoke citizenship for egregious actions that are done against a national interest, and so the recent changes that Parliament made in June to expand the grounds for citizenship revocation limited to specific actions—namely convictions for high treason, treason, spying, terrorism, or being in the service of an organized armed group or armed force engaged in armed combat with Canada—is broadly in line with what like-minded countries already do.

I would also like to add that with regard to fairness, there are many safeguards that are provided in the law and as a matter of procedure with regard to the revocation process itself. Those include notice; the ability of the person concerned to know the grounds against them; to see the evidence; to have an opportunity to respond and make their submissions; to receive a decision in writing; to potentially have a hearing with the decision maker; and of course, to seek judicial review if in the end that decision is against them and revoking their citizenship.

Thank you.

**Mr. John Carmichael:** Thank you. Quite frankly, I think that is in line with the general consensus amongst Canadians today that citizenship is a privilege and should be respected as such. I appreciate your comments. Thank you.

I’d like to address this to Mr. Coulombe, perhaps, and you can direct it elsewhere, with regard to informants.
If an informant is involved with more than one investigation, they must have his or her identity released. It seems like you're left with a tough decision, a tough task in how to deal with that. The decision you need to make is between giving up their identity and risking losing intelligence that's been gathered from other ongoing investigations in hopes of getting a conviction, or risking losing that conviction to maintain other investigations.

Would this be an accurate portrayal of the situation, without having the similar protections afforded to informants to Canadian law enforcement agencies?

Mr. Michel Coulombe: It’s actually a very accurate picture of what we’re facing.

I would add one more thing. It is true at the moment that a judge can afford protection case by case, but because of those case-by-case uncertainties it is more difficult to recruit or get people to actually cooperate because there is that uncertainty in terms of their protection.

Mr. John Carmichael: The uncertainty is about their safety.

Mr. Michel Coulombe: Their safety, yes.

Mr. John Carmichael: Once they’ve provided that information, they’re vulnerable.

Mr. Michel Coulombe: Yes.

Mr. John Carmichael: That’s an important part of what we’re dealing with today, clearly.

Mr. Michel Coulombe: For us it is crucial.

Mr. John Carmichael: Do I have time, Chair?

The Chair: You still have another minute, sir.

Mr. John Carmichael: Monsieur Coulombe, without the assurance that their identity is being protected, has CSIS ever had issues with possible informants coming forward with information, and does that have a possible effect on the safety of the public? And to that, is there a strong likelihood that without that security that informant will walk away from providing that information?

Mr. Michel Coulombe: Well, there is always that possibility. I don’t want to go into specifics, but again there’s always a possibility that somebody with information, knowing that his identity could be revealed, would decide not to share that information.

Mr. John Carmichael: Thank you.

The Chair: Thank you very much.

We’ll now go to Mr. Garrison, please, for seven minutes.

Mr. Randall Garrison: Thank you very much, Mr. Chair. I’m glad to see you back in the chair.

I guess one concern I was raising with the minister is that in fact part of national security, protecting the country, is protecting the rule of law. I just want to go to something that Director General Giraldeau said. In terms of the revocation of citizenship of dual citizens, she said there was the right to see evidence.

I’m wondering how the provisions in Bill C-44 protecting the identity of CSIS human sources connect with the citizenship process. In other words, if evidence that’s being used from CSIS sources is the evidence that’s being used for the revocation of citizenship, then what provisions are there? The only exemption for defence here is about criminal prosecutions, not citizenship.
there an inner section between the two bills there, or any exemption provided for use in those
citizenship processes?

Ms. Nicole Girard: Thank you for your question.

I would just respond by stating that the two provisions of this bill are distinct. They are not
intended to be related other than they both support the objectives of the safety and security of
Canadians.

Then the other point more directly in response to your question is that citizenship revocation
cases would be initiated based on objective, open-source information to determine whether the
provisions apply.

That's how I would respond to your question.

Thank you.

Mr. Randall Garrison: There is no provision for using CSIS information in those
proceedings.

Ms. Nicole Girard: There is not as contemplated by Bill C-44 nor the changes under the
Strengthening Canadian Citizenship Act.

Mr. Randall Garrison: Thank you very much.

I'm going to turn to Deputy Minister Guimont. I'm going to go back to the question of advice
on constitutionality of this exemption provision from the Minister of Justice. The minister talked
around the point, I think is the most terrible I can be. Can you tell us whether you received
advice on that specific point from the Minister of Justice or the Department of Justice, and if you
received written advice would you table it with the committee?

Mr. François Guimont (Deputy Minister, Department of Public Safety and Emergency
Preparedness): The advice from justice is always factored in the cabinet process, always. That's
number one. Number two, the aspects of the bill are consistent with the charter and Canadian
law. That's number two. Number three is this is part of cabinet confidence. I'm not trying to be
difficult. I'm trying to be respectful of the committee but you are aware of how that
system unfolds, so that's my answer.

Mr. Randall Garrison: I respect that, and I am aware, certainly, and expected you to say it
was a cabinet confidence, something the minister, of course, could have said, but there is a
problem here then. We really need more time to have experts in on this so that we can get our
own advice in the committee on whether or not it's constitutional since we can't see the
government's advice on this, and that is where we run up against the time limits and the number
of limited witnesses here makes it very difficult for us to do.

On a similar question, I would go directly to ask if any other like-minded countries, the Five
Eyes countries, have provisions in their acts that allow ignoring the law of other countries or
ignoring international law in the collection of

Mr. Michel Guimont: On specifically having it in their legislation, I'm not aware of any.

You have to understand that each and we'll talk, for example, of the Five Eyes partners—
everybody is working under different legislation, different frameworks, so it's very difficult to
compare.

I'm not aware of any other countries, partners that would have the same type of legislation.

Mr. Randall Garrison: What would be the response of the government then if we had a
foreign intelligence agency collecting intelligence in Canada in contravention of Canadian laws?
How do you deal with that? There seems to be a normal principle, which I think is called comity
of international law, where we don't violate each other's sovereignty and we don't conduct illegal
surveillance in each other's countries which, to me, would seem to be part of that.
If we're now telling people we might be doing that to them, what would our response be to another country saying it is going to do the same thing in Canada?

Mr. Michel Coulombe: Maybe I can just correct my previous answer because I'm not an expert on the legislation. Just quickly reading this, actually New Zealand, in its legislation with regard to foreign intelligence warrants, which is what we're talking about here, says that it can be issues notwithstanding anything to the contrary to any other act.

Mr. Randall Garrison: That's any other act of New Zealand, not of any other country.

Mr. Michel Coulombe: We can certainly dig down on that question and provide the committee with a better answer. As I said, I'm not coming here prepared to—

Mr. Randall Garrison: I appreciate that, and I thank you for being cooperative. I just will remind you that our deadline is going to be before next Monday since we're going to be moving on to amendments to this bill.

I guess it still comes back to the question what is the Canadian response then to foreign intelligence agencies conducting things that would be illegal here. How do we respond to that if we're now saying “We may do the same thing to you?” I find it troubling.

Mr. Michel Coulombe: You have to understand that with like-minded partners, we do work overseas jointly. It's not like we would go into a friendly country and do things covertly. As a security intelligence service, and not just as a service—all of our partners do conduct covert operations. That's kind of obvious, and although it might not be specific in their legislation, that's what a security service will do at times but most of the time for the service we do our work overtly with our partners when they are like-minded, but there could be occasions when we're sending intelligence officers, for example, into countries that are not like-minded where we might not tell that country what we're doing because of the national interests of Canada but also for the safety of our officers.

The Chair: Very briefly.

Mrs. Ritu Banerjee (Director, Intelligence Policy Division, National and Cyber Security Branch, Department of Public Safety and Emergency Preparedness): In the past when there have been issues of espionage in Canada we have used the security certificate provisions to seek the removal of those individuals. I'm thinking of Russian spy cases. So there are limited uses of our current legal framework to manage that, but it is very sensitive and very difficult.

The Chair: Thank you very much, Mr. Garrison.

Now we will go seven minutes.

Mr. Ted Falk please.

Mr. Ted Falk (Provencher, CPC): Thank you, Mr. Chairman.

Thank you to our witnesses here today for joining us. I've enjoyed listening to your presentations and your responses. I just want to clarify again that in the proposed legislation that we're discussing today there are no new authorities. Is that correct?

Mr. Michel Coulombe: Yes that is correct.

Mr. Ted Falk: It's a clarification of existing authorities.

Mr. Michel Coulombe: Exactly following the federal court decision of last year, and the federal court of appeal this year.

Mr. Ted Falk: Good.
So when we're conducting surveillance, or intelligence gathering in foreign countries what
kinds of activities would require a warrant in our country, or obtaining a warrant from the
judicial?

Mr. Michel Coulombe: When section 8 of the charter is at play.

Mr. Ted Falk: Let me clarify a little bit. Would it be fair to say that we would secure a
warrant from a judge if we were involved in any activity that would require a warrant here in
Canada?

Mr. Michel Coulombe: Yes that's a fair description.

Mr. Ted Falk: So we apply the same standard when we work outside of Canada than we do
here inside.

Mr. Michel Coulombe: Yes in fact Bill C-44 all it does in terms of section 21 is one that
deals with an acquisition of warrants we're just adding "outside". So it is the same article, the
same criteria that are going to be used.

Mr. Ted Falk: Good.

There's also been concerns raised regarding the rights of terrorists to a fair trial if they don't
know who their accuser is, or from where the information is being sourced. Can you maybe just
expand on that a little bit and comment on that, and whoever feels they want. Mr. Guimont I
do n't mind if you comment on that as well.

Mr. Michel Coulombe: Again, I think what's in the bill is exactly equivalent to class privilege
protection that police informants have. It was mentioned earlier, that has been tested a number of
times in court, so that's not different. Plus, there are exceptions if it is believed that it is essential
to devolve the identity of that source to prove the innocence of the person accused.

Mr. Ted Falk: Okay. In situations where we have to identify our source, do we provide
witness protection programs going forward?

Mr. Michel Coulombe: We could certainly look into it if we get there. With what's proposed
in Bill C-44, if we come to a point where we would have to identify our source, I guess with
discussion there's either the option—and it's a crown decision—to pull the information and
possibly the case would collapse, or we disclose the identity of the source and then there's the
question of assessing the risk to the security of that source and what we can do to mitigate that.

Mr. Ted Falk: But they've provided the information to us on the basis that we will respect—

Mr. Michel Coulombe: In confidence, yes.

Mr. Ted Falk: —their confidentiality. That creates a difficult situation in some scenarios.

Mr. Michel Coulombe: It does, and it goes back to my earlier comment, that I truly believe
there's also a duty on the part of the state, when you make that promise of confidentiality that
you have the measures in place to assure that promise you have with that person.

Mr. Ted Falk: When we're using the resource of a confidential informant, is there a practice
or procedure in place that confirms the information that's provided?

Mr. Michel Coulombe: We always try to corroborate information coming from sources, and
not just the human sources. We always try to corroborate and it doesn't matter if it comes from
partners or others, we always try to corroborate in order to better assess the validity of that
information.
Mr. Ted Falk: Okay. And these laws that we currently have on the books and that we're proposing to strengthen and clarify, are they consistent with laws that our allies would be applying?

Mr. Michel Coulombe: Again, it is difficult to compare because of different legislation, but yes, they are in terms of being able to operate overseas. Again, the regime of obtaining warrants might be different, but overall it is consistent.

Mr. Ted Falk: Okay.

The Chair: You still have another two minutes.

Mr. Ted Falk: Two minutes, all right.

Some concerns we've heard regard the ability of the federal court to issue warrants within the scope of relevant Canadian law when issuing warrants to authorize CSIS to undertake certain activities to investigate a threat to the security of Canada outside of Canada. Some may wonder why warrants would not be more appropriate coming from the nation where the activities are taking place. Could you comment on why this is important, as some of those countries may not exactly have a court system that can be approached for a warrant, as well as the transnational nature of these investigations.

Mr. Michel Coulombe: I'll answer your question as when I appeared in October and we talked about Canadians who are currently overseas involving threat-related activities. I mentioned countries like Syria, Iraq, Somalia, Yemen, Afghanistan, so you can just imagine going through the court system or the judicial system of those countries to try to get authorization. I'm not sure it would be practical.

Mr. Ted Falk: Mr. Clairmont, a question for you. You're representing cyber security here this afternoon. Cyber security is something that can be done anywhere. Is it necessary to operate outside of Canada to completely provide the security that we require here? Or do we do everything here?

Mrs. Lynda Clairmont: No, we don't. Cyber security is borderless. I would say, so it can be done within a country and outside of the country.

Mr. Ted Falk: Do you anticipate any changes affecting your operations with any of the legislative issues here?

Mrs. Lynda Clairmont: No, we don't.

The Chair: Thank you very much, Mr. Falk.

We will now go to Mr. Easter for seven minutes.

Hon. Wayne Easter: Thank you, Mr. Chair.

I do want to put on the record, Mr. Chair, starting my question because the minister said we had robust oversight for security agencies, I would sincerely disagree. The fact is we're the only one of the so-called "Five Eyes" that doesn't have parliamentary oversight for security agencies. I think the government, if it was thinking about bringing in a balance, would bring in such a body. There is a report from 2005 where all parties agreed on such a body. I'd just make that point. As Ms. Girard said, related to the revocation of citizenship, Canada is alone as compared to other democratic countries when it comes to that issue. We're also alone when it comes to the "Five Eyes" on parliamentary oversight. I just want to make that point in the beginning.

I think the probably the rub of the issue, in terms of this bill, is the substantive changes to CSIS on its, if I could call it, extraterritorial activities. Where I come from—and the deputy or
head of CSIS can correct me if I'm wrong—I think originally when CSIS came in it was envisioned that we'd depend on our foreign relations or liaison relations with other countries to provide us information, and that's how we'd operate, rather than so much as having agents abroad. In the reality of today the world has changed. We're dealing with, to a certain extent, I think, a stateless world in some regards.

I would ask the question this way: doesn't this bill, in terms of CSIS, now give wide extraterritorial applications for Canadian judicial decisions abroad in terms of how we operate?

Do you understand what I asked?

Mr. Michel Coulombe: Not the last part, I'm sorry.

Voices: Oh, oh!


In this bill, I can put it this way, with judicial decisions, judges, authorizing certain activities for CSIS abroad, aren't we now getting into, I guess, the extraterritorial application of what CSIS does from where we were?

Mr. Michel Coulombe: First of all, in terms of CSIS conducting activities outside Canada, and you talked about the Macdonald Commission, but I'm not going to quote, I'm pretty sure in the report it does talk about the creation of CSIS, that you would have to be very careful, but they were already seeing the possibility that we would have to do this. It has always been our understanding that we have that authority. That's why this is just a clarification; making it explicit in the act that we can actually do what we've been doing for basically 30 years, because that was the interpretation of... If you look at section 16, there's a clear restriction: it's within Canada, which you do not find in section 12.

Hon. Wayne Easter: I'm not disagreeing with the approach here, but I think we need to be fairly open about what we are doing. I don't think CSIS has always done this, maybe in the last 20 years. But one of the difficulties I think now with this act, and with what we're talking about CSIS doing, is we are getting into a new area... or I guess we're laying out in law more clearly a new area that Canada has always opposed other nations' security agencies doing when it's applied to Canada. Is that correct?

Mr. Michel Coulombe: Again, I don't think it's a new area. When you've stated that it's actually putting it into law explicitly in the act, I think that's correct, but I don't think it's a new area.

In terms of the second part, again, you have to look at this in terms of: if you're thinking about us acting in other countries, when it's with like-minded partners most of the time this is done jointly, with the acknowledgement of that country, just like we expect them to do the same here.

When there's cases of non-like-minded country, like it was mentioned earlier, with, for example, cases of Russian espionage, then we would investigate, and if there's a case we would pass it to the RCMP.

Hon. Wayne Easter: I think you make a very good point because we're really dealing with several different types of countries, Mr. Chair, on the earlier question by Randall I do have the Library of Parliament question we asked him here that basically states we were talking about the wording "within or outside Canada" and I do have a Library of Parliament document here I can provide to the committee. It's only in English but if you wanted to get it translated. It states exact or similar wording to that found in Bill 8 of C-44 is not found in the relative legislation of Five Eyes Nations. They name the relevant pieces. So if the committee wants that I can table it.
The last question is on the source. On the sources protected is there any different protection to sources outside Canada versus inside Canada, and those outside Canada how do you perceive to protect those sources?

Mr. Michel Coulombe: There are no differences. It's not a question of where the source is actually residing. It's a question of do we promise confidentiality. So there is no difference in terms of a source living here, or living abroad.

The Chair: Fine thank you very much.

Now we will go to Madame Doré Lefebvre five minutes.

[Fransais]

Mme Rosane Doré Lefebvre: Merci, monsieur le président.

Je remercie les tennins d'être restés pendant la deuxième heure pour répondre à nos questions.

Pour l'instant, mes questions portent probablement plus sur le fait de savoir si le SCRS a les ressources suffisantes pour appliquer ces nouvelles mesures en vertu de la Loi sur le service canadien du renseignement de la sécurité? Nous savons que tout les ministères ont subi des compressions au cours des dernières années. Le ministère de la Sécurité publique en a également subi. Donc le SCRS également. Avez-vous les ressources nécessaires actuellement? Sinon, ou alliez-vous les prendre pour avoir un personnel suffisant sur le terrain afin de faire le travail demandé en vertu du nouveau mandat du SCRS?

M. Michel Coulombe: Comme nous l'avons précédemment mentionné, le projet de loi C-44 ne nous donne pas de nouveaux pouvoirs ou outils. Il fait juste clarifier ce que nous faisons déjà et une certaine part que nous avons arrêté de faire suite à la décision de la Cour fédérale, l'automne dernier.

Ce n'est donc rien de nouveau en termes de ce que nous pouvons faire. Ce n'est pas un ajout, si vous voulez, en termes de pouvoirs ou d'outils que nous pouvons utiliser. Cela n'a pas d'impact sur les ressources du service.

Mme Rosane Doré Lefebvre: Actuellement, le SCRS a-t-il les ressources nécessaires pour faire le travail qui lui est demandé?

M. Michel Coulombe: Le service, comme toute autre organisation, travaille à l'intérieur de son budget. Nous devons établir des priorités et allouer les ressources en fonction de celles-ci qui découlent des renseignements qui sont fournis par le gouvernement. Ensuite, nous avons nos façons d'évaluer les matrices pour juger de la menace que représentent les différents sujets d'enquête. Nous allouons les ressources en fonction de cela.

Mme Rosane Doré Lefebvre: Avez-vous supprimé des emplois qui sont directement liés à l'échange d'informations entre nos alliés à l'échelle internationale, au cours des dernières années?

M. Michel Coulombe: Non.

Mme Rosane Doré Lefebvre: J'aurais aussi voulu savoir, toujours à propos de l'échange de renseignements, le projet de loi C-44 va-t-il faciliter la coopération entre la GRC et le SCRS?

Des mesures vont-elles vous aider auprès de la GRC?

M. Michel Coulombe: Le projet de loi C-44 lui-même n'a aucun impact sur notre relation avec la GRC.

Mme Rosane Doré Lefebvre: En ce qui a trait au profilage générique d'une source humaine du SCRS, comment le projet de loi va-t-il faciliter les enquêtes de votre service? Pouvez-vous nous éclairer un peu plus dans ce sens? Monsieur Coulombe, ou monsieur Guimond pourriez peut-être nous répondre.
M. Michel Coulombé: La première manière de faciliter les enquêtes, comme je l'ai mentionné tout à l'heure, avec la certitude, sauf pour les exceptions, de protéger l'identité des sources, c'est celle-ci. Il existerait plus de gens portés à nous donner de l'information, ce serait plus facile pour le service d'obtenir la coopération des individus à devenir des sources. S'ils avaient la certitude que leur identité sera protégée.

Lorsque nous arrivons en cour criminelle par exemple, pour la protection des sources, votre collègue l'a mentionné plus tôt, le système actuel juge les situations au cas par cas. C'est très intensif au plan des ressources. Nous devons consacrer beaucoup de ressources sur cette question. Cela nous amène encore à la question d'incertitude, à savoir si, dans chaque cas, l'identité de la source va être dévoilée ou pas. En vertu du projet de loi C-44, la protection des sources va vraiment faciliter l'apport volontaire des sources d'information, le recrutement des gens et la gestion des cas et des dossiers quand nous irons en Cour criminelle ou ailleurs.

Marc Rosane Doré Lefebvre: Il y a aussi une provision dans le projet de loi C-44 qui parle de mieux protéger ou de moins divulguer l'information en ce qui a trait aux agents du SCRS. On parle aussi de structures d'agents. C'est ce qu'on a plus de détails parce que cela pourrait être pratiquement d'importance qui travaillent au SCRS selon la façon dont le projet de loi C-44 est rédigé. Est-ce qu'il serait plus facile de cibler davantage les gens qu'on aimerait potentiellement envoyer en tant qu'agents à l'international? Cette provision est vraiment très vaste.

M. Michel Coulombé: Premièrement, la loi actuelle offre cette protection pour les individus qui sont présentement et qui étaient dans le passé impliqués dans ces activités. En fait, le projet de loi C-44 rajoute ceux qui pourraient être simultanément impliqués.

La problématique avec le fait d'essayer de mettre un cadre plus serré de qui on parle, la menace et le contexte évoluent tellement rapidement qu'il y a des individus aujourd'hui qui sont impliqués dans ce genre d'activités que même moi, il y a peut-être cinq ou dix ans, je n'aurais jamais pensé qu'ils seraient impliqués là-dedans. Il ne s'agit pas seulement des agents de renseignement qui peuvent être impliqués. Donc, il y aurait un danger de limiter vraiment la protection d'identité des employés du service.

Par ailleurs, encore une fois, comme toute autre activité du service, en terme de désigner des employés qui relèvent de cette protection, cela tombe sous la révision du CSARS. C'est quelque chose qu'ils peuvent définitivement surveiller dans le cadre de leur révision annuelle.

[English]

The Chair: Thank you very much, Madame Lefebvre.

Mrs. James, five minutes, please.

Ms. Roxane James: Thank you, Mr. Chair.

A question to Mr. Coulombé in regard to warrants. There have been some discussions comparing us to our Five Eyes partners and the fact that the same explicit text is not necessarily contained in other legislation from other countries.

I just wanted to confirm that in fact we have been able to issue warrants since the CSIS Act was first established in 1984, and similar countries have the same abilities but maybe not necessarily the same wording in their legislation.

The problem we have here in Canada, as people recognize, we also have different court systems and the judiciary interprets laws differently. We have the Charter of Rights and Freedoms, which may not be identical to other countries as well.

The problem we have is that the courts have specifically called into question the ability for CSIS to operate overseas, to issue these types of warrants. In fact, the legislation, the very text we're putting in this new bill will clarify, will clearly spell out the capabilities that CSIS has...
always had, in order to ensure that the courts no longer call it into question. Is that a fair statement?

If you could, comment on that, please.

Mr. Michel Coulombe: Well, you're right that since 1984 warrants have been issued, but warrants have been issued in terms of activities here in Canada.

Starting around 2009, and the Federal Court decision last November by Justice Mosley called into question the authority of the service to operate abroad, certainly not the authority of the service from Canada because the interception had to be done from Canada, but being able to do it when the targets or investigations are overseas.

Yes, since 1984 warrants have been issued, but they were here in Canada. What you are doing is making it clear, number one, that we can operate overseas, and that yes, the Federal Court has the jurisdiction to issue warrants that would apply overseas.

Ms. Roxanne James: Do you know if other countries that we're sometimes compared against have had similar court decisions that have questioned their authority to be able to operate overseas or communicate with their allies as such?

Mr. Michel Coulombe: I'm not aware of any. What you have to understand also, if you look at the Five Eyes partners, for example, they have separate foreign intelligence security service with a clear mandate to operate overseas. The issue we're debating today, they don't have that issue because they have separate agencies where their mandate is to operate overseas.

Ms. Roxanne James: I actually posed this question to the minister with regard to the CSIS Act was first passed back in 1984. I actually wrote down something you said, that one reason we need to clarify this law is that the threat to our national security has evolved, terrorism has evolved.

I think back to 1984. Without disclosing my age, I think I was still in high school, maybe, I had no email, I had no Internet. I had no computer. In fact, I remember lugging my father's old typewriter in that big old case up the stairs to write my first resume to get a part-time job. A lot has changed. I actually recall answering my rotary phone when they called for an interview.

When we talk about how the threat has evolved, obviously a lot has changed since 1984. How has the threat actually evolved? You didn't really expand on it at that time.

Mr. Michel Coulombe: Not to reveal my age, but I was working with the RCMP in 1985.

Some hon. members: Oh, Oh.

Mr. Michel Coulombe: The threat has evolved in a number of ways. You just talked about technology. The Internet has changed, you don't have to go back to 1984... 10 years ago, so the pace at which technology is evolving, as we all know, is extremely rapid. That's certainly one.

The nature of the threat, back in 1984, really, the priority was Cold War espionage. Now it's terrorism. The mobility of people has greatly increased also, and the facility of people travelling, so that has changed the nature of the threat, but the velocity, also, at which that threat can develop. Communication, again going back to the Internet, with the facility with which you can communicate between Canada and Yemen and the Sahel, and elsewhere in the world - it doesn't matter where - has changed that threat.

So there are many factors, and it's not just the threat itself that moves more from a CI threat to more of a terrorism threat. But everything surrounding it, as I said, the technology, mobility of people, that has dramatically changed the environment in which we work today.

The Chair: Thank you very much.
We will now go to Mr. Garrison for five minutes, please.

Mr. Randall Garrison: Thank you very much, Mr. Chair.

I'm not sure who I should ask this question to. There's a bit of a problem I have in understanding in terms of the legal drafting of this bill. Who here today can talk about that? Certainly, Mr. Coulombe, you said that there are no new powers for CSIS here, so in clause 8 where it adds to the warrant question the words, "Without regard to any other law, including that of a foreign state...", my question is, could that be removed from this bill? If it was removed, would that change anything materially here. Certainly, to me, it would affect the reputation of what we're doing in other countries. So I'm not sure who's responsible for the drafting of that and what impact that would have to remove those words from this bill?

Mr. Michel Coulombe: That's something, Mr. Chair, if we could go back to the committee, because that's a very technical, legal question.

Mr. Randall Garrison: I respect that. That's why I said, I have some trouble seeing if you had anybody at the table today who could really respond to that.

Mr. Michel Coulombe: But I just want to go back to what I said earlier that you have to realize the type of environment and the type of countries that we're talking about. Again, if you're talking about activities that we were going to do overseas, it would have to be lawful in the country where they're going to take place, and, again, I'm not sure that's a viable, practical system.

The Chair: Thank you very much. (Inaud) anybody else. I guess possibly what we're trying to say is, we're looking for perfect legislation to deal with an imperfect world. But carry on.

Mr. Randall Garrison: Yes, those are words I would not accept. I think what we're looking for is legislation that will stand up to legal challenges so that we're actually doing something effective in defence of national security.

Mrs. Ritu Baberjee: Maybe I can add a little bit more to that. Part of the reason it's drafted the way it is, is if we go back to the Federal Court of Appeal decision, the court made it clear, and this is again following up from what Mr. Coulombe just said, that it would have the jurisdiction to issue such a warrant, and I'm quoting the decision, "...where the interception is lawful where it occurs". Because that is very challenging to operationalize, we had to ensure that the law was clear for judges, that they had to consider was relevant to Canadian law, primarily the charter and the CSIS act. So that's why it's written the way it is.

(1715)

Mr. Randall Garrison: Thank you. I think that is helpful.

Mr. Michel Coulombe: I don't know if I have time to add one little thing, because in terms of being lawful in the country where it's going to take place, you can imagine the difficulties in the countries I listed earlier. But I just talked about mobility. If we were to obtain a warrant where it would be lawful to do whatever we want to do in Syria, and the next week now that person is in Iraq, and the following week that person is elsewhere, again, in terms of, as we say in French, "...la réponse pratique...". I'm not sure how that system would be workable.

Mr. Randall Garrison: Okay.

In clause 9 of Bill C-44, it makes reference to making information that's otherwise protected by the protection of identified sources available to SIRC, and again we don't have anyone from
SirC here, but it seems to me that this provides an element which is more complicated than some of the other stuff that SirC has dealt with in the past. I’m just wondering about the capacity of SirC as the oversight body to deal with this new responsibility that I believe—I know the Minister says there’s nothing about oversight here—does add a responsibility to SirC. I wonder if CSIS maybe shares that same interpretation that there is a new responsibility for SirC here included in the bill?

Mr. François Guimont: Well actually I would say, Mr. Chairman, that it’s new in the sense of being defined in that bill, but in reality SirC can look at all aspects of CSIS activity as long as it is not cabinet confidence. Their power is very broad, so that’s the first observation I would make.

The second observation is that it is a review responsibility, and their resource— I think they have 16 individuals, plus or minus—is a significant number of individuals who are very capable and understand the business of CSIS. I would like to think that they are probably equipped to do a good job at carrying out a review, should they decide to do so.

Mr. Randall Garrison: So you would say this section is again, really more a clarification, and this information is not excluded from the review responsibilities.

Mr. François Guimont: It is clarification.

Mr. Randall Garrison: Okay, thank you.

Do I have another minute?

The Chair: You have about 15 seconds.

Mr. Randall Garrison: Oh, 15 seconds. I think we’ll let that go at this point.

The Chair: Fine, thank you very much. I appreciate your consideration, Mr. Garrison.

We will now go to Mr. Norlock.

Mr. Rick Norlock: Thank you very much, Mr. Chair.

Through you once again to the witnesses, thank you for attending.

I’ll start out by saying that we live in a new world and I don’t want to have an organization like CSIS or any other organization that treats the rest of the world like some— I don’t want to belong to a country that’s naive or acts like a Pollyanna and expects the whole world. You know, we respect everything you do and we would never do anything... We know that other countries are recruiting terrorists, whether they be naturalized Canadians, people who were born here, or people with dual citizenship, who are now embedded in our country and want to do irreparable harm not only to individuals in Canada, but to the very foundation... The very building we’re in is the place where we exercise our democracy.

At least on five or six occasions all the questions asked in many different ways here all come down to what Mr. Guimont just said. This is not an earth-shattering, new, ominous tremendous load on CSIS. This is just a simple clarification of existing rules and regulations on which a court has said “You need to clarify that.”

Mr. Guimont, you can tell me if I’m making this as simple as possible. For my constituents who are out there, who don’t want to belong to a country that’s naive and believes that if we’re just nice to everybody else they’ll be nice to us, this legislation tries to impart to CSIS the same kind of judicial acceptance of protection for human resources—in other words, for informants who want to give CSIS information in a way that won’t identify them—or in other words, it gives them the same type of protection that police already have with informants. Is that correct?
Mr. François Guimont: Yes, and as was said earlier on by the minister and others, essentially Bill C-44 is a result of court decisions. If you wish—in one case, that of Justice Mosley—so we are essentially fixing this very transparently.

My colleague in CSIS was operating under a regime that we thought was understood, so we're clarifying that. That's why the word "clarifying" is always there, even in the bill, as I remember.

With respect to the protection of sources, it is also as a result of court proceedings—the Harkar decision, essentially. Again, out of the logic put forward by my colleague, Monsieur Coulombe, we feel that being able to offer that protection is important for them to be effective in delivering protection to Canada.

Mr. Rick Norlock: Thank you very much.

It's as simple as that.

Another observation that I'll make is that I can't support legislation by finding little bits and pieces that you disagree with but the bottom line is this is simply a clarification based on what judges have observed and all we're trying to do is straighten it out.

Thank you for that.

My next question is to Ms. Girard. You mentioned in your response to one of the questions that in this legislation that refers to another piece of legislation with regard to the revocation of citizenship this is just in line with other like-minded countries who have the same kind of legislation that says if one does something that imperils or is found to be treasonous, then that is done or there's a death penalty up until very recently that if you want to do something that really splinter to the privilege of being a Canadian then the state should revoke that privilege.

I wonder if you are aware of any other countries that share the rights and freedoms that we have, the values that we have? Perhaps you could list a couple of those countries so that my constituents know that there are other countries that they may come from that share this kind of opinion.

The Chair: Very briefly please.

Ms. Nicole Girard: Thank you. Yes.

So the provisions in the Strengthening Canadian Citizenship Act which enabled revocation of citizenship from dual citizens who have done these actions against the national interest that I referred to are broadly similar to provisions that exist in the United Kingdom, Australia and New Zealand and other democratic European countries that we looked at including France, Italy, Germany, Netherlands, Switzerland. So that gives you a bit of flavor.

The Chair: Thank you very much, Mr. Norlock.

Mr. Randall Garrison: I actually have perhaps more than one point of order so I'll just try to deal with them in pieces.

One is that we've had an offer of some additional information being made available to the committee. My concern is that given our tight schedule that the witnesses are aware that we would have to have that this week, really in order to deal with it effectively as we are going to clause-by-clause next Monday.

So I guess I'm looking for a commitment from the witnesses if they would be able within 48 hours to provide us with the information. I know that is somewhat unreasonable but I'm not setting the timeframes on this committee.
That's my first point.

The Chair: Okay, first of all, briefly and encapsulation of that first request directed to Mr. Guimont.

Mr. Randall Garrison: Yes.

The Chair: Are you familiar with the information as requested, Mr. Guimont?

Mr. François Guimont: I think, Mr. Chairman, there was a bit of back and forth and it would be very good for all of us if the chair could clarify exactly what is expected by witnesses.

The Chair: Then please go ahead and repeat the information that you requested.

Mr. Randall Garrison: Well at the time—and I'm trying to remember exactly because I didn't keep detailed notes because I thought the witnesses were—but it had to do with certain clauses of the bill and the exception and if that exception deals with things like bail and detention? That's my main concern. There are a couple of other points but that's my main. So the ability for request the exception does it deal with, it says the presumption of innocence but does that include the other stages of the legal process including bail and detention?

The Chair: Is that available to our witnesses to provide that?

Mr. François Guimont: Yes, sir, we will provide the information as requested. I want to do justice to Mr. Easter, he has been committed by the minister and he'll get an answer to his questions as well to be filed with the department.

The Chair: Fine. Thank you very much.

Were those the two pieces of information you were looking for?

Mr. Randall Garrison: That was the piece I was looking for. The others were just questions.

My second point of order is given the short timeframe we're on I guess I'm looking for unanimous consent of the committee to authorize the chair that if there are any witness slots that haven't been filled for Wednesday due to scheduling considerations could the chair be authorized to invite any of those who have approached the committee through the chair, which I know includes the privacy commissioner, he allowed to fill those slots, starting with the privacy commissioner and any others who approached the chair because we are on such a tight timeframe that people may not be able to get.

The Chair: The motion is in order, but it would require unanimous consent to move it.

Yes, Ms. James.

Ms. Roxanne James: I have just a quick point. We have a couple of other witnesses so we don't know whether those slots would be filled. I can't give you an answer at this point in time.

The Chair: Yes, Mr. Easter, speaking on the same point.

Hon. Wayne Easter: Yes. Certainly on that, maybe the parliamentary secretary doesn't have the information available yet, but given the Privacy Commissioner's interest, the Privacy Commissioner could be put on standby should a spot be found to be vacant at the next hearing.

The Chair: Yes, Ms. James.

Ms. Roxanne James: That I would agree with if there were a spot available for the Privacy Commissioner to come as well, but again, I don't know until we are able to get hold of the other witnesses.
The Chair: The chair would only point out one thing. This does change the
concentration of sources of witnesses per party, so as long as we have unanimous consent for this,
the chair is comfortable with that.

Hon. Wayne Easter: Mr. Chair, that's such foolishness anyway, that balance. If they are good
witnesses, bring them on.

The Chair: Mr. Norlock.

Mr. Rick Norlock: Yes, I'm not prepared to give my consent to something that I'm not aware
of as to the witness lists etc. I think it's not appropriate for me to make a decision at this point
because I haven't seen the complete witness list, so I'm not going to say yes or no to a unanimous
motion until I have all the facts and I do not have them.

I can assure Mr. Easter that any witness the government would bring forward would add value
to this enterprise.

Hon. Wayne Easter: It's a political theme, if I could say so.

The Chair: Okay, seeing no consent at this point, that obviously is a no go now, but what I
might suggest is there could be conservation between the parliamentary secretary and co-chairs
and we will see how this evolves, and if something can be worked out, fine, and if not, we all
understand the realities.

Mr. Norlock, the clerk has advised me that the witness lists have been distributed to all
members.

Mr. Rick Norlock: Thank you very much. I'll look at it and be able to get back with regard to
unanimous consent.

The Chair: Thank you very much.

To our witnesses, thank you very kindly for giving us your time and your expertise.

The meeting is adjourned.
On November 26, 2014, expert academics appeared at the House of Commons National Security Committee (SECU) to testify on matters related to Bill C-44. Main topics of discussion were: Parliamentary and independent oversight; CSIS extraterritorial operational mandate; constitutionality of clauses put forth in Bill C-44; comparisons to allied intelligence mandates; confidential informant class-privilege; and information sharing.

Below are key statements made at the Committee:

Prof. Craig Forcese (Associate Professor, Faculty of Law, University of Ottawa. As an Individual):

"In our system, Parliament has authority to grant expressly powers that violate international law so long as these powers do not then also violate the Constitution. I personally see no constitutional complaint. assuming we are confining our discussion to surveillance issues and not, for instance, including interrogation or other more aggressive forms of investigation. As noted, however, I do see several critical omissions in this bill."

"First, it is not clear when the service will be obliged to obtain a foreign surveillance warrant. The existing statute speaks of belief on reasonable grounds that a warrant is required. In a domestic surveillance operation, these grounds arise when failure to obtain a warrant would violate section eight of the charter governing searches and seizures or Part VI of the Criminal Code. But the applicability of these two laws and especially the charter to foreign surveillance is uncertain. As a consequence, the existing reasonable grounds threshold is unhelpfully ambiguous when applied to the new warrant powers in this bill.

I think in the analysis a warrant will be required whenever foreign surveillance involves covert interception of telecommunications. I also believe the amendments may be interpreted as requiring a warrant any time an operation may violate international or foreign law. These would be sensible standards, but because the bill is not emphatic, establishing these standards may require another round of litigation. I strongly urge the committee therefore to pre-empt the necessity of another half-decade of uncertainty by adding clear language on the trigger for seeking a foreign surveillance warrant."

"Right now, there is no clear law on CSIS international intercept sharing. At best there is a generic more open-ended permission in the Privacy Act which seems unlikely to survive a constitutional challenge. I would strongly urge this committee to again pre-empt years of litigation by codifying an express statutory authorization for intercept sharing that also includes required safeguards."

"I note with profound concern that Parliament has failed to legislate any of (the Arar Commission's) critical recommendations dealing with coordination between the review bodies for CSIS, CSE, and the RCMP. Instead, we have closer and deeper coordination between security services but review remains firmly limited to institutional sites, and indeed we have reported instances of the security services questioning and perhaps impeding the ability of review bodies to coordinate their review functions. This bill gives CSIS a freer hand and will necessarily deepen its relationship with CSE and foreign agencies. The bill should also include provisions that augment the authority of the review bodies to keep tabs."

"CSIS's review body, SRRC, is suffering the effects of neglect. Its membership has been below strength for a considerable period of time. It has been rocked by scandal at the leadership level, and its level of resourcing has not kept pace with growth in the operational budget of CSIS. For all of these reasons, I would ask this committee to move on the issue of accountability."

"The problem is that implicit trigger and its application outside of the country is unclear, because we don't know when the charter will reach outside of the country."

"It's not sufficiently emphatic to constitute a use of section 33 of the Charter of Rights. It's not an override of the charter. Any other law presumably would include the bill of rights, although again I'm not sure if it's sufficiently emphatic there. My reading of this, my assumption, has been that "any other law" refers to international law. So by including foreign law, we know that for example the law of the foreign jurisdiction is inapplicable. say it's rules on privacy, but also international law principles that
might relate to sovereignty would presumably be inapplicable."

"I would imagine that federal court judge would rightly to superimpose all sorts of conditions on the conduct of the operations, which would minimize both the degree to which it violates the foreign law, and also limits the prospect that it will have these knock-on effects that would embarrass both CSIS and the Canadian government."

"I would say that this bill is unique in the degree to which it emphatically now authorizes a judicial officer to allow a Canadian executive agency to violate foreign law."

"It's a question of stalling (SRC I seriously and earnestly making the members full-time appointees. Resourcing those members properly. And then legislatively, it means reacting to the inquiries, very important recommendations that there be the capacity for three review bodies we have in essence to coordinate their review functions so that they can actually follow investigations across institutional boundaries."

"I believe (Parliamentary oversight) is necessary. I don't believe that the arguments that are made that it's redundant have resonance. I think the more eyes on the spies, the better. If you'll forgive my litigation... The ideal model in my view was one where there is robust capacity on the part of the parliamentary committee to access the information they need."

"I would imagine that a federal court who risks the prospect to be dragged into some international scandal would be even more adamant that there was a necessity undergirding this investigation and would superimpose all sorts of obligations."

"So in the context of information sharing, there are circumstances where we simply can't share the information, and where the human rights implications are so dire. So there are legal fixes and then there's also good judgement."

Wesley Wark (Professor, Graduate School of Public and International Affairs, University of Ottawa, As an Individual):

"CSIS has become a de facto, a hybrid service, required to deal with an ever-expanding range of threats to national security and to operate both at home and abroad."

"I intend to focus on what I think are its key provisions regarding CSIS overseas operations, including those targeting Canadians."

"Whatever is ultimately decided by the courts with regard to the lawful enlistment by CSIS of foreign security agencies, there are other issues of principle and practice at stake. The most important such issue concerns sovereign control. To enlist the aid of foreign security partners, such as the Five Eyes countries, in intelligence sharing is one thing, to outsource intelligence collection to a foreign partner, no matter how close and trusted an ally, is another."

"C-44 cements the evolution of CSIS into a hybrid agency that conducts both domestic security intelligence and foreign intelligence missions."

"What the bill does not do is provide any sensible underlying definition of the kind of hybrid agency that CSIS has now become, and it does not provide any added controls, accountability measures, cooperative frameworks, or transparency measures around increased overseas operations by CSIS."

"In a post-9/11 world, I would suggest that a distinction between foreign and security intelligence is meaningless for Canada, and the fact of its meaningless underscores the need for a more root-and-branch readjusting of the CSIS Act itself."

"Why the government decided down two separate forks of the road, with partial amendments to the CSIS Act and with an appeal to the Supreme Court, when these two forks might well bring them to a collision at a future junction, remains a mystery to me."

"(There) are indications that not all is well in terms of the relationship between the service and the minister, and that ministerial accountability for CSIS may be less rigorous than it should be."

"Last but not least, Bill C-44 is silent on the issue of the need for a dedicated, security cleared parliamentary committee to ensure the ability of Parliament to properly scrutinize the activities of CSIS..."
"In conclusion, Bill C-44 in my view is a poor quality handmaid, (and) is unimaginative and it fails to address the most significant legacy issues around the CSIS Act.... It persists with an artificial statutory distinction between security and foreign intelligence, offers insufficient clarity about CSIS powers, and offers no new measures of transparency and accountability concomitant with the new and increased role being played by CSIS."

"In terms of parliamentary committee construction, focused on the activities of individual government departments, that's not how the Canadian security and intelligence community will, large is actually organized. It's an integrated or semi-integrated collection of different agencies operating under different departmental mandates and controls."

Prof. Kent Roach (Professor, Faculty of Law, University of Toronto, As an Individual):

"CSIS may make premature promises of anonymity to informants that could hinder or even thwart subsequent prosecutions. These are not hypothetical concerns and I should mention that I spent four years as director of research and legal studies on the Air India Commission studying this question. The police and prosecutors may have a very difficult time dealing with the consequence of this near absolute privilege that would be bestowed on all CSIS human sources under Bill C-44."

"So it would be my submission that you should consider expanding the "innocence at stake" exception to allow judges to order disclosure that would pierce the privilege whenever it is required under section 7 of the Charter."

"I would also propose that when you go into clause by clause, you should look at the section 2 language of the promise of confidentiality. That language should at least be limited so that it is only an explicit promise made by CSIS of anonymity that would trigger this broad privilege that, as I suggested, could hinder subsequent police investigations and prosecutions."

"CSIS needs to be able to conduct its investigations outside of Canada. But I do have some concerns about the "without regard to any law including that of any foreign state" language. I have concerns that this may override the restrictions that the National Defence Act places on CSEC or signals intelligence agency. But also I think that there is a need for an integrated review of at least statutory gateways, as advocated by the Arar Commission and as Professor Forescue, in his submission, advocated to you, and indeed has proposed, some language to that effect. I would also add that there is a need to ensure both ministerial and parliamentary oversight as CSIS uses its new powers to act abroad."

"It makes a lot of sense to have a whole-of-government approach to our security threat. The problem is that too often we're still. One of my concerns is that there might be a warrant granted under Bill C-44 that not only should the Minister of Public Safety be aware of, but his or her cabinet colleagues in foreign affairs and defence should also be aware of. So I do think that it's necessary for CSIS to be able to act outside of Canada. But I think the political risks of that are significant. I think that Bill C-44 could be improved by having some form of ministerial notification."
Dr. Christian Leuprecht (Associate Dean and Associate Professor, Department of Political Science, Royal Military College of Canada, As an Individual):

“Critics like to cite the case of Mahar Arar. As tragic as that case may be, a single case does not make a pattern. To the contrary, it demonstrates the learning effects in our security sector by virtue of the fact that a case like Arar’s would be highly unlikely to recur given the changes in policies now in place.”

“He who sacrifices freedom for security deserves neither, Benjamin Franklin famously said. But what about he who sacrifices security for freedom? Freedom and security are not a zero-sum dichotomy. To the contrary, they are complementary. You cannot enjoy one without the other. However, you cannot enjoy your freedoms if you are dead.”

“Critics concerned about changes to Bill C-44 are also the ones who will be first to complain why CSIS did not do more should an extremist traveller return to Canada and commit mischief here. Overall, they fail to account for the possibility of keeping individuals safe in spite of themselves, that sharing intelligence may allow for intervention abroad to prevent individuals from harming themselves, Canada, Canadians, and Canadian interests. I value my freedoms, but I value my life and the lives of my compatriots even more.”

“Canada’s administrative and judicial system would necessarily be sensitive to the revocation of Canadian citizenship in circumstances where that imposes demonstrable risks for an individual’s life. Ergo, revocation is judiciable, and thus has a built-in review mechanism.”

“While Justice Mosley may have been within his right to render the decision he did, the far-reaching implications of his decision could have let past practice prevail for a limited amount of time to allow for a legislative remedy to be introduced.”

“Given the current global security environment, including the challenge of extremist travellers, the federal government has an obligation to Canadians to pass precisely the sort of amendments that Bill C-44 proposes, and that those in the vital interest of Canada and Canadians. Tactically, operationally, strategically and fiscally, this is the sort of way to compensate for the limits on CSIS to engage in foreign human intelligence gathering.”

“We don’t have a mechanism that provides ongoing accountability in as effective a manner as we could, and we have a mechanism that reports to the political executive rather than being accountable to Parliament the major change that would require is members of Parliament to be security cleared to have privileged access to the information that they are being provided, and this would be a significant step for Canadian Parliament to take.”

Craig Scott, NDP: “We need much better oversight and review mechanisms, including parliamentary review and including the much better coordinated oversight mechanism for all intelligence agencies... It’s just ‘intel oversight 101’, and yet a decade later we’re still not there. It’s important to note that the privacy commissioner is supporting exactly what [Foreese’s] saying, in a letter he has sent today. Mr. Therrien has said ‘Clear statutory rules should be enacted to prevent information sharing by CSIS from resulting in a violation of Canada’s international obligations’.”
Wednesday, November 26, 2014 - Le mercredi 26 novembre

The Chair (Mr. Daryl Kramp (Prince Edward—Hastings, CPC)): Welcome to our witnesses and colleagues to meeting number 41 of the Standing Committee on Public Safety and National Security. Today we have, of course, two hours of testimony and questioning. For the first hour we have three witnesses. For the second hour we'll have three witnesses also. In the second hour two of them will be joining us by video conference. Just for the attention of the committee—of course we always have opening statements for up to 10 minutes but then we generally limit it at that in order to allow time for questioning—I've been advised by our one witness that his opening statement would be substantially longer so he has agreed to abbreviate his statement but he would like his full statement into the record read or introduced to the clerk so that is available to the committee to be evaluated but you're not going to hear his full statement. You'll hear his abbreviated version and of course in q and a you ask him on anything. But if not, his full statement will be available to the committee to be able to be observed.

Yes, Mr. Scott.

Mr. Craig Scott (Toronto—Danforth, NDP): Mr. Chair, the full statement beyond what he says will be translated first before it's made available.

The Chair: Yes, absolutely. The only other alternative would be to lengthen the statement but then, of course, if we go full length with the statement that's less time for the committee to be able to discuss with our witnesses. The chair thought that would be the best way to approach that and I thank you for your cooperation.
So, we now have with us Craig Forrest, associate professor of the faculty of law University of Ottawa. We have Wesley Wark, professor of graduate school of public and international affairs University of Ottawa. From the Canadian Police Association we have Tom Stamatakis, president.

Gentlemen, we will go straight to your opening statements if we will for this first hour.

We'll start off with Mr. Forrest, please.

**Prof. Craig Forrest (Associate Professor, Faculty of Law, University of Ottawa, As an Individual):** Thanks very much and thanks to the committee for asking me to testify today.

I'm going to focus exclusively on the foreign surveillance aspects of the bill that is before this committee. Later today Professor Kent Roach will be appearing before you and he will be speaking to the informer privilege component.

My views in brief. I support the proposed amendments to sections 12 and 21 of the CSIS Act. That said, I think there are three omissions in this bill that this committee should correct. I see this corrections as necessary to pre-empt another half-decade of litigation, controversy, and uncertainty.

Clause eight in the bill addresses the core confusion flowing from three Federal Court decisions. In enacting these amendments, you will now be emphatically asking a court to bless CSIS covert surveillance that may violate international or foreign law. In our system, Parliament has authority to grant expressly powers that violate international law so long as those powers do not then also violate the Constitution. I personally see no constitutional complaint, assuming we are confining our discussion to surveillance issues and not, for instance, including interrogation or other more aggressive forms of investigation.

As noted, however, I do see several critical omissions in this bill.

First, it is not clear when the service will be obliged to obtain a foreign surveillance warrant. The existing statute speaks of belief on reasonable grounds that a warrant is required. In a domestic surveillance operation, those grounds arise when failure to obtain a warrant would violate section eight of the charter governing searches and seizures or Part V of the Criminal Code. But the applicability of these two laws, and especially the charter, to foreign surveillance is uncertain. As a consequence, the existing reasonable grounds threshold is unhelpfully ambiguous when applied to the new warrant powers in this bill.

I think in the final analysis a warrant will be required whenever foreign surveillance involves covert interception of telecommunications. I also believe the amendments may be interpreted as requiring a warrant any time an operation may violate international or foreign law. Those would be sensible standards, but because the bill is not emphatic, establishing these standards may require another round of litigation. I strongly urge the committee therefore to pre-empt the necessity of another half-decade of uncertainty by adding clear language on the trigger for seeking a foreign surveillance warrant. I have proposed language in an annex to my brief which I have supplied to the clerk, and which, pending a translation, will be available to you.

Second, since this bill was tabled, the Supreme Court has issued its decision in Wakeling. That case concerned the RCMP but the holding extends in practice equally to CSIS. A majority of the court concluded that section eight of the charter applies to sharing between Canadian authorities and foreign counterparts. The majority's decision is constitutional, a reasonable law must authorize intercept sharing. A reasonable law is one that includes sufficient accountability and safeguard regimes, according to the court. Right now, there is no clear law on CSIS international intercept sharing. At best there is some more open-ended permission in the Privacy Act which seems unlikely to survive a constitutional challenge.

I would strongly urge this committee to again pre-empt years of litigation by codifying an express statutory authorization for intercept sharing that also includes required safeguards. I have proposed language in the annex addressing this issue.
I act, we are now at the tenth anniversary of the Arar commission. I note with profound concern that Parliament has failed to legislate any of that commission's critical recommendations dealing with coordination between the review bodies for CSIS, CSE, and the RCMP. Instead, we have closer and deeper coordination between security services but review remains firmly limited to institutional silos, and indeed we have reported instances of the security services questioning and perhaps impeding the ability of review bodies to coordinate their review functions.

This bill gives CSIS a freer hand and will necessarily deepen its relationship with CSE and foreign agencies. The bill should also include provisions that augment the authority of the review bodies to keep tabs.

Again, I propose language in the annex that addresses this concern.

Let me end with a related plea. CSIS's review body, SIRC, is suffering the effects of neglect. Its membership has been below strength for a considerable period of time. It has been rocked by scandal at the leadership level, and its level of resourcing has not kept pace with growth in the operational budget of CSIS. For all of these reasons, I would ask this committee to move on the issue of accountability.

Let me end there.

Thank you very much.

The Chair: Thank you very much, Mr. Forcetse.

We will now go to Mr. Wark.

You have the floor, sir.

Mr. Wesley Wark (Professor, Graduate School of Public and International Affairs, University of Ottawa, As an Individual): Thank you, Mr. Chair.

Ladies and gentlemen of the committee, it's a privilege to appear before you. I'm grateful for the opportunity. I'm the long-winded witness, so I'm going to read a condensed version of my statement.

Since the 9/11 attacks, the role of intelligence in Canadian national security policy has been revolutionized. Canadian intelligence has become more significant, more powerful, better resourced, more closely aligned with allied partners, and more globalized in terms of its operations and capabilities. As an important constituent of what is called the Canadian Security and Intelligence Community, the Canadian Security Intelligence Service, CSIS, has undergone its share of revolutionary change since 2001. CSIS has become, de facto, a hybrid service, required to deal with an ever-expanding range of threats to national security and to operate both at home and abroad.

The issues that arise with regard to Bill C-44 reflect the fact that CSIS's functions have changed enormously since the 9/11 attacks, and also, clearly, since the passage of the original CSIS Act itself, and have changed both in terms of the kinds of threats that CSIS must operate against and in terms of its geopolitical scope.

In my specific remarks on C-44, I intend to focus on what I think are its key provisions regarding CSIS overseas operations, including those targeting Canadians. C-44 would add clarifying language to Section 12 of the act, indicating that in the performance of its security intelligence function, it can operate both within and outside Canada. It further adds that Federal Court judges may issue warrants to allow CSIS to collect threat-related intelligence on Canadians abroad under its Section 12 powers. C-44 also stipulates, in amendments to Section 21 of the CSIS Act, that CSIS may apply for warrants to conduct Section 16 operations, that is, the authorized collection of foreign intelligence within Canada.
To understand the key elements of Bill C-44 we need to put these in the context of a series of judgments made by the Federal Court with regard to CSIS extraterritorial warrant applications. This history begins in 2005 and follows a winding and complex path down to the present. There is not time in these hearings to adequately summarize this history, but let me note that the current stage was set by a ruling from the Federal Court of Appeal this past summer, which has been followed by an appeal by the Attorney General to the Supreme Court which remains pending.

In his application for leave to appeal, originally dated September 29, 2014, and unsealed in November of this year, the Attorney General summarized what was at stake as follows:

"This case is about how the Canadian Security Intelligence Service may lawfully enlist the aid of foreign security agencies in monitoring the activities of that small number of Canadians who have the capability to engage in activities that threaten national security."

Whatever is ultimately decided by the courts with regard to the lawful enlistment by CSIS of foreign security agencies, there are other issues of principle and practice at stake. The most important such issue concerns sovereign control. To enlist the aid of foreign security partners, such as the Five Eyes countries, in intelligence sharing is one thing; to outsource intelligence collection to a foreign partner, no matter how close and trusted an ally, is another. Outsourcing means potential loss of control of an operation, loss of control of Canadian intelligence, and loss of control over outcomes. The Security Intelligence Review Committee commented on this matter by saying:

"The risk to CSIS, then, is the ability of a Five Eyes partner to not independently use CSIS-collected information. That, in turn, carries the possible risk of detention or harm of a target based on information that originated with CSIS. SIRC found that while there are clear advantages to leveraging second-party assets..."

That is, the Five Eyes countries.

"In the execution of this new warrant power—the so-called CSIS 30-08 warrant—and indeed this is essential for the process to be effective, there are also clear hazards, including the lack of control over the intelligence once it is shared."

C-44 cements the evolution of CSIS into a hybrid agency that conducts both domestic security intelligence and foreign intelligence missions. Clarification of the legal standing of CSIS in these regards poses the danger of closing off discussion of the eventual need for a separate foreign intelligence service as a better solution to Canada's intelligence needs, and a solution much more in keeping with the practices of our close Five Eyes partners.

More important than what C-44 does is the question of what it does not do. What it does not do is provide any sensible underlying definition of the kind of hybrid agency that CSIS has now become, and it does not provide any added controls, accountability measures, cooperative frameworks, or transparency measures around increased overseas operations by CSIS.

I want to conclude with just a selection of some of the issues that I see arising from Bill C-44.

Bill C-44 applies legal band-aids to the conduct of section 12 and section 16 operations only because we persist with a wholly artificial legacy distinction between security intelligence and foreign intelligence. CSIS officials used to make the distinction between security intelligence being what Canada needed to have, and foreign intelligence being a category of knowledge that it might be nice to have.

In a post-9/11 world, I would suggest that a distinction between foreign and security intelligence is meaningless for Canada, and the fact of its meaninglessness underscores the need for a more root-and-branch redrafting of the CSIS Act itself.

Having decided to appeal to the Supreme Court the Federal Court of Appeal's ruling with regard to the Mosley judgment on CSIS' use of extraterritorial warrants, the legislative provisions of Bill C-44 may be rendered null or may require further amendments, depending on whether the Supreme Court agrees to hear the appeal and depending on the nature of its findings.
The Federal Court of Appeal's decision was available to the government long before Bill C-44 was tabled. Why the government decided down two separate forks of the road, with partial amendments to the CSIS Act and with an appeal, to the Supreme Court, when these two forks might well bring them to a collision at a future junction, remains a mystery to me.

Bill C-44 does not add any new provisions to the CSIS Act to ensure proper consultation between the service and its minister, the Minister of Public Safety, and the two departments must likely to be affected by expanded CSIS overseas operations—the Department of Foreign Affairs, Trade, and Development, and the Department of National Defence. Both of these departments engage in their own overseas intelligence and information collection through dedicated branches.

Bill C-44 does not add any statutory requirements on the part of the CSIS director to inform the minister with regard to the undertaking of sensitive overseas intelligence collection. The most recent SIRC annual report found that CSIS needed to keep the minister more fully informed about foreign operations and section 16 investigations. SIRC, in a special study of what it calls a “sensitive CSIS activity” also urged that CSIS reporting to the minister be done in a “timely and systematic manner.”

These are indications that not all is well in terms of the relationship between the service and the minister, and that ministerial accountability for CSIS may be less rigorous than it should be.

Bill C-44 does not restore the functions of the Inspector General’s office, originally established in the CSIS Act in 1984, and closed down by the government as part of an omnibus budget implementation bill in 2012. The role of the Inspector General as the eyes and ears of the minister might be considered all the more critical in an age of expanding CSIS overseas operations. As the former long-serving CSIS IG, Evi Plunkett, stated, the abolition of the IG function was a “huge loss” for ministerial accountability.

Bill C-44 adds no new clarifying mandate or resources for the Security Intelligence Review Committee, in keeping with the statutory provisions authorizing CSIS collection under section 12 abroad.

Last but not least, Bill C-44 is silent on the issue of the need for a dedicated, security cleared parliamentary committee to ensure the ability of Parliament to properly scrutinize the activities of CSIS and related Canadian intelligence agencies in an age of globalized operations and diverse threats to national security. Such a committee of Parliament was recently proposed by Joyce Murray in her Private Member’s Bill C-622, and has also been proposed in the Senate Bill S-220 advanced by now retired Senators Hugh Segal and Romeo Dallaire. Wayne Easter of this committee earlier offered the House a similar version of proposed legislation, Bill C-551. The government continues to deny the need for such a new structure, despite all-party support for just this thing in 2005.

In conclusion, Bill C-44 in my view is a poor quality bandaid. It may also be a very temporary one, depending on a future Supreme Court ruling. It is unimaginative and it fails to address the most significant legacy issues around the CSIS Act, which is now 30 years old and was created for different threat environment, in a different technological age, and in a different climate of democratic legitimacy.

The Chair: Thank you. Please.

Mr. Tom Stamatakis (President, Canadian Police Association): Thank you, Mr. Chair, and good afternoon to members of the committee.
I appreciate having the opportunity to speak with you all today, in person for a nice change, regarding your ongoing study of Bill C-44. I’m appearing today on behalf of the Canadian Police Association, an organization that represents over 54,000 front line civilian and sworn police personnel serving Canada’s communities from coast to coast to coast.

My opening statement will be quite brief this afternoon as I hope to leave enough time to answer any questions you might have. I’m going to focus particularly, in the area of the protection of human intelligence sources by law enforcement in the course of our duties. That being said, this is my first opportunity to appear here in Ottawa since the tragic events that took place on October 22 that claimed the life of Corporal Nathan Cirillo only a few blocks from where we’re sitting today. Shot by a terrorist who would have claimed even more victims if not for the courageous actions of those who are sworn to protect Canadians. From members of the Ottawa Police Service to the Royal Canadian Mounted Police, as well as our colleagues within the House of Commons Protective Service. I’d like to offer my personal thanks for their efforts that day.

The reason I raise this, particularly in the context of my appearance here today is to highlight the need for adapting our laws in this country to provide law enforcement with the necessary tools to combat the rapidly evolving threats that can very clearly cause tremendous danger here in this country and which is why we’re quite pleased to speak in support of Bill C-44 here today.

One of the most important jobs that has been given to our national security services, and that would certainly include both municipal and provincial police in that grouping, is the gathering of the necessary intelligence that would eventually help our members prevent attacks from taking place within our communities. Gathering that intelligence, however, has never been more difficult. Technology has given criminals and terrorists rapidly evolving tools that often allow them to be steps ahead of those who are working to protect Canadians. Whether it is in the national security context or dealing with local street crime, finding and protecting informants is often an invaluable tool for police when it comes to leveling the playing field and obtaining the intelligence necessary, and I firmly believe that Bill C-44 and the provisions within that dealing with the protection of sources will be a positive step in protecting Canadians.

I should also note, particularly with respect to informants, that their use often goes beyond one single case and that underscores their continued importance and why so many efforts are taken to protect their identities. Compromising their anonymity not only can put their personal safety at risk, but can jeopardize months and sometimes years worth of investigations and of police personal time.

Furthermore, informants would often be reluctant to step forward and provide valuable information to law enforcement without as many guarantees as possible regarding their safety and anonymity, as they are often called on to testify against those who may know them best, their former and sometimes even current colleagues, family members, and other people with whom they’ve developed relationships.

As I mentioned, I did want to keep my opening remarks brief as I understand members may have questions regarding the current practices within law enforcement in Canada and I’ll try to do my best to provide that information.

Once again, thank you very much for the invitation to appear today and I look forward to any questions you might have.

Thank you.

The Chair: Thank you very much, and thank you, gentlemen, all of you, for giving us the time to be able to go in the committee now to ask questions.

We’ll start off the first round of questioning for seven minutes.

Ms. James.
Ms. Rosanne James (Scarborough Centre, CPC): Thank you, Mr. Chair.

I'm actually going to pass my time to Mr. Norlock.

The Chair: Fine.

Mr. Norlock.

Mr. Rick Norlock (Northumberland—Quinte West, CPC): Thank you very much, Mr. Chair, and through you to the witnesses, thank you for attending today.

I want to especially thank Mr. Stamatakis for his statement that he just made, because my question was going to be based on those premises that as a human resource as they relate to criminal investigations, and in this case, protecting Canadians through intelligence sources. One of the key components in this legislation and there are basically only three, has to do with protecting human sources.

So I'm going to go through a few things. Some of the complaints we've heard is that you know who some of the players are, how come they're not arrested? Would you agree with me that sometimes during the course of investigations you let the little fish go because you're actually trying to identify a bigger fish that will lead you to a better conclusion to the problem that you already have?

Mr. Tom Stamatakis: That's very true and it's a practice that occurs every day in law enforcement.

Mr. Rick Norlock: So you may have enough to charge an individual with some offence, but that offence is probably minor in regard to what you're really after, let's say the kingpin or the person involved in the investigation.

Mr. Tom Stamatakis: Often, it's a higher level player particularly when you're dealing with organized crime or some of the activity we've seen more recently in Canada with respect to the recent incidents, one of which I referred to, the focus is always on making the greatest impact with the resources that we have at our disposal to prevent, to be proactive and protect Canadians.

Mr. Rick Norlock: Drawing similar conclusions between the two because they're almost one in the same, so you're some investigations within Canada, let's say over a certain type of crime—we don't need to get into the types of crime—and it might lead you through your human resources, to the knowledge that some of the people that you need to get information from are outside your borders—in other words, in other countries—and that there are people there who you need to talk to, and information that they may have that lead you to the ultimate goal that you have. Does it make sense to you—and I think in your opening statement that it's quite obvious—that in order to protect those human sources of information that CSIS does not have the legislative power to do now, that this piece of legislation gives them the kind of protections that the police have when utilizing human sources?

Mr. Tom Stamatakis: It makes perfect sense to me from a front line law enforcement perspective absolutely.

Mr. Rick Norlock: So when you looked at this piece of legislation, would I be correct in saying that's what you personally observed?

Mr. Tom Stamatakis: Yes. In fact, I guess the comment I would make is that it probably doesn't go as far as what the police have at their disposal locally. So I think this is very much a step in the right direction in terms of protecting human sources, for sure.

Mr. Rick Norlock: Would I also be correct if I were to state that we did hear from CSIS so if I said, CSIS commented on Monday that it would possibly have to drop cases if they would be forced to give up their source, as they are often sources for other investigations as well.
My question basically is, do you think it would be advisable to have CSIS unable to assist in the following through any criminal investigations and prosecutions or would protecting the source of multiple future prosecutions be advisable?

Mr. Tom Stamatakis: Very advisable, I think I reflected that in my comments.

Mr. Rick Norlock: Yes, thank you.

I just needed to get a couple of these questions answered because we hear various comments from different quarters wondering the need to do these things. I think if we can relate to the protection of human sources of information, both local and internationally, then we are to what currently is accepted investigative procedures in Canada. I think it helps the average citizen because my messaging, at least I try to make my messaging from Parliament is not so much for the people that populate here but for the people at home so they can understand what we're doing and appreciate what we're doing in trying to either in this case trying to protect them from events as you rightly mentioned on October the 20 and 22.

I especially want to thank you for mentioning the great men and women on the Parliamentary precinct who protect us and protected us, but I especially think it's worthy to mention the Sergeant at Arms, who is, quite frankly, I think our collective hero right across the board in Parliament.

How much time left, Mr. Chair?

The Chair: You have another minute and a half.

Mr. Rick Norlock: Oh great.

Mr. Foreese, I noticed that you saw some things that in this legislation that you think we need to continue to do, and thank you for that. I wonder if you've given some thought to...one of the protections that people have as far as protections under the charter is that CSIS would still have to obtain warrants with regard to receiving information or obtaining information from certain sources. If I can go back, I made some notes so I just want to make sure my notes are clear so that helps me. You thought that was appropriate but you made a couple of other suggestions in regard to those warrants, I thought.

Prof. Craig Foreese: Yes, the CSIS Act in its present form indicates that the government or CSIS needs to obtain a warrant where there are reasonable grounds to believe that such a thing is necessary, which is essentially coded language for saying...where there's a charter interest in play under section 8 or to immunize and intercept what would otherwise be a crime under Part VI of the Criminal Code.

The problem is that implicit trigger and its application outside of the country is unclear, because we don't know when the charter will reach outside of the country. In fact we have a Supreme Court case called "Egan" suggesting that many forms of police investigations and presumably also CSIS investigations don't trigger the same charter implications when they take place outside of the country.

If I were now left to ponder this provision and I was asking when I need to go to federal court in order to obtain a warrant, I'd have to puzzle through that, and it wouldn't necessarily be very clear.

As I noted, I had some proposed language or sample language, and what I was proposing was that there be an emphatic instruction inserted in the bill indicating when this foreign surveillance warrant would be required. As CSIS, when would you be obliged to go to court to get it?

Mr. Rick Norlock: So what you're basically saying is you think it should be more prescriptive.

Prof. Craig Foreese: I think it should be clearer, it should be more definite. Yes, absolutely.
Mr. Rick Norlock: Thank you.

The Chair: Thank you, Mr. Forcese.

We will now go to Mr. Scott, please. Seven minutes.

Mr. Craig Scott: Thank you, Mr. Chair, and thank you to our witnesses.

Just a couple of preliminary points... it's important to know as Mr. Garrison made clear on Monday, that these are very abbreviated proceedings for something that witness after witness, we now learning is more complicated and involves a lot more need for attention that we're giving it. This is our only day as official opposition to have two witnesses we specifically want to hear and they're getting part of one panel in one half of a two-hour session. So this is really an inadequate process.

The second thing is... I am very grateful to the witnesses for making sure the whole question of oversight and review has not been lost in this. The fact that the inspector general is gone, and the fact that since the Arar inquiry we've known we need much better oversight and review mechanisms, including parliamentary review and including the much better coordinated oversight mechanism for all intelligence agencies.... It's just "intel oversight 101", and yet a decade later we're still not there.

It's important to note that the privacy commissioner is supporting exactly what you're saying in a letter he has sent today. Mr. Therrien has said clear statutory rules should be enacted to prevent information sharing by CSIS from resulting in a violation of Canada's international obligations.

So that's on the whole clarity point. It's also, I think, ultimately on the Wakeling case implications. Also, he says:

A balanced legislative approach would also include in Bill C-43 measures to make the activities of all federal departments and agencies involved in national security subject to independent oversight.

He goes on to elaborate a little bit.

So, people thinking about the implications of both clarifying and extending CSIS's powers are also saying that we shouldn't be doing this without a more comprehensive understanding of how oversight and review needs to catch up not only with the problems in the past but with what's now happening in the bill.

I'd like to focus, Professor Forcese, if I could, on a couple of your points. On the warrants. basically clause 8 indicates that a new section 21(3.1) would say:

Without regard to any other law, including that of any foreign state, a judge may in a warrant authorize activities outside.

The activities that he or she authorizes are investigative activities. That refers to an earlier provision. Now, you've indicated that you're assuming this would only be confined to surveillance and not interrogation. But is there anything in the language that would suggest that's necessarily the case?

Prof. Craig Forcese: No. There's the historical context. That is, the Federal Court cases, which are the genesis of this bill, have dealt with extra-territorial surveillance. But, of course, the CSIS mandate in section 12 is not confined to surveillance, covert or otherwise. Of course, we do have instances where CSIS members have gone abroad to conduct interrogations. The most notorious example of that is Guantanamo Bay with Omar Khadr. Presumably, in conducting that interrogation, they were acting within their section 12 mandate.

The issue, in my view, is... is what sort of supervision might there be in a context above and beyond surveillance for overseas activities? I think that if we're talking about CSIS conducting
interrogations overseas, that the constitutional issues are potentially dramatically different in the sense that it's no longer a question of section 8 of the charter anymore, but now it's a question of section 7, the very provision that was in issue in the Khadr case. That's one reason just to refer back to the comments about clarifying language where I would hope that the committee might consider, including very specific language indicating that in every circumstance where the conduct of CSIS may infringe international law or foreign law, that there be an obligation first to go and get this warrant. So it's not confined simply to overseas surveillance, but every form of CSIS operation. Presumably, at that point, it's subject then to direct oversight by a court that can presumably then impose conditions on the nature of whatever overseas operation might be involved, including presumptively interrogations.

Mr. Craig Scott: I'll come back to that because I'm not quite sure what it would look like to involve our courts when CSIS comes and says, “You know, we're going to do something that we think may likely, or will, violate international law, or foreign or local law, and now we want you, a domestic judge, to tell us we can do it.” I'm not exactly sure what test they would apply to say, “Here's your warrant”. So we have to figure that one out, I think.

Could I ask, when it says, “without regard to any other law”, is this a term of our “any other law”? Does that mean any other legal system, or does this mean any other law in Canada?

Prof. Craig Forcese: That would be a question of—

Mr. Craig Scott: It would just be excluding the charter, for example.

Prof. Craig Forcese: It's not sufficiently emphatic to constitute a use of section 33 of the Charter of Rights. It's not an override of the charter. Any other law presumptively would include the bill of rights, although again I'm not sure if it's sufficiently emphatic there.

My reading of this, my assumption, has been that "any other law" refers to international law. So by including foreign law, we know that for example the law of the foreign jurisdiction is inapplicable, say its rules on privacy, but also international law principles that might relate to sovereignty would presumptively be inapplicable.

(1615)

Mr. Craig Scott: I do have some concerns about how unclear that is.

What about the question of foreign law where the issue is that CSIS is going to do things that would not be allowable under the foreign law? The Minister told us that's not an issue because we have better laws than dictators. Well, there are many other states where CSIS would operate that have perfectly functional systems where their own authorities may need to get warrants. We have heard in the past that CSIC, the Communications Security Establishment Canada, has on occasion done the bidding of foreign service agencies, if you believe some of what's in the famous book, called Spyworld by Mike Frost. We may even have been involved in spying on cabinet ministers in the U.K. at the behest of intelligence agencies there because it would be against the law for them to do it. Whether this is true or not factually, it's a scenario. The question is, what would you say to a judge if CSIS were completely forthcoming and said, "This is what we want to do. We want to do something that the foreign intelligence agency cannot do under its own law?"

Prof. Craig Forcese: You can imagine that a Federal Court judge confronted with that prospect and the prospect of being enlisted in operation conducted by CSIS, it would be a diplomatic firestorm if it were ever revealed. That Federal Court judge, I think, would be quite anxious to make sure that CSIS had crossed its "Ts" and dotted its "I"s. I think in not the fact that a Federal Court judge is invested in supervising these sorts of activities is a gain for accountability because of the anxiety that would likely be produced by being placed in this position. What a Federal Court judge might do in practice, it's hard to discuss outside of an immediate factual context, but I would imagine that federal court judge would rush to superimpose all sorts of conditions on the conduct of the operations, which would minimize both the degree to which it violates the foreign law, and also limits the prospect that it will have these knock-on effects that would embarrass both CSIS and the Canadian government.
The Chair: Fine, thank you very much.

Thank you, Mr. Scott and thank you, Mr. Foreese.

We'll now go to Ms. Abloncy, please, for seven minutes.

Hon, Diane Abloncy (Calgary—Nose Hill, CPC): Thank you.

Thank you to the witnesses for your thoughtful comment and analysis. It's very helpful.

As you know, the CSIS Act is about 30 years old so unfortunately it certainly has not kept up with the rapidly evolving pace of the threats to our country.

The purpose of this act is fairly simple, in fact, I believe someone has called it "the filling of gaps identified in recent court cases". But there have been some questions that the court has raised so this act attempts to address that, to give authority for CSIS to conduct investigations outside Canada to confirm that the federal court can issue warrants for such investigation, to give the federal court authority to consider only relevant Canadian law, and to protect the identity of both CSIS sources and employees. There may be other areas that will have to be addressed but this is the purpose of this law.

I wonder if either of the professors can tell us what kind of requirements are on the intelligence communities in the countries of our allies, the Five Eyes or in the countries we cooperate with. Are any of these required to get court warrants before they undertake activities in other countries? How is our regime comparable to those of our allies, is the question?

Prof. Craig Forcese: It's a bit of a mixed bag. Not purporting to have reviewed in detail the laws of hundreds of foreign countries, I would say that this bill is unique in the degree to which it emphatically now authorizes a judicial officer to allow a Canadian executive agency to violate foreign law.

In other jurisdictions that I have looked at that have foreign intelligence operations, their laws are creatively ambiguous on that point. So the reality, as we all know, is that spies spy and in the course of spying they may violate the laws of the countries in which they spy, and international law in terms of state sovereignty.

But again, not having exhaustively reviewed all the comparative law, I am not aware of a statute that as emphatically indicates that a court may authorize spying in violation of international and foreign law.

I think also in the text of the document you were referring to earlier, called it "courageous" at some levels that the Parliament of Canada is prepared to put its stamp on a law that emphatically signals that we are prepared to violate the laws of foreign countries, potentially including allies, in conducting foreign surveillance.

That potentially has political implications and I imagine there are people in the Department of Foreign Affairs who are quite exercised or potentially quite exercised about the potential fallout that might occasion.

But to answer your question, in my albeit limited experience, this law is fairly unique.

Mr. Wesley Wark: If I could just add to that, we could look at the Five Eyes partners in particular and I think we would find in that look that they all have different forms of judicial or executive authorization for surveillance abroad, and indeed for surveillance at home. So they're probably all variations on a theme.

I think what makes the Canadian legislation unique is a product of the fact that what we're trying to do is find a legislative scheme for an agency that is, as I've said, hybrid. CSIS started out being a domestic security intelligence service and we fashioned laws to allow them to perform that function and to control that function in terms of possible abuses. Now it is, in
addition, a foreign intelligence service in a way that there is no parallel among any of our Five Eyes partners.

All of our Five Eyes partners have separate foreign intelligence services and domestic security intelligence services. They have made those separations over time for reasons that they think are very good reasons, and I think they're reasons that stand up in terms of international perspective as being very good reasons.

They are very different skill sets, very different training regimes, very different resources, very different kinds of forms of internal accountability, and external review that are required for those two very different kinds of operations, operating abroad versus operating at home.

What we're trying to do is find a kind of legislative fix-up for an agency that we've allowed to evolve into this hybrid model, without giving that evolution any serious consideration. That is the concern that I think Parliament and anyone interested in the functioning of the Canadian intelligence community should have.

Hon. Diane Atkinson: It's always an interesting debate. That's why academics love this kind of thing, but it does have implications and I appreciate you letting them out.

Mr. Stamatakas, you mentioned the events of October 22 and, of course, the apprehension that Canada is vulnerable to these kinds of activities that threaten the security of smaller or larger groups in our country.

I just want to ask you where you see the need for tools to our security agencies heading in the future? As I mentioned, this act, Bill C-44, has a fairly limited scope, but we know that there has to be other tools provided to our security agencies. Can you comment on what those might look like, from your point of view?

Mr. Tom Stamatakas: I don't know that I'm qualified to make any kind of comprehensive suggestions. My experience is limited to local Canadian law enforcement and, from our perspective, this is a step in the right direction in terms of the human source handling piece, the ability to gather intelligence.

I can tell you that municipal and provincial police, and the RCMP engaged in municipal and provincial policing activities in this country, are actively gathering that kind of intelligence from citizens who are obtaining information from the people that they know and that they are engaged in relationships with. That's certainly an important tool.

I certainly think it's appropriate for our security services that are going to be engaged in those activities, internally and externally, to have the same sorts of tools that our local law enforcement has in terms of the ability to engage in activities and practices that allow them to get the best information in a timely way, so that they can be in a position to proactively prevent incidents or activities that pose a risk to Canadians.

I think that these are the kinds of discussions that we need to be having and we need to be moving forward on. But I'm not in a position here to make a lot of recommendations in that regard.

The Chair: Thank you very much, Mr. Stamatakas.

We will now go to Mr. Casey, please. Seven minutes.

Mr. Sean Casey (Charlottetown, Lib.): Thank you, Mr. Chair.

Witnesses, I expect that you were probably expecting to see Mr. Easter in this seat. I am not a former Solicitor General as he is. Usually I'm on the justice committee, so I'm not as well-armed. If my questions appear to be less eloquent and clumsier, there's good reason for that. Although, I will say that yesterday we went through the Victim's Bill of Rights clause-by-clause, and one o'
the decisions that was taken in connection with that bill was to not include victims of terrorist acts abroad, such as the 9/11 victims. So there's a peripheral connection.

I'd like to start with you, Professor is it...Foreese?

Prof. Craig Foreese: Foreese.

Mr. Sean Casey: Towards the end of your remarks, you referenced accountability and you talked about the vacancies within CIRC. Could I ask you to expand on that a little further?

As you know, Mr. Easter and Joyce Murray, as was referenced by Professor Work, have championed parliamentary oversight and Professor Work went into some detail on that. Could I ask you to talk a little further about what needs to be done, in your view, to get the level of accountability that you referred to up to the international standards of our allies?

Prof. Craig Foreese: Structurally at CIRC, ideal membership is five. Even when they are at five, they're part-time which is an enormous undertaking for a review of CSIS. If you are full-time let alone part-time. They've been at three for some time. As you know, two chairs have resigned in controversy, and as a consequence, the continuity of leadership has been uneven at CIRC.

Resource wise, you can map the growth and operational funds of CSIS. CIRC operational funds have also increased but not proportionately. And so what was always an auditing function, CIRC when it reviews...CSIS doesn't look at everything. CSIS has been doing its peaceman presumably because its scale is now diminished relative to the scale of CSIS operations. It's even more peaceman than it has been in the past.

It's a question of staffing is seriously and earnestly. Making the members full-time appointees. Resourcing those members properly. And then legislatively, it means reacting to the inquiries. Very important recommendations that there be the capacity for three review bodies we have in essence to coordinate their review functions so that they can actually follow investigations across institutional boundaries.

There was some reporting from the Globe and Mail earlier this past year suggesting that an informal effort was made by the Commissioner of the CSE in one of his reviews to coordinate with CIRC and the government response was to challenge the legal competency of the commissioner to do so. In fact as I understand it, there was some threat that the commissioner might be in violation of his and his staff's secrecy and security obligations by coordinating. That requires a legislative fix and it's a long time in coming.

Mr. Sean Casey: With regards to parliamentary oversight, in your view, was it necessary and what's the optimal model? If you agree that it is necessary, what should it look like?

© (1620)

Prof. Craig Foreese: Well, I believe it is necessary. I don't believe that the arguments that are made that it's redundant have resonance. I think the more eyes on the spies, the better. If you'll forgive my iteration.

I also think it's important to enhance your ability as parliamentarians to understand the inner workings of the security services so there's institutional knowledge within Parliament itself.

The ideal model in my view was one where there is robust capacity on the part of the parliamentary committee to access the information they need.

If you look at the models that are deployed by the allies, UK and Australia being notable examples, there is some variability in terms of how much information the committee can actually extract from the security services. So on one level the Australian model is better in terms of the way that it's structured, but it's not all that robust in terms of their capacity to compel the presence of information from the services. So I would look as a primary ingredient of any parliamentary committee model, the ability of parliamentarians to access the information in
question, subject to obviously secrecy obligations than that are imposed on parliamentarians themselves.

Mr. Sean Casey: Professor Forcuse, you talked about the response that we get when we ask for parliamentary oversight is that it's redundant. Now you talked in your remarks in some detail about the decline of ministerial accountability and the measures that have been attempted to bring in parliamentary oversight. So I take it that you've also studied or at least read the debates and the positions taken by the various parties on the.

I would invite you to critique the responses that we get when we ask for parliamentary oversight. So it's redundant. We already have adequate oversight. What's your critique of those positions?

Mr. Wesley Wark: Mr. Casey, I think it's an excellent question.

Let me first give you my view of the nature of the critiques and they're very close to the way in which you present them. One of the responses to any kind of measure to reform the nature of the parliamentary review of security and intelligence in Canada is an argument that existing departmentally focused, if you like, parliamentary committees can adequately do this job. This committee can adequately review the security and intelligence practices of the Canadian community.

It seems to me that there are two problems, perhaps more than two problems, but two problems that immediately come to mind with that.

One is that in terms of parliamentary committees construction, focused on the activities of individual government departments, that's not how the Canadian security and intelligence community is actually organized. It's an integrated or semi-integrated collection of different agencies operating under different departmental mandates and controls. One of the things that the Azar inquiry pointed out is that we lack any capacity, either with regard to an independent review body to look at that overall work of the security and intelligence community and in regard to parliament, we don't have that capacity at the moment to do that integrated kind of review. As my colleague Craig suggests as well, there is a deep problem in terms of access to the kind of information that a parliamentary committee or a committee of parliamentarians would genuinely need in order to scrutinize properly the activities of a secretive intelligence and security community.

There are models that have been made to work among our Five Eyes partners that are of longstanding. The model that we have typically looked to post 9/11 in Canada has been the British model, the model for the intelligence and security committee, which is a rather unusual construction admittedly. It's a committee of parliamentarians, not a standard parliamentary committee. It was built that way on the assumption that it would provide better access to classified information according to the provisions available to them and that it would also generate significant sustained, serious, non-partisan discussion of these issues if it was constructed in a certain kind of manner.

I assisted Joyce Murray in the construction of her private members' bill and we looked at various models very seriously, but I think the essence of what parliament needs is a dedicated committee that can look at the broad range of security intelligence operations that may need to require both membership to the House and the Senate. It would certainly need additional resources compared to what an ordinary parliamentary committee would have in terms of research staff and it would need—

The Chair: if you could sum up please, Mr. Wark.

Mr. Wesley Wark: a non-partisan atmosphere to work

The Chair: Fine and thank you very much for the little over time there I think it was, you can understand.

We will now go to Mr. Scott.
Mr. Craig Scott: Thank you, Chair.

I believe I have five minutes so I'll try to be short and also ask the witnesses to respond as quickly as possible.

There are two things I want to look at, one is the lack of any provisions in this bill for the kinds of consultations that both of you raised, in particular Professor Forcese. I think I'm correct that there's no provision in this for the need for CSIS to have first consulted with the Department of Foreign Affairs before they come to the court and no requirement that the judge require that before the he or she would issue the warrant. It would have to be left to the good graces of judges to say, is this kind of thing I think we need to know a bit more about what its implications are and I'm right the person to judge it, get the Minister of Foreign Affairs to weigh in.

Am I correct on that? That there's nothing in the bill that would require CSIS now that it's formally and officially venturing around the globe to consult and coordinate with either the Department of Foreign Affairs or for example the Department of National Defence.

Mr. Wesley Wark: That's absolutely correct. There's nothing explicit in the bill at all and what the existing practice is in that regard informally is a matter of official secrets.

Mr. Craig Scott: Professor Forcese also picked up on that theme and I'm not sure if he revealed a bit more than he wanted to, but he indicated that it almost sounded like there were at least rumours from the other side of Ottawa, at least in the Department of Foreign Affairs people are not necessarily all that thrilled about CSIS now being given this formal mandate in a way that's converted it into an agency that may be in practice it had elements of, but was never official.

Am I correct that foreign affairs should want to be more connected to CSIS when it starts operating abroad or are they happy for CSIS to do whatever it wants?

Prof. Craig Forcese: That was entirely speculation on my part. I don't pretend to have ears inside the Department of Foreign Affairs.

Mr. Craig Scott: But you were speculating for a reason, were you not?

Prof. Craig Forcese: I was speculating only on the base that's if you've got CSIS conducting extraterritorial operations it may violate foreign laws and that then becomes a matter of record and suddenly it's on the front page of The Washington Post; that then creates certain headaches for the diplomatic core.

Mr. Craig Scott: So then I'd come back to the question I said I'd leave the last time which is what would you want a judge to do? Keeping in mind there's an element of the dignity of the courts within the framework of the comedy of nations where courts are basically there to say to other courts, you're not in the business of contributing the violation of your laws. However much international spying is kind of internationally lawful, unlawful, the question is involving our courts in this especially where you said one of the triggers should be anytime CSIS thinks they might be breaching international or foreign law, could you just indicate to me what a judge would do with that? How would the judge say, okay, go ahead and do it even though that's the reason you're coming to me, you're going to break foreign law and now I'm going to go on the record saying you can do it.

Prof. Craig Forcese: Well, to be honest, I'm not in a position to imagine what a judge would do in every individual case. Let me note though that the warrant provisions that would apply both for domestic and foreign warrants require CSIS to demonstrate that this is really a necessary undertaking, that there are no other means that are available other than to engage in this practice in order to gather information necessary for its investigation.

The best answer I can give you, Mr. Scott, is that I would imaging a court confronted with this warrant application would be extremely demanding of CSIS and already as my understanding is
if you speak at least to the folks in CSIS, they will tell you that the warrant application process is quite an arduous one and that the courts are quite demanding.

Mr. Craig Scott: Internally.

Prof. Craig Furese: Of course it's ex-parte in camera proceedings.

I would imagine that a federal court who risks the prospect to be dragged into some international scandal would be even more adamant that there was a necessity underlying this investigation and would superimpose all sorts of obligations.

Mr. Craig Scott: Thank you, that's great.

I did want to return to the Wakeling case that just came down roughly a week ago from the Supreme Court. And you indicated that from the combined majority holding that already this law is going to need at least an amendment with respect to much clearer legal provisions on some of the aspects of what the warrant might authorize including sharing of the information that might be produced by the activities authorized by the warrant. That's clear from the majority reasoning. So this bill already needs an amendment based on the Supreme Court case.

The dissent agrees with that but they went a bit further. And I want to read a passage and ask whether you think this as a policy matter is something we as Parliament should take seriously.

However, when information is shared across jurisdictional lines.

The Chair: I'm going to have to interrupt, Mr. Scott.

Mr. Craig Scott:

safeguards apply and domestic investigations lose their force. The requirement of prior judicial authorization does not provide sufficient protection against inappropriate future acts, such as with partners and their partners, the failure to require release as the law stands on the use of disclosed information is unbelievable.

The Chair: Sorry, Mr. Scott. Your time is well over and we have no time for response. You are well into that. So thank you very much.

We have just about two minutes left for Mr. Carmichael.

Mr. John Carmichael (Don Valley West, CPC): A few minutes, Mr. Chair.

The Chair: That's correct, sir.

Mr. John Carmichael: Thank you. That's generous.

Well, let me welcome our witness today. Thank you for being here.

Mr. Furese. I'd like to just start with you, if I could. That may be as far as we go.

Clearly we all recognize that terrorism is a global threat today in Canada after last month's activities is not immune. And in your article with the National Post back in October, I believe it was yours or your colleague that was quoted. It said the new bill puts surveillance outside Canada on a clear legal footing. This is a reasonable fly in a globalized security environment indeed. The bill is diplomatically courageous as you've already stated. You go on to say that there do however remain outstanding issues when CSIS investigates abroad. The risks of misconduct including complicity in human rights violations increase and that behaviour would raise legal issues.
We will now suspend while we go to the second hour.

The Chair: Thank you very much. I know you'd love to continue, Mr. Carmichael, but we have now expended our first hour.

The chair, certainly on behalf of the committee, would like to thank our witnesses for obviously your experience and your thoughtful comment here today. Once again, it's a serious issue. Public safety, the protection of the public, there really is no greater responsibility of parliamentarian. So we thank you for your contributions here today.

We will now suspend while we go to the second hour.

The Chair: We're back in session. We will now proceed with the introduction of our witnesses.

With us here in person, we have Kent Roach, Professor, Faculty of Law, University of Toronto—welcome, sir—and by video conference, from Burnaby, British Columbia, as an individual, we have Garth Davies, Associate Professor of Simon Fraser University—welcome, sir—and we will have joining us also by video conference, but it will be another 15 or 20 minutes before he's live with us here, Christian Leuprecht, Associate Dean and Associate Professor from the Department of Political Science, RMC, in Kingston.

Ladies and gentlemen, we will first start off with opening comments.

We will go to you, Mr. Roach. Carry on, please, sir.

Prof. Kent Roach (Professor, Faculty of Law, University of Toronto, As an Individual):

Thank you very much, Chair.

I'd like to thank the committee for inviting me to appear here today.

The terrible terrorist attacks last month confirmed Parliament's wisdom in 2013 in enacting four new terrorist offences that can apply to foreign terrorist fighters. Unfortunately however, Bill C-44 may have the unintended effect of making it more difficult to apply these valuable new offences to potential foreign terrorist fighters. That will be my primary focus in my submissions.
My second focus will be that the innocence at stake exception to the new CSIS human source privilege is required by the charter, but it is unconstitutionally under inclusive as applied to non-criminal proceedings where section 7 charter rights are in play.

Finally, I will suggest that while it is correct that Bill C-44 gives CSIS new powers to conduct investigations outside of Canada and that this responds to the threat environment that we live in, there is a concern that we need new and integrated review mechanisms as well as better ministerial and parliamentary oversight of CSIS foreign activities.

To move to my first point, Bill C-44 would overturn the Supreme Court's recent decision in Harkat as well as reject the recommendations of the Commission of Inquiry into the Investigation of the Bombing of Air India that CSIS informants not be given the same privilege as police informants. Both the Supreme Court and the Air India commission stress the danger that because of its intelligence gathering mandate, CSIS may make premature promises of anonymity to informants that could hinder or even thwart subsequent prosecutions.

Section 2 of Bill C-44 would give CSIS human sources a veto on disclosure of any identifying information once they have received "a promise of confidentiality" from CSIS. The courts have most recently, in 2013, in the context of police informer privilege said that these promises of confidentiality may even be implicit. I do have a concern that virtually every human source that CSIS talks to under the proposed legislation would then have the benefit of the privilege and a veto on any identifying information being disclosed, whether it's to defend a search warrant in a terrorist investigation or whether it's to be called as a witness in a terrorism prosecution.

These are not hypothetical concerns and I should mention that I spent four years as director of research and legal studies on the Air India Commission studying this question. In 1987, the prosecution of Talwinder Singh Pandi, the alleged mastermind of the Air India bombing, collapsed when an informant refused to allow his name to be disclosed. Now that informant was in a very difficult position and the crown attorney, at the time said in open court that if he was in that informant's position he would have made the same decision because of fear for his life as you have heard from earlier witnesses. The fact is that the prosecution fell apart because of the informer privilege and the informant's ability to veto disclosing any identifying information. This legislation would have given the two informants in the Toronto terrorism prosecution a veto on whether they would be called as witnesses or to disclose any identifying information about them because as you heard yesterday, CSIS is not in the business of collecting evidence. It was for that reason that the Air India commission wanted that it would have an incentive to promise anonymity and confidentiality when necessary to fulfill CSIS' intelligence mandate.

This is not an issue of CSIS deliberately abusing the privilege, but simply because of its functions it will have an incentive to promise confidentiality and then later on down the stream, perhaps months or even years later, the police and prosecutors may have a very difficult time dealing with the consequence of the near absolute privilege that would be bestowed on all CSIS human sources under Bill C-44.

The Air India Commission was acutely aware that there is a dilemma. Sometimes it is more important to have intelligence than prosecution, but it's solution that this that dilemma should not be resolved unilaterally by CSIS, or indeed by the RCMP, but that decisions should be made in the public interest on the basis of all available information by the Prime Minister's National Security Advisor.

My second point is simply that the "innocence at stake" exception in section 18.1(4)(b), as required by the Charter would apply in criminal prosecutions. But the Supreme Court, in Chanulli, has made it very clear that section 7 also applies in the non-criminal context, and in particular the security certificate context. So it would be my submission that you should consider expanding the "innocence at stake" exception to allow judges to order disclosure that would pierce the privilege whenever it is required under section 7 of the Charter.

Similarly, I realize that a policy decision to extent to privilege may have been made, but I would also propose that when you go into clause by clause, you should look at the section 2 language of the promise of confidentiality. That language should at least be limited so that it is
only an explicit promise made by CSIS of anonymity that would trigger this broad privilege that, as I suggested, could hinder subsequent police investigations and prosecutions.

Finally, my last point is that I agree that, given the threat environment, CSIS needs to be able to conduct its investigations outside of Canada. But I do have some concerns about the “without regard to any law including that of any foreign state” language. I have concerns that this may override the restrictions that the National Defence Act places on CSIS or signals intelligence agency. But also I think that there is a need for an integrated review of at least statutory gateways, as recommended by the Arar Commission and as Professor Fontes, in his submission, advocated to you, and indeed has proposed, some language to that effect.

I would also add that there is a need to ensure both ministerial and parliamentary oversight as CSIS uses its new powers to act abroad.

Thank you very much.

(1645)

The Chair: Thank you very much, sir.

We will now go to an opening statement from Mr. Davies, please. You're on, sir.

Mr. Garth Davies (Associate Professor, Simon Fraser University, As an Individual): Thank you very much for inviting me here today. I want to keep my comments brief. I would echo pretty much everything that's been said up until this point in terms of the need for ministerial oversight. I think we all agree with that. I would think we would all agree that the context that we're talking about, in terms of the changing nature of terrorism, is such that we need to allow CSIS to have the appropriate tools to operate in an environment that is changing rapidly and is really, in many ways, different than what we've sort of experienced historically. In terms of the level of threat that we're talking about with regards to the foreign fighter problem, with regards to the nature of groups such as ISIS, and trying to balance that with the rights and freedoms that we all cherish so dearly.

I really just wanted to be here today to try to be of assistance in any way that I could in terms of answering any questions that people had. I wanted to just minimize my time here and cede the floor to people that had anything else that they would like to say.

Thank you.

The Chair: Well, fine, and thank you very much.

We will give Mr. Leuprecht a moment to settle in and get comfortable. He's actually a little earlier than we anticipated.

So we'll give him a couple of minutes here and suspend for one minute or two till our next witness comes live.

Dr. Christian Leuprecht (Associate Dean and Associate Professor, Department of Political Science, Royal Military College of Canada, As an Individual): I'm ready for you, sir.

The Chair: Okay, can you hear me now, Mr. Leuprecht?

Dr. Christian Leuprecht: Yes, I can hear you.
Fine, you have the floor for an opening statement up to 10 minutes, should you wish, sir.

[Français]

M. Christian Leuprecht: Mesdames et messieurs, je vais faire ma présentation en anglais, mais je peux répondre à n'importe quelle question dans les deux langues officielles.

Monsieur le président, membres distingués du conseil.

[English]

I've entitled my intervention Peace, Order and Good Government: Parliamentary supremacy as the ultimate sovereign constitutional responsibility.

There is a ubiquitous claim that Canada does not have a foreign intelligence service. This is a misunderstanding of Canada's security intelligence community. Given the legislated limitations on the Canadian Security Intelligence's Areas Of Operations (AOR) beyond Canada, one might say that Canada does not have a human foreign intelligence service, certainly not one of the scope of the human services operated by some of our key allies, especially the Five Eyes' CIA, MI5, and ASIS (the Australian Secret Intelligence Service). However, Canada has a—

The Chair: Mr. Leuprecht, I'm going to interrupt you for one second. If you could slow down just a little bit to give our translation an opportunity to keep up with you, please.

Carry on.

Dr. Christian Leuprecht: However, Canada has a foreign signals intelligence service, the Communication Security Establishment, and a very good and respected one at that. Canada has compensated for AOR limitations on CSIS in several important ways.

Two of the key mechanisms had hitherto been under specific conditions, exchange of certain human intelligence information on certain Canadian citizens and residents and some other individuals with a direct bearing on Canada and Canadian interest, with allied foreign HUMINT services in general, and with the three of mentioned Five Eyes partners in particular. New Zealand's Security Intelligence Service, similar to CSIS, does not have a broad foreign human intelligence mandate akin to that of the US, UK, and Australia.

Second, under specific conditions, exchange of signals intelligence on certain Canadian citizens and residents and some other individuals with a direct bearing on Canada and Canadian interest with CSE, the Communications Security Establishment.

As reported widely in the media, including the Globe and Mail, in November 2014, Justice Richard Mosley of the Superior Court of Canada found that CSIS had not been sufficiently open about all the surveillance alliances it planned to form. Five years ago, CSIS had persuaded him to sign off on a foundational eavesdropping warrant to extend its reach outside Canada. Judge Mosley learned the full extent of the information sharing between Canadian spy agencies and also foreign allies after reading the watchdog’s public reports.

His ruling indicates he had never been told of this by Canada's intelligence agencies during five years of secret hearings. He took the extraordinary step of reopening a case he had settled in 2009. In the November 2014 ruling, he rebuked CSIS and the Communication Security Establishment for breaching their duty of candour to his court. And a statement released by the Court added that, despite perceptions to the contrary, “the Court considers it necessary to state that the use of the assets of the Five Eyes community is not authorized under any warrant issued.”

The case appears to be related to concerns about one particular instance where CSIS failed to disclose to the court one specific piece of information about a certain individual. In effect, the result of Justice Mosley’s decision has been to blind CSIS once Canadians and non-Canadians with court-authorized surveillance leave the country.
The merits of the decision with respect to that particular instance of disclosure to the court aside, Justice Morley's decision raises at least two fundamental issues. In light of the at least 130 Canadian extremist travellers who have left the country as reported in testimony before this committee by the Director of CSIS, and another at least 80 returnees, this is problematic. CSIS now has trouble following extremist travellers and their activities outside of the country. This has second-order effects with respect to its ability to provide timely and accurate advice to the administrative branch of government and the political executive to which it reports, and the ability to liaise tactically with criminal intelligence and enforcement agencies, notably the RCMP and CBSA.

Second, what is and should be the purview of judicial supremacy with respect to matters of national security? The committee will already have heard plenty of testimony with respect to the former. I shall not belabour the proximate implications of this point, other than to reinforce the point and concerns raised by others about the deleterious tactical, operational, and strategic consequences of this decision for CSIS, national security policy and enforcement, and Canada's political executive ability to make informed decisions with respect to public safety and Canada's national interest.

The second point, by contrast, has more distal implications. Canada is a democracy. Its ideological foundations are premised on those of small-L liberalism. That is, limited state intervention in people's lives, with a core value of freedom and subsidiary values of equality and justice. One of the hallmarks of this type of democracy is the rule of law, an independent and impartial judiciary. By virtue of being in this room, we are all agreed on these basic principles that underlie Canada's Westminster constitutional monarchical system.

Constitutionally, however, Canada balances the promise of limited state intervention with a small-C, conservative ideological premise about the role of the state in general, and about the role of the federal government in particular. Quoting from the preamble of section 91 of the British North America Act:

It shall be lawful for the Queen, by and with the Advice and Consent of the Senate and House of Commons, to make Laws for the Peace, Order, and good Government of Canada, in relation to all Matters not coming within the Classes of Subjects by this Act assigned exclusively to the Legislature of the Provinces.

For our purposes, at least two observations follow.

Insofar as security is demonstrably of national concern, it falls within the purview of the federal government. Such the case in terms of national security intelligence and its interactions with foreign security intelligence entities.

Second, the federal government has an overarching duty to ensure the peace, order, and good government of Canada. That is, the federal government has inherent obligations for the collective security of Canadian society.

What exactly POCSI denotes has been defined and circumscribed by both the Judicial Committee of the Privy Council and the Supreme Court of Canada and shall not detain us here. Suffice it to say that Canada's Constitution imposes limits on judicial supremacy.

Unlike Americans, Canadians are not inherently skeptical and mistrusting of their government. This is readily demonstrable empirically in terms of polling.

I shall skip over this section and it can be read into the record at a later time.

My point here is that people may have concerns about particular issues, but by in large, confidence in our security institutions and the federal government's handling of national security is very high.

The security sector, of course, is one form of government intervention. One might argue that it is actually the ultimate form of government intervention precisely because it empowers the government to curtail freedoms in a pretty dramatic way. Critics like to cite the case of Mahar
Arar. As tragic as that case may be, a single case does not make a pattern. To the contrary, it demonstrates the learning effects in our security sector by virtue of the fact that a case like Arar's would be highly unlikely to recur given the changes in policies now in place. Moreover, it is public knowledge that intelligence from the Arar case came from the RCMP and not from CSIS. And so to be sure, there are other cases where judges have had certain questions about CSIS evidence but none of this has called into question the professionalism and lawful conduct of the organization. Similarly, CSIS's watchdog has repeatedly affirmed the lawful and professional conduct of its activities.

So where does the skepticism arise?

It appears to be driven by a curiously denatured interpretation of the Canadian Constitution, since the introduction of the Canadian Charter of Rights and Freedoms, that somehow the sole and primary purpose of the Constitution is somehow to limit government intervention in the lives of citizens. The result of this interpretation would have it that privacy, civil liberties, and due process, as well as judicial supremacy, should trump any and all other considerations. As someone who has published on Canadian constitutional politics, the conventional view is that of the Constitution that actually enables government to do good in people's lives, at least when it comes to fundamental obligations, such as peace, order, and good government.

At times, that means having to balance considerations of due process with those of public safety and national interest. Confidential informants may be anathema to lawyers, but certain dimensions of security intelligence would be difficult to carry out without such confidentiality and the trust that we have as a result from our allies.

Again, here, a section that will be read into the record.

Allies such as the UK, France, Germany, and Spain have had to learn to live with terrorism for decades. As a result, their courts and their societies have developed greater sensitivity towards the protection of public safety. He who sacrifices freedom for security deserves neither, Benjamin Franklin famously said. But what about he who sacrifices security for freedom? Freedom and security are not a zero-sum dichotomy. To the contrary, they are complementary. You cannot enjoy one without the other. However, you cannot enjoy your freedoms if you are dead.

CSIS exists at the fulcrum of public safety. Critics concerned about changes to Bill C-44 are also the ones who will be first to complain why CSIS did not do more should an extremist traveller return to Canada and commit mischief here. Overall, they fail to account for the possibility of keeping individuals safe in spite of themselves, that sharing intelligence may allow for intervention abroad to prevent individuals from harming themselves, Canada, Canadians, and Canadian interests. I value my freedoms, but I value my life and the lives of my compatriots even more.

By the same token, with respect to changes proposed to the Strengthening Canadian Citizenship Act, I believe that the potential for revocation of citizenship imposes an important deterrent against bringing one's citizenship into disrepute. After all, those who hold dual citizenship have made a conscientious choice to divide their loyalty. As a naturalized dual citizen myself, I should know, Those who wish to protect themselves against the eventualities introduced by this amendment have the option to renounce their second citizenship. Some countries make it impossible to renounce citizenship, so the onus is on such citizens to conduct themselves in a manner so as not to run afoul of the amendment being proposed. Canada's administrative and judicial system would necessarily be sensitive to the revocation of Canadian citizenship in circumstances where that imposes demonstrable risks for an individual's life. Ergo, revocation is judicial, and thus has a built-in review mechanism.

The current equilibrium needs rebalancing. Justice Mosley deemed it within his purview to constrain certain types of intelligence-sharing activity, but he did so in a somewhat unusual fashion. Often, judges will give Parliament time to remedy these types of deficits. Justice Mosley afforded no such opportunity in Parliament. This, in my view, is disconcerting. While Justice Mosley may have been within his right to render the decision he did, the far-reaching
implies that his decision could have let past practice prevail for a limited amount of time to allow for a legislative remedy to be introduced.

The Chair: Fine. Thank you very much.

Could you sum up then, please, Mr. Leuprecht?

(1700)

Dr. Christian Leuprecht: In essence, I endorse the current amendments. However, Bill C-11 does in my world commit one sin of omission. Many more expensive powers for security intelligence should be balanced with robust parliamentary accountability, not to be confused with oversight. My preferred model is Belgium’s, where two permanent agencies headed by judges are empowered to audit not only past, but also ongoing investigations in real time and report their findings directly to a select group of security-cleared members of Parliament.

The Chair: Fine.

Thank you very much. We do appreciate that and thank you for closing off as well. So we will now go to the round of questioning.

We will go to Mr. Carmichael who was so short-changed the last time. You have the first shot here, Mr. Carmichael.

Mr. John Carmichael: Thank you, Mr. Chair, and it’s seven minutes?

The Chair: It is seven minutes for you, sir, so you get the bonus.

Mr. John Carmichael: I get the bonus.

Welcome to our witnesses.

Mr. Davies, I’d like to start with you if I could.

Today, I think we have universal agreement that terrorism is a global threat and certainly, after last month’s tragic events, has demonstrated Canada is not immune to that threat whether initiated overseas or internally.

I wonder if you could just tell us why it is important that CSIS have the clear mandate to conduct investigations outside Canada?

Mr. Garth Davies: Thank you for the question.

I think that we have to consider that we’re increasingly talking these days about the issue of foreign fighters, the foreign fighter problem. I think we understand that they constitute an increasing threat to our country. There is evidence that while they don’t engage in a significant number of acts when they come back to their countries of origin, the acts that they do engage in are increasingly problematic in terms of levels of seriousness.

I also think what has been lost in some of the discussion of the foreign fighter issue is that by allowing these foreign fighters to go overseas, we’re continuing to supply these groups, ISIS. They appear to be, at least in some instances, increasingly dependent on foreign fighters to maintain their operations and their tactics and their ability to operate. So I think CSIS’ ability and I’m focusing just on one particular issue, but I think we need to be cognizant of it from both perspectives, going both ways. It’s not simply a matter of them coming back here, which is problematic, but we’re providing a pipeline for these groups as well that is probably something that we need to consider very closely as to stemming that flow.

Mr. John Carmichael: Dr. Leuprecht, would you like to briefly add to that?

Dr. Christian Leuprecht: Sure. If I may, I will read you one paragraph that I skipped over that I think responds to your question.
I value limited state intervention, but I also value peace, order and good government. So, when confronted with the rare and hard choice between individual freedoms, civil liberties, and privacy on the one hand, and public safety and collective security, it is within the federal government's constitutional purview and obligation to err on the side of the latter, including foreign intelligence activity. The Canadian public gives Parliament and the security agencies that report to Canada's political executive the benefit of the doubt. So I would go—

The Chair: Excuse me, Mr. Leuprecht, you going to have to slow down just a little more, please. Our translators are having a little challenge.

Thank you.

Dr. Christian Leuprecht: Sure.

I would go so far as saying that given the current global security environment, including the challenge of extremist travellers, the federal government has an obligation to Canadians to pass precisely the sort of amendments that Bill C-44 proposes, and that those are in the vital interest of Canada and Canadians. Tactically, operationally, strategically and fiscally, this is the sort of way to compensate for the limits on CSIS to engage in foreign human intelligence gathering.

So in light of the current global security environment, indeed, it is vital that CSIS be able to conduct and to be able to have the capacities that are being introduced in terms of sharing with foreign human intelligence and security intelligence in order for the Canadian government to realize its responsibilities.

Mr. John Carmichael: Thank you very much.

Welcome, Mr. Roach.

I'd like to just step back. It's important that the CSIS Act be clarified for explicit authority for activities overseas, and outside of Canada specifically.

How do these amendments compare to laws governing allied nations and security agencies? That's question number one.

Are judicial warrants required for other western nations? That's something I've heard briefly today. Are they held in such high judicial authorization?

Prof. Kent Roach: Certainly not in the United Kingdom where there's ministerial authorization, much as is available with CSFC. In the United States the Foreign Intelligence Surveillance Court does grant warrants. I think there are some examples of a judicial warrant, there are some examples of a ministerial warrant.

Bill C-44 has decided to opt for the judicial model. I think that's probably a wise choice.

Mr. John Carmichael: Good, thank you.

How much time do I have?

The Chair: You still have another four minutes.

Mr. John Carmichael: Good.

Some concerns we've heard regard the ability of the Federal Court to issue warrants within the scope of relevant Canadian law when issuing warrants to authorize CSIS to undertake certain activities to investigate a threat to the security of Canada outside of Canada. Some may wonder why warrants would not be more appropriate coming from the nation the activities were taking place in, and clearly we've had some examples of that today.
Could you comment on why this is important, as some of those countries may not exactly have a court system that can be approached for a warrant, as well as the transnational nature of these investigations?

Prof. Kent Roach: I think that, as you heard from Professor Furese and as we argued in our joint National Post piece, Parliament is being candid about the reality that some of these warrants may actually violate foreign law.

It seems to me that one of the remedies for that really has to be more political and ministerial than judicial. Obviously courts will have to grapple with this problem, but I agree with Professor Furese and I think that we need some ministerial oversight. Of course, in our security environment—and this is part of the accountability problem—if makes a lot of sense to have a whole-of-government approach to our security threat. The problem is that too often we're still remaining in silos. One of my concerns is that there might be a warrant granted under Bill C-44 that not only should the Minister of Public Safety be aware of, but his or her cabinet colleagues in foreign affairs and defence should also be aware of.

So I do think that it's necessary for CSIS to be able to act outside of Canada, but I think the political risks of that are significant. I think that Bill C-44 could be improved by having some form of ministerial notification.

I would note that SIRC in its latest 2013-14 report has raised concerns that CSIS is not always keeping the minister informed. I agree that under a parliamentary system, the responsible minister has to be aware.

But I think that in the post-9/11 environment where we have a whole-of-government approach to security, ultimately the accountability must rest at the prime ministerial level. That was one of the reasons why, after a lot of thought and deliberation, the Air India commission recommended not what Bill C-44 is enacting, which is a privilege for CSIS, but rather a privilege for the prime minister's national security advisor who the commission thought would be in the best position to determine the competing roles of promising confidentiality to get intelligence now—and that's sometimes going to be the right decision—or not promising confidentiality because we want to be able to prosecute people later. These are very difficult tenses. There's no "one size fits all" solution.

But my concern about Bill C-44 is that it may mean that CSIS makes even rational decisions at a preliminary stage of a counterterrorism investigation that could actually have repercussions and prevent us from being able to successfully prosecute extremist foreign terrorist fighters down the road.

The Chair: Fine, thank you, Mr. Roach.

Time is up. Mr. Carmichael.

We will now go to Mr. Scott, please for seven minutes.

Mr. Craig Scott: Thank you, Mr. Chair, and thank you Professor Roach for being here.

I wanted to follow up on the conversation you were just having with Mr. Carmichael just so that everybody listening is clear. The issue, if I'm correct, is that in the intelligence context there are not the same overarching considerations and incentives for the intelligence community to take care in giving promises to sources because they're not thinking about down the road prosecution. That's the real difference, am I correct?

© (1749)

Prof. Kent Roach: That's right.

And that is partly the story of Air India, but the Air India commission also looked at the contemporary relationship between RCMP and CSIS and found that there were still some problems. Again, I'm not saying that this is a personal fault of either of those two organisations
but you have organisations that have very different mandates and sometimes those are conflicting mandates.

Mr. Craig Scott: Is there a way to deal with the concern? It's true that the court said that there doesn't exist a current, in common law, class privilege and that's what now being accorded by Bill C-44. Is your sense though that the courts were more or less content with the case by case qualified privilege and is that what you think should remain?

Prof. Kent Roach: Yes, I think that the case by case privilege makes a lot of sense because certainly CSIS will tell you this enables us to give an iron clad guarantee to our human sources that there will never be any identifying information. That's not quite right in law because the innocence at stake exception, which also applies to people who become material witnesses or agents during a counter-terrorism investigation. Given the breadth of terrorism offences it may well be that CSIS sources may actually lose that privilege. It seems to me that at the end of the day this is a difficult area, absoluetly not possible. That's why I would prefer a case by case judicial decision and tailor it.

Mr. Craig Scott: Is the case currently under the class privilege that the innocence exception applies in any case, right? So it would apply whether it's case by case or whether it's this broader class.

Prof. Kent Roach: Exactly.

Mr. Craig Scott: To be fair to the way the government is thinking about this, I'm assuming it's not just... You put it, sometimes the issue is it's more important to have intel then to have prosecution. Yes, in a very operational frame. But in a broader frame I suppose we could say the decision that we have to be conscious is being made in the bill. It may be that's more important to have prevention than prosecution. If the government were to present it that way at least we would be conscious of what the tradeoff is. Would you agree with that?

Prof. Kent Roach: Yes, although I do go back to what I started with. I very much mean this and I've written this, not only for domestic but for international audiences. I do think Parliament was ahead of the foreign terrorist fighter curve when they enacted the four new terrorism offences in 2011. I support those offences and I think that the best way to deal with the foreign terrorist problem, sure prevention would be great but there needs to be denunciation and there needs to be incapacitation.

My concern is, and I know this is not the intent of the government, but my concern is that one of the unintended consequences of this bill may make prosecutions under those very new valuable offences more difficult rather than less difficult. I think that we need to... Obviously not all the information is out about what happened at Saint-Jean-sur-Richelieu but we have to ask ourselves the question, why was there enough intelligence to take away that person's passport but not enough to charge him under one of the many terrorism offences that we have in our criminal code?

Mr. Craig Scott: That's great, thank you.

I'd like to move on to constitutionality. You referred to the unconstitutional underinclusive because the provisions here are limiting the right to have the identity of the human source revealed by a judicial decision after an application to prosecutions, and not to all the other contexts in which that source could be behind jeopardy for people's interests, whether it's deportation or security certificates, et cetera.

I clearly understand that you've told us that this is a constitutional problem for that. Despite, I'd have to say, the minister telling us two days ago that this is the most constitutional law the government had ever put forward—I appreciate that.

But there's another point. With respect to the applications either to reveal the identity because it's necessary to make a defence for the person being charged, or for this slightly more nebulous seeking an order declaring an individual's not a human source or that the identity of the...well we'll leave it at that—that other provision. In each case the hearing is held in private and in the absence of the applicant and their counsel, unless the judge orders otherwise.
I have serious concerns about that, as does the Canadian Federation of Law Societies. I'm just wondering if that's included in your worries about constitutionality. Are you okay with that?

Prof. Kent Roach: Thank you for that question, Mr. Scott.

I actually have been reading up on the case law there, and I have to say that I'm a little less concerned than the Federation of Law Societies—I hope it doesn't take away my certificate to practice law.

The Supreme Court's jurisprudence on this actually does suggest that at the first level hearing, it does have to be done in camera, which means with the public not there, and with the other side not there. That is because this privilege is viewed as such an absolute, or near absolute, privilege.

On further reflection, I think that proposed subsection 18.1(7), which you're referring to, would present problems if it didn't have the phrase "...unless the judge orders otherwise." I think that gives the judge enough leeway to follow the Supreme Court's instructions, which are that closed hearings without the applicant being present are sometimes necessary in order to preserve the privilege.

Once the person's identity is out—

The Chair: I'm sorry, we're well past time.

We will now go to Mr. Falk, please.

Mr. Ted Falk (Proponent, CPC): Thank you, Mr. Chairman.

I want to thank all the witnesses for coming here today with their interventions.

Professor Roach, I'd like to start with you.

One of the first comments you made is that this proposed legislation adds new powers. Yet we've heard from the minister and also from previous witnesses that this act does not provide any new provisions. Can you perhaps expand a little further on that seeming contradiction?

Prof. Kent Roach: The issue of whether CSIS has extraterritorial powers is a matter that has actually been under litigation under the act before Bill C-44. Actually Justice Blanchard said in a decision that it didn't have extraterritorial powers. Justice Mosley—and here my interpretation is a little bit different than Professor Leuprecht's—actually said that it did have extraterritorial powers. He only drew it back when he found out that it was using the Five Eyes to exercise what he had authorized as extraterritorial CSIS investigations.

When I say "new powers", I mean that this is a matter of legal dispute. Leave to appeal the Justice Mosley decision is now, I understand, being sought from the Supreme Court of Canada. It is possible the Supreme Court of Canada will hear that case, we really don't know right now.

When I say "new powers", I mean kind of black letter law, new powers that spell it out.

But you're right that the Attorney General of Canada has argued that in the existing CSIS Act there are powers for CSIS to conduct investigations outside of Canada.

Mr. Ted Falk: Right, and that this act just provides more clarity to that. In general you would agree with that?

Prof. Kent Roach: Yes, I would.

Mr. Ted Falk: Okay. You've referenced also that there could be implied confidentiality, that it's something we could inadvertently do?

Prof. Kent Roach: Yes.
Mr. Ted Falk: Or unintentionally provide for someone?

Prof. Kent Roach: Yes.

Mr. Ted Falk: Can you expand a little how we might address that—

Prof. Kent Roach: Sure.

Mr. Ted Falk: —or why you believe that to be the case?

Prof. Kent Roach: Sure.

Well, the reference in clause 2 of the bill, I can understand why a promise of confidentiality was chosen. That is used in the jurisprudence. But in a 2013 Supreme Court of Canada case called Named Person B, the Supreme Court said it can also be an implied promise of confidentiality. So my worry is if you’re going ahead with a CSIS privilege, that perhaps you should revisit that language and talk about an explicit promise of anonymity.

When CSIS agents go to talk to someone, it’s almost always confidential, so my concern is that this privilege will apply virtually to every human source that CSIS interacts with and I think it is important for there to be legislative guidance that narrows that privilege, because of the potential downstream effect of the privilege on the prosecution process.

I would also add that it might be wise to require some form of a review or ministerial oversight about how this privilege, if it is enacted, works out. Because, as I said, rightly or wrongly, the Air India Commission after four years of deliberation certainly looked at this proposal, but on balance rejected it because of concern that this might hinder terrorism prosecutions.

Mr. Ted Falk: Good, thank you.

Mr. Davies, a question for you. Why do you think it’s important for the CSIS Act to give explicit authority to conduct investigations outside of Canada?

Mr. Garth Davies: I think tight now the legal gray area that they’re operating in is probably holding them back from the kinds of things that we would need for them in terms of gathering information. I suspect that it has limited what they feel they can do. They’re operating sort of with one arm tied behind their back. So I think the clarification is required to know they’ll be safe in terms of the information that they’re collecting.

Mr. Ted Falk: Good, thank you.

Dr. Christian Leuprecht: The precise nature of the statement was that I’m concerned that when hard pressed we have a tendency in Canada to err on the side of individual freedoms, civil liberties, and privacy rather than on the side of public safety and security for Canadian society as a whole.

I would suggest that some of our allies have perhaps struck a bit of a more mature balance because they’ve had to live with the phenomenon of terrorism much longer than we have. So we need to recognize that there are certain collective obligations that the government has and that given the nature of the security environment in which we live, when forced to make a choice between the two, I would err on the side of peace, order, and good government over the side of necessarily protecting itemized individual civil rights and privileges if, as a result, the life, liberty, equality and justice of Canadians and Canadian society as a whole may be called into question.
Mr. Ted Falk: Okay.

This bill says that when CSIS or CSIS agents operate on an international level that they must operate within the scope of Canadian laws. Do you think this is an appropriate balance?

Dr. Christian Leuprecht: I do indeed. Teaching at the Royal Military College this is the framework in which the Canadian Forces are deployed and I think we have ample examples of not just the Canadian Forces, but of other government departments conducting operations abroad and doing so within the legal and constitutional framework that Canada applies and expects of those organizations.

The Chair: Mr. Casey, you have the floor, sir.

Mr. Sean Casey: Thank you, Mr. Chair.

I'd like to start with you, Professor Leuprecht. At the end of your remarks you indicated that—and I'm paraphrasing here—the biggest weakness, or the biggest error is an error of omission with respect to accountability but not oversight I think, and you cited the Belgium model as the gold standard. Could you talk a little more about the Belgium model and highlight the differences between what we have here, and what we would need to do to get to what you think is the optimum model?

Dr. Christian Leuprecht: The Belgium model came out of a catastrophic failure in the Dutil case and I would suggest that one of the reasons we would want to look at accountability is precisely to avoid any risk of such catastrophic failure of a security system. Without going into all the details, I would be happy to provide the committee with the contact of the senior judge who heads the organization in Belgium who I know quite well. The key about the organization of Belgium is that the accountability is provided through a mechanism that is paid for by Parliament and the mechanism is directly accountable to Parliament, not to the political executive. It has a staff of about 100 people. The key element of their accountability is that they do not provide accountability just for files that are closed, but they have the ability to see files of any active investigation that is being carried out within the Belgian security framework. So it doesn't just provide accountability after the fact, it provides accountability in the actual process of investigations.

The challenge I think that we currently have in Canada is that we have annual reviews and alter the fact accountability, but we don't have a mechanism that provides ongoing accountability in as effective a manner as we could, and we have a mechanism that reports to the political executive rather than being accountable to Parliament, the major change that would require is members of Parliament to be security cleared to have privileged access to the information that they are being provided, and this would be a significant step for Canadian Parliament to take.

Mr. Sean Casey: But one that you feel represents the best practices internationally.

Dr. Christian Leuprecht: I do think the Belgium model is perhaps one of the most effective in terms of the accountability that it provides both in terms of the tactical operational accountability for the organization in question, and the way that accountability is reported to the legislative branch.

Mr. Sean Casey: Thank you.

To Professor Davies and perhaps I'll get Professor Roach to chime in on this as well. Yesterday the committee received a letter from the Privacy Commissioner of Canada and the privacy commissioner expressed concerns related to privacy issues, and the means by which information is gathered related to the extraterritoriality provisions of the bill. He also commented specifically on the adequacy of existing safeguards to ensure against the risk of such violations including the risk of torture.

Could I have Professor Davies and Professor Roach offer any comments they wish on the concerns expressed by the Privacy Commissioner of Canada to the committee yesterday?
Hon. Diane Ablonczy: A point of order.

The Chair: A point of order, Ms. Ablonczy.

Hon. Diane Ablonczy: At our last meeting we had a discussion about the fact the privacy commissioner put forward certain views, but declined to attend to answer questions on the views. I don't know whether we made a decision about whether to deal with his views absent his appearance before the committee. Can you just clarify that for me?

The Chair: The chair does recall that the privacy commissioner did not appear. I would ask the clerk, was he invited?

The Clerk of the Committee (Mr. Leif-Erik Aune): The privacy commissioner was not invited to appear before the committee for its study of Bill C-44.

The Chair: Okay.

Hon. Diane Ablonczy: So why do we have this information then?

The Chair: What I'm suggesting then obviously the privacy commissioner was not invited as a witness prior to, however, he did send a letter, and the letter was received by the committee, but it has not been authorized to accept in as evidence other than being received by the committee. So that would take a motion by committee to be able to establish that as evidence within the committee otherwise it is there for the committee's personal use.

Hon. Diane Ablonczy: So is this question in order then?

The Chair: There's been an objection raised. That would be up to this committee now to decide whether or not they wish to. It is in order unless an objection is made. There's an objection and the objection can be sustained based on whether or not it's in order.

Hon. Diane Ablonczy: We're always happy to have information, but does that mean anybody can write a letter to the committee and then we have to consider it because that could get a bit messy, I would think?

The Chair: I will read the paragraph that does apply to this because it is for open ball. It says:

There are no specific rules governing the nature of question which may be put to witnesses before appearing before committee beyond the general requirement of relevance to the issue before the committee.

Now there is an issue of relevance in that when the letter was directed to the committee it was relevant to Bill C-44. So it is relevant so at this particular point it would then be admissible and accepted according to the paragraph that is in here. So yes it is in order.

Hon. Diane Ablonczy: Thank you, Mr. Chairman.

The Chair: Carry on please.

Mr. Sean Casey: Professor Roach, Professor Davies, are you okay with the question? Do you need me to repeat it and are you ready to respond?

The Chair: I'm sorry, sir, but we are running out of time now with that. We have about 30 seconds left.

Prof. Kent Roach: Just quickly it does go back to the need for parliamentary oversight and parliamentary access to secret the information. Certainly the resolution of the Afghan detainee case shows that there are some problems there.

The Chair: Fine thank you very much.
Time is now over. I have one little budget issue I would like the committee to deal with, however, I would excuse the witnesses and thank them very kindly on behalf of all of the committee and its members.

Colleagues, I have a budget request that you have had sent to you.

A voice: Sorry to disrupt your time. My name is Michel [inaudible] and I was born January 1174. [inaudible]

Mr. Rick Norlock: A point of order.

Mr. Chair, this is an interference in a parliamentary process.

The Chair: Excuse me. Will you have the gentleman removed please. I would like to call security please. What I would like, colleagues, is I have a witness testimony budget request approved, or not.

An hon. member: I approve it.

The Chair: Meeting adjourned.
THE STANDING SENATE COMMITTEE ON NATIONAL SECURITY
AND DEFENCE
EVIDENCE

OTTAWA, Monday, November 17, 2014

The Standing Senate Committee on National Security and Defence met this day at 1 p.m. to study and report on security threats facing Canada.

Senator Daniel Lang (Chair) in the chair.

The Chair: On June 19, 2014, the Senate agreed that the Standing Senate Committee on National Security and Defence be authorized to report and study on security threats to Canada including and not limited to cyber-espionage, threats to critical infrastructure, terrorist operations and prosecution, and that the committee report to the Senate no later than December 31, 2015.

To begin with, colleagues, before we welcome the witnesses, we will introduce ourselves. I am Dan Lang, senator for Yukon. On my left is the clerk of the committee, Josée Thérien. I would like to invite each senator to introduce themselves.

[French follows - Senator Dagenais: Sénateur Dagenais, du Québec.]

[après anglais](The Chair continues - each senator to introduce themselves.)

Le sénateur Dagenais : Sénateur Dagenais, du Québec.

La sénatrice Fortin-Duplessis : Sénatrice Fortin-Duplessis, du Québec.

[Sen. Ngo : Thanh Hai Ngo from Ontario.]

[anglais suit]

[Following French - Senator Fortin-Duplessis : Sénatrice Fortin-Duplessis, du Québec.]

Senator Ngo: Thanh Hai Ngo from Ontario.

Senator Beyak: Lynn Beyak, Ontario.

Senator White: Vernon White, Ontario.


The Chair: Colleagues, before we start with our witnesses, I just want to go back and review what we've done in the past number of weeks.

During our earlier hearings, the committee received evidence that we have between 135 and 145 Canadians who are dual nationals fighting in Syria and Iraq with ISIS. In addition, we have approximately 80 who returned to Canada and we also have presently some 93 people on a high-risk traveller watch list. This, I believe, is quite troubling, especially if one considers the responsibilities that our law enforcement agencies assume to oversee these individuals.

We also heard that there were 51 terrorist organizations recognized in Canada in 2010, and today our government has designated 53 terrorist organizations in one capacity or another.

Also, when it comes to supporting terrorism with money, we learned that terrorist financing from Canada is in the six figures and often disguised as humanitarian aid. The committee heard that we have very few terrorism prosecutions in Canada under section 83 of the Criminal Code. This in itself is disturbing when one
considers that our laws under section 83 allow for charges when one provides material support to a terrorist group or organization.

This afternoon, the committee will be meeting for three panels of discussion as we look at the threats to Canada: specifically, terrorism. We will be focused specifically on the issue of countering terrorism and what law enforcement and government is doing to meet these growing threats.

Joining us today to discuss counterterrorism and counter-radicalization are three representatives from Public Safety Canada, Mr. Gary Robertson, Assistant Deputy Minister, National and Cyber Security Branch; Mr. John Davies, Director General, National Security Policy, National and Cyber Security Branch; and Ms. Anna Gray-Hernschel, Senior Director, National Security Policy Division. From the Canadian Security Intelligence Service we have Mr. Tom Venner, Assistant Director, Policy and Strategic Partnerships.

I understand Mr. Robertson and Mr. Venner have opening statements, and we will be beginning with Mr. Robertson.

Gary Robertson, Assistant Deputy Minister, National and Cyber Security Branch, Public Safety Canada:
A little more than two years ago, the Government of Canada unveiled its counterterrorism strategy, a multifaceted response to a threat that is both national and global in nature.

Canadian security and law enforcement agencies have been successful in detecting terrorists and denying them the means and opportunity to carry out their activities. Over the past decade, they've uncovered and disrupted a series of terrorist plots that would have had devastating consequences had they succeeded.

Nevertheless, in the last month the events remind us that the threat of extremist violence remains. It affects us both as a nation and as individual Canadians.

Terrorist groups like ISIS and al Qaeda may seem distant to most Canadians, but lone actors inspired by their toxic ideology can represent a direct threat to Canadians.
Ce qui nous amène à poser une question cruciale : comment empêcher la radicalisation menant à la violence dès le départ?

The Government of Canada is committed to the “Prevent” element of the CT strategy; it is committed to countering violent extremism in all of its aspects. Our preventive approach, which laid out the “Feature Focus” of responding to violent extremism in this year’s public threat report, is built around three mutually supportive themes.

We’re building community capacity and law enforcement capacity, and we’re using early intervention to redirect people away from pathways that lead to extremist violence.

Nous ne devons pas oublier que la lutte contre l’extrémisme violent ne concerne pas seulement le gouvernement, la police ou les agents du renseignement; elle concerne les collectivités.

Family members, peers, religious community leaders, even teachers, doctors, nurses and social workers, are better placed to identify and respond to the changes in attitude and behaviour that are precursors to violent extremist action. And, with support, they are better placed to take meaningful and positive action to address those early warning signs before they become problems.

So community knowledge of radicalization to violence and community awareness of the dynamics and precursors of radicalization to violence are the keys to a preventive approach to countering violent extremism. Outreach and engagement networks built up by local police services, the RCMP and advisory and liaison groups like the Cross-Cultural Roundtable on Security are absolutely fundamental to building that knowledge and awareness.

We are instiating conversations with communities in which we discuss violent extremism in the context of people’s life experiences. This is accomplished with the help of professional facilitators who create a “safe space” for communities to talk about radicalization to violence and to identify opportunities for individual and community intervention. With the help of the Cross-Cultural Roundtable on Security,
we've conducted seven facilitated sessions in Quebec, Ontario and Alberta. Response has been overwhelmingly positive. Demand for sessions currently outstrips supply, so we are developing training for community facilitators.

(French follows in 1310 - Mr. Robertson continuing - Notre travail à cet égard a été...)

We referenced the police a moment ago, and the importance of the trust and community networks built up over the years by the RCMP and by our provincial and municipal police services across Canada. Obviously outreach and engagement is a big part of countering violent extremism strategy. Outreach and engagement is something that the police do very well because it is rooted in the most basic principles of community policing.

(French follows - Mr. Robertson continuing -- Les services de police communautaires...)

Les services de police communautaires consistent sur des agents de police avertis et capables de détecter les signes avant-coureurs et d'intervenir de façon appropriée dans un contexte communautaire.

We want communities to understand the threat of violent extremism, so it follows that police officers will be supporting those communities in their countering violent extremism efforts must be equally knowledgeable.

(French follows -- Mr. Robertson continuing -- Le gouvernement du Canada aidera...)

Le gouvernement du Canada aidera à promouvoir et à améliorer le matériel de formation existant sur l'extrême violence.

Particularly, we want to build on the success of our programming like the RCMP Counter Terrorism Officer initiative. CTIO presides front-line police officers and other first responders with the critical training.
around the warnings and indicators of violent extremism. Approximately 2,000 candidates have participated in this program since it was established five years ago.

A community policing response to violent extremism does not replace the necessity for investigation, arrest, and prosecution; but it does support the kind of preventive approach that permits law enforcement resources to be focused on the most serious of crimes.

(French follows — Mr. Robertson continuing — il est évident que les enquêtes, les arrestations et les poursuites doivent entrer en jeu lorsque les mesures de prévention ne donnent pas fruit.

(M. Robertson : But what, potentially, does a...

(anglais suit)

(Following French — Mr. Robertson continuing — prévention ne donnent pas fruit.)

But what, potentially, does a prevention-based response to radicalization to violence look like? How do we divert and dissuade people who are radicalizing but who have not yet crossed the threshold of extremist violence, whether it’s here in Canada or abroad?

(French follows — Mr. Robertson continuing — L’établissement d’un programme...

(M. Robertson : A shared initiative between police...

(anglais suit)

(Following French — Mr. Robertson continuing — contre l’extrémisme violent.)

A shared initiative between police and communities, early intervention programming should be aimed at people at the periphery of violent extremist activity but who haven’t yet progressed to the point where disruptive action — investigation, criminal charges or prosecution — is warranted. Having community-based mentors to provide advice, support and counselling aimed at promoting constructive responses to violent extremist ideology is a best practice.

(French follows — Mr. Robertson continuing — Une intervention précoce ne garantit...

(après anglais)(M. Robertson)

Une intervention précoce ne garantit pas que des personnes ne se radicaliseront pas ou qu’elles ne voyageront pas à l’étranger pour prendre part aux activités terroristes.

(M. Robertson : But as a tool for diverting potential...

(anglais suit)

(Following French — Mr. Robertson continuing — prendre part aux activités terroristes.)

But as a tool for diverting potential violent extremists, it is a constructive alternative to investigation and prosecution.

Ultimately, it represents a joint community/law enforcement response so the problem of radicalization to violence and to the challenge of fascist travel.
Violent extremist ideologies remain powerful. They continue to encourage people to take part in operations on the other side of the globe. They continue to evolve and, as the terrible events of October show, they continue to inspire and influence people here in Canada.

[French follows -- Mr. Robertson continuing -- Même c'est un problème...]

[après anglais] [M. Robertson]

Même c'est un problème qui ne se règle pas avec des arrestations.

(M. Robertson : As a society, the task facing...)

[anglais suit]

(Following French -- Mr. Robertson continuing -- pas avec des arrestations)

As a society, the task facing us is to counter violent extremism at the community level.

As a government, our task is to ensure that communities are equipped with an array of options in support of prevention and intervention. Thank you.

The Chair: I believe Mr. Venner has a presentation.

(French follows -- Tom Venner, Assistant Director, Policy and Strategic Partnerships, Canadian Security Intelligence Service: Bonjour, je vous...)

[après anglais]

Tom Venner, directeur adjoint, Politiques et partenariats stratégiques, Service canadien du renseignement de sécurité: Bonjour, je vous remercie de m'avoir invité à participer à votre étude des menaces qui pèsent sur la sécurité du Canada. Je suis heureux d'être ici aujourd'hui pour discuter des mesures prises par le Canada et, en particulier, du rôle que joue le Service pour appuyer l'aspect « prévention » de la Stratégie antiterroriste.

(M. Venner : Everything the service does is rooted in...)

[anglais suit]

(Following French -- Mr. Venner continuing -- « prévention » de la Stratégie antiterroriste.)

Everything the service does is rooted in its mandate, which is clearly articulated in the CSIS Act. Through our national security mandate, we are authorized to collect and analyze information on threats to the security of Canada, and to provide advice to partners. For the purpose of today's discussion, it is important to underline that CSIS is not authorized to act directly to disrupt threats or to prevent radicalization to violence.

We can and do, however, support the government's efforts to prevent the radicalization to violence in meaningful ways, both by understanding the threat environment and the dynamics of radicalization, and by supporting community engagement.

[French follows -- Mr. Venner continuing -- Afin que les partenaires au sein du...]

[après anglais] [M. Venner]

Afin que les partenaires au sein du gouvernement puissent élaborer des stratégies efficaces de lutte contre l'extrémisme violent, ils doivent comprendre comment et où se manifeste l'extrémisme. C'est dans ce domaine que le SCRS possède des compétences considérables. Le SCRS est bien placé pour donner une idée de l'étendue et de la nature du phénomène, à la fois au Canada et dans le monde, grâce à ses enquêtes, à ses analyses et à ses solides relations avec ses alliés.
Of course, CSIS is most commonly associated with its investigative function, which puts us at the forefront of efforts to detect terrorist activities. But the service does more than detect threats to the security of Canada. We also seek to understand them, which was the subject of my colleague's introductory remarks before honourable senators late last month. We are doing important work to deepen the understanding of the dynamics of radicalization — trying to understand, in other words, what makes certain people vulnerable to extremist ideologies. The more we understand about the radicalization process, the more effective strategies to counter that process will be.

To that end, the service is active participant in the public safety's Kanishka Project and also maintains its own independent research capacity. This analytical work is integrated with our collection and operational activities and, in turn, is shared with partners to inform their own research, policy and programs. We also participate in the Canadian Network on Terrorism, Security and Society, which fosters communication and collaboration between Canadian academics and policy-makers on national security issues.

While the service does not have a legal mandate to engage directly in outreach per se, we have, nonetheless, been strong proponents of such initiatives, including the Cross-Cultural Roundtable on Security, the CERS. The CERS has given us access to representatives from various communities, creating opportunities to raise awareness and to learn more about some of the communities we serve. In the last four years, CSIS has participated in 12 CERS events on a wide range of issues. And through our regional presence across the country, CSIS also participates in a range of community outreach initiatives led by our partners, the RCMP.

Senator Beyak: Thank you very much, chair. Thank you for your presentations, gentlemen. I wonder if you can tell me in formulating our policy how much you have looked at other nations' policies. The problems in France, Belgium, and the United Kingdom specifically, the problem is getting worse there and not better. I wonder what you're doing different or what you have used from them. Thank you.

Mr. Robertson: We have looked quite a bit internationally at what is going on and recently had a delegation in France dealing with a number of our international colleagues. I would say we have leveraged quite highly and quite heavily the information that's available elsewhere, especially what has been shown to be effective; but the approach that we have taken is a little bit unique in that we've developed narratives...
that really engage, in a much more meaningful way, the communities that we're attempting to work with, and in fact it's been seen to be a bit of a best practice internationally.

Senator Beyak: Why do you think it's getting worse in those countries, specifically France, Belgium and the United Kingdom?

Mr. Robertson: I would say there is an international problem right now that is of great concern. I wouldn't characterize it as getting worse, but I would say any problem that continues to exist continues to fester, and we definitely have an issue on that scale. It's a material issue, as we've been seeing in the last months or so here in Canada. It's one we've been experiencing for years, and it's certainly one we want to get a better handle on.

Senator Beyak: Last question: Do you have a strategy for doing that?

Mr. Robertson: Yes. Not to use propaganda, per se, but we have a strategy that's been in place since 2012, and we're working within that framework.

At Public Safety, we are principally involved in the preventative, but we are involved in the other three pillars to some degree as well, whether it's through coordination or other activities. But we're certainly attempting to execute the strategy we already have in place.

Senator Day: Ladies and gentlemen, thank you very much for being here. I think it would be helpful for the record if we had some clarification on Mr. Vermer's comments in relation to Public Safety's Kanishka project. Can you tell us a bit about that project that you were saying is a good thing?

Mr. Robertson: It's a Public Safety Canada initiative, and back in 2011, it was launched by the Prime Minister. Basically, $10 million of investment went towards enhancing community capacity. So we have a number of initiatives, largely funded through grants and contributions, with organizations that are doing research in the areas that we're most interested in.

Senator Day: So it's been in existence for a number of years now and it has some public money put into it each year. Which budget does that come out of? If I was to trace that back, where would I find it?

Mr. Robertson: For grants and contributions, $10 million over five years works out to $1.5 million to $2 million in this current fiscal year.

Senator Day: Thank you. The other area I'd like you to tell us about is with respect to a Cross-Cultural Roundtable on Security that we've heard more about, but we've also heard different points of view on this particular round table, so could you tell us first of all how long it has been in existence? How many permanent members are there on the board? Where do they get their funding? Give us a background on that, whatever information you might have, please.

Anna Gray-Henschel, Senior Director, National Security Policy Division, Public Safety Canada: It was created out of the National Security Policy in about 2004. Its first meeting was in about 2005.

Its terms of reference allow for up to 15 members, and these members are selected across Canada from diverse communities, diverse genders and diverse backgrounds. They're all considered leaders within their communities. Members have come and gone over the years. I don't have the answer. I don't know about its funding. It's through our Citizen Engagement Branch, but I can get that information for you. Sorry. I'm a psychologist, not a finance person.

Senator Day: If you could follow up on that for us and let us know the total amount of funding, over what number of years, 10 years, $1.5 million a year, whatever it might be, and it's up to 15 members. You can send that in to us so we have a full understanding. It's up to 15 members?

Ms. Gray-Henschel: Yes.

Senator Day: But how many members are actually there now? Have any of you been involved in recommending any members for this round table, for example?
Mr. Robertson: As Anna said, we'll go back and get the financial numbers you requested.

The meetings are quite frequent. Oftentimes, it's interesting to note the members contribute their time on weekends. It's often a Friday night, Saturday and a good portion of Sunday. The next meeting is actually scheduled for this Friday, so I'm heading out to the East Coast to participate in that along with Anna.

Senator Day: The East Coast?

Mr. Robertson: Yes, so closer to home.

Senator Day: This is good. I noticed you didn't have the East Coast and you have conducted seven facilitated sessions in Quebec, Ontario, and Alberta, and I said what about B.C. and the east? So you are filling that gap; half of it, anyhow.

Senator White: Thanks to all of you for being here today. I'm going to refer to the Securing Open Society document from about a decade ago. I'm trying to figure out whether we've had an update. Where are we in relation to the changes that we've seen in the last 10 years that would cause us to maybe shift or at least come up with a new document in relation to national security threats?

Mr. Robertson: What I would say is while the nature of the threat evolves and the participants and the threat evolve, the fundamentals remain fairly unchanged. So the foundation piece of it hasn't evolved a lot. What has changed quite a bit is how we focus our resources to address the emerging threats. As I said, back in 2012, we developed a counterterrorism strategy, and that clearly laid out the four pillars we're approaching under it.

Maybe more to your question is what changed back in 2012 was the government's commitment to actually report on progress. So in the last two years, we actually issued an annual report as to what has been occurring, how it's been evolving, what we're investing and how we're seeing benefits from it. The most recent report is the 2014 Public Report on the Terrorist Threat to Canada, and it's quite a useful document; it's publicly available.

The only other thing I would say as it relates to the report is, as you would expect, it relates to the previous period. You won't find 2014 activities, at least not the ones that were fairly close to the publishing deadline, but you'll get a very good flavour for how things have evolved since then.

Senator White: The second question I have is probably more for Mr. Venner, if I may. We hear a lot about radicalization and indoctrination, and it seems people focus on the internet, but there is also, as we know, that same type of movement in the more formal locations. Some would argue whether or not it's a school atmosphere or at least in a religious foundation atmosphere.

I'm trying to figure out where we are from CSIS's perspective on combating or making a shift in those more formal arenas. If I go back to the Toronto 18 as an example, we know that at least some of the evidence told us that, in fact, some of the indoctrination happened in that type of arena. Today we are trying to combat some of that in Canada, and I think there is more we should do from a legislative perspective to try and combat that as well.

Mr. Venner: I think I'll start with going back to the point I made at the outset about our role in terms of collecting intelligence on threats. Our focus is on threat-related activities, and we target investigated individuals engaged in those activities, so we don't focus on institutions per se.

Senator White: Individuals and institutions possibly?

Mr. Venner: Possibly, but we wouldn't define that as investigating an institution.

Senator White: Understood.

Mr. Venner: The results of those investigations are obviously the type of thing that we may share with our partners so that they may decide to take action, whether it's, for example, in relation to counteracting violent extremism, which the service doesn't have a front line role in per se. That's more for the types of
mechanisms that are alerted to for the RCMP and, as I think Gary mentioned, the significance of a front-line community policing approach to that problem.

So I think I would try and make sure that there isn’t a view that we would stray from that. We obviously gather, on occasion, helpful information that could be shared, but that’s not really our focus. We’re there to worry about the threat-related activities that could potentially pose danger to public safety, and then if we can develop through those investigations our analysis trends or aspects of radicalization, we think it would be helpful for our partners to use and we would certainly be sharing that.

Senator White: Thank you for that. I’ll certainly ask a similar question later when the RCMP are in front of us.

I have a question for Public Safety, though. If I may, around the sharing of information and whether or not we’re actually sharing. Look, our two largest provinces and none of our largest police services are policed by this country’s national police service, right?

I guess I’m trying to figure out whether or not we actually have the ability to share at every level we need to with those police agencies when they may or may not meet the security requirements to receive the information — sure, they can feed in, but can they receive it back — and whether or not Public Safety Canada believes we should have a national standard that all police organizations and their officers meet to be able to receive the information that, I would argue, they have to receive, particularly in this day.

Mr. Robertson: You may want to pose this to the RCMP when they appear before you later today.

We have five INSETS teams across the country whose sole purpose is to integrate the activities of the various police forces, whether municipal, provincial or federal, and to pursue investigations where it’s required. That’s definitely a focus of the law enforcement community.

I think the point that we were hoping to make today is more people appreciate the enforcement side of the equation, which, unfortunately, often happens once things have escalated too far. On the prevent side, we’re hoping to promote to a greater degree the work that’s been going on that law enforcement has been co-leading, in terms of helping communities understand that there are interventions possible earlier, that there are law enforcement personnel who are well trained and sensitized to these unique issues, that they understand how to work with the community practitioners, as I said to your earlier question, whether they be school counsellors, nurse practitioners or whoever it might be; and that it doesn't necessarily lead to incarceration should the family or friends of a person whom someone is concerned about approach law enforcement.

The Chair: Colleagues, I’d like to follow up with Mr. Venner on a few of the questions of Senator White to get some clarification on the record.

Do I understand that CSIS has no responsibility at all in respect to institutions that are perhaps teaching this radical Islamic doctrine or any other religious political doctrine at a religious institution or at a university campus? The reason I ask this question, if you have been reading the international news, there was a report out recently in respect to England. I believe, where it is being said that a lot of this indoctrination for the radicalization of young people is happening in various institutions. If no one is monitoring it, how do we know if it's happening or not happening? If you're not doing it, who is doing it?

Mr. Venner: I will try to clarify. I didn’t mean to suggest that there are sort of areas of refuge where the service would be not looking and not investigating. We have policy that deals with how to approach investigations that may touch upon sensitive institutions such as educational institutions and religious institutions, because of the various sensitivities around any sort of investigative or operational activity that could potentially impact them or touch on them.

It's not to say that we ignore them or consider those off limits, but we treat those investigations with a certain degree of sensitivity and care. As I said, we’re not going to be targeting those institutions per se; we’re going to be worried about individuals who may be engaging in threat-related activities conceivably attached to those institutions. We're not targeting the institution. We're following that threat-related
activity wherever it may be. When it comes to sensitive institutions, we are obviously very careful about how we do that. There are policies to make sure that that is authorized at the appropriate levels and within the right framework and parameters.

The Chair: Let's get clarification on the record. What you're saying is for those types of institutions, you do have the authority, if needed, and if there is a threat that you feel is being posed, you can monitor to see if indoctrination is taking place, and then, of course, obviously maybe appropriate action can be taken.

Secondly, these institutions are provincial institutions in some cases. What relationship do you have with the provinces in respect to that as well, if any?

Mr. Venner: I'm not sure what you mean by an institution. Are you talking about an educational institution?

The Chair: Yes.

Mr. Venner: Our issue there is the nature of the institution, whether it's federal or provincial. The point is it would be deemed a sensitive institution. If that's a university or another place of education, that's how we define it. We don't really say, "Well, it's provincial, so we're not going to go there."

The other question was?

The Chair: In respect to your authority to be able to go into these institutions, religious or educational, you do have the authority and you do monitor it, and then you take appropriate action if you find, for example, the definition of advocating hate were to come into play. Then you would report this to the RCMP and the integrated group; is that correct?

Mr. Venner: First of all, in terms of our threshold for investigations, generally, we have to have reasonable grounds to suspect that an activity is related to a threat to the security of Canada. That would be our threshold for whether or not we would go there.

In terms of how we would do that, as I mentioned, we have our internal policy in terms of if you've got an investigation that's going to touch upon that type of institution, you would have to adhere to that. It obviously means higher levels of approval and things like that to make sure it's being treated appropriately.

I'm not sure what else I could add to that. Certainly, we have the authority to do that, but that's how it's in effect treated.

The Chair: I'm sure Senator White may follow up on that a little later. I think he indicated that.

(French follows – Senator Dagenais – Ma question s’adresse à M. Davies.)

(après anglais)

Le sénateur Dagenais : Ma question s’adresse à M. Davies. Le commissaire de la GRC, Bob Paulson, a dit au comité qu’il voulait que soit abaissé le niveau de preuve nécessaire pour obtenir du procureur général l’autorisation d’imposer un engagement de ne pas troubler l’ordre public à une cible de sécurité nationale. Il a déclaré qu’il y avait lieu de soupçon raisonnable, il devrait suffire d’avoir la croyance raisonnable qu’une infraction est commise ou que quelqu’un est mêlé à cette infraction.

Il a ajouté que bien qu’il suffise à l’agent de la GRC d’avoir des motifs raisonnables de croire qu’une mesure comme la détention préventive s’impose pour empêcher, au terme de l’article 83.3 du Code criminel, une personne liée par un engagement de ne pas troubler l’ordre public, de commettre une infraction de terrorisme, il doit d’abord convenir le procureur général qu’il y a motif raisonnable de croire que le sujet a commis ou complotera une infraction terroriste.

Le même jour, M. Brian Saunders, Directeur des poursuites pénales, Service des poursuites pénales du Canada nous a dit que l’obtention du consentement du procureur général ne posait pas de problème à la police. On a cependant rappelé au comité que le Code criminel autorise l’arrestation préventive sans
consentement du procureur général ni mandat. Si les circonstances l’exigent, ils peuvent arrêter quelqu’un, obtenir ensuite le consentement puis déposer la dénun- ...

Quelle est la position de Sécurité publique Canada sur l’abaissement du niveau de preuve nécessaire pour obtenir du procureur général l’autorisation d’imposer un engagement assorti de conditions ?

M. Davies : Je vous remercie de votre question sénateur.

(anglais suit dans 1340 - My apologies)

(Following French in 1330 -- Mr. Davies (cont’g) — votre question sénateur.)

My apologies. I’m not going to have a great answer for you. I know the commissioner made some comments. There’s a lot of things in discussion right now, post events in Ottawa, and just given the extremist travel overall, in terms of looking at thresholds and other policy and program legislative approaches that we could be taking, there are a number of things being worked out with the minister now that are advice to the minister and to cabinet. It’s difficult for me to discuss any particular proposal that may be on the table.

Obviously, we’re interested in thresholds. We’re interested in getting intelligence in the courtroom in a safe way that protects the sensitivity of that information. We’re interested in improving information sharing. It’s difficult to talk in details right now.

(French follows — Le sénateur Dagenais : Pour la version britannique …)

(après anglais - in details right now.)

Le sénateur Dagenais : Pour la version britannique de l’engagement assorti de conditions, l’ordre d’enquête et de prévention du terrorisme a une durée d’effet maximale de deux ans, contre un an seulement pour l’engagement de ne pas troubler l’ordre public. Pour quelle raison aurait-on décidé de limiter la durée d’effet de l’engagement assorti de conditions à 12 mois ?

(Mr. Davies: First of all, I think they’ve …)

(anglais suit)

(Following French – Senator Dagenais – … conditions à 12 mois?)

Mr. Davies : First of all, I think they’ve just put some new proposals forward. I think Prime Minister Cameron in Australia announced new changes. We haven’t had a chance to have a detailed look at those. In the past, when they’ve done work in this area, they’ve had trouble in the courts. A lot of the proposals haven’t held up well. A lot of the work going on now is led by the Department of Justice. I’m not sure if you’re meeting with colleagues from Justice in this committee on this issue, but they’re the lead on this issue in terms of any advice on the way forward on peace bonds or recognizance with conditions and the other provisions in what was 7.

The Chair : As a committee, this is what we’re trying to get to, to see whether or not the thresholds presently are too high. Because we’ve been informed on this committee, we have at least 240 Canadians and dual citizens involved in terrorism or at least identified in one manner or another, and yet there are no charges being laid except for, my understanding, in one particular case. The question is: Is the threshold too high? If the threshold is too high, sit: what do we have to do to lower it so we can expect you and the law enforcement agencies to do the job we expect?

Mr. Davies : It’s not just an issue of thresholds. Thresholds are an important part, but there is also the issue of making sure intelligence is usable in the court of law. It’s not necessarily just about thresholds.

Thresholds are an important piece, but making sure information can be used in a court in a way it’s protected is also an important piece; and also ensuring information gets to the intelligence agencies so that they can use it, which then can be used effectively in a court of law. You have to look at this from all angles.
There are also administrative tools at our disposal, whether that's passports, watch listing, immigration actions and so on. It's not just about the issue of criminal thresholds.

Mr. Robertson: One other point, if I might. We also need to look at whether some of the other mechanisms John just referred to are contributing to less arrest detentions under the section that you referred to than we would expect.

Another program is the listings program. By shining a bright light on organizations or individuals who are engaged in particular activities that we deem to be quite harmful, rarely is there a subsequent infraction within a Canadian jurisdiction. Oftentimes those folks don't return to Canada. They don't come back or don't incur problems here in Canada because it has been made clear there's an issue with the behaviours that we're focused on.

Just another point as to the absence or few charges under the one regime, ideally if we were preventing and causing all the mechanisms that act in concert to be successful, we wouldn't see a large number of charges because we wouldn't have a large number of incidents.

The Chair: I'm sorry, colleagues, but I don't think we should leave this. We've been informed that there's in the neighbourhood of 80 Canadians or dual citizens who will return back to this country from being involved in one manner or another in terrorism activities, at least identified. You just told me if we identify the organization, they don't come back.

Mr. Robertson: In some cases, I wasn't using a generalization. Let me take another approach. Just because an individual went overseas, we focus more on the extreme cases where they're actually taking up armed conflict or involved in other things. Others go over and receive minor training or leave. Some are peripherally involved in financing, whether it's their intention originally or not. In some cases people come back quite disillusioned, and so it's quite possible and one would expect some segment out of that 80 are folks who would have had no intention of pursuing anything further along the lines we're discussing today because they've seen enough that they don't wish to have or they didn't have the extreme experiences some others do and they haven't glorified it. I'm not characterizing the full 80 by any means; I'm suggesting there are subsections of that list that aren't necessarily as high a risk as others.

Senator White: I'm trying to figure out how we walk through gathering and sharing some of the information. I'll try not to talk about institutions, because Mr. Vennet doesn't want me to. The reality is that things are happening at some institutions by individuals, and that information is out there. We've seen a number of the cases we've disrupted in this country successfully and prosecuted successfully have been because that information was shared. I have to say that I'm not hearing that we have either enough resources out in the communities right now engaging and gathering and sharing, and it's okay that we say it could come from a teacher or a nurse practitioner happening to work in an institution that could gather it, but the reality is it still has to move its way through a system to go from information to intelligence and often into evidence.

I know Ms. Gray-Henschel's background. I'm sure she'll walk us through this. I'm not convinced we have the resources in those communities to pick up this information to drive so we can successfully disrupt, as we have in the past, and we've done extremely well in this country for a decade. I'm not sure our future is as bright now, to be fair.

My question will be to Ms. Gray-Henschel. Have we actually moved the yardsticks forward, kept them where they were over the past decade, or are we falling behind when it comes to resource levels and our ability to combat this? I will disregard the two incidents in October, to be fair. But overall, as a country, are we in the right place? And I'm not apologizing for putting you on the spot.

Ms. Gray-Henschel: It's okay. Thank you for the question. A lot of effort has gone through law enforcement in earning the trust of communities. That's through your basic law enforcement work, so they can engage and feel comfortable in engaging in this radicalization to violence space. In the future focus one of the things we talked about was building community capacity.
As we ask communities to come forward, to intervene in the pre-criminal space, but also if they cross the line, to trust law enforcement and its agencies. They need to have the information as to what are the indicators. We have to equip them. A lot of parents, teachers, nurses and doctors have a number of threats. We are reaching out to educate them through telling the stories.

We have that foundation, which a lot of countries envy. Law enforcement in Canada enjoys the trust of many communities. Can we do better? Of course, we can always do better. But now that we have that, people are willing to have a focused discussion on radicalization to violence, and that’s where our energy will be. Recently at a federal-provincial-territorial meeting, we talked about bringing those other orders of government in. Our way forward is to leverage those good relationships in general and to how do the early intervention and prevention.

Senator White: I accept that we are doing much better when it comes to educating those people who are in positions of gathering that information. But we also know that if they don’t understand exactly what they should be looking for, too much information that isn’t relevant will be less helpful than no information. I’m trying to figure out how to make this more formal in this information sharing. I’m back to the question earlier: Do we need a standard in this country to ensure people are at the right level to receive the information that we want them to get? Here is what you should be looking for: Specifically, we have a concern about this group, here’s how they’re radicalizing; because if we can’t tell them that, I’m going to argue they can’t tell us what we need to hear.

Have we actually got to the point where now in this country we need to have a standard to push out across the country for all police agencies? The members of most police agencies in this country don’t meet a level whereby they would receive some of the same information you have on your desk, let alone the other agencies we’re trying to deal with. Are we at a point where we should be pushing that forward so that we can have 66,000 police officers in this country sharing information more readily than we have in the past?

Ms. Gray-Henschel: What I can say is that in speaking with communities and listening to communities, they’ve asked for that information and we’ve had really good dialogue around that. They’re able to provide us with their perspectives and the points of intervention. It’s very much a two-way dialogue. With the threat being so diffuse, we need everybody to recognize changes in behaviour, changes in attitude.

A lot of that discussion is not of a classified nature. To be quite honest, it’s in the pre-criminal space. So there is a lot of work going into that and communities have received us very positively when we’ve come and told the stories and talked about those changes and attitudes and behaviours, because they’re the ones that are seeing it, then follow-up discussion will be held. What do we do with that information? Who are our resources within the community? That’s where our priority is right now with the other orders of government.

Senator White: Did you want to add to that, Mr. Robertson? I notice you’re nodding your head.

Mr. Robertson: We’re obviously at that point of reflection right now. We’re looking at a wide variety of things that we might want to consider, especially back to your point as well. Nothing is off the table. We’re going through and looking at what makes sense. Even when I talked about the program that we’ve been leading, we’ve had great success with the number of people, but we’re not in the quantum you’ve discussed. One of the responses is to go to a more of a train-the-trainers approach, because we know we will never have the resources we need to directly interface with every community member who has an interest or every law enforcement member who is inclined to go through that standards-based process. Nothing is off the table right now.

Senator White: Thank both of you for your responses. I appreciate it.

(French follows – La sénatrice Fortin-Duplessis : C’est ma toute première)

(après anglais – Senator White – I appreciate it.)

La sénatrice Fortin-Duplessis : C’est ma toute première fois au Comité de la défense. Je suis très heureuse de vous avoir entendus.
Ma première question est la suivante. Quand prévoyez-vous que le ministre de la Sécurité publique déposera son prochain rapport annuel sur les cas d'arrestations sans mandats, aux termes de l'article 83.3 du Code criminel l'année en cours? J'ai ensuite deux autres questions.

(Mr. Robertson: The report that's tabled annually is typically prepared...)

(French suit)

(Following French — Senator Fortin-Duplessis — deux autres petites questions)

Mr. Robertson: The report that's tabled annually is typically prepared during the spring and early summer periods, and usually published late summer/early fall. That would be the next opportunity, probably August or September of 2015.

(French suit — Le sénatrice Fortin-Duplessis : Le rapport de 2014)

(après anglais — Mr. Robertson — September of 2015.)

La sénatrice Fortin-Duplessis : Le rapport de 2014 a-t-il déjà été déposé?

(Mr. Robertson: Yes, it's been prepared and published...)

(French suit)

(Following French — Senator Fortin-Duplessis — déjà été déposé?)

Mr. Robertson: Yes, it's been prepared and published. In fact, we can obtain a copy for you, if you would like.

(French suit — La sénatrice Fortin-Duplessis : Le ministre de la Sécurité)

(après anglais — Mr. Robertson — if you would like.)

La sénatrice Fortin-Duplessis : Le ministre de la Sécurité publique est tenu, aux termes de l'article 83.3(1) du Code criminel, d'exprimer dans le rapport annuel son opinion de l'opportunité ou non de proroger l'article 83.3.

Croyez-vous que le ministre se prononcera en faveur de la reconduction de cette disposition telle qu'elle est actuellement formulée?

(Mr. Robertson: I'm not sure that I fully understood that...)

(French suit)

(Following French — Senator Fortin-Duplessis — est actuellement formulée?)

Mr. Robertson: I'm not sure I fully understood that. Could I ask you to restate?

(French suit — Mr. Robertson continuing — Pouvez-vous reformuler?)

(après anglais — M. Robertson — ask you to just restate?)

Pouvez-vous reformuler?

La sénatrice Fortin-Duplessis : la formule peut-être que je vous le dise en anglais?

(Sen. Fortin-Duplessis: Do you anticipate that the minister will support...)

(French suit)

(following French — Senator Fortin-Duplessis continuing — vous le dire en anglais?)
Do you anticipate that the minister will support extension of this provision as currently formulated concerning section 83.3 of the Criminal Code?

Mr. Robertson: I'm not sure that I have that information. I'm sorry, that's my response, but I'm not sure, John?

Mr. Davies: I don't recall 83.3. What is that provision?

(French follows -- La sénatrice Fortin-Duplessis : "C'est l'article 83.3(1)."

(The Chair: May I can just clarify this.)

(English suit)

(Following French -- Senator Fortin-Duplessis – article 83.3(1).)

The Chair: May I can just clarify this? My understanding under section 83.3 of the Criminal Code, there are requirement, for the minister, therefore the department, to be tabling a list in respect to what's taken place as far as that section is concerned. Our understanding is there's not been a report tabled since 2007. Is that correct? If it is so, is there an intention to comply with that particular section of the Criminal Code?

Mr. Davies: We'd have to get back to you on that. I believe this is the list of warrants or applications for warrants by the RCMP. I'm going off memory here, but this is not our group that's responsible for that, but we'll look into that and get back to you.

Mr. Robertson: I'm sorry that I didn't have a response for you.

(French follows -- La sénatrice Fortin-Duplessis : Vous pouvez nous)

(après anglais – Mr. Robertson – a response for you.)

La sénatrice Fortin-Duplessis : Vous pouvez nous envoyer par écrit?

Mr. Robertson : Oui, bien sûr.

[Sen. Beyak: Thank you, gentlemen. To turn my first question...]

[anglais suit]

[Following French -- Mr. Robertson ; Oui, bien sûr.]

Senator Beyak: Thank you, gentlemen. To further my first question, and Senator Lang's questions as well: There are countries where it isn't working. Have we looked at countries where it is? Australia seems to have a good policy. I'm hearing in your presentation the words "violent extremism," but I'm not hearing what's internationally known as violent Islamic jihadist extremism. If we can't acknowledge the problem, how can we find a solution? It's like there's an elephant in the room that nobody wants to talk about.

I believe the FBI in the United States have the tools to go into institutions that they believe are radical, that are teaching radical extremism from their podiums. If we don't have the tools to go into those institutions, what do we need to change? How can we give you the tools for Canadians who want solutions? We're all working hard, I acknowledge that, but we seemed to be talking a lot and not actually doing anything to solve this problem.

Mr. Robertson: The comment I would make is we certainly have seen the repercussions of a particular brand of extremism lately, and it has been severe and certainly noteworthy. It's not, as I believe my
colleague from the service would say, the only threat we face. We have other extremists and different ecological extremists. There are a wide variety of folks who pose challenges to our country.

I fully agree with you. We need to make sure we’re fully aware of where folks are being indoctrinated, if I can say it that way. But again, I think there are huge benefits to living in Canada. There’s a huge desire from many people internationally to find their home here, and it’s mostly because we’re fairly embracing of each other and respectful of each other’s views, to a point where it’s reasonable, up to the point it becomes extreme.

Again, our program we’ve been speaking about in terms of prevention is to basically do a better job both from the law enforcement side but also from community side, to clearly define where that is, apart from the Criminal Code, apart from the formality of it, and have an agreement that we shouldn’t move beyond that point. When we’re facing situations where we’re approaching them, that we want to intervene earlier. Hopefully, that’s at least a partial response to your question.

Ms. Gray-Henschel: Can I please answer as well? We are very fortunate to have close relationships with our Five Eyes and some of the countries that you’ve mentioned. We share a lot of information about this. One of the things that we learned about is that communities that take ownership of this problem and work together with law enforcement, with social services, with mental health professionals, like the Channel program in the U.K., you can develop a tailored program for that individual person’s factors, which might be different. They have been forthright in sharing that success, as well as some of the materials around the narratives. The United Kingdom and Australia again have shared that.

The opposite is that Canada has also shared what we have learned. One of our best practices is the Cross-Cultural Roundtable on Security and the partnership that we have and how they vouch for us within communities and build networks right down to the ground. We are sharing that and really trying to work in the space together — not an easy space, but we have a trusted relationship. Regardless of how the threat is evolving, we need to keep adding to the tools so communities can take what they need based on the gender and age of the person, who the credible voices are for that person. Is it a peer? Is it an older person? Is it a coach? Is it a teacher? Thank you very much for that question.

Senator Beyak: Do you need an additional tool to be able to go into mosques that you suspect have radical programs? We’ve heard about them in the press. I’m not telling any secrets here. Do we need one further tool to be able to go to where we may be harbouring radical teachers?

Ms. Gray-Henschel: Radicalization occurs in our neighbourhoods and on our streets, and is facilitated through social media. We need those conversations to take place in these safe spaces and to really rely on the leaders as to what they need and we need to provide them with those tools and that support for whatever they need but they need to adapt it to their own situation. That is where that dialogue is really productive.

I’m very excited about Canada’s approach in this. The RCMP has really built that foundation of trust so now we can have those difficult, emotionally charged discussions and ask what we can do. Here is what we expect. What do you expect? What do you know about this? Here is what we know about this. Here are some response actions. Who’s going to do what? And do it in a nice, coordinated way so that we have the best chance of redirecting that young person from that pathway to one where they’re a meaningful, productive Canadian citizen.

My parents came to Canada and as a young person I was taught that in Canada you can be whoever you want as long as you don’t hurt someone. That was really comforting to me and held me together with all of my friends. Those are the really productive discussions that we’re having with diverse communities right across the country, and those are where the most meaningful, preventive responses take place.

Senator Beyak: I’m just concerned that we’re not timing it fast enough with what’s going on.

Senator Day: I’m trying to get my arms around all the different programs that are out there from a preventive point of view and a sociological point of view, which I think is an important aspect that we’ve got to be looking at here.
I made a list of the various programs since the 2004 national security policy came into being. There's the Kanishka Project that's about to sunset unless something happens and has an interesting mandate to look into the psychology of just what is this radicalization is all about. We have to know a little bit more about the fundamentals before we can start talking about preventive measures. I think it's a good program from the point of view of understanding its fundamental approach.

There's the Canadian Safety and Security Program, which I'd like you to tell me a little bit about. We've talked about the Kanishka Project earlier. There's a National Security Community Outreach Initiative by the RCMP. You may say we should talk to them when they come before us, but I think Mr. Venner indicated participation in that outreach initiative. There's the round table, the Cross-Cultural Roundtable on Security, and you're going to get me the information on that. Then I found the Canadian Network for Research on Terrorism, Security and Society and there's CSIS. Mr. Venner indicated you're also fostering your own communications and collaborative activities with academics and the public, et cetera.

Have I named all of the programs and are these all of the initiatives going on? Are they all coming out of the 2004 security policy statement by the government? Are any of you working on something a little bit more up to date? That's 14 years ago now. Who would like to start?

Mr. Davies: For the most part no, it didn't come out of the 2004 national security paper.

A lot of the mechanisms you talked about came out of the government's Air India Action Plan, for example the Kanishka research funding of $10 million. We don't know of another example in another Western country doing this amount of research into the issue of violent extremism. Amongst our allies we are definitely looking to as a leader in pure research on violent extremism.

Senator Day: Did Kanishka flow from the recommendations in the Air India Inquiry?

Mr. Davies: Yes. Some of the other mechanisms are actually funded from Kanishka. You mentioned the TSA. I can't remember the acronym.

Senator Day: I tried to use the full name.

Mr. Davies: I believe it is a UBC-led project with nine universities across the country. Really the idea is to create a network of scholars on terrorism and violent extremism.

The CCRS, as Anna mentioned, a bit of the history of that predates the mid-2000s.

Senator Day: The cross-cultural round table.

Mr. Davies: The RCMP has probably been doing outreach since it was created. A lot of the public safety related engagement is entwined or certainly aware of the RCMP engagement. We will reinforce and complement each other. A lot of these initiatives are in the prevention, engagement space. There are mechanisms to make sure they're talking to each other and they don't overlap, but I think most of them are probably most recent than the 2004 national security policy.

Senator Day: Would anyone like to tackle the question of whether we are working on a new national security policy, white paper, green paper from the government? Are you participating in that?

Mr. Robertson: Not to my knowledge. We are certainly re-examining the various tools we have at our disposal right now and certainly there are a number of discussions under way, but no, we weren't contemplating a white paper.

Senator Day: I can't find it right now, but the Canadian Armed Forces research branch is also involved in developing security communications equipment. You have the Canadian Armed Forces hierarchy, you have CSIS and you have Public Safety Canada involved in the RCMP all in different programs you're funding partially or with others. I think part of the concern here is that when you try to develop a policy you would like it to be directed into bringing all of these pieces together.
Ms. Gray-Henschel: We have an interdepartmental countering violent extremism working group and that is where we share information about the different initiatives and priorities and work together as a whole-of-government approach. On some of this research we sit and evaluate and we’re asked to look at the Canadian security CSSP proposals. This is where we provide feedback and try to coordinate that research, but we also coordinate our activities through that committee. It meets every couple of weeks.

Senator Day: We’ve created a number of silos and periodically they get together to talk about what each silo is up to. That’s what it sounds like. If we want a whole-of-government approach, then why don’t we have one department or one agency looking after this in order to understand where we’re going? Did I misinterpret your comment?

Mr. Robertson: If I may, this subject is still early in its evolution. It’s not something where we fully understand all the characteristics, permutations and solutions in play, and thus can sort of run them out like a sausage maker.

Another area of similar concern is cyber, where you will have 20 different departments all involved from their own perspectives, where DND has a legitimate reason to be involved in cyber even though Public Safety Canada is seen to be the policy coordinator. In the CT space it’s helpful to a large number of folks involved in the issue. They all have their own legitimate mandate to be involved, and what is really important is they’re not doing it in isolation. So when we do examine and evaluate the programs that the various leads are pushing forward, as a community we can actually understand which ones are providing us with the best return, the best bang for our buck, the most impact in a positive way and then focus system-wide resources on those.

We’re still fairly early in this. The Kanishka initiative was only announced in 2011. As you said it is a sunsetting five-year program in the absence of a renewal, but four years for pure research is still pretty fresh. We’re still moving through to the point where we would have a much better understanding.

Mr. Verner: You had asked if you had sort of captured the main vehicles, and from the services perspective you did. CCRS, TSAS and Kanishka are the main ways in which we are participating.

I would also add that there was a reference earlier to the CTIO program, the Counter Terrorism Information Officer service, and we supported the development of that program. We also offer advice and guidance in the development of CVE programs to be implemented by others. Those are a couple of other ways in which we are contributing, in addition to the ones you mentioned.

Senator Day: I didn’t get that last acronym.

Mr. Verner: Counterterrorism programs.

Senator Day: To clarify the record, the other departments that I didn’t mention when I was naming all the departments, Foreign Affairs and Justice are also involved.

The Chair: And DND.

Senator Day: I mentioned DND.

The Chair: We wouldn’t want to forget any one of them.

Senator Day: No, I wouldn’t want to do that.

Ms. Gray-Henschel: May I add a clarification? I don’t want to leave the impression that these activities aren’t coordinated. This is a very busy space, and we leverage all those different departments. We are constantly on the phone and on emails because Foreign Affairs has a mandate, but they rely on us for advice and we’ll look to them for advice. It’s the same thing with the Department of Justice: national crime prevention programming, the RCMP’s mandate, the services mandate.

We are constantly sharing information, and people are conducting those activities according to their mandates. I see them as complementary, to be quite honest.
Senator Days: I guess the point I was trying to make is that 10 years is a long time in the space that's evolving so rapidly. Maybe this coordination, which is very important, would be a bit more precise and better if we had a new national security policy generated.

Senator White: I'm going to change track. I am going to ask a question of Public Safety, but anyone can jump in if they like, in relation specifically to the financing of terrorism and our success or lack thereof in prosecuting such cases. I could only find one, but I could be corrected.

I was trying to go back and see if the Tamil Tigers had any prosecution. I don't think they did either, even though they operated for a number of years.

Does the legislation need to be changed or are we lacking the tools — whether human resources or other resources — to prepare the cases for prosecution? Is the test too high when it comes to approving charges from Justice? I think I'm looking for a perspective more than anything.

Mr. Robertson: I think you've had appear before you, in the recent past, FINTRAC. They talked about their approach to identifying suspicious transactions.

I think probably what they would have told you is they flag a large number and they pass them on to law enforcement organizations and then they do a screening, vetting of them and pursue them.

In terms of the numbers, sometimes the numbers can mean something different than what you expect. Again, it can be helpful to have convictions in particular cases where there has been money laundering or use of funds for terrorist financing. In other cases it's a good sign.

In the not-so-distant past the Government of Canada listed an organization that was known or promoted to be a charitable organization. Again, one wouldn't expect to have a prosecution of someone affiliated with that organization because one would expect that all of the activities around that organization would stop the day it was listed.

It goes back into sort of the chicken and egg zone. If we're on top of the listings and identifying the organizations and individuals that are likely to commit these types of crimes, we may not end up having convictions because we've blocked them from doing something.

Senator White: So disrupting the practice is disrupting the organization because of listing.

Mr. Robertson: That's just one example. Another one in another domain would be Kanishka, which John talked about coming out of Air India. There are also some boarding issues with some individuals and a specified persons list where folks are flagged and they don't get on planes if they pose an imminent threat. There are a large number of preventive mechanisms in place.

Senator White: Would we have agreement from these investigative agencies that this disruption is happening and it's not a tool perspective when it comes to either preparing a case or the prosecution? Would you suggest the RCMP and every other police agency we'll hear from would say the same thing?

Mr. Robertson: I think what every organization would tell you is they can always do more if they have more, but there's never a never-ending flow of funds, as you would know.

It's about hitting the right balance point where you're getting a good return for the investment you've got. I won't propose to speak for the commissioner, or the director for that matter.

The Chair: I just want to follow up on that, if I could, with Mr. Robertson.

A number of weeks ago we were informed that there were charitable organizations registered to carry out humanitarian contributions. We were told on the record that there were some organizations raising money to aid and abet terrorism, and it was estimated to be in the range of six figures.
Are you saying that we haven't identified those organizations, so therefore they're doing it? I'm not quite clear on what you just told us. You said that as long as we identify them they won't continue what they're doing?

Mr. Robertson: I would say there is a process. One, you identify the potential that someone is doing something, and then there is a process we use in government to vet that allegation or suspicion. If it's found to be proven, yes, we would go forward and list the entity. At that point it would become a criminal act for the entity to continue operations or for anyone to support the activities of that organization. There could be entities that are currently being examined where the suspicion is that they're doing that.

As you know, charities, because of their nature, and not-for-profit organizations, are a favourite target for money launderers or terrorists financiers because they deal largely in cash and they often have global operations. There are a number of them that were set up for good reasons that can be misused.

The Chair: I'm not going to belabour that. I guess the question is why there haven't been any charges over the course of the last 10 years if these organizations have been operating directly or indirectly in Canada. Are we not investigating properly? How do we have to change it to prevent this money from being "laundered," as you used that word, in respect to terrorist activity? That is the question I have. That's the question a viewer would have. We have had no charges laid in 10 years.

Mr. Robertson: Again, all I can say is I understand that if we are aware of facts that show that someone has been doing those activities, charges would be laid, but I don't believe we've been able to demonstrate that fact. What I suspect is that some degree of that is related to preventative activities we've taken.

Would I suggest they have addressed all of them? No, but certainly there have been impacts to the programs in place.

The Chair: Colleagues, if you don't mind I would like to follow up. We're getting close to the end of our time. I would like to refer back to Mr. Venner on a number of issues.

There is a question of CSIS responsibility for the purposes of vetting individuals in respect to the appointment of individuals to various boards. For example, I want to refer back to the RCMP's decision to distance itself from the United Against Terrorism handbook that was made public a number of weeks ago. They were part of the publishing of that document, and at the last minute withdrew their support. It was found that, I believe, there were four co-conspirators identified from the United States as advisers in respect to putting that manual together.

Does CSIS take on the responsibility as advisers to ensure, when we're appointing individuals, that those individuals are who they say they are? I don't understand how the RCMP could be putting themselves in a position to have individuals of this background involved so closely with them, yet at the same time knowing that those individuals are who they and what they belong to.

Mr. Venner: I'm afraid I can't speak to the specifics of that case. I'm not aware of the service having been asked in any way in relation to that issue.

The Chair: I have a further question. I don't know if you can answer it, but I'd like you to get back to us if you can't.

When we're looking for appointments to various boards, to advisory committees in this very area that Ms. Gray mentioned, it's an area that we do need a public conversation on to ensure the individuals representing the various organizations are who they say they are, that they don't have another message that they're giving somewhere else.

Are we ensuring, through CSIS, that those individuals are coming with the full backing of the general public they are supposed to be representing?

Mr. Venner: Since I've been in this position, I'm not aware of the service having been asked to vet anybody in that regard.
The Chair: I guess you would do it if you were asked.

Mr. Verner: Well, the question I guess is if it's a request because is there something in information at their disposal that would lead us think that this is falling within our mandate? For example, is there some reasonable ground to suspect that there is some sort of threat-related activity going on here where the service should play a role in determining if there's an issue? And if there is, through section 19 of the act we have the ability to disclose information to that effect, but it would depend on the nature of the concern or the request that was made and the information they had that we were being asked to look at.

The Chair: The other area I'd just like to follow on if I could; you admitted a little bit earlier talking about the question of the investigation of what you referred to, I believe, as sensitive Institutions, where it was sensitive. I can to some degree agree that this is probably a very good description of what we're dealing with when we're dealing with institutions such as schools or perhaps religious organizations, that type of thing. At the same time, there's got to be a concern to all of us if certain things are being said behind closed doors and individuals are being indoctrinated. That is what has to be our concern from the Canadian public's point of view.

You said there was a policy in place, if requested, to look at that type of situation. Could you provide us with those guidelines?

Mr. Verner: Absolutely, yes.

The Chair: Thank you.

Senator Beyak: I have a question, and then I wanted a clarification. We identified glorification as a problem in the process toward radicalization, and I wonder if you have enough policies and laws in place to go to the Internet providers and have them shut down accounts that are glorifying radicalization — the tweets, the twitters — or if you need more tools in that capacity?

Mr. Robertson: I think what I would say is we've got a very good relationship with the telco providers in Canada, and many are willing to look at removing objectionable material when it's identified just based on good governance and good citizen engagement. What I would say, though, is unfortunately much of this material resides in servers that are outside of Canada, thus are outside of the jurisdiction. So that's, again, where our relationship with our international allies comes into play, because if we have a positive relationship, we have shared values, we can reach out and they can, in turn, have those discussions with their telcos. If, however, they're in jurisdictions where we don't have that positive relationship, it is likely that material will continue to reside on the servers.

Senator Beyak: Is there anything we could do as a committee to help, a new policy?

Mr. Robertson: I think we're looking at glorification as one of the issues. The challenge with it is how do you characterize it in a helpful way, because Canada, as many other progressive countries do, promotes the open Internet, promotes governance outside of government because it's such a helpful tool to promote democracy amongst other positive initiatives.

Every line we put in a restraint on it, it brings that kind of approach into question. So to the degree that it parallels things like hate crimes or hate speech, I think we can look at examining those. We don't want to go too far into the Internet governance domain beyond that.

The Chair: Perhaps you can maybe enlighten us in view of the fact that you are meeting with our allies. Are you having discussions about the question when it comes down to spreading of hate and those types of teachings? Perhaps you could tell us where you're at.

Mr. Robertson: Every jurisdiction is struggling with this, because it's quite clear what the source is. Different people have had different approaches. The U.K. has a particular approach, as you would be aware. The issue is none of them have come to ground and been proven to be quite effective in balance with all the other things. So, yes, we are looking at them, yes we're aware of what is in play right now, but we're back to Senator Day's response. We're still assessing what is the best approach that has the maximum impact.
The Chair: Colleagues, it's 25 past 2.00. I would like to take a very brief recess, thank our witnesses for coming before us. We appreciate what you do, and we're here to assist the government in any way we can in respect to dealing with the issue that's confronting Canadians.

Joining us this afternoon from the RCMP are Superintendent Shirley Cullierrier, Director General, Partnerships and External Relations; and Sergeant Renuka Dash, Acting Officer in Charge, Federal Policing, Public Engagement.

I understand Superintendent Cullierrier has an opening statement, so would you please proceed.

(French follows — Ms. Cullierrier: Monsieur le président, membres du comité, bonjour...)

Surintendante Shirley Cullierrier, directrice générale, Partenariats et relations externes, Gendarmerie royale du Canada: Monsieur le président, membres du comité, bonjour.

J'aimerais tout d'abord vous remercier de m'avoir invitée à vous parler aujourd'hui du travail de prévention que nous faisons à la GRC pour combattre le terrorisme.

La prévention constitue le premier volet de la Stratégie antiterroriste du Canada. Nous comprenons maintenant que notre meilleure arme pour atténuer la menace terroriste, au Canada et à l'étranger, est d'empêcher la radicalisation menant à la violence.

En résumé, nous ne pouvons pas compter uniquement sur nos activités de détection et de perturbation pour lutter efficacement contre la menace, il faut miser davantage sur la prévention. C'est dans cette optique que la GRC concentre ses efforts de prévention sur le programme de lutte contre l'extrémisme violent, ou LEV.

(Ms. Cullierrier: It must be stated clearly that the process...)

(английский сург — англійська версія)

(Québec — LEV)

It must be stated clearly that the process of radicalization to violence is an incredibly complex issue and one that is constantly evolving. It is also an issue that law enforcement and our partners in the security and intelligence community cannot address alone. A whole-of-society approach is required. As such, the RCMP is currently focusing on collaborative efforts with the community and developing new and innovative programming.

With me today is Sergeant Renuka Dash, Acting Director of the Public Engagement Team and one of the officers leading the design and the roll-out of the RCMP's Countering Violent Extremism, or CVE, program. We are both happy to respond to any of your questions at the conclusion of my comments.

The issue of terrorism and radicalization to violence has been at the forefront of public consciousness since the devastating attacks in late October in both Quebec and Ontario. Earlier this year, a different violent ideology led to the targeting and murder of three RCMP officers and another attack in New Brunswick. In all of these attacks, it was Canadians committing acts of violence against fellow Canadians.

We are also experiencing the phenomenon of individuals either travelling or seeking to travel abroad to engage in terrorist activities in several countries around the world. These are examples of the range of results of radicalization to violence.

When I reference radicalization to violence, I am not speaking of individuals who have radical beliefs or who have passionate views. Every citizen has the right of their own beliefs. What I am specifically referring to is the process by which individuals come to believe that inflicting violence upon others will advance their cause. It is when it is heading towards, or when it reaches this point, that it becomes of particular concern for law enforcement and society at large.
While the decision to engage in violent acts is often sudden and unpredictable, there are often indicators that a change in belief is under way. Often, these behavioural changes are the first indications that radicalization and, more importantly, radicalization to violence, is taking hold.

Indicators vary, from withdrawal from positive social interactions and activities to isolation and segregation. They could manifest as expressing increased hatred or espousing the virtues of violence and expressing an "us versus them" mentality.

Of course, none of these are criminal or should necessarily be of concern in and of themselves, but they could be signs of change to those closest to an individual. That is why we stress the importance of the community, family and friends to identify their concerns to us at the earliest opportunity.

(French follows — Ms. Cullierrier — Comme le commissaire l'a mentionné lors de...)

(après anglais)(Mme Cullierrier)

Comme le commissaire l'a mentionné lors de sa comparution, il est loin d'être facile de dépister ce type de changements chez une personne, même pour ses proches, et encore moins pour les responsables de l'application de la loi. Il n'existe pas de modèle ou de parcours unique. Certaines personnes montrent peu de signes extérieurs très manifestes. De plus, ces personnes ont peu de traits en commun, si ce n'est qu'elles pourraient en venir à se livrer à des actes violents.

Le dépistage pose un défi, mais il est tout aussi difficile de trouver la meilleure façon d'aborder ces personnes.

Les responsables de l'application de la loi disposent d'outils pour expliquer le comportement d'une personne en fonction du contexte, mais les adeptes de la violence font rarement confiance à l'État.

Cette réalité restreint notre capacité collective à obtenir la coopération de ces individus et à les orienter vers une voie plus positive.

(Ms. Cullierrier: Community members, family and friends,...)

(anglais suit)

(Following French in 1430 — Ms. Cullierrier continuing — voie plus positive)

Community members, family and friends are often in a much better position to identify and engage with individuals at risk, but often lack the information, the knowledge of indicators and the resources necessary to intervene.

The RCMP is seeking to address these challenges through its new CVE program. The program builds on the RCMP's vast experience in engaging with communities through our decades-long approach to community policing. The RCMP is seeking to build capacity and opportunities in two ways: by providing education and awareness, and by establishing methods for collaborative engagement at the community level.

Fundamentally, the RCMP's objective is to provide community and law enforcement with the tools they need to identify and engage with individuals at risk. It is also to create avenues of support, which are needed to help steer individuals away from a path of violence.

The program's new training regimen is being developed to ensure that police officers and community stakeholders have the means to understand the issue of radicalization to violence and empower them with effective tools.

The training includes context on the wider threat environment and clear indication of early behavioural indicators and vulnerabilities. It also provides information on existing and evolving methods of radicalization to violence, such as the widespread use of social media and other areas of the Internet.
The second component consists of enabling avenues of support, through collaboration between communities and law enforcement that we refer to as "community hubs."

Community hubs are multi-agency networks of law enforcement, community organizations and human service professionals. They consist of representatives at the municipal and provincial levels designed to ensure that a collaborative approach is used to engage with individuals at risk. A multi-agency approach helps to ensure that the right people or groups, with the greatest chance for success, are empowered to act.

It is important to note that the focus of the RCMP CVE program is limited to those individuals who have not yet committed violent action.

As I said earlier, our goal is to prevent radicalization to violence before it occurs, in what we refer to as "pre-criminal" space. Once it becomes clear that an individual is becoming fully committed to pursuing violence, our national security investigators begin a criminal investigation. In this way, we ensure that all of the tools at the RCMP's disposal are being used to address the threat.

While I am confident that our program will have a positive impact in addressing the threats, our efforts will not be enough on their own. It is important that we continue to educate Canadians to understand the critical role that they play in contributing to our collective security.

To be successful, all of society must be engaged and informed for our collective efforts to work. As I have mentioned, family members, friends and the community are best placed to know when something isn't "right," when someone close to them has changed.

In conclusion, let me reiterate that the RCMP is taking active prevention measures. We want to assure the public that they should feel comfortable in reporting their concerns to the RCMP or their police service of jurisdiction.

We will continue our efforts to build mutual trust and understanding between the RCMP and other law enforcement agencies in Canada and communities affected by criminal activity.

Our goal is a collaborative approach, with law enforcement and communities working together to better protect all Canadians.

(Revenue follows - Ms. Cuillierrier continuing - Je tiens à vous remercier...)

(French follows - Ms. Cuillierrier - working better to protect all Canadians.)

Je tiens à vous remercier de m'avoir offert l'occasion de vous parler du travail de prévention de la GRC. Le sergent Dash et moi-même serons heureux de répondre à vos questions.

(The Chair: Thank you very much, superintendent...)}

[English follows]

(Following French - Ms. Cuillierrier - répondre à vos questions.)

The Chair: Thank you very much, superintendent. I just want to reinforce the responsibilities that you have in relation to informing the public of your responsibilities and how the individual Canadian has responsibilities. One of the reasons we're having these hearings is to have this public conversation so that more and more Canadians become aware of the threats but also how we can prevent them.

Senator White: Thank you very much, superintendent and sergeant. Thanks for being here today.

I appreciate your walking us through the program you have. Without naming names, can you give us an example of how this has worked in one location and we've actually been able to pre-empt, as you call it, at the pre-criminal stage or pre-crime stage? Can you give us one example of how it has worked, possibly with another agency in particular?

Ms. Cuillierrier: Thank you for the question.
We're in the process of rolling out components of our program, and we've started with training. It's still too soon to be able to speak about individual interventions or success. We have a performance measurement framework because we recognize that it will be important to be able to track our progress in terms of doing these interventions. We started with components of rolling out training, where we have approximately 30 qualified trainers across the country now.

Sergeant Renuka Dash, Acting Officer in Charge, Federal Policing, Public Engagement, Royal Canadian Mounted Police: One thing I would add is that when we were looking at researching the different types of diversion programs, we did find there has been a lot of success within Canada. Whether they are programs about drug awareness, organized crime or mentoring children at different stages, those diversion programs have been very successful. Our program is layering a national security component to those. We have every confidence that we're going to actually be successful with this program, because it's early on for vulnerable individuals at risk that we are going to be providing support to.

Senator White: I'm glad to hear that you're engaged with other agencies as well. The RCMP are not the largest police service in the two largest provinces or any of the major cities in the top 10 cities in the country. How has the engagement been going with those police agencies to ensure they are training their staff at the same time?

Ms. Cuiillierrier: In September of this year, we had a police officer from the U.K. Prevent program, who came here, and, along with Sergeant Dash, we offered training to nine police agencies, inclusive of the RCMP, where we trained a portion of the 30 that I had initially mentioned.

We recognize that there is an absolute need in the country, and we are trying to manage the requests that are coming in right now, but we've been involved in speaking with Toronto police, Calgary police, Montreal police, Peel and Vancouver, and there's no shortage of requests. It's just a question now of being able to manage expectations with the resources that we have.

Senator White: Do the resources you have meet the needs and demands? Obviously, they don't. You just told me that. What would the need or demand look like, if we tried to meet it?

Ms. Cuiillierrier: One of the positive aspects of our CVE program is we want to recognize that there's a lot of competent Canadian police officers in the country that we could do a train-the-trainer with. Our CVE program is essentially built on that model, train-the-trainer. Part of those 30 folks are from different police agencies across the country, and the idea is that they will, in turn, work with their colleagues in their respective police agency, as well as work with community members to talk about radicalization and to recognize the indicators and the vulnerabilities of individuals who are at risk.

Senator White: So you don't have any idea how many resources you need to meet the needs?

Ms. Cuiillierrier: We have a small team in headquarters, in Ottawa, and essentially we're trying to do the very best we can and leverage as much as we can through the bigger police services in the country. We're also working with the Canadian Association of Chiefs of Police, so we're trying to operate on a force multiplier in terms of trying to deliver this training as quickly as we can in a professional manner.

Senator White: I appreciate that. Thank you for your response.

[French follows — Senator Fortin-Duplessis: Madame la surintendante, madame la Sergent...]

(sparse anglais)

La sénatrice Fortin-Duplessis : Madame la surintendante, madame la Sergent, soyez les bienvenues. Je vous remercie pour votre mémoire.

Vous savez, c'est rassurant, dans le mémoire que vous nous avez présenté, de voir que vous avez des outils pour lutter contre le terrorisme. Un ancien professeur d'études religieuses de l'Université de Calgary, M. Aaron Hughes, a déclaré à la presse que les dirigeants de l'université n'avaient tenu aucun compte de ses mises en garde au sujet de la radicalisation apparente de certains étudiants.
Pouvez-vous nous parler un peu de la manière dont la GRC et les services de police locaux encouragent les établissements d'enseignement à coopérer avec eux pour sensibiliser la société à la radicalisation sur les campus et dans les collèges?

**Mme Cuillierrier :** Notre approche consiste à travailler avec les corps policiers locaux dans la perspective qu'à leur tour ils travailleront avec les communautés pour partager l'information. Cela peut aussi être avec des CEGEPs ou des universités. Concernant l'université que vous avez mentionnée, en même temps que ce professeur faisait des remarques aux journalistes, il y avait une grosse conférence à Calgary regroupant le corps policier municipal, la GRC, des membres de la communauté, ainsi que, je crois, des membres des institutions académiques. Tous ces gens sont venus pour discuter de ce point, à savoir comment identifier des indicateurs ou le comportement de gens qui se trouvent dans la période avant de faire l'objet d'une enquête pour des raisons criminelles. Notre programme vise donc à livrer le message et procurer des outils tant aux communautés qu'aux policiers.

**La sénatice Fortin-Duplessis :** Merci beaucoup.

**Le sénateur Dagenais :** Mesdames, merci. En référence à votre mémoire de présentation, vous dites à la dernière page, vouloir instaurer un climat de coopération afin que les organismes d'application de la loi et les communautés travaillent ensemble pour améliorer la protection des Canadiens.

Vous me corrigeriez si je me trompe ; je vous réfère à une publication intitulée *Unis contre le terrorisme*, qui était le fruit d'un effort d'action communautaire avec la GRC. Je pense que vous vous êtes retiré ou désolidarisé de cette publication ; si oui, j'aimerais savoir quelle expérience vous en avez tirée.

**Mme Cuillierrier :** Je crois que mon comissaire, lorsqu'il a témoigné devant le comité, en a parlé un peu. Pour le partie numéro 3 de ce livret, nous avons participé et nous y tenons. C'est une section dans laquelle nous avons contribué à tout ce qui y est écrit, mais nous n'avons pas contribué au reste du livret. La GRC, qui déploie beaucoup d'efforts pour constamment travailler avec les communautés, valorise le fait que des communautés se réunissent pour livrer un message et redonner à la jeunesse de leurs communautés. Il est important d'établir ce niveau de confiance avec les communautés. Cela prend du travail et cela ne se fait pas du jour au lendemain ; cela prend parfois des mois et des années. À la GRC, d'un bout à l'autre du Canada, nous sommes très fiers de nos efforts et de notre approche envers la police communautaire.

**Le sénateur Dagenais :** Dans un autre ordre d'idée, des gens veulent entrer au pays ou y sont entrés et ont des doctrines religieuses différentes et ils ont des fois participé à des activités terroristes. Pourriez-vous me dire dans quelle mesure le Canada a examiné les motivations de ces gens qui entrent ou veulent entrer au pays avec leur doctrine religieuse?

**Mme Cuillierrier :** Notre programme parle plus de la période avant que nous ne commençons une enquête criminelle. Nos collègues qui procèdent aux enquêtes seraient, je crois, plus en mesure de répondre à cette question ; la sergente Dash voudrait peut-être ajouter quelque chose?

**Sgt. Dash :** That's correct. Our program is really about the pre-criminal space....

(anglais suit)

(Following French---Ms. Cuillierrier --- l'ajouter a quoi?)

Sgt. Dash: That's correct. Our program is really about the pre-criminal space. If you look at law enforcement in general, we've got criminal space and pre-criminal space. Our whole program is to identify individuals at the very earliest stages, before they mobilize to commit any type of violence. So anybody returning or has already been assessed to be a threat to Canada's national security will go directly into the criminal operations side.

**Senator Day :** Thank you, each of you, for being here. My question is, in part, Senator Dagenais' question and a follow-up to it.
I'm concerned that an awful lot of the violent extremism that we read and hear about seems to be tied into some religious ideology, and that's not necessarily the case. In many cases, you will see extremism being developed in a community, and they don't have any church affiliation. They might dislike people in uniform; they might have a violent tendency against political figures.

That's pre-criminal. They haven't done anything criminal yet, but they're developing a radicalization that isn't tied into an ideology. Have we skipped that one? Are we just relying on the ideological approach at this stage?

**Ms. Cutillierrier:** Our CVE program is very broad, and we're not going to focus on religious or political ideology. We're going to look at vulnerability, risk and behaviour. As Sergeant Dash mentioned, because we're working in the pre-criminal space, in policing, it would not be unusual to look at somebody who is vulnerable or exhibiting behaviour where they potentially may be recruited into organized crime purposes or a young lady being recruited online for sex trafficking or a young man who is being radicalized to violence within a national security threat.

Our program is essentially based on looking at behaviour, the indicators, and in a pre-criminal space around all criminality.

**Senator Day:** I'm thinking of an individual who grew up in a small community, like Senator Beyak and me, or maybe she grew up somewhere else but has moved into a large community. First is the identification and then trying to do something about it, not letting that person progress to the radical stage.

There was a recent case here in Ottawa, and that individual had lived in a lot of different places. The community wouldn't know that person well enough to be able to detect behavioural changes. Your program is not designed towards that, because you talk about using the community as the main focus for your program to try to prevent this.

The community members may not be able to help because you haven't identified the individual, first of all, or they wouldn't be able to help identify the individual because they haven't known this person that long, and then suddenly he has radicalized himself. He might, at the last moment, look for some religious affiliation to psychologically justify his activity, but he wasn't radicalized as a result of that religious ideology. That was just a handy tool along the way.

Can you fit that kind of situation into your program or is your program more streamlined than that?

**Ms. Dash:** Radicalization can occur in many circumstances. What is different is that the pathways are different for every individual, and as law enforcement we recognize that. That's why we recognize first responders as law enforcement police officers. We receive the information on behavioural changes, and that's what the program is going to be focused on. The consistency is behavioural changes and the best people to recognize those are family, peers, teachers; it's beyond just community.

What our program is going to do is the force multipliers, front-line police officers have that dialogue and that casual discussion with wherever calls of service that they go to. If it's a school liaison officer, they will be able to have that dialogue with teachers who may be able to see some behavioural changes and there's a concern.

Our program is to educate the front line so they can have that dialogue just like they have a dialogue about drugs, about organized crime, about truancy. So that's really the program. The heart of the program is aimed at front-line policing and the individuals that are going to recognize the inconsistent behavioural changes.

**Senator Day:** Just as a follow-up, I think the critical point is that the person has to be in a community and thereafter be identified by community leaders. If you don't have that, then your program is not going to work at all. You can't go any further. You don't know who it is.

**Ms. Dash:** Actually, the communities could be family, friends, teachers. It could be anybody. We're not really focusing our efforts on community leaders. The community can be anybody, anybody that this
individual is associated with. The program will work, and as long as we’re provided that information, we’re going to provide the appropriate service and support.

Senator Beysaik: At the risk of repeating myself, I asked of the previous presenters, I believe we have an elephant in the room that everyone is afraid to acknowledge. We are talking about extreme violence here in Canada, but the world is referring to it as extreme jihadist Islamic terrorism. Are we addressing it adequately? Is there perhaps an anonymous tip line that parents can call if they hear something in an institution, whether it’s a school or a mosque, if they hear something from their kids or their friends? Is there an anonymous place where people can phone and report and have it investigated, or are we just talking in the communities? The problem is severe, and Canadians are concerned. I feel as though we’re moving very slowly.

Ms. Cullisierrier: Senator, as I mentioned before, we’re not going to focus on religion and we’re not going to focus on a type of ideology. I think that’s a really important piece to communicate to communities. We will not focus on ethnicity, particular communities, but we do build relationships with all communities in the RCMP across Canada, as do our policing partners.

Working with young people in school is really important, to be able to message early. I believe that our program will work as long as we lay the fertile environment, fertile grounds for having parents, teachers, coaches, taxi drivers to be able to call the police service of jurisdiction and know that perhaps there is a different tool that the police will utilize as opposed to perhaps strictly going to a criminal investigation.

People need to know that there are different options available to them, particularly parents, and that those options could be exercised at a community level with human service professionals. It might be Social Services; it might be health; it might be the police, but to have that conversation in all of the communities in the country.

I’ve been around long enough to know that when community people decide to tackle something, even if it’s in a criminal space, because it is a threat to them and they’re afraid, they come together and they move forward.

We have used MADD often when we speak to police officers in Canada. We have our naysayers even within policing that say this is going to be a very difficult job but if you’ve worked in the community long enough, you recognize that when people are determined to make change, they will come together. We’re just providing that fertile environment for them to come together and have the discussions.

The Chair: Earlier, Senator Dagenais referred to the handbook United Against Terrorism. You had indicated, superintendent, and the commissioner of the RCMP also indicated, that you were quite pleased with what you had provided as part of that handbook, yet you withdrew from the handbook. Can you tell us why you withdrew from the handbook if you were pleased with what you presented?

Ms. Cullisierrier: The position of the RCMP on the United Against Terrorism handbook is that the tone of the book was a little off, and that was a decision of the commissioner. As he indicated, we stand behind section 3 that we contributed to.

The Chair: I have a general question but it’s specifically in respect to the individuals that were involved and being promoted in that particular publication.

There were four individuals that had been identified in the United States as co-conspirators in respect to the US Justice Department. That is my understanding. What I don’t understand is, how would a government publication get to that point, utilizing individuals who obviously are very questionable in respect to what you would want them to be promoting? I asked this of the representative from CSIS today, why aren’t the individuals that we’re calling upon to represent the community that is at risk, no matter whether it be the Islamic community or any other community, ensuring that those spokespeople are who they say they are and they’re not necessarily bringing forward a membership in some other organization, either indirectly or directly, like the Muslim Brotherhood or otherwise?
Do you think it would be a good idea to put a policy in place to ensure that individuals are scrutinized to ensure that they are going to meet the test of time in respect to what you’re expecting to do?

Ms. Cuillierrier: In terms of your first question, senator, I’m not aware of these four co-conspirators. I had no knowledge of them.

In terms of our due diligence when the RCMP does partner with folks on a publication or a partnering, I trust that due diligence is given in terms of who we partner with.

As I indicated perhaps earlier with Senator Dagenais, I think when communities come together to support countering violent extremism, it takes a bit of courage to get to that. My understanding in the case where this occurred in Manitoba, there was an event that took place a year ago with the community that was actually quite extensive and we had a lot of police partners. I’ll let Sgt. Dash speak to that.

Ms. Dash: The event was really bringing together community members, and they were quite concerned about, not just extremism, but about drugs, about their children and what they are involved in, material online.

Speaking to our program, this is what we want communities to come together to do, to share and have the dialogue and have this discussion about the critical concerns that they have.

That was a really fruitful discussion, and that’s where we want communities to get to, to have the open, honest discussion with all of the partners there. That happened about a year ago and we’re very proud that we actually have communities asking us to be part of their discussion. It’s been a very difficult road in some communities. We’ve had to rebuild relationships and re-engage, but for communities to have this difficult discussion with parents I think it was a success.

The Chair: Sergeant, no one is arguing that, and I assume everyone around this table would support that, but the question is whether due diligence is being taken with respect to background checks to ensure these people who are representing the community are who they say they are. Do you have a policy in place that do that due diligence so we don’t get into a situation like we did with this particular handbook that we referred to earlier?

Ms. Cuillierrier: I’m not aware of a policy, although there could be one. I have been in the organization long enough that I do know that we do bring due diligence in terms of who we partner with and what we support. I think that’s a critical piece because we want the confidence of communities and we want the confidence of Canadians. That is extremely important to us.

The Chair: I look forward to seeing if you do have a policy in place, if you could report back.

Ms. Cuillierrier: Okay.

The Chair: You refer to pre-criminal space. I have a question and I’m going to voice a concern here. It’s a very fine line you walk. I would say, in respect to your job as an enforcement agency versus trying to reach out in the community and trying to prevent getting into that situation where there’s criminality.

What concerns me is that there seems to be a number of offences or appearances of offences having been committed in the area of terrorism. We have Canadians with dual nationality coming back from being involved in terrorist activities, being overseas and actually contributing and fighting with ISIS. There seems to be an attitude by some that because they’re not necessarily fighting but just involved on the Internet that’s a lesser offence, yet we come back here and we have these hearings and very few, if any, court proceedings are going forward at all. I think Canadians are asking themselves exactly what is taking place if these people are that high risk.

That’s the question that has to be asked. The question I have is this: Where is that line between pre-criminality versus criminality as you reach out in the community and you know that some individual has already been involved in some terrorist attack that is against the Criminal Code — at least the way I read it -- and we’re not proceeding?
Ms. Cullierrief: In terms of returnees, our countering extreme violence program is focused on the pre-criminal space. When an individual does return from perhaps allegedly fighting or involved in terrorist activities, we leave it to our national security investigators to do whatever they need to do upon the individual returning to Canada. Again, our program will focus on the front end.

Ms. Oshin: I think what maybe needs to be emphasized is that the pre-criminal space is early on indicators and that's where our program is focusing. If at any point in that time you want to look at as a continuum that the individual who is at risk is displaying signs of behaviour that they're going towards the criminal space, that information will be shared just like any calls to service and we will get our operations involved. We would not put any operations at risk and our line is very clear. We are helping individuals at risk at the very early stages.

Senator White: I congratulate you on the restorative method you're using in particular with young people and trying to engage them before they become involved in the criminal activity that we're talking about for the most part here.

I appreciate the fact that your focus is on the communities and the people in those communities. In fact, we've seen similar success in Canada when it comes to gang outreach in Calgary and, to be fair, here in Ottawa and Toronto as well. I think that is the answer down the road. The challenge we're having is that we've faced a couple of incidents over the past few weeks that tell us we've missed a few pieces somewhere along the line, and whether or not we're doing enough to engage the people who are going to be violent or are travelling overseas and getting training or are going overseas and helping to fund extremism and terrorist acts. If I may, that's one of the disconnects as a precursor to my question.

So you understand, this isn't about whether what you're doing is working, I think it is and I think it will, but there is a second piece that we're stuck with and that is what isn't working and whether or not we're engaging the people coming back.

My question now is whether we're seeing enough involvement from the community's leadership when it comes to engaging those communities. Are we actually hearing community leaders saying they are as concerned? You've given them a safe environment. You're telling them you're not looking to arrest their children. From what you may tell us, we're saying we need to engage them at some point in time to find a solution.

Are you seeing leaders believe that now and come forward and saying we want you to be a part of our community and speaking at some of the events we have and engaging at a higher level so that you're hitting more, or are you still doing it one by one by one?

Ms. Cullierrief: I think the tides are shifting in terms of community engagement and community leaders coming forward. I recognized certainly in the last year any time that the RCMP has made arrests around a terrorism charge community leaders have come forth to the media. They have talked about how they've worked with the police of jurisdiction or with the RCMP.

In speaking with other Canadian police officers who were here in September in Ottawa for our train the trainer workshop, they are noticing a change at the community level with community leaders and religious leaders. I do think the tides are changing and communities recognize and need to get involved sooner than later, as opposed to waiting for arrests to happen or for tragedies to come forward.

I sense that as we move forward and we do have a force multiplier with other police agencies across Canada and that interaction and that deliberation, whether it happens in a university setting or at a town hall, I do believe people will come forward. We've had mothers come forward and say, "I didn't know what was going on and now that I recognize what I should have seen perhaps I would have acted differently." That's a switch in thinking.

Again, I think and I know that by engaging more people in this conversation we'll have that effect of people coming forward to police or community human service professionals.
Senator Day: The program that we’ve been discussing here today on counter violence, it flowed out of Canada’s counterterrorism strategy that was issued by Public Safety Canada in 2012: is that correct?

Ms. Cullierrier: Yes. We’re working on under the “prevent” pillar, yes.

Senator Day: Was there new funding that came out as a result of that policy announcement?

Ms. Cullierrier: That predates my time in this position. If I’m really not aware if there was funding in 2012.

Senator Day: If you’re able to determine that for us, it would be helpful. What I’m interested in knowing is the total amount that is dedicated to your particular CVE, counteracting violent extremism program, and you indicated you had 30 trainees across Canada now. Are they being paid specifically to do this job or are they in uniform and doing that as part of their normal RCMP attachment?

Ms. Cullierrier: Of the 30 qualified trainers that we have across the country at this point in time, for some of them it is their full-time job. Some of them may be school liaison officers. Some of them may work in different areas but have an interest in working at communities and/or are very good facilitators and able to train other police officers. That is the reason they would have been selected to come on the training.

Senator Day: Are they paid in addition to their normal salary for this particular training job that they’re doing?

Ms. Cullierrier: No. This would be part of their core function in terms of their--

Senator Day: Okay. So back to your secretariat here in Ottawa, that’s the only place where you have people who are working on this particular initiative. Can you tell me how much money is being dedicated? Is it coming only out of operations, or do you have a separate line item of expenses that we could go to?

Ms. Cullierrier: I would suggest that in terms of questions about budgets, perhaps the chief financial officer of the RCMP would be in a better position to respond to those questions around funding and budgets. I essentially work with the people I have and recognize that I can work with the INSET teams that are located across Canada, as well as the different municipal police services that are expressing an interest in working with us around CVE.

Senator Day: If you needed more funding, superintendent, would you go on the line of command and say, “I need more bodies,” or would you be told to put that in your budget for the next year? Do you work out a budget for your operation?

Ms. Cullierrier: I do, and my answer would be I do both. I put forward a projected budget, and I also look at speaking to my command around some of the pressures or requests that are coming in on our new program.

Senator Day: I think the sergeant had an answer that she was going to give here as well.

Ms. Dash: I was going to add to the superintendent’s comments in regard to Public Safety Canada. We have been working collaboratively under the Kanishka funding, so we have received benefits from some of the research and tools that they have been able to provide to front-line officers, so we have been using Public Safety Canada in that sense.

Senator Day: I’m glad to hear that. We learned that that is funding that will expire next year, 2015.

Senator Beyak: Thank you for your presentation. I’m still afraid that we’re not addressing the big issue hard enough, but I’m very appreciative of your work at the community level.

In March of 2011, the Senate did a report where we identified the four steps to jihad. I will have to read it, because it was quite long. Stage one, the state of how you were. Stage two, self-identification. Stage three, indoctrination. Stage four, jihadiization, when one decides to actually act. Now, it seems we can only influence the radical Islamist during stage 2, self-identification, and stage 3, indoctrination. What
specifically are you doing to counter indoctrination, and when do you refer it to the national security investigators that you talked to? You talked in your presentation about the community hubs, but I still don’t see how they’re going to actually deal with someone who is on the verge of doing what happened in Ottawa.

Ms. Dash: Our program is addressing the early indicators of an individual that is going down the path of criminality and potentially there may be a nexus to national security. I know I’ve made comments before that early indicators and behavioural changes are best really seen by family, friends and teachers. Early on, the signs could be that there is a language that changes, us versus them mentality. There is also language in regard to maybe political ideology or religious ideology. When that type of information is brought to the attention of law enforcement or a community leader or a trusted individual, that is when we could potentially get involved. We would then look at and assess the situation and provide the appropriate resource. It could be a mentor, someone who would come in and maybe have a discussion with the individual to say, “This is the interpretation of the ideology, and it’s not what you’re thinking.” It depends. It’s a case-by-case basis, and we would look at that. That’s how we would get involved early on.

The four stages that you’ve described are pretty much when the individual has radicalized. That could happen over two months or three months, or it can take years, and that is all in the criminal space.

Senator Beyak: When do they call in the national security investigators? At what point in the community hub would someone identify that there is a problem?

Ms. Dash: It would depend on the assessment. If there is an intervention that’s taking place and the individual is really not responding to the support, an assessment is done, and that’s when there’s going to be a decision made as to what the next steps will be.

The Chair: Colleagues, I’d like to go back in respect to the individuals that have been involved in some terrorism activity outside the country and have come back and have been identified.

Superintendent, you identified that there were some who had come back quite disillusioned. It wasn’t what they thought it was going to be. They are back in the country because they didn’t want to stay where they were and continue doing what perhaps they were doing. In respect to your program and these individuals that have come back, how many have you identified, in rough numbers, that have come back because they’re disillusioned? Are you utilizing these individuals, for example, in your program to go to these particular communities to tell these young people just what the real world really is? Do you do that? If you don’t, why not?

Ms. Cullierier: Senator, as I mentioned earlier, when individuals return, they are handled and managed through our criminal investigations and our national security criminal investigations, so they do the follow-up. They do the interviewing or surveillance or whatever police technique is required based on the information in the criminal file or the investigation.

In terms of our program in the pre-criminal space, in terms of utilizing returnees or people who have had experience, that is something we’ve looked at. Our international partners have in some cases done that, and it certainly is effective. In fact, there is one tool that we will be using in one of our training sessions that actually speaks to one of those examples where a young person has been incarcerated in the United Kingdom and had agreed to actually do a video and walk people through his journey. Then it becomes very evident where community and human service professionals can actually intervene had they been aware or had a little bit of awareness in terms of what radicalization to violence looks like and what the indicators are.

Your idea is a good one. We have thought about it. We are not quite in a position in this country to have that kind of tool available to us, but we have been working with Public Safety Canada on an initiative with the consultant to develop Canadian tools that would actually tell the story as you’re suggesting.

The Chair: As I said earlier, the purpose of these hearings is to have a public conversation to let Canadians know exactly what we face or what we don’t face. Of the 80 that have come back, how many have come back disillusioned and have come back just because it didn’t work out the way they wanted it to work out? Could you maybe go back and find out the numbers we’re talking about here?
Ms. Cuillierier: If I could make a suggestion, that’s a question better posed of our folks who work in criminal operations around the returnees to be able to give you a sense of what that looks like. I’m sure they would be happy to give you a broad idea of what takes place when these individuals return to Canada.

The Chair: Colleagues, we’ll wait and see if we can get some information on that.

I’d just like to turn to one other area, if I could, before we come to a conclusion. One program that’s been referred to is called countering violent extremism training, as part of some of the programs that are available. You’re familiar with that? One of the programs you’re working on is counter violent extremism?

Ms. Cuillierier: Yes.

The Chair: I’d like you to provide us the list, if you could, of the individuals involved in that program, training in the program, and those who are outside the government sphere who are being used as advisers in respect to that, if you could do that for us.

Ms. Cuillierier: In terms of the police trainers, that would be easy to do. In terms of our community resources, that is certainly not a comprehensive list at this point in time. That’s something that literally on a daily basis we’re working on.

The Chair: Whatever list you have.

Ms. Cuillierier: Okay, we’re connecting.

The Chair: We know it’s a moving list. That’s fine.

Ms. Cuillierier: Fair enough.

The Chair: Thank you, superintendent.

Senator Day: A brief question to gain a better understanding of your community outreach. In 2004, the Cross-Cultural Roundtable on Security was created for the specific purpose of helping to develop trust and understanding in the various ethnic communities, and obviously the RCMP and CSIS have been involved in community outreach for a long while, and that’s how they recruit informants to gather information. What is it about your community outreach in this particular initiative that’s different from the community outreach that you’ve already been involved with?

Ms. Cuillierier: In the case of countering violent extremism, as you indicated, senator, we have certainly a long history of doing community work. Community policing is certainly at the core of how we do policing in Canada, and that’s writ large across the country.

In terms of what’s different, I’d like to say that it’s very much about leveraging what we already do very well, and that’s essentially building the trust with the communities. I think training police officers, imparting the information, awareness and education is something we do on an ongoing basis. This is a new phenomenon. Police officers in Canada want this kind of information and education, but what police officers also want is: Okay, so I have this knowledge. I recognize or I get a phone call from a family member. What do I do with it? Where do I go and what do I do to triage or help this individual or this family? That’s what’s different about this program. It’s a combination of the training, awareness and education, and then it’s leveraging those human service professionals at a community level, whether we’re dealing in the past perhaps with sexual assault, gang violence, truancy, this time it’s going to be about layering countering violent extremism and getting people in the community, those professionals, understanding what radicalization to violence is.

We have health professionals out there who are very much in position to be able to help and provide information. We have teachers out there who are very much in position to recognize when a young person’s behaviour or language or perhaps now they dress is changing. It’s capitalizing on everything that we have been doing but bringing it in together to look at countering violent extremism, radicalization to violence.
Senator Day: Thank you. That was helpful. The CVE, countering violent extremism program, is that within the RCMP part of the Canadian Safety and Security Program? Do you know that term? We heard about that in the last session.

Ms. Cuillierrier: I don't.

Senator Day: Are you part of that? The Canadian Safety and Security Program works under a different funding mechanism. We learned about it at the same time as the Kanishka Project, which you indicated you do get some funding indirectly for or from.

If you don't know about it, then you're obviously not part of it.

Ms. Dashi: No.

Senator Day: That answers that.

The Chair: Thank you, senator.

I'd like to thank our witnesses for coming here today. We certainly appreciate you taking the time to come here and participate in our hearings because it's very important to the general public to hear from members of the RCMP, obviously. We appreciate the work you do.

With us in this final panel of the day is Deputy Commissioner Scott Tod, Ontario Provincial Police, Co-chair of the Counter Terrorism and National Security Committee. Welcome to the committee. We're pleased to have you with us today.

We do have prepared text of your presentation. Colleagues, it's in English. I'm wondering I could have a notion to disseminate it as a draft so that we have something to follow. Moved by Senator Day. Agreed.

Deputy Commissioner Scott Tod, the floor is yours.

Deputy Commissioner Scott Tod, Ontario Provincial Police, Co-chair of the Counter Terrorism and National Security Committee: Distinguished members of the Senate, I am pleased to accept your invitation to be here today representing CACP President, Chief Clyde Wayne, the Canadian Association of Chiefs of Police and as Co-chair of the Counter Terrorism and National Security Committee.

The mandate of the CACP is safety and security for all Canadians through innovative police leadership. This mandate is accomplished through activities and special projects of a number of committees and through active liaison with various levels of government and departmental ministries having legislative and executive responsibilities in law and policing.

The Counter Terrorism and National Security Committee is one CACP committee with the specific mandate to harmonize the work of the Canadian law enforcement community in identifying, preventing, deterring, investigating and responding to criminal activities related to terrorism and national security.

The strategic priorities of the CTNS committee are, one, to promote collaboration and integration amongst law enforcement agencies with appropriate public-private security and intelligence partners; two, to improve the ability to operate in a cooperative and integrated manner with the view of addressing emerging trends; three, to develop processes and facilitate strong communication at all levels; four, to recommend legislative reforms, and, five, to promote education and training in matters of counter-terrorism and national security.

The CTNS committee consists of national representation from police services across Canada at the executive level and government agencies with the operational mandates that include a response to the threats to Canada's national security. I can provide a list of member agencies, if you wish.

The committee gathers partner agencies that assess and address counter-terrorism and national security related issues, either from an operational or intelligence perspective. Private industry may also attend our meetings on an advisory basis or when approved and invited by the co-chairs.
During the past year, the CTNS committee has continued to strengthen communication, cooperation and coordination amongst the law enforcement community and key partners dedicated to community safety and well-being.

Activities of the committee include the initiative to create a counter-terrorism guide for the implementation of provincial counter-terrorism measures and strategies across Canada. The purpose of the guide is to create a toolbox for chiefs of police in Canada, which would be in line with Canada's Counter-terrorism Strategy.

The CTNS committee held a national forum this past September 16 and 17 at the RCMP National Headquarters to provide participants with an understanding of the national security threat; the challenges associated with counter-terrorism investigative efforts; and information on the four pillars of prevent, detect, deny and respond. More than 125 law enforcement and government agency representatives attended that conference.

The international law enforcement community is confronted with the challenge of increasing its efforts to detect and prevent acts of terrorism. This challenge has been exacerbated by the global dispersion of terrorist groups and individuals causing police executives to place greater emphasis on the important relationships that extend beyond our cities, our provinces and our nation.

In response to this critical threat, the RCMP co-leads an international group of like-minded countries and agencies designed to integrate our approaches to leadership, terrorism and intelligence, with a focus on strategic thinking, prevention and a global vision.

The CACP CTNS committee assisted the RCMP by assessing and selecting the Canadian law enforcement and security agency candidates for participation and learning opportunities within an international setting.

The Canadian law enforcement representatives are required to complete an action paper as part of their commitment to attending. The committee has assisted in completing a review of those papers and also in approving candidates for the upcoming conference. The approved topics are centred again on the four pillars of prevent, detect, deny and respond.

At a typical CTNS committee meeting, members are provided an overview of the current threat environment within Canada. This is a standing agenda item to generate discussion on issues affecting all of the CTNS member agencies. Bulletins and notices are created by the member agencies and shared nationally through the CTNS committee and the CACP on issues related to threats, trends and law enforcement practices.

Threats, trends, best practices and other timely topics are discussed at meetings. A recent presentation was made to the committee by the Federal Ombudsman for Victims of Crime. Other presentations and discussion include the work being done by the RCMP on radicalization prevention and the development of community engagement programs.

In addition to the work of the CACP CTNS committee, there are other law enforcement activities ongoing to address the threat of terrorism. An example of the provincial activity is the Provincial Anti-Terrorism Section, more commonly known as PATS, in Ontario.

The PATS section is an Ontario Provincial Police-led joint forces operation comprised of intelligence members from eight municipal police services, along with provincial and federal agencies, including the Canada Border Services Agency.

The PATS team is mandated to conduct multi-jurisdictional, strategic intelligence operations on matters involving international, domestic and other specific acts related to terrorism in Ontario.

The PATS team works hand-in-hand with the RCMP-led national security teams in Ontario and meet regularly to share information and support each other on terrorism-related investigations.
Most recently at the municipal level, the Calgary Police Service hosted a conference on countering radicalization. The conference had experts, academics and presenters from other countries, and most notably from across Canada.

Law enforcement officials and other public safety officials attended the two-day conference as an example of the need to inform and share our best practices, observations, research and solutions to the issue of radicalization and extremist activities.

Hopefully I have provided a fair review of the activities and actions that the CACP CTNS committee and its members have undertaken in regard to terrorism and national security at the federal, provincial and municipal levels.

Thank you, and I look forward to answering your questions.

Senator White: Thank you to the deputy for being here today.

I appreciate your referring a lot to the RCMP and the support they provide. The RCMP doesn't police our two largest provinces or any of the largest cities in the country. Do the chiefs of police and the agencies -- I'll look at Ontario for your sake -- get the right amount of intelligence from CSIS, for example, and others? Does it always go through the RCMP? Is there an opportunity as well?

When I was the chief in Durham, one of my biggest complaints was that CSIS would try to give the information to INSET or others to give to me, which could take weeks in some cases before I received it. Should they be going directly to the municipal partners?

Mr. Tod: As you well know, in Ontario the Police Services Act describes the responsibilities of a chief of police and the investigation of criminal conduct or a criminal matter. We're providing public safety for that at the decision and discretion of that chief of police.

In regard to national security, I can tell you that there is an information flow that occurs from the bottom up and from the top down. I'll start with an example of the bottom-up approach.

In Ontario the PATS team that I spoke about is eight police services and we have a number of other informal partners. We also have a liaison program involving private industry. It all provides information into the PATS unit, which feeds into the INSET teams and is then mixed with the information that's provided from CSIS to the INSET team to develop a clear picture and understanding of a threat.

CSIS does provide information to the RCMP INSET team. They do it in the one-vision concept, in the sharing of that information. They do it within the laws of Canada. I have no concerns in regard to the lack of sharing. Perhaps it's because of the fact that I do sit on the CTNS committee, and CSIS sits on that committee as a representative.

More recently we've been active and robust in the sharing of information in collaboration. I think a lot of it has to do with the trust that's occurred within law enforcement in the last couple of years in Ontario.

Senator White: We've had a lot of discussions with people before us asking about legislation. Do we need more legislation or changes to legislation?

A good example is one police leader questioned the need for AG approval on peace bonds. Do you see any sorts of changes that we need to recommend of that we should be focusing our attention on when it comes to terrorism and the Criminal Code in particular?

Mr. Tod: The recent legislation I've seen proposed within the federal context in regard to additional powers for CSIS, for example, has been in regard to the protection of informants. I think it's a necessary aspect that the security service needs. I think the other legislation we're looking at in regard to Canadian citizens who travel, Canadian citizens who have an opportunity to travel, is also an important piece of legislation which would support our efforts.
Specifically, in regard to the Criminal Code, I think the Bill S-10 amendments or other laws that have come in have been satisfactory. I can't sit here today and think of any legislation that I could consider being a strong proponent of at this time from the CACP's perspective.

Senator Dagenais: Thank you, Mr. Tod. I have two short questions.

What can we do to ensure better coordination between all law enforcement bodies during all stages of terrorism matters from notification of threats to prosecution?

Mr. Tod: As I opened up with the comments in regard to the legislative permissions that are given to chiefs of police, I will speak for Ontario only. In the Ontario Police Services Act, it provides the legislated obligations, roles and responsibilities to a chief of police. Although it doesn't specifically talk about terrorism, it talks about public safety and about rights and freedoms.

The regulations that we have in Ontario speak specifically to terrorism, counterterrorism, planning and preparedness for a chief of police. One of those things it talks about is a coordinated role, working with other agencies that provide that service.

The difficult part is in regard to when an event occurs, who carries the responsibility? Legislation will tell you it's the chief of police, but in some instances that may not be the best decision maker for something like that. That, to me, at times is confounding in regard to what other pieces of the puzzle we have in place to ensure the coordinated effort is occurring.

For example, the chief of police has the option not to call for a national security team, not to call for a provincial security team or not to call a fellow or neighbouring police agency for assistance.

The other part on the coordination piece is the intelligence part. The piece of readiness is, "How ready are we?" That is the question we always ask ourselves. I have learned that readiness can only occur through collaboration, coordination and sharing information.

That's why the PATS team, which comprises many police services in Ontario, works hand in hand with the federal police service on the national security enforcement teams. We've learned the best way to provide and learn information is by being at the table with them and coordinating and sharing.

I hope I've answered your question. Again, it's the individual chief of police who really has the say in how much collaboration and coordination will occur.

Senator Dagenais: How much, in terms of resources, do our local police forces dedicate toward counterterrorism and counter-radicalization matters?

Mr. Tod: For terrorism, we have the national security enforcement teams. I believe there are six across Canada. Those teams invite municipal and provincial police services to join them. In Ontario, I believe the national security enforcement team in Toronto has eight other police services that are partnered, co-located with them. The other team, the national security enforcement team in Ottawa, has three police services that are working together.

The collaboration occurs in regard to the larger police services, the police services that carry a substantial amount of population and a substantial amount of a potential threat, and are engaged with the national security environment.

On the radicalization process, that is something relatively new. I would say within the last year or two certainly, two years of policing. How much work occurs, I think you've heard from previous witnesses here today about the efforts of the RCMP. I mentioned one conference that was recently held in Calgary. I know of two others being held in December -- one in the Niagara Falls area and one in Ottawa -- to counter violent extremism and radicalization.

I think there are substantial efforts ongoing now in regards to it. As I said, it has been a recent phenomenon, within the last year, that we've paid a close amount of attention to it.
That's from a policing perspective. Our security partners at the federal level have had that, in my opinion, on their radar a little longer than we have.

**Senator Beyak:** Thank you very much for your presentation. We had a representative from FINTRAC a little while back. I wondered how involved the local police services and the OPP would be in laying charges and pursuing a case for financing terrorism. The RCMP has a national role, but I'm assuming you would have a role to play at the local level.

**Mr. Tod:** FINTRAC sits as a representative at the national table with the CALP CTNS committee. They provide information in regard to money laundering and financing of terrorism to the table. That information is available to any police service upon request or with notification from FINTRAC.

The money laundering is one aspect we look at, especially right now on the issue of radicalization. It's the high-risk traveller, for example, and the radicalization process to high-risk travellers, but also the facilitation of the travel itself is very important. We do look at how the funding is obtained and where the funding comes from. We can't do that without FINTRAC assisting us.

**Senator Kenny:** I attended the conference in Calgary this past week. It was a remarkable two days. One of the issues that came up was the question of separating a community outreach program, much like what the last set of witnesses was talking about, from the folks involved in gathering intelligence in an organization.

Do you think, in a practical sense, that actually can work?

**Mr. Tod:** I do, senator. Speaking on behalf of the Ontario Provincial Police, as a result of undergoing an extensive review of our actions in regard to Coteau Ipperwash and as a result of a public inquiry that was held, we had an opportunity to look at the organization and how we manage information and how we do community outreach. We created something called our provincial liaison teams; it's individuals out there to work with the communities, work with the groups, work with individuals, and to be able to provide a perspective of both sides or a perspective in regard to law, a perspective in regard to someone else's rights, someone else's position on something. I do think that's a very important role, separate and apart from intelligence.

The purpose of our provincial liaison teams' is not to collect intelligence and provide information back to the centre or back to an analysis function, but to provide perspective, to provide dialogue, to provide an open door for engagement. I think a similar program in regard to radicalization or community engagement or CVE -- countering violent extremism -- is very possible.

In Ontario, at a government level, right now we have a community safety plan working group. We're developing community safety plans for communities. I hope that radicalization and CVE -- countering violent extremism -- will become one aspect within those community safety working group discussions and that looking to the criminogenic factors of poverty, homelessness, addiction and mental health, that we will also use those criminogenic factors and look at extremism and radicalization also in a similar light so we can identify vulnerable individuals who may cause harm to themselves or society.

**Senator Kenny:** What would happen within the OPP if somebody in community outreach came across actionable intelligence? What would they do?

**Mr. Tod:** Within the confines of the provincial police policy, they are required to report that, information that would prevent a criminal act from occurring, information that would prevent someone from being hurt, information of a breach of some other practice or policy that's important to the policing organization.

**Senator Kenny:** The outreach programs are dependent on the trust of people they're engaging with. I find myself putting my head in the place of a mother whose son is starting to behave in a problematic way. What do you have to go through as a police officer to persuade that mother to know where the line is when she can come forward and that will be of benefit to her son, or when she decides otherwise? There's bound to be a measure of mistrust initially, at least.
Mr. Tod: Absolutely, senator. I heard a previous witness describe pre-criminal space. On the aspect of mobilization and engagement, it's not a police function; it's a community function. So the police are facilitators of liaison and engagement. We would prefer actually not to do it, the full act, but we would prefer to facilitate how community mobilization engagement occurs.

In the instance of the mother, we would hopefully build trust within a community leader, a community champion or an issue-specific champion within that community that can represent or advocate on behalf of not just the police but on behalf of the citizens in the community to do the right thing.

Having the police fulfill all the responsibilities and obligations on engagement and liaison we know is not the right answer. We have to have community facilitation occur. We have to actively go out and, for the sake of a better word, recruit trusted leaders within communities and issue-specific concerns in our communities to deliver the message or to be the trusted person I think you're speaking about.

Senator Beyak: As a follow-up to my previous question, just for the benefit of those watching, with the money laundering, the terrorism financing and the facilitation of travel that you mentioned, what role would each level of police force play in building a case to lay charges there, the local police, the OPP and the RCMP?

Mr. Tod: Many police services have a relationship with FINTRAC. Where it is ideal is the relationship with the federal national security enforcement teams that do financing and laundering investigations on terrorism. A police service itself to do that investigation requires expertise in accounting, forensic accounting, understanding the economic management system we have in Canada. Generally, they would seek expertise from a larger organization or another agency that has that specific experience and knowledge on how to do money laundering investigations.

But it starts with a patrol officer. It really does. It starts with the understanding by the patrol officer that for a person to travel outside of Canada it costs money. In many places it's very expensive, depending on the mode of travel. That officer understands that they have an opportunity to look for plane tickets, Visa bills, receipts, cash, things that occur with the individual or the environment of the person who is travelling, and I'm using high-risk travellers here, or in other types of individuals who may be entered into terrorist acts in Canada. Everyone plays a role. I'm talking about the patrol officer, but also senior executives at my level to make sure that we're working cooperatively together, especially FINTRAC. They do provide annual reporting to all the police leaders in the country to make sure we're all working together.

The Chair: Colleagues, could I follow up on this? I think this is an important area. We've been informed that we went from 50 to 53 identified terrorist organizations operating in one capacity or another here in Canada. That's the information we received at this committee. Second, we've been told there is a serious problem identified of financing of terrorism organizations through charitable organizations that contend they're doing humanitarian work.

What I don't understand is, we have had a number of witnesses come here, say that it's a problem, outline what the problem is and the magnitude of the problem, and yet at the same time, to my knowledge, we have had no charges laid over the course of the last 10 years.

Is the threshold too high, from what we, within the judicial system, are asking in respect to laying charges, or is there another way we should be doing this type of investigation so that we can get the necessary evidence to lay those charges? It has to be a concern to you and to the general public if this is obviously going on, and there are no ramifications to it at the end of the day. Do you want to comment on that?

Mr. Tod: Yes, Chair. Very true. We are concerned about financing of terrorist activities in Canada or outside of Canada by Canadian citizens. The difficulty in the past is the ability to prove that the funds themselves were used to facilitate terrorism and follow the funds — "follow the money" is the term we used when I was a fraud investigator — and the end result that the money truly facilitated a terrorist act or terrorism in one way or another. That has always been the difficulty.

In the past, some of it was experience, knowledge of police services. I think we've worked well towards that. But it speaks to the large picture of how much money actually from Canada is used to facilitate terrorist acts in Canada and around the world, and I don't have that number. I can't tell you what the country-specific
amount is, what the country-specific percentage is to global terrorism. I don’t know. It may be a combination of many things, but it is something that we are always looking at in regard to investigations involving terrorist activities, and something we always look at is the facilitation and source of funds. Amounts really aren’t that large often as we look at it.

The Chair: We were informed here, I believe it was at our last committee meeting, that it’s as high as six figures. We’re talking hundreds of thousands of dollars maybe through one organization, according to the testimony that was provided.

I want to go back to my question again. Is the threshold too high in respect of organizations such as your police force or others? Is it being requested so that charges aren’t laid, or could I ask this question: In your experience and your knowledge of other police forces, is information being compiled, investigations being done by the various law enforcement agencies and then being brought forward to the Crown prosecutor’s office and then not being taken forward? Is that what’s happening?

Mr. Tod: I can’t answer that question with a specific answer, my apologies.

Senator Day: This meeting that just took place in Calgary was under the auspices of what organization, the chiefs of police?

Mr. Tod: It was the chief of the Calgary Police Service.

Senator Day: How does that happen? You mentioned a number of others that will be happening. Is it the initiative of the taxpayers in a particular region to cover the cost of this? Do you have a rotation within the Canadian Association of Chiefs of Police saying it’s your turn to do something?

Mr. Tod: We don’t have a rotation. The forum I spoke about on September 16 and 17 was in fact the very first forum we’ve ever held as the CACP/CTNS committee. We have spoken about extremism before in the CACP environment. This was the very first specific forum we had on terrorism. As I mentioned in my opening comments, each individual chief of police is responsible for public safety within their own jurisdiction.

Senator Day: Yes.

Mr. Tod: Chief Hanson in Calgary took it upon himself, largely as a result of the phenomenon of radicalization that has really become a large specific topic in the past year that many of the chiefs have decided to take action on their own. The CACP/CTNS committee has a member of the Calgary Police Service on it. Whether the CTNS committee, as a result of our work on radicalization and terrorism, and that member returned to the service and suggested it or not I can’t speak to, but we do have and we do monitor and we provide assistance in the way of speakers and expertise to chiefs of police who wish to put on conferences around terrorism.

Senator Day: That’s quite haphazard though. You’re just hoping that the next chief in some other area will decide to call a conference so you can exchange information rather than it being objectively looked at and saying we should be sharing this information on a regular basis, every six months or whatever you decided.

Mr. Tod: It’s largely a result of the phenomenon of radicalization that has really become a large specific topic in the past year that many of the chiefs have decided to take action on their own. The CACP/CTNS committee has a member of the Calgary Police Service on it. Whether the CTNS committee, as a result of our work on radicalization and terrorism, and that member returned to the service and suggested it or not I can’t speak to, but we do have and we do monitor and we provide assistance in the way of speakers and expertise to chiefs of police who wish to put on conferences around terrorism.

Senator Day: Have you participated in the round table on countering extremism?

Mr. Tod: I don’t participate in that forum.

Senator Day: Is that something you would get invited to participate in from time to time?
Mr. Tod: My apologies, I can’t answer without knowing the specifics.


Mr. Tod: I’m not familiar with that committee at all.

Senator Day: How about the CVE program that we just learned about. RCMP countering violent extremism program and the various training sessions that they’re having; are you familiar with that?

Mr. Tod: I’ve received two presentations in regard to that, yes.

Senator Day: Is that a helpful thing that should in your view be continued.

Mr. Tod: Extremely and timely.

Senator Day: Thank you. That’s helpful.

Senator Ngo: I would like to continue the question raised by the chair and some others here. We know that more than 130 Canadians overseas brought some related terrorism activities. We know about 80-something returned to Canada, and this included involvement in training, fundraising, promoting radical views and even planning terrorist violence.

In the Combating Terrorism Act, does it allow you to arrest those people suspected of terrorism for a period of time?

Mr. Tod: Temporary detentions?

Senator Ngo: Yes, temporary detentions, because in the Combating Terrorism Act they allow you to do that. Have you done it so far? According to the chair so far we have only one charge.

Mr. Tod: I have no knowledge of that, no.

Senator Ngo: Did you know how many times the Combating Terrorism Act has been used to detain these individuals?

Mr. Tod: I can’t answer that question either, sir.

The Chair: Colleagues, I think we’re all trying to understand what the RCMP does or what your organization does, and other organizations within the law enforcement agencies.

I just want to go back to the 80–to 90-some-odd individuals who have been identified as high risk in security. Is only the RCMP involved in that or are you involved if it’s in the province of Ontario in part of that surveillance and monitoring these individuals who are determined high risk?

Mr. Tod: We provide assistance to the national security enforcement teams— and I’m speaking of the OPP— we provide specific support and investigative assistance to the national security enforcement team in regard to all of its activities, whether it be a high-risk traveller or a planned and deliberate attack. We provide resources to them all the time, of which surveillance would be one, as well as technical assistance and intelligence analysis. We provide the assistance to them continuously. That’s true of the partnership we have within Ontario.

The Chair: But just follow this through. You’re not the decision-maker whether or not a charge would be laid, you don’t bring that before the prosecutor, it’s the RCMP, is that correct?

Mr. Tod: To a large extent, yes, that’s correct.

The Chair: Could you?

Mr. Tod: We could, yes, absolutely. Any chief of police in Ontario has the ability to do that.
The Chair: The question I would have to you is, in following through this, with the laws that are on the books and have been passed by Parliament in respect to terrorism — and I think they’re very clear, I don’t think there’s any question of what it says — why aren’t we proceeding with charges with some of these individuals with the knowledge we have? Is the threshold too high that you have to meet from a point of view of evidence in order to lay a charge?

Mr. Tod: The individuals you’re talking about, are you talking about the high-risk travellers?

The Chair: Yes.

Mr. Tod: I would say the threshold is not too high. The ability to collect, analyze and understand the criminal information so that we can propagate a criminal charge is a challenge for police officers. It’s resource extensive. In order to understand the surveillance aspect of it, if an individual is under surveillance 24/7 we are required to put probably a combination of 30 officers a day on one individual.

The number you spoke about, senator, 130, or the returning 80, if you multiply that 30 per day it’s staggering in terms of police resources. That’s just the human element with the physical surveillance. There’s also the technical surveillance, which is extremely challenging for police services. We could actually deplete much of our surveillance resources and our technical resources looking after the high-risk travellers and leave organized crime and other facilitators of crime in our communities alone.

The challenge for us is to first determine the threat level of individuals in the group we’re talking about, and I don’t have a specific number with me today. The number grows and ebbs.

The Chair: Can you get us that information?

Mr. Tod: I can access that information if I need it, yes.

The Chair: You can get it for us though?

Mr. Tod: I will.

Senator White: I appreciate your discussion around working together.

We had the commissioner of the RCMP in recently, and we have had other police representatives. We know what cuts the RCMP have also faced over the past number of years. Does the RCMP have the resources available to them today to maintain the things they’re doing and to actually focus energy that all of us need them to focus on this threat? Since you don’t work for the RCMP, you can say this bluntly, I’m sure.

Mr. Tod: I am familiar with specific aspects of the RCMP in regard to deployment. I can’t speak to the national deployment picture, the provincial deployment picture or any other federal responsibilities they share. It may be unfair.

Let me specifically say that the phenomenon of the high-risk traveller has caused an incredible resource pull on the OPP. We are evaluating not only the terrorism and national security projects we’re doing but also all the other projects on the organized crime side in regard to gaming and criminal activity involving outlaw motorcycle gangs. We are evaluating all of those projects or targets of investigation and are challenged with the fact that we need resources to deal with the most immediate threat to our communities. The most attention we’re having right now is in regard to the high-risk traveller phenomena.

Do they have enough? I think the commissioner of the RCMP can answer that much better than I can. Could we use more? I would suggest the answer is yes, and I’m saying that with great caution because I understand the challenges faced in the economics of policing. I understand what it’s costing our communities. I understand that. We are challenged every day with deploying our resources in the most effective manner, and we attempt to do that all the time.

Senator White: I appreciate that response, deputy. I do. I think it was the Monday afternoon we had Mr. Yaworski from CSIS here speaking to us, the same afternoon the soldier was killed in Quebec, actually I think around the same time. We asked him the question, and I can’t remember who asked it, about whether
or not we had enough resources in this country to track the 85, not including the medium-risk and the low-risk that may shift back and forth between medium and high, if we understand that. His answer was we have to always kind of risk it out and figure out where our priorities lie. That week, we had two incidents where people, one who was under watch, one who was not, were successful in what they set out to do.

We are saying, though, regardless whether the RCMP have enough resources, we don't in Canada, in your mind, have enough resources to do everything we're doing and take on this challenge. Would that be correct?

Mr. Tod: Again, it's a very difficult question. I think it comes down to the risk management ability, the ability to manage the risk of an organization. The smaller the organization, the less ability you have to manage a risk. The larger the organization, the larger your police budget; the larger, human-resource capital you have, the better ability you have to manage a risk. I think the very large organizations in law enforcement in Canada can manage the risk within the restrictions they have of people and money. I'm evading giving you a true answer on this one but, as I said, could we always use more? Absolutely. It comes down to the risk management strategy of an organization and what attention you're applying to that. Through the various governance models we have as police services and who we report to, that's questions that should be asked to the police leaders in Canada. What risks are you taking? What risks are you managing? That's where the discussion deserves to be held in regard to resourcing and deployment.

The Chair: But doesn't it also go back to the threshold in respect to what's being asked for you to do the work you do in order to be able to proceed in the court system? If you have to give 30 police officers a day to do surveillance on an individual, we don't print enough money in Canada to do that, if we keep continuing with these numbers that are continuing to escalate. There have to be other remedies other than just strictly surveillance and things of that nature. It's a multifaceted question out there. Would you not agree?

Mr. Tod: Absolutely, Senator. I agree. The ability to collect that criminal information, as you said, is expensive in regard to surveillance and the human resources capital that's required. Technically, it's very expensive in regard to the technical capabilities. Again, the threshold to determine criminality, if I can use that word, the terrorist activity that requires that a criminal charge be charge laid, that's threshold is fine. The ability to collect the information and analyze the information and have access to the information for everyone is what is critically important in regard to determining our threat and the ability to lay a charge.

The Chair: Well, obviously we're not collecting the information, because we're not laying any charges at this date, except for one particular case.

Senator Day: I just wanted you to comment on the community outreach issue we were talking about earlier. Various police forces have been doing that for quite a time, the larger ones in particular, gathering information with respect to organized crime, motorcycle gangs, et cetera. Now we're into the anti-terrorism side of things, which is pre-criminal and takes up a lot more resources. I'm assuming from what you've said that it's only the larger police forces that would be able to get involved in that to any great extent because the smaller ones are pretty busy with their detection and prosecution side of things.

From the point of view of those police forces that are involved in this pre-criminal gathering of information, community outreach, trying to see if there's anything strange happening, is it the Canadian Association of Chiefs of Police, or do you again leave it up to each chief of police to talk about gender sensitivity and ethnic balance and all those factors that are important, particularly so in a community outreach situation? Where does the influence come from in that regard?

Mr. Tod: I can't speak to the other committee work that's being done by other committees in the CACP. I'll speak specifically in regard to Ontario.

As I mentioned, since 2009, the policing model of preference in Ontario is the Ontario mobilization engagement, community mobilization and engagement model, and the four specific action areas within that model are mobilization and engagement, liaison and engagement, the risk-driven collaboration piece, which is that community-police piece together, and finally the last one is the law enforcement suppression piece. Any service, regardless of size, has the opportunity to fill all four of those quadrants in the mobilization engagement model.
I will speak for Ontario specifically. That is the model of preference we have taken in regard to moving forward with our safety community working groups and the opportunity for the community to actually lead the aspect of liaison and engagement, in other words, liaison in regard to working with the community and assisting the community in being healthy and vibrant, but the engagement rests within the community. The police facilitate. We step back. We play the back room portion of that and allow the community itself to engage and the community itself to work towards identifying what we call acutely elevated individuals, largely because of criminological factors -- mental health, addictions, truancy, homelessness, poverty, those sorts of things. After that, we have the suppression piece, the policing enforcement. The criminal space is where we operate in.

When you talk about pre-criminal space, I look at the pre-criminal space in Ontario as being the liaison and engagement piece. That's pre-criminal where police have a very small responsibility and role to play in that. The criminal space is actually that community collaboration piece. That is where the police and the community leaders are sitting together identifying acutely elevated individuals, problems or concerns, and working together on collaboration.

The last piece is simply the collaboration is not going to work, the liaison is not going to work, the engagement is not going to work, and we have the suppression piece where we have to go and be the police and investigate, charge and prosecute people.

Senator Day: We were informed by the RCMP that this new initiative with respect to countering violent extremism is in the pre-criminal phase and there is a community outreach aspect to that that's very important, but that's not something that the chiefs of police or the police forces across Canada, other than the national ones, are getting involved in very much.

Mr. Tod: I think every police service will be involved in that. I know police leaders across Canada now understand the aspect of engagement and liaison and that risk group, and I call it risk-driven collaboration. It's working together with communities.

In 2008, I visited Prince Albert, and Chief McFerrin, now deputy minister McFerrin, was starting up the whole aspect of community mobilization.

Over the years, it has grown into a true collaborative approach in identifying what they call the hub environment, and there are many hubs. You may have heard that.

Senator Day: We did hear that term, yes.

Mr. Tod: That's where the whole aspect of CVE belongs, within that liaison engagement. Collaboration occurs in the community hub where people can identify teachers, social services agencies, community youth groups or sporting groups. They can identify an individual or a concern and work together collaboratively on it without having the police come in to run it and drive it and provide all the resources for it. If that truly works, then we have resources that we can dedicate back out to things like investigations on terrorism, investigations on organized crime and other work that falls within the responsibility of the police.

I may be generalizing here, but the innovative leaders that we talk about in our mandate of CACP, leadership through innovation, those police leaders understand the whole aspect of community collaboration and where it belongs. That pre-criminal space is a community responsibility on engagement, liaison, and the policing responsibility starts to work in the collaborative approach working with our partners. Then at times there are people out there in the organized crime world who are neither addicted, homeless or poor, they've gone to school and they are still members of a large criminal organization. That's where the police come in and that's where we work best.

The Chair: I'd just like to go into one other area. I'm going to ask you a question. I may be putting you on the spot here, so if I am, bear with me.

It was announced by Prime Minister Cameron that I believe they intend to bring in legislation where if a citizen of Britain leaves the country and is involved in a terrorist organization that has been identified by their
country, their citizenship will be revoked for at least two years. This was announced, I believe, down in Australia.

Do you have any comments on that? The reason I ask this question is because when I went home over the past week, a number of people asked, “Well, if people want to become involved in this, why are we allowing them back into the country?” Obviously, it puts you in a situation and all the members that you represent of having to monitor and put these individuals under surveillance in view of the fact of what they’ve been involved with upon leaving the country.

So have you given any thought to that type of legislation perhaps being considered by Canada or other countries?

Mr. Tod: I haven’t, senator. I haven’t given it much thought, but I would much rather spend our time and resources with the citizens we now have in Canada by preventing them from becoming radicalized and working towards the whole aspect of someone travelling abroad.

I don’t think it’s as simple an answer as revoking citizenship. I don’t think that will stop terrorism and diminish the threat we have in regards to that. I don’t think I can answer that. It’s just not a simple question for me to sit here and answer.

The Chair: Colleagues, we have come to the end of the time that has been set aside for this particular committee hearing. I’d like to thank our witness for appearing. We appreciate your forthright responses to our questions.

I would like to go in camera for a few minutes prior to leaving. Thank you.

(The committee continued in camera.)
OTTAWA, Monday, October 27, 2014

The Standing Senate Committee on National Security and Defence met this day at 1 p.m. to study and report on security threats facing Canada and on national security and defence issues in Indo-Asia Pacific relations and their implications for Canada’s national security and defence policies, practices, circumstances and capabilities.

Senator Daniel Lang (Chair) in the chair.

The Chair: I would like to welcome everyone to the Standing Senate Committee on National Security and Defence on Monday, October 27, 2014.

Before we welcome our witnesses, I would like to begin by introducing the people around the table. My name is Dan Lang, senator for Yukon. On my immediate left is the clerk of the committee, Josée Thérien and on my far right is our Library of Parliament analyst assigned to the committee, Holly Porteous. I will now go around the table and invite each senator to introduce themselves and state the region they represent.

Senator Mitchell: Grant Mitchell, deputy chair of the committee and I’m from Alberta.

Senator Stewart Olsen: Carolyn Stewart Olsen, senator from New Brunswick.

Senator Kenny: Colin Kenny from Ontario.

Senator Beyak: Senator Lynn Beyak, Ontario.

Senator Ngo: Senator Ngo from Ontario.

Senator Day: Joseph Day from —

Senator White: Vern White, Ontario.

The Chair: Colleagues, this afternoon the committee will be meeting to continue our two studies pertaining to our mandate of national security and defence. In the first two hours, we will look at the terrorist threats in Canada and in the third hour we will focus on the Indo-Asia Pacific region as part of our second study.

Before we begin our study I wish to express, on behalf of all members and all senators on this committee, our deepest condolences to the families of Warrant Officer Patrice Vincent and Cpl. Nathan Cirillo, our two Canadian Armed Forces members who were murdered by terrorists in Canada last week in two separate incidents. Canadians are proud of our women and men in uniform and we will not be intimidated, nor will we surrender to those who promote hateful religious and non-religious views as a means of advancing their political objectives. I would also want to point out like many other Canadians and on behalf of members of this committee that we like to see our soldiers proudly wearing their uniforms in public. We must not be intimidated.

On June 19, 2014 the Senate agreed that the Standing Senate Committee on National Security and Defence be authorized to study and report on security threats facing Canada including but not limited to cyber espionage, threats to critical infrastructure, terrorist recruitment and financing, terrorism operations and prosecutions, and that the committee report to the Senate no later than December 31, 2015. The Senate commenced this study because we, like all Canadians, are concerned about the threats to our safety and security. We wish to get to the core of the issue in a reasoned and well-informed manner.
Commissioner Paulson, we are very glad to have you here with us today along with Mike Caouano, Deputy Commissioner, Federal Policing and Peter Henschel, Deputy Commissioner, Specialized Policing Services. You are not strangers to this committee and I welcome you back. We hope this will be an informative session and that at the end of the day Canadians will have a better understanding of the magnitude of the threat, the nature of support for those threats, a better sense of what radicalization means and counter-radicalization that is taking place.

Commissioner I understand you have an opening statement.

Bob Paulson, Commissioner, Royal Canadian Mounted Police: Thank you, Mr. Chair and members of the committee.

(French follows ... Mr. Paulson con't q ... je tiens évidemment à vous ...)

(après anglais) (M. Paulson ... and members of the committee.)

Je tiens évidemment à vous assurer que nous présenterons au comité une copie de mes commentaires d'ouverture dès que possible, dans les deux langues officielles.

Compte tenu de l'évolution de la situation et de notre compréhension des événements de la semaine dernière, nous avons dû faire les dernières mises à jour ce matin. Nous vous remercions de votre compréhension à cet égard.

(Mr. Paulson: Thank you for the invitation to discuss ...)

(english suit)

(Following French -- Mr. Paulson con't q -- à cette ...)

Thank you for the invitation to discuss the range of security threats facing Canada now and into the foreseeable future. I had originally intended to focus any comments on topics including cybercrime, cyber espionage and threats to critical infrastructure to name a few. However, in light of recent events in Quebec and Ottawa I will focus on the threat of terrorism, specifically those intending to commit acts of terrorism both in Canada and abroad. That said, my colleagues and I are happy to take your questions on the range of security threats.

At the outset, I would like to again express the RCMP's condolences to the family and friends of Warrant Officer Patrice Vincent and Cpl. Nathan Cirillo, as well as to all the women and men of the Canadian Armed Forces.

Terrorism has been a threat to Canada and to the safety and security of Canadians for many years. We are not and have not been immune to acts of terrorism. However, it does feel as though the events of the last seven days have led to a sense of loss and vulnerability not felt in this country for a long time. Perhaps most hurtful is that the attackers were Canadians. They were members of our own communities who somehow turned against their friends and families to commit violence and spread terror.

In light of such senseless acts it is natural to have a desire to seek those who want to do us harm. However, we must be mindful that Canada is a nation of laws and the Charter ensures the protection of all citizens. Terrorism is a serious crime with harsh penalties and we must be sure that our pursuit of justice is based on evidence, which will support prosecutions, secure convictions and bring eventual penalties. Our approach must be balanced with dogged police work, evidence gathering and collaborative efforts with our partners, particularly those in the Public Prosecution Service of Canada to ensure that the full weight of Canadian law is brought to bear.

The RCMP is mandated to investigate and prevent terrorist activities. It is one of our most important duties and we take this responsibility extremely seriously. Over the past decade we have been successful in detecting, disrupting, investigating and charging terrorists across the country. In total, 17 individuals have been convicted under Canada's anti-terrorism laws.
Just last week, Misbahuddin Ahmed, who was convicted in July, received a 12-year sentence for terrorist activities. We have also prevented a number of terrorist attacks through other disruptive means. We are leveraging our long-standing and effective partnerships with the police departments across the country, indeed the entire safety and security community, to combat this growing threat. Terrorism is one of our most challenging investigative areas. It is extremely difficult to detect the early signs of radicalization and ultimately determine if an individual may be preparing to launch an attack on any scale. Many of these individuals often show few signs of being disposed to violent action. Even those under close investigation often exhibit little to know warning signs before an attack is carried out. Ironically, the more elaborate the plot the greater the opportunity for successful disruption.

(French follows -- Mr. Paulson cont’d -- Le terrorisme est un type de crime...)

Le terrorisme est un type de crime qui compte parmi les plus problématiques sur lesquels nous avons à enquêter.

Il est extrêmement difficile de détecter des signes de radicalisation de façon précoce et de déterminer si un individu donné est en train de préparer un attentat qu’il en soit l’ampouleur. Bien souvent, le terroriste ne montre aucun signe permettant de croire qu’il soit disposé à la violence. Dans la majorité des cas, même chez les individus faisant l’objet d’une enquête suivie, rien ou presque rien ne laisse supposer qu’ils sont sur le point de passer à l’acte. Ironiquement, plus un complot comporte un haut degré d’élaboration, plus élevées sont nos chances d’y faire échec.

(Following French -- Mr. Paulson cont’d -- chances d’y faire échec...)

Further, there is little commonality amongst these individuals besides their eventual radicalization. Our holdings tell us that they come from different socio-economic backgrounds, are of different races and have taken vastly different paths to their eventual radicalization to violence. The attacks of last week underscore the challenges faced by the security and intelligence committee. These acts were carried out with no advance warning and, thus far, seemingly little to no preparation. The events of last week are clear examples of just how suddenly these attacks can occur and how unpredictable radicalized individuals can be.

As you are all aware on Monday, October 20 at 11:40 a.m., Martin Couture-Rouleau struck Canadian Armed Forces members with his vehicle in the parking lot of a shopping plaza in Saint-Jean-sur-Richelieu and on October 22, beginning at 9:52 a.m., Michael Joseph Zehaf-Bibeau opened fire on the ceremonial guards at the war memorial. He then headed to Parliament Hill. After entering the grounds, he commandeered a vehicle and drove to the main entrance while being pursued by RCMP. Upon entering Centre Block, he engaged in an exchange with House of Commons security and RCMP officers where he was killed. Neither of the individuals in these events were linked, nor were they a part of a coordinated attack.

If prevention poses challenges when we are aware of an individual, it is even more daunting to prevent the acts of someone unknown to us. We did not learn until after the attack that Zehaf-Bibeau was hoping to leave for the Middle East. While we now have video he made describing his ideological and political motives, our investigation is determining whether he had shared or communicated these intentions to commit violence to anyone. Just like the earlier incident that week, the attack came without warning. Unfortunately, we are all too familiar with the unpredictability of these events.

These attacks were similar to the deadly events of last June in Moncton, New Brunswick, where three RCMP officers were murdered and another two wounded by an individual radicalized to violence by another political ideology. While hindsight offered some indication of potential violence, there was no forewarning. While we are facing this threat at home, we must focus efforts on preventing individuals from travelling abroad to commit acts of terrorism. Preventing the individuals from travelling is critical. If these individuals return with training and/or battle experience, they pose an even greater threat to Canada and our allies.
We are seeing a growing number of Canadians drawn into the ranks of ISIS and ISIL and al Qaeda and attempting to or travelling abroad to conduct terrorist-related activities. In January 2013, two Canadians participated in an attack on an Algerian gas plant where 36 people were killed. Since then, still others have gone to join conflict zones in places such as Syria and Iraq.

We are taking active measures to address these threats. Internally, we have implemented a range of activities to detect, prevent and respond to terrorist activity. This includes leveraging our domestic and international partners and identifying new and unique ways to combat this threat. Operationally, the RCMP-led Integrated National Security Enforcement Teams, based across the country, have been fully mobilized to address the threat of high-risk travellers. In addition to the existing 170 resources, we are reallocating the necessary funds and personnel from other priority areas to combat this threat. In recent months, and over the past week, over 300 additional resources were transferred to enhance the capacity of INSET from other federal policing priority areas such as organized crime and financial crime.

We are continually assessing the threat and the required resource levels and taking the necessary steps to reallocate resources as required. Additionally, other partners have contributed resources to our INSETs. Further, the wider law enforcement communities in Canada and abroad continue to offer their help and assistance.

We are meeting daily with our partners at the Canadian Security Intelligence Service to assess the threat posed by known high-risk travellers and those radicalized to violence. The RCMP has established a group which has resulted in an unprecedented level of interdepartmental cooperation. The high-risk travel case joint operations centre is housed within the RCMP ops centre in order to respond in an expedient manner to changes in threat and to bring the full powers of the Government of Canada to bear the moment an individual is identified.

Our partnerships are not limited to the security and intelligence community or law enforcement. The active engagement, cooperation and support of the community are key to our efforts. It is likely that family, friends, teachers and community members will be the first to see the radicalization process begin and perhaps hear the first threats of violence.

For example, it was the concern and vigilance of the family and friends of Couture-Rouleau that brought him to our attention.

Early notification of sudden changes can be key in assisting an individual before they become radicalized to violence. These changes vary. It could be anything from withdrawal from positive social interactions and activities to isolation, segregation, expressing increased hatred or espousing the virtues of violence and expressing an "us versus them" understanding of the world. These are often not criminal actions -- far from it -- but we would suggest that friends and family members pay close attention to these indicators and reach out to law enforcement or other services in the community if there are concerns.

The RCMP and the broader law enforcement community recognize that the best way to prevent terrorism is to prevent radicalization in the first place. We are doing this through countering violent extremism efforts and programming. The RCMP in collaboration with key partners is implementing a program to provide frontline police officers and the community with the tools that they need to recognize and assist individuals at risk.

Including I would like to reiterate what I said in my comments to the media last week. Canadians are safe. Fundamentally, the events of last week have not changed us. This was evident last Wednesday when citizens joined with police, medical technicians and military personnel to protect and provide medical aid to Corporal Nathan Cirillo. There were other acts of bravery and examples where citizens cooperated with law enforcement. In the face of this adversity, Canadians of all faiths, races and political persuasions came together to protect and support one another. I am confident that this will continue.

Thank you very much for your time and we're happy to answer any questions.

The Chair: Thank you very much, commissioner, for being with us this afternoon and for your informative presentation. I would like to begin with a question. The question that's outstanding for
Canadians is, what exactly is the magnitude of the public threat that we as a country and as Canadians face going forward? I want to refer you back to the document called *Security, Freedom and the Complex Terrorist Threat: Positive Steps Ahead* that was a report by the Special Senate Committee in March 2011 chaired by Senator Segal and Senator Joyal.

The statement was made:

...the RCMP has estimated that as many as 50 terrorism organizations are present in some capacity in Canada, and, as of May 2010, CSIS was investigating over 200 individuals in Canada suspected of terrorism-related activities.

Commissioner, can you provide us with an update for 2014 in view of what we were facing back in 2010?

Mr. Paulson: Thank you, Mr. Chair. I guess the best way to frame up the magnitude of the threat, you will have heard perhaps that I had sort of assigned a number when I was at another committee hearing, talking about the number of individuals who were identified as high-risk travellers. At the time, I think I identified 90; last week it was 93. It’s a number that fluctuates in terms of the identification of people who for one reason or another and to one level of understanding or another want to go abroad, participate in terrorist activities, participate in jihad. That is one way of understanding that element of the threat.

We do, however, have a number of other active investigations in partnership with the intelligence service. How to frame that in terms of the numbers of individuals; there are both individuals who are of high risk, perhaps arising from radicalization, and there are others who are being actively investigated for criminal offences related to national security. So I think the magnitude of the threat is best characterized as serious and present and one that requires all people in the national security business, in the law enforcement business — indeed, all Canadian citizens — to be vigilant.

The Chair: I want to pursue my initial question. I go back to the statement that the RCMP estimated as many as 50 terrorist organizations — not individuals, organizations — are present in some capacity in Canada. Is that true today?

Mr. Paulson: I can’t really say in terms of the number of terrorist organizations. We are framing up our targeting on the back of individuals, some of whom are inspired by the broader sort of al Qaeda threat, and others who are inspired by the recent ISIL phenomena.

In terms of the organizations, I’ll ask my colleague Mike Cabana to speak to you.

Mike Cabana, Deputy Commissioner, Federal Policing, Royal Canadian Mounted Police: Thank you, commissioner.

Senator, maybe my answer will not be quite as helpful as you would like. We start first by understanding that 53 different organizations are listed as terrorist entities in Canada currently, so, there is a slight increase from 2011. But I think the danger in trying to quantify or define the level of the threat through numbers is rather daunting but also a dangerous one.

The threat is multi-dimensional. It involves the high-risk traveller that has been the subject of much discussion over the past week or so, but it also involves actual organizations that are operating in Canada. There are individuals coming back to Canada from participating in foreign conflicts. We have individuals in Canada who are attempting to travel abroad for the purpose of participation. Then, of course, we have organizations here in Canada that are involved in supporting the terrorist organizations through recruiting and funding. I would caution in trying to put an inventory in place and define the threat based on number of organizations.

The Chair: Perhaps I could pursue that later on.

Senator Mitchell: Thank you to each of you for being here. I do want to underline the gratitude of the people of Canada, but for every person on the Hill and who works there it was clear that there were a lot of uniformed men and women going directly at that gunfire, and it was very inspiring to see that.
I would like to do two things to refine further the Chair's question.

First of all, he is talking about the magnitude of the threat. Maybe it's a fine distinction, but the nature of the threat. Is it more likely we have the single gunman, the single car driver? How do you compare that possibility to larger attacks, bombs or even more coordinated attacks with more coordinated, organized organizations?

Mr. Paulson: Thank you, senator. As I said in my opening comments, ironically the more elaborate the plot is the more likely it is we are able to respond in advance. There are probably more indicators that will come to our attention of a developing plot.

To the heart of your question, I think the evolution of the threat, which is continually evolving but is now predominantly being understood as that sort of single individual actor doing things like using his vehicle as a weapon, and so that presents a much more challenging threat. In that sense, I would suggest that the threat has evolved to a state which is much more challenging and disconcerting for law enforcement in terms of responding to that lone actor.

Senator Mitchell: And to go further, still, in pursuing this line of questioning, over the last number of days I've been asked this question many times — we read about it — how is it that if there are 90 returnees that you and others have alluded to, from fighting or some terrorist activity abroad, that they can still be functioning here in Canada in freedom? How is it that somebody whose passport has been taken back, as was the case with Couture-Rouleau, we can't secure that person more? If there are 90 people who you are following, what level of restrictions and monitoring can be brought to bear?

Are there gaps in your authority? Are community programs not broadly enough based? Is that outreach not working? I don't mean to be critical; I'm trying to get to the root and nature of the problem.

Mr. Paulson: Perhaps I could begin to answer your question. I will invite my colleague to weigh in, because it's an important question. Couture-Rouleau is a very good example of having the suspicion, having the instinct and intuition that his intention was to travel abroad to participate in jihad. Certainly that was the family's concern as he was radicalizing.

In a law enforcement response, we have to translate those misgivings, intuitions, thoughts and concerns into evidence that will permit us to make an arrest, bring a prosecution, and provide the evidence to a court to have a conviction.

The challenges are multi-dimensional in the sense that we need to have evidence of his intent. Never mind him for a second, but somebody else who has been abroad and come back and we have evidence that they did participate in some of these activities that were related to a terrorist group, so it's the transition from the apparent belief and suspicion to the hard-core evidence that is tangible, articulable and transferable to a courtroom.

Mr. Cabana: Actually, commissioner, it was very eloquent. I'm not sure there is much I can add. In terms of whether there are gaps in the tools that we have is actually the subject of analysis and review on an ongoing basis.

I can assure you that the RCMP and its security partners, including the rest of the law enforcement community in Canada, work consistently at identifying what those tools are and leveraging every tool that is at our disposal to try to prevent anything else from happening.

Senator Mitchell: This relationship between the preliminary work that CSIS does — and CSIS has told us that they follow people up to a point, and there is a threshold point at which the RCMP become involved — how is that coordination working? Would it not be more productive to have the RCMP involved earlier? Is there a strong coordination of those two forces or is that a place where there is a weakness?

Mr. Paulson: I would say that's a place where we're quite strong. We have been working on that since I've been in Ottawa, and we have gotten the relationship and the day-to-day operations between CSIS and the RCMP to a place that is very effective.
I understand you are going to talk to our colleagues in the Canadian Security intelligence Service. We continue to be challenged with the transition of intelligence into evidence. That is a seemingly intractable condition of our work, because on the one hand we would have intelligence that the service might have from other sources or from their sources and methods that cannot be revealed. It makes it a challenge to bring that intelligence, which may give rise to a very strong suspicion and belief into the criminal context, which requires a complete examination and exposure of the sources, to be able to weigh and test the nature and quality of that intelligence.

We have done a lot of improvements over the years in terms of handing off investigations, us being involved in the early part of the CSIS work, to be able to assist in informing the criminality that is arising to a point that requires intervention; hence, our 17 successful convictions, frankly. That has all been done through painstaking work between CSIS and the RCMP.

Every day we're sitting down with those folks, looking at our holdings and deconflicting our holdings, and we continue to work effectively. But I would be less than forthright if I said it was all blue skies and green lights. We have challenges with respect to transferring intelligence to evidence.

Senator Stewart Olsen: Thank you for coming. After the events on the Hill and being at home this weekend in New Brunswick, we live in a country that people are not accepting of acts like this. One of the things that was very clear to me when I stopped at the War Memorial this morning is that people want to know what they can do to assist. They don't expect our security and police services to do everything. You did mention something about ramping up programs so that Canadians can help, but if you could give some idea of what they can do, because overriding our meetings in this study is the security of Canadians and protecting Canadians. I know that's your overriding principle as well.

Mr. Paulson: Thank you for that question. Let me begin by saying you're absolutely right that a key solution to our challenges lies within our communities. What I mean is what I mentioned in my opening comments, which was encouraging and having people in our communities confident in referring changes in behaviours, unusual developments and suspicious circumstances to police.

I will use the analogy of a parent who is concerned about a child's drug use. They recognize that there is a problem, but they're reticent, and understandably so, to bring that forward to the police because the police response will be understood as an enforcement action on that drug use. We need to persuade Canadians and to develop their trust such that the problem of a significant change in behaviour giving rise to misgivings about a person's radicalization needs to be quickly identified to the appropriate authorities. We have a very effective network of law enforcement across this country, not just the RCMP but municipal police forces and provincial police forces, which are informed and ready to be able to manage that response. I think that's where a big chunk of the answer lies.

Senator Stewart Olsen: Having gone through the whole situation in Moncton as well, New Brunswickers are very concerned and wanting to help prevent something like that from happening again. They have identified, though, that they don't know quite how to go about it.

Do you have something in place that is easily accessed and perhaps secure for them? Of course, there's always a fear if you tell the police or whatever. They will need some specific information about how to get a hold of you, how to report and also perhaps that list of what you should look for. I'm just hoping that you will be able to reassure me that you're thinking of how to put this all in place.

Mr. Paulson: Certainly, we're thinking about it, and indeed, much of it is already in place. One of the features of our countering violent extremism strategy is every police force across this country has effective access points for the community to reach in on matters of prevention and matters of interventions. One of the things that we're doing is using that infrastructure, if I can refer to it, to overlay the national security response.

We also have several other programs that I've referred to in other appearances. Our front-line counter-terrorism information officers bring those pre-attack indicators and suspicious behaviours not just to the attention of police officers on the front line, which is vital to have, but also into the community so that people understand what it is they're seeing, what it might mean. It's one thing to say, "Johnny is behaving in
a strange way." It's another thing to say that strange behaviour requires some steps beyond those that I can provide as a parent, a friend, a colleague or a neighbour.

Senator Day: Commissioner, gentlemen, thank you very much for being here. I support all the comments that have been made in relation to our support for the men and women in uniform. I hope you will take that back to the members of the RCMP, that we're fully supportive. The questions we are asking will hopefully be helpful. Both of the points that I wanted to follow up have already been touched on.

The first one, commissioner, is the relationship with CSIS. I think it can't be over-emphasized the importance of the transition from the intelligence investigation that CSIS does and the criminal investigation that you do and the relationship thereof. We don't want two solitudes here. I heard what you said and your answer. I'm going to assume that you feel that things are flowing nicely, but I will ask the same question of CSIS when they are here in that regard.

You may comment on that if you like, and if there is some investigation or study going on to make sure that flows, I would be reassured by that.

Mr. Paulson: Let me take a quick second to say that for the last seven or eight years, I personally have been involved with colleagues in recognizing the importance of that relationship, recognizing that in this context, everything that we do, every piece of information that we have in the national security business, CSIS gets. We are continually making sure that they get all of our information.

In terms of getting the information from CSIS, as I mentioned in my previous answer, we need to be particular and purposeful in how we take that information from CSIS to build our investigations. We will continue to and often do run parallel investigations, not tripping over each other. We have accomplished some significant breakthroughs in terms of relying on each other's equipment and relying on each other's authorizations lawfully. We have come quite a long way. The relationship with CSIS is very strong, sound and functional.

Senator Day: Thank you. The other area Senator Stewart Olsen touched on, and I would like to re-emphasize, all of us here have returned to our regions across Canada. I happen to be from the same province as the senator. Our communities are smaller, and most of the people I have talked to can't understand why someone who is starting to change his or her attitudes and is starting to say things that are worrisome, why that can't be brought to your attention. You're doing in many of the provinces as well, and hopefully all of your officers doing either national or provincial work will be trained the same way.

It seems what we're seeing now is not necessarily an ideological driving force but someone who has an emotional or mental problem and is focusing on people in uniform to vent that hatred that has developed. It seems to me that the ideological aspect of this is an adjunct to looking for some place to hang your hat and say, "I'm doing this because of this."

So it's the importance of being able to monitor activity that could develop into something very serious, like we've seen. With that background, could you tell me what your counterterrorism information officer and that newly created position is doing along those lines?

Mr. Paulson: Maybe I'll invite my colleague Deputy Commissioner Cabana to speak to that. I've mentioned some of it. We have the countering violent extremism program that we are, as we speak, rolling out across the country. We have other programs that pre-exist and are being supported and have been quite successful in many regards. I will ask Mr. Cabana to speak to that.

Mr. Cabana: Thank you, commissioner. Senator, as Commissioner Paulson mentioned, there are a number of programs; the most recent one being the countering violent extremism strategy that has been implemented, which seeks to provide front-line enforcement resources from other agencies, but also from the RCMP, with the necessary tools and know how to be able to identify if they are potentially dealing with the onset of radicalization but also how to deal with it.

There are many different components to it, but I would say one of the key components is the creation of community hubs, which engage a number of different specialists from different fields, such as health and
social services, that come together once cases have been identified and develop a custom tailored approach to each individual in an effort to provide them with the necessary support in order to change their way of thinking, if you want.

Mr. Paulson: In other words, if it’s, as you mentioned, a mental illness issue perhaps or a drug addiction issue, compounding and interfering with the ability to get that person off the road of violent radicalization, then we will bring in and assist people at brainstorming, problem-solving and providing professional support to get to the heart of the matter.

Senator Day: I’d like you to comment on whether you have the sufficient resources and legislation to do just that, the intervention and preventing it from getting worse.

Mr. Paulson: As I’ve said — I’m not sure if I said it here or not, but I have said it in other places, current circumstances are requiring that we move our resources around within federal policing, and we’re bringing all the resources we need to do this and it’s getting done. What’s happening is other areas of our responsibilities and our mandate are being impacted, perhaps in organized crime or in financial integrity matters, but we have the resources that we are devoting to get this up, running and effective.

Senator Ngo: Thank you, commissioner. You mentioned you have about 90 or 93 high-risk individuals who have been identified, who have left for abroad and have come back. Those are the high risk. Do you have anything like medium risk? If you have medium risk who supports or associates with radical Islamic extremism, do you have a list and do you have any idea how many people are on that list? Can you characterize what “medium risk” means?

Mr. Paulson: Thank you for that question. You’re referring as I mentioned before, to our high-risk travellers program, which is now a task force, where I had recently identified 93 individuals as having been listed as high-risk travellers either from individuals who want to go abroad or who are abroad and want to come back. We are investigating that and we are managing that, and in fact, we are working with our partners at CSIS in a daily re-evaluation of that.

Let me talk about that other group of individuals, let’s call them high-risk individuals, who for one reason or another we have a basis to suspect have taken the path towards radicalization. We have a number of those individuals as well. What we’ve been doing in the recent past with the service has been going back over all of our holdings, all of them. We have sort of recast and re-evaluated the basis upon which we have come to understand the threat posed by these individuals; and with our partners across law enforcement in Canada, with the service, with us, we have made sure that the evaluation of the threat on those people is articulated and is responded to in a way that gives us confidence that the threat posed by the individual is being responded to by either the intelligence service, the RCMP or the partner police agency.

Senator Ngo: Thank you, commissioner. If that’s the case, how do you approach them, the so-called medium risk? I’m talking about not the 90 high risk you mentioned? How do you approach them? Do you seize the passport or what are the steps you have taken in order to evaluate the medium risk; and if there is, do you face any other radical Islamic extremists in Canada?

Mr. Paulson: The way we assess the risk is on the basis of reliability and accuracy of either the intelligence or information that is bringing them to our attention in the first place. There is an evaluation process that is applied. Who are these people? What is it that is being said they are intending to do? What is the nature and quality of the evidence and intelligence giving us an indication of what they intend to do? Then we will classify them as requiring immediate response, perhaps, in terms of a criminal investigation that is featuring wiretaps, surveillance; perhaps even, if it’s manifest enough, an arrest and charge, all the way down to surveillance, to intervention for an interview, to perhaps an intelligence file for the service. The seizing of passports or the application for a revocation of passport is one of numerous tools that are available in this sort of non-charge space.

The ideal condition for me, the simple country cop, is we’ve got evidence, we bring this person under arrest, we bring him to court, charge him and convict him and deal with him. That’s how we would like to roll.
There are a number of cases, as I have been mentioning, that fall short of that, and so we have to have a strategy to intervene, surveil, acquire more evidence, intervene, prevent, as well as detect and prosecute. That's in a nutshell, our strategy.

The Chair: Could I perhaps go further on that question? At the outset we talked about wanting to look at the magnitude of the public threat that Canadians are facing. We've been told, and you have been very transparent and clear about this, there are 90, 93 travellers. It moves, it is fluid.

What I'd like to get at is, below those travellers, the high risk, let's go down to that medium level or even the lower level. What are we talking about in magnitude of individuals involved in this type of ideology, this type of mindset? Are we talking 300, 500, 1,000 people that between the RCMP and the CSIS have been identified so that eventually as they become more involved then they become high risk? They have to be identified at the beginning, so perhaps you could expand on that.

Mr. Paulson: I don't know how useful it is to understanding the threat to have a number assigned to that. Just for an order of magnitude, frame of reference, we can talk about thousands of police occurrences where people will have identified individuals who will require a response.

Those would be from "I don't like the look of that person I saw on that bus today, really looked shifty" to "I was in the bar last night and I heard this person plotting to blow something up" to "got pictures of this person putting together a plan." That's the range.

I think that, again, it's not particularly helpful to understand the magnitude of the threat, because as we go through the events, such as the terrible events that we have just gone through in this past week, people's interest spike and we begin to get a lot of "don't like the cut of that person's jib on the bus this morning," but we are talking as an order of magnitude in the thousands.

Senator White: Thank you for being here today and congratulations to your members in managing both incidents last week, one as a secondary but one as a primary and thanks for that. Also, thanks for the transparency you showed. I think it was helpful to people living in the city to see you show the videos and explain the circumstances.

My question is going to speak a little bit, Deputy Cabana, if you don't mind, you talked about the radicalization and the shape and a little about the perspective even around the New Brunswick incident is some form of radicalizing of someone's ideology, which isn't what we think about when we think about radicalization. We often hear about the Internet and how it allows people to become radicalized, but we also hear, if we look at the Toronto 18 case, circumstances around radicalization happening face-to-face often in institutions in this country.

Do you have the tools to manage those face-to-face encounters from an ability to stop some of the activity happening that does take someone who is at risk mentally, drug induced or others, stop those individuals from radicalizing the people that we are seeing committing the acts, or do we need to step forward and start having changes in hate legislation or something else that allows us to attack those individuals? I can't repeat the question. I apologize.

Mr. Cabana: No, I don't think you need to. It's not an easy question to answer, whether we have the necessary tools to be able to address that issue.

Of course, first and foremost, it's important for us to have the knowledge that the issue exists in the first place with respect to certain individuals. I would say that when we have that knowledge and the individuals are brought to our attention or identified for us, whether the discussion occurred face to face, if you want, or even over the Internet, we're leveraging the tools we have to the extent that we can.

Unfortunately, as we saw in recent events, the ability -- I'm not sure what kind of tool we would have to have in place to be able to prevent all kinds of incidents like the ones we saw last week, especially if the planning behind the incident is done just by one individual with very little collaboration from anybody else.
I realize I probably didn't provide the answer you're looking for, but I can't think of a tool that would actually allow us to make sure that there will never be any other incident.

Senator White: Have we successfully prosecuted anyone for successfully radicalizing someone else in the country? Is there a prosecutable offence?

Mr. Paulson: Yes, there is.

Mr. Cabana: There is. We have not, but yes, there is.

Senator White: So we have the tool from a legislative perspective?

Mr. Cabana: Yes, we do.

Mr. Paulson: That's right. In fact, not just these recent events, but that's a focus of our concern in the follow-up investigation, particularly in the Ottawa event, is to satisfy ourselves that there is no one behind this character. Were we to have the evidence, we would certainly bring a prosecution or a charge against those individuals — not just asking community members to give us indicators of people's behaviours but asking people to give us information about people who are leading this radicalization effort, because some people are vulnerable and some people are being taken advantage of and some people are taking advantage of these people, and those are high-value targets, in my mind.

Senator Kenny: I have three areas I want to touch on.

The first has to do with cooperation with CSIS. Your organizations have different objectives. For some time we've had the impression that the objectives would be at cross purposes. If you want to collect evidence and prosecute somebody, and they want to collect intelligence and keep on collecting intelligence, from the way you described it, you make it sound like everything's working well there. My impression is that this is a constant debate and that's a challenge.

Mr. Paulson: I would agree with you, Senator. You will recall my misgivings about our abilities to transition intelligence to evidence. Let me give you a real, concrete example of where we, in the police, have taken steps to contribute to a much more effective relationship, and that is in the case of these boats that were trying to come to Canada. We have shipped officers shoulder to shoulder with CSIS and other agencies of the Government of Canada abroad, and we had to demonstrate and say, "Let's, we're not going to wreck everything by insisting that we manage everything towards a prosecution. We're going to help get to prevention." Prevention is equally our mandate, as is enforcement.

It's taken a little bit of a culture change within our world, which I'm proud to say that we've accomplished in that sense. But there is still work to be done on the broader sort of issue of that intelligence to evidence.

Senator Kenny: Did I understand you correctly through an earlier question saying that you saw no further need for legislation to enhance your ability to do your work?

Mr. Paulson: No, I didn't say that.

Senator Kenny: Were you close to that? The question came up with Senator Day about what sort of tools you require, and he was referring, I believe, to legislation. If you didn't say it, could you tell us what tools you do need in the way of legislation?

Mr. Paulson: I think that is being examined as we speak in terms of what some of the options would be. Frankly, generally speaking, I am of the view that in some areas we need to be able to lower the threshold and perhaps include some steps, for example, getting consent from the Attorney General in respect of bringing a peace bond against a national security target. I think that the thresholds for belief of either an offence being made or an individual being involved in that offence need to be lowered to a reasonable suspicion as opposed to a reasonable belief. There are some things that need to be addressed in the short term, and they've been identified and certainly we've raised them. Hopefully we'll be able to see some — it has to be balanced, of course, as you will know, senator. It has to be balanced against Canadians' rightful
expectation that they’re free and that they’re safe from the improper application of police powers. I think there is a balance that can be reached there.

Senator Kenny: Finally, resources. You gave the impression — at least I got the impression earlier — that you were happy with the financial resources that you have. In light of the fact that the budget of the RCMP has been decreased 15 per cent over the last three years, I can’t understand how you’re okay. I know about the efficiencies that you’re creating in headquarters, but it just seems to me remarkable that we’re in this state of affairs and we’re cutting back on the budget of the police.

Mr. Paulson: Senator, I prepared to come and speak with you here today. One of the things I did was review the testimony of other people who have appeared before you. Let me put it this way: We’re doing what we can with what we’ve got.

Senator White: I guess a little bit on the discussion around mental illness and radicalization. I gave an interview last week with a CBC reporter who tried to suggest somebody who was mentally ill couldn’t be a terrorist or couldn’t commit a terrorist act. Just to clear the air — because a couple of people have jumped on that again this weekend, in particular in relation to the Individual in Quebec — your perspective on the fact that a mentally ill person could commit a terrorist act.

Mr. Paulson: I’m not a psychiatrist. I understand mental illness and I understand the ravages that it can have on families and people. Certainly when it comes to some of the purposeful, deliberate, considered, premeditated actions that flow into some of the things that we’ve seen recently. I’m not persuaded that mental illness drives these things. What’s driving these things is a distorted world view of what’s happening around these individuals perhaps coming to fruition on the back of somebody who has some mental challenges. But they are entirely distinguishable, in my estimation.

Senator Beyak: Thank you very much, gentlemen. You have our admiration, respect and gratitude. Like Senator Stewart Olsen, all weekend I heard from constituents that we live in a great nation, and they want to keep it that way and do their part.

I have a three-part question about the 93 travellers. People wonder how many of them, if all or a majority, are what are commonly internationally known as radical Islamic jihadists extremists. If that is the case, how often are they travelling? How are they getting back? Do we need more tools to prevent them from coming back? Is this war more than a criminal court due process thing?

Mr. Paulson: Thank you, senator, for your comments at the outset of your question. I guess I would say that it’s my view — and I would defer to my colleague to my right in terms of these individuals. Again, we’re just talking about the high-risk travellers. I would suspect at varying levels of belief, all of them have some indications of radicalized behaviour. That’s the first thing.

How often are they travelling? We are endeavoring to make sure that they not travel. But that’s not the objective, because I think there is a reasonable analysis that flows from stopping one of these radicalized individuals from travelling, but you better be ready to do something about that when you stop them.

So we’re very concerned, as are our partners at CSIS, about individuals who come back from the war zone, from the terrorist activity abroad, with these skills and this mindset that they have acquired over there. That is an area of focus for us.

I must confess that I don’t remember the third part of your question.

Senator Beyak: The third part was how many of them are born here to radical Muslim parents or are Canadian citizens, dual citizens, visas, temporary?

Mr. Paulson: We do have that data. I don’t know that I could provide it to you now. We do know that I would say most of the individuals are Canadians. Let me defer to someone who does know with a little more confidence.

Mr. Cabana: Thank you, commissioner.
Senator, there is not one profile of someone who is been radicalized. A significant percentage are Canadian, a good percentage of whom were born in Canada. But not all of them — actually, very few of them — were born to what you term “radical parents.” Radicalization occurs often outside the family unit.

Mr. Paulson: As I indicated in my comments, the most troubling and offensive element of these recent attacks is that they were both Canadians.

Senator Beyak: Thank you very much.

(French follows — Le sénateur Dagenais: Merci à nos trois invités ...

[après anglais]

Le sénateur Dagenais: Merci à nos trois invités pour leur présence aujourd'hui.

Dans un premier temps, j’aimerais féliciter toute votre équipe pour l’excellent travail qui a été fait les semaines dernières. Ayant été moi-même policier pendant plusieurs années, je comprends les difficultés auxquelles on peut faire face lors d’événements semblables.

J’ai deux questions, que je vais vous poser en anglais.

(Sen. Dagenais: For the sake of clarity, was ...

[anglais suit]

[Following French — Senator Dagenais contd after: ... poser en anglais]

For the sake of clarity, was Martin Couture-Rouleau under national security criminal investigation by the RCMP? Can you advise the public when the video of Mr. Zehaf-Bibeau will be released so that Canadians can make their assessment pertinent to this attack?

(French follows — M. Paulson: Je vous remercie ...

[après anglais]

M. Paulson: Je vous remercie pour vos questions, sénateur.

(M. Paulson: Couture-Rouleau was a subject...

[anglais suit]

[Following French — Mr. Paulson contd after: ... pour vos questions]

Couture Rouleau was a subject of a national security investigation. I think we have been fairly forthright in describing that; and I don’t know that there is much more to add. We have tried to sort of depict the challenges in that investigation in terms of what our actions were, how we intervened and how we worked with the family and others, meeting with them as recently as October 9, prior to this attack. He was the subject of a criminal investigation, and had we had sufficient evidence to charge him, we would have charged him.

The video on Mr. Zehaf-Bibeau is being analyzed right now for its intelligence and evidence value. We are all interested in getting that before the public, but we’re interested in making sure that we have secured and are confident in its intelligence and evidence value. I don’t know when it’s going to be released. It will certainly be released someday, but I would be a fool to say when it will be released. I am inclined to overcome those challenges and get it released as soon as possible.

Senator Dagenais: Second, how would you characterize the level of monitoring applied to Couture Rouleau? Was it equivalent to that of the other 89 persons suspected of terrorist activities or sympathies that you are currently monitoring?
Mr. Paulson: I would say this about Couture Rouleau: We had a number of individuals in our national security investigative team personally engage with him and his family in frequent, if not constant, contact with family members. It was very aggressive in terms of trying to engage and monitor him. How would I characterize that against other individuals we are monitoring? It goes, as I said earlier, to the evaluation and assessment of the threat that the individual poses. It would be no surprise, and hopefully Canadians would understand, that there are individuals we are monitoring continually to try to get evidence that they are doing criminal acts; there are individuals that we have just learned about and are assessing; there are individuals that we have spoken to; and there are individuals that we have succeeded, in our view, in turning around. There is a complete range of activity.

Although it ended very badly with respect to Couture Rouleau, the officers in particular, and Mike would know better than I, were horrified — horrified — that things had happened, as were all Canadians. They were heavily invested in this man, and we're rethinking all of that.

Senator Mitchell: I would like to pursue the point you made that you've reallocated, I think you said, 300 people. I don't know what each one of those people makes, but if you made a rough estimate you're talking about $25 million. It sounds to me, one could argue, that you need them. You have allocated them, and you are $25 million short, not to mention what you might need for better community based intervention to solve the problem before it occurs.

Bluntly asked, do you have the resources? How long will you need those 300 people? Where will you find the money to sustain that?

Mr. Paulson: Frankly speaking, one of the challenges in managing and leading a police organization is that you never have enough money — you never do. I will never have enough money. So what's your strategy? Get more money or manage effectively with what you have, and make periodic appeals for more money.

Given the threat, what's happened and how it's developed, I'm satisfied as we continue to check daily our ability to move resources from one area of our operations to another. If we were blue-skying how we were going to increase our resourcing, for example, a lot of things would have to be put in place. We just now have our recruitment and depot training system and all those elements operating in a very finely tuned way, so we need to be thoughtful around how we're going to approach that if there is a need to ramp up.

I didn't come here to get resources. I came here to help understand the nature of the threat. We are going to make decisions; we have made decisions; and we will continue to make decisions on moving resources to respond to the greatest threat to the safety of Canadians. That's sort of my mantra.

Senator Kenny: Commissioner, the government is going ahead with the building of a $50-million visitor centre here on Parliament Hill. Have you or has the RCMP been consulted about it? Are you satisfied that it will address the problems that exist now, such as people being searched for the first time right under the Peace Tower and those sorts of things? Is it going to be a plus from a point of view of security?

Mr. Paulson: I don't know that I'm in a position to give an answer to that.

Mr. Cabana: Not to the level of detail that Senator Kenny is looking for. There have been preliminary discussions with us so I know that we're engaged. In terms of knowing what impact it will have on the security posture on the Hill and checking people, unfortunately I can't answer that.

Senator White: Commissioner, you mentioned the possibility of removing a step for approval on peace bonds to the Attorney General of Canada. Have we had a problem with the Attorney General refusing peace bonds or is it just the timing?

Mr. Paulson: No. It's the preparation and the amount of extra work required to accomplish that. It seems to me that the Attorney General's consent in most of our national security investigations and charges is well thought out and properly placed. In respect of these peace bonds, there is an argument to be made that cops can handle that.
Senator Day: Someone reading the transcript of this hearing or watching it on television might come to the conclusion that the term “radicalization” relates only to religious-based radicalization. You indicated that it is a term and an offence under the Criminal Code. I don’t have my Criminal Code here but maybe you can give us a brief understanding of “radicalization.”

Mr. Paulson: It’s probably laid out differently within the code. When we talk about radicalization, and don’t let me be too elementary, there is no crime in having radical thoughts. It’s the act of moving someone into doing something violent or in support of a terrorist activity that attracts our attention. The radicalization phenomenon is sort of recognized as being an individual who has maybe strong or contentious thoughts or those that are not in the mainstream, and that’s generally no crime. It’s moving that radical thought into an area where you begin to act and move towards violence, which is where we kick in.

It’s probably no surprise or shock to anyone that there are individuals who would be developing and exploiting people’s weaknesses at radicalizing their views and bringing them along. Even that, in terms of some areas, is not a crime. The moment they begin to advocate for violence then that’s a very serious engagement on the terrorist offence.

Senator Day: Thank you. I think that will be helpful.

Senator Beyak: I don’t mean this question to sound critical in any way. I want an understanding of something I don’t know.

I worked for the last five years with very moderate Muslims in the United States and Canada. I don’t think I can say their names, but I was a little appalled and glad that you repudiated the handbook, United Against Terrorism, but there were some pretty radical Muslim groups that were part of that book and I wondered how we were associated with them and why. I’m glad that you repudiated it and, if you’re going to take a stand, would you explain a little bit why you were associating in the first place with them?

As I said, I don’t mean to be critical, but I just didn’t like the book at all.

Mr. Paulson: I’m used to being criticized.

In respect of that pamphlet, first, it needs to be said that in terms of our prevention activities we need to engage and hang out with people of all different ideas and all different activities. While I did make a statement with respect to the ultimate pamphlet that was produced, our chapter within that pamphlet is pretty solid and I stand by what we had to say about our role and how we respond to the threat. It’s unfortunate that I had to ask that we not put a public aspect to an announcement of that. But really, when you look at our chapter in that book, we stand by that.

Senator Beyak: There’s talk that three of the groups were unindicted co-conspirators in radical Islam. Do you have any comment on that or did you have any knowledge of that?

Mr. Paulson: I’m afraid I don’t know what you’re referring to.

Senator Beyak: Okay, thank you.

The Chair: I have one question on the threshold of the legal framework we presently work under and that we could in some areas lower it to allow you and your force to do the job we ask you to do.

Right now we have 93 individuals, as I understand it, and Canadians have heard that 93 individuals out there are under some sort of surveillance, or at least identified that they could be of some violent consequence to the general public. If we were to lower the threshold in a number of areas that perhaps you and other departments of the government could recommend, would that put us in a position where you as a law enforcement agent could perhaps constrain, restrain or detain these individuals for a period of time so that at least you have an opportunity to deal with this radicalization as opposed to trying to deal with it at the doorstep?

Mr. Paulson: Yes, that’s right. There are two areas where I think we could examine and discuss the lowering of thresholds. As we’ve talked about already, one in respect of the peace bond. After an
application to a court, the peace bond assigns conditions to restrict the movement of an individual, have them account perhaps, have them report or have them do this or have them do that. I think that's entirely reasonable.

Another area is in getting assistance from various corners of our communities and society, in terms of getting information. Information has become very difficult to come by. Privacy interests are very strong, and properly in many instances, but in getting information perhaps relating to Internet registration or getting information in respect of telephone numbers. The world is changing rapidly, not only in terms of the threat that we've been discussing but also in terms of the technology that people are using that we have to keep up with.

You've heard this lament perhaps before, but I think there is room to be able to discuss lower thresholds of assistance orders to individuals to provide information where it's reasonably suspected an offence has or will take place and where it's reasonably suspected that an individual is perhaps contributing to that offence.

The Chair: Commissioner, I appreciate your giving us the time you have. We felt it was an important enough issue for Canadians that we should take as much time as we can.

I want to thank you and your colleagues for appearing. Obviously this is a committee you're familiar with and I'm sure we will be seeing you in the future. Thank you for doing the job you do.

As we continue our look at terrorist threats to Canada, we're pleased to have with us Michael Pelcxe, Assistant Director Intelligence, CSIS. I apologize for the lateness of our start. I know we were due to start at two o'clock, but, in view of events, you can see why it has taken a little bit more time. We appreciate the time that you have taken out of our schedule to be here with us today. I understand that you have an opening statement.

Michael Pelcxe, Assistant Director Intelligence, Canadian Security Intelligence Service: Good afternoon, honourable senators. Thank you for your invitation today to discuss the terrorist threat to Canada.

Mr. Chair, first, on behalf of the men and women of the Canadian Security Intelligence Service, I would like to express my deepest respects for Warrant Officer Vincent and Corporal Cirillo, as well as my condolences to their families, friends, and fellow members of the Canadian Armed Forces. We can assure Canadians that, though we, too, are deeply affected by these acts, we are firm in our resolve to protect Canadians and the security of Canada.

Mr. Chair, unfortunately, as Canadians now know firsthand, the threat posed by radicalized individuals, be they inspired by the Islamic State of Iraq and the Levant, which I will refer to as ISIL, Al Qaeda or other things on social media, is, as our director recently said, all too real. While I will not speak of the specifics of the recent events -- it's simply too soon for us to do that -- I will endeavour to address some of the questions that have been raised in the aftermath of those events.

Honourable senators recently heard from the service's Deputy Director of Operations, Jeff Yaworski, who is responsible for the service's human intelligence collection activities. As Assistant Director of Intelligence, I am responsible for the production and dissemination of intelligence assessments.

The service's intelligence assessment function is integral to the conduct of our investigations. In fact, our analytical work is increasingly integrated with our collection and operational activities. Just as my analysts draw on insights gained through the service's operations, those same analysts provide direct support to operations. These core functions of the service are mutually reinforcing.

Our assessments are also outward facing and strategic in nature. They enhance the government's awareness of the nature and magnitude of the threat, assist decision makers in their efforts to counter these threats, support the mandates of other domestic and foreign partners and identify gaps and emerging issues regarding the national security agenda.

Classified CSIS threat assessments are shared widely with partners such as the Royal Canadian Mounted Police, Canadian Border Service Agency, Communications Security Establishment, Citizenship and Immigration Canada, Public Safety and other government departments and agencies. The timely
dissemination of these assessments is critical as it enhances our partners' situational awareness and allows them to consider their response to any new developments or trends. To be clear, this is in addition to the operational cooperation between the service and its provincial, federal and foreign partners. I should also point out that the Integrated Terrorism Assessment Centre, ITAC, which is a community-wide resource housed within CSIS — and when I say "community-wide," I mean within the national security community — is responsible for producing integrated, comprehensive and timely threat assessments for all levels of government with security responsibilities, first-line responders, such as law enforcement, and, as appropriate, critical infrastructure stakeholders in the private sector. ITAC's all-source assessments are likewise shared so that measures can be taken to prevent and mitigate threats.

While my analysts produce assessments related to all threats to the security of Canada — cyber, counter-espionage, counter-proliferation — as you might expect, terrorism, including radicalization and terrorist travel, is our top intelligence priority. Though what we know continues to evolve, CSIS has to date found that radicalized individuals in Canada come from varied social backgrounds and varied age groups, tend to be educated and tend not to come from impoverished circumstances. I say that in contrast to the profile that we see from European radicalized individuals. They often at least appear to be integrated into society. Whether these characteristics apply equally to lone actors is an area of continuing study.

Just as the service has prioritized operations, likewise our assessment branch has mobilized all available resources and continues to work diligently with domestic and foreign partners to leverage all available intelligence against this terrorist threat. This is because, as noted, there is not one set of identifiable characteristics or behaviours amongst extremists. There isn't one profile that you can say, "This is it. If we had that profile, it would be easy to target those individuals in our investigations." Rather, we know the threat posed by radicalized individuals is diffuse and can materialize quickly. For these reasons, terrorism continues to pose a consistent tactical threat in Canada and facing Canadian interests.

One constant is the extremist narrative which holds that the West is at war with Islam. This narrative continues to exert a powerful influence. We are concerned about the emergence of new, more violent and radical groups such as ISIL, as it's clear that their violent and extremist ideologies are resonating, unfortunately, with some individuals within Canada.

The Internet and social media increasingly play a role in the radicalization of individuals, their mobilization to violence and the facilitation of threat activity, be that fundraising activity, recruitment, training or planning. We have also seen that extremists and their networks are resilient, adaptive and opportunistic. I want to assure honourable members of this subcommittee and all Canadians that CSIS is taking every step to identify terrorists and their activities, to assess the threat and to share information with our partners.

It's important to stress in this regard that CSIS is not an enforcement agency. We are not authorized to arrest, detain, revoke status or deny travel. CSIS does, however, support its partners who have their powers in their efforts to administer and enforce Canadian law.

While what we do and how we do it must remain classified so as not to jeopardize our ability to investigate threats to the security of Canada, by sharing advice or assessments with our partners they are able to take action in accordance with their mandates. In relation to our own authorities who have been the subject of much discussion, I respectfully request that the proposed measures recently announced by the government, which will soon be introduced — very soon — be discussed at a subsequent appearance. This is both to respect the parliamentary process and also to allow senators the opportunity to consider the proposed amendments. On that note, I will conclude my remarks to allow time for questions.

The Chair: Thank you, Mr. Pierce. We appreciate you coming here today. Once again, we apologize for the lateness of beginning the proceedings.

From your perspective, could you speak for a minute or two with respect to the magnitude of the threat that Canadians face? That is in part why we're having this study, namely to define what the threat is and to
look at what we can recommend in respect to confronting the threat and perhaps resolving some of the issues. Could you expand a little on that?

Mr. Peirce: To begin with, the magnitude of the threat, as the director and the deputy director of operations have both recently said, it is a very real threat here in Canada. It's a tactical and persistent threat. The scope of the threat is affected significantly by the travellers' issue, often referred to as foreign fighters' issue as well. I'm sure you've heard considerable testimony about the fact that 230, 135, 140 Canadians who have a nexus to extremist activity have travelled abroad. We have approximately -- and I say "approximately" because the number changes; we have concrete numbers but within 10 minutes the number could have changed because of a development out there -- 180 individuals who have returned. These are significant numbers and much more significant than the numbers we saw, for instance, during the late 1990s, early 2000s, where we had individuals travelling to the Afghanistan/Pakistan region. Those individuals returned to Canada and we had 10 years of counterterrorism work to do as a result. The numbers are far more significant today. As well, I think the nature of the threat is different. The ability to communicate through social media has changed that threat. It is more diffuse and it is able to change rather rapidly. It is a significant challenge for us which increases the threat.

There's been a lot of focus on the numbers; that is, the 130 to 140, the 80 returnees. We have to be careful not to be distracted by the numbers. In addition to the travellers' issue, we have existing and ongoing investigations into terrorist threats within Canada. That is, individuals who may not want to travel. There is that component of it as well. In addition, when we talk about numbers, there is always a definition tied to that particular number and we could parse the definitions differently. It gives you a picture of the idea of the volume of the threat, but we shouldn't focus too much on the numbers by themselves. The nature of the terrorism threat has grown; it is a real threat.

Senator Mitchell: Thank you, Mr. Peirce. Last week Mr. Yaworski wasn't Pollyanna about it, but he said Canadians are safe. Today Canadians probably feel quite safe, but maybe a little less secure than they did prior to last Monday. What are you doing or thinking about doing today that, a week ago yesterday, you weren't doing? Have you tapped or changed your game in some way as a result of the realization of these threats last week in two cases?

Mr. Peirce: The first thing we have done, and I think it is a natural reaction, is make sure that you have been doing already has been done well and that you're not missing anything. As a result, everyone takes their files and goes over them as carefully as possible. We've been working 24-7 to do that to make sure there isn't something out there we're missing that wasn't apparent in our files.

We have shifted both operational and our assessment resources to make sure we can give that kind of coverage, both as an immediate response and then doing so on an ongoing basis. Frankly, it's the nature of our organization that we have to be nimble. We have to be able to respond to changing threats. We have seen an increase in threats in a number of areas, so it's not just the terrorism area that we have to address in that regard.

Senator Mitchell: You use the word in the context of ISIL, of how it's possibly resonating, in Canada. I'd like to have you assist us in qualifying that in the sense of resonating. Would it be that there is a specific, coordinated effort on the part of ISIL to send agents or to recruit them in a place like Canada to develop a coordinated plan of attack? Or is it more that they're through the Internet and the news media, and just the fact that they're doing what they're doing that somehow captures the imagination of people who are vulnerable to radicalization or have other problems?

Mr. Peirce: ISIL first and foremost are focused on the area in which they are at war. That said, the Internet is a very effective recruiting tool and it is the number one tool for recruitment and radicalization. That is one of the differences we see whereas in the late 1990s, early 2000s, individuals who went to Afghanistan or Pakistan to train had to come back to Canada to radicalize individuals. They were in relatively small numbers, as I have indicated, so it was a much more contained message. Now you see it all over the Internet. You can go on YouTube and see things that you ought not to spend too much time watching, frankly. There is a serious aspect that way.
As well, because we have a number of Canadians — approximately 50 or so in the Syria, Iraq area -- who have travelled there and individuals who have come back, they both bring with them the ability to radicalize. When they come back, in particular, they have tremendous what we call “street cred.” They come back and they’re the cool kids. Kids want to listen to them, and that has an impact. They can do that from Syria and Iraq. They can run a website and send out Twitter messages from Syria and Iraq and have that impact, but when it’s in person it has that much more impact.

It’s not so much a matter of a planned attack by ISIL. We don’t have a clear, developed plan of attack against Canada by ISIL. What we have are individuals who are being radicalized and encouraged to action.

This isn’t an entirely new activity. Certainly under al Qaeda in the Arabian Peninsula they used to put out a magazine called Inspire. You may have heard of it. It encouraged lone actor attacks the same way ISIL has. What’s different is this has happened in Canada now.

Senator White: Thank you very much for being here, sir.

My question is going to talk quickly about the information that came out a couple of weeks ago surrounding nuclear power plants. My understanding is the Canadian Nuclear Security Commission advising nuclear power plants to tell people living within a certain area that need to be prescribed with iodine tablets. I’m trying to get my head around if this is a warning from CSIS and if so, why there wasn’t a broader discussion. I know in relation to the Darlington, Pickering nuclear power plants the police service wasn’t engaged in any discussion about a possible threat and whether that came from CSIS.

Mr. Peirce: The assessment of threats does come from CSIS on a number of levels and a number of ways. We share with our government partners. We don’t have the mandate to advise the private sector. As to a specific threat to the Darlington station, I don’t believe that that was direct advice from CSIS.

We provide advice, as I said, to the Government of Canada and that advice may have gone on.

Senator White: I used to meet with the Canadian Nuclear Security Commission regularly and they receive information regularly from CSIS. My question surrounds the local police service jurisdiction, the Durham Regional Police Service, which is 1,300 strong, receiving no advice from anyone in relation to that same threat, then that’s a concern of mine. Local police agencies are the ones who will respond to the call, as we saw last week at least in part here on Parliament Hill and just off Parliament Hill. Is there a thought that information should be shared more broadly with police agencies that will respond to those calls instead of them hearing it from, I think it was, CBC that actually reported on it?

Mr. Peirce: I can’t speak again specifically to that particular situation, but I can say that ITAC, the Integrated Terrorist Assessment Centre, does provide threat assessments to first responders, including the police. And generally speaking, I would expect that if threat advice was provided in regard to Darlington station that it would have been provided to the local police as well.

Senator Stewart Olsen: Just to continue a bit on the provision of threat assessment warnings, ITAC was originally conceived as a service that would provide the threat warning requirements to a range of clients, some of which operate at a non-classified level. Can you give me some idea of what the difference is between classified and non-classified? How many would be non-classified?

Mr. Peirce: I don’t know the exact numbers, as to how many would be non-classified. The bulk of individuals or organizations receiving intelligence either from ITAC or CSIS will be receiving it at a classified level.

There are sometimes difficulties in their holding the intelligence. They may not have appropriately secure facilities for holding the intelligence so they may receive it in a written form that’s at a non-classified level. The bottom line threat message will be consistent whether it’s at a classified or unclassified level. The difference will be in the detail that can be given.

For instance, if you’re providing unclassified threat advice, you will endeavour to obscure your sources so that you can protect those sources.
Senator Stewart Olsen: If I might just follow up, you say your client base. Does that extend beyond the federal government and selected law enforcement agencies? What is your client base?

Mr. Peirce: For CSIS, formally and officially, our mandate is to advise the Government of Canada. We will share, with foreign partners for example, and the purpose of that is to ensure that they're informed and can help protect Canadian interests. Obviously, it helps us if they are well enough informed. We will also share on what's called a give-to-get basis. We need to get information, and often to get information we have to provide some information. We will share in that way.

ITAC does have a broader mandate for sharing of their assessments and it does include, as I said, first responders, provincial governments; it does include local police forces. It's a broader base in that respect.

Senator Stewart Olsen: Basically, when you say first responders, fire departments, ambulance, it is not just law enforcement; ITAC would make a decision as to who should be informed, depending on the threat?

Mr. Peirce: Absolutely. Whenever you are disseminating intelligence, one of the things you have to make a determination as to who should be receiving that intelligence and ensure that it gets into the right people's hands.

Senator Day: ITAC is integrated terrorism and you say assessment or analysis.

Mr. Peirce: Analysis.

Senator Day: I hear both. It was a threat analysis centre previously described. Have you restricted your activity for financial reasons or just because terrorism is one of the threats that is most important from your point of view now?

Mr. Peirce: To be clear, I'm not the head of ITAC. ITAC is an independent organization but we work very closely together. The mandate of ITAC was changed a few years ago. Now the organization is 10 years old; it's just celebrated its tenth anniversary. It was changed simply to focus that mandate on terrorism. That is, I should say, consistent with what we see among our international partners. The Brits have ITAC; the Americans have NCTC. They're terrorism focused.

Senator Day: I'm hearing both. Are there other threat assessment focused entities in Canada or the Five Eyes, for example, the other countries that we share a lot with that deal with other types of threat assessment that we participate in and that CSIS is part of?

Mr. Peirce: We do, but the others are generally structured in the same way that CSIS is, which is that we cover the broad range of threats. There aren't necessarily bodies that are targeted specifically to the national counter-proliferation centre.

Senator Day: Cyber-threat, for example.

Mr. Peirce: Cyber-threat; there are different parts of the federal government that deal with the cyber-threat; the Communications Security Establishment, CSIS, and Public Safety all.

Senator Day: Where is that Integrated Threat Assessment Centre located for cyber-threat?

Mr. Peirce: There isn't a single, integrated centre for it. Each of us has a piece of the responsibility, but we work all very closely together and are closely integrated in that respect.

Senator Day: I wanted to clarify your point earlier about ISIS and International Islam suggesting that or encouraging single terrorist activity, one-person activity. You are not suggesting that all of these one-person terrorist activities that we are starting to see a bit of here in Canada and some in the United States are all ideologically based as opposed to other types of focus for these individuals. Maybe they have a personal reason to remove them.
Mr. Peirce: I think it's a very important point that you're making, senator. We should not jump to conclusions about the drivers. It's actually very difficult, as I'm sure you know, to determine the threshold factor that motivated an individual to violence. We should be very careful in reaching those conclusions.

In saying that, I'm not speaking at all about the two recent events. I really don't think that this is a moment for us to do that and certainly not for CSIS to do that.

Senator Day: My question wasn't specifically on the two recent events either.

Senator Beyak: Thank you very much for your excellent intelligence work.

I asked a question of the group that was here previously, the RCMP, and I'd like to ask a similar one of you.

Mr. Peirce: Did you get a good answer?

Senator Beyak: I did.

Mr. Peirce: That's what I wanted to know.

Senator Beyak: Canadians are tolerant, welcoming, open-minded, flexible, and I've worked for years, since 2008, with moderate Muslim groups and Muslims in Canada and the United States. But there is a concern amongst Canadians about the term "radical Islamists" and the RCMP said that 93 of their travellers, the vast majority are associated with what is commonly known internationally as the radical Jihadist Islamist state, ISIS. Could you tell me how many individuals you follow who are radicalized and what your concerns are, and if you have the tools to do it effectively.

Mr. Peirce: On the first part of the question, while we have talked about traveller numbers, one of the things we haven't talked about and we hold very closely is the number of targets of investigation that we have. That remains classified information. I wouldn't go down that road.

Senator Beyak: I was afraid of that.

Mr. Peirce: In terms of the tools that we have, that does lead us over into events that are taking place momentarily, which is some new legislation I believe that is being introduced. We will see some developments in that area. Certainly they are welcome developments but we'll await a subsequent opportunity to speak to those.

Senator Beyak: Thank you very much. I thought it would be classified, but I had to ask.

(French follows - Le sénateur Dagenais : Monsieur Peirce, je vais avoir quatre questions pour vous, si le président m'en donne la permission.)

Le sénateur Dagenais : Monsieur Peirce, je vais avoir quatre questions pour vous, si le président m'en donne la permission.

(Sen. Dagenais: That's a very short question ...) 

(English follows - Senator Dagenais continuing - n'en donne la permission.) 

That's a very short question.

The Chair: If I could do it for Senator Day, I could do it for Senator Dagenais.

Senator Dagenais: I will begin with two.

Senator Day: I began with one.
Senator Dagenais: Mr. Peirce, thank you very much. Thailand has been going through political turmoil for the past five or six years. Could you provide us with an overview of the current situation in the country now?

Mr. Peirce: There's going to be follow-up to that, too?

Senator Dagenais: Would you like to have the other questions right now?

Mr. Peirce: I think that I should be very cautious about speaking now. A country, first of all, and their particular circumstances. Certainly, there's been a difficult past there that we are aware of and we have seen progress in some areas.

The threat certainly has not been eliminated in relation to Thailand and it is an area of ongoing concern. Beyond that, as I say, I should be cautious about my comments.

Senator Dagenais: What are the prospects for a stable solution?

Mr. Peirce: With caution, what I'll say is this: I am optimistic about progress that has been made.

Senator Dagenais: Thank you so much. I will keep my other questions for the second round.

Senator Kenny: Could you please put on the record for us what your products are and why they're useful? I think Canadians know you don't predict the future but you're more inclined to give context and options.

Talk to the committee, if you would, for a few minutes about the sort of products, why they're useful, who uses them, and I'm going to be asking about a reallocation of resources after that.

Mr. Peirce: Excellent. Let me start with our products then. We provide, out of my directorate, which is the intelligence directorate, two primary kinds of products. One is intelligence assessment. Those are assessed intelligence, where we've taken the intelligence from multiple sources. It will be our own collection, but we'll be informed by intelligence from foreign agencies as well as open source intelligence, and assess it to give a picture of an evolving or developing threat.

As you say, prediction isn't our business; prediction is a fraught exercise, but being able to indicate things to look for, sign posts. "If you see this happening, this is a concern." When we talk about operational intelligence, we talk about trip wires: "When we see this event take place, you should now be watching for the following threat."

That is our assessed intelligence. We also provide raw intelligence, and we provide thousands of raw CSIS intelligence reports. Those are set in context. We have some reference to the source so there is some context for the reliability of what we are providing. We provide it to other government departments and agencies, as well as, in appropriate circumstances, to our foreign partners.

Assessed intelligence can be used for everything from guiding decision makers, including policy makers within the government of Canada, including up to the highest level on potential threats. The assessed intelligence may also inform our operational people. As I said, it may give an indication that here are five indicators of terrorist travel, and if you see these indicators then you should watch that your target may be predicting to travel; so that kind of assessed piece.

The raw intelligence we don't provide for the purpose of making direct policy decisions. We don't want individuals to take a single piece of raw intelligence and make a policy decision on that. We want to make sure they're informed and they can come back to us and ask us an assessed view of the intelligence if it's on an issue of relevance to them. That single piece of raw intelligence is a bit dangerous by itself, so you want to make sure. We educate our clients about that regularly. We disseminate those, as I said, to our government departments and agencies. Then they're aware of evolving threats and can come back to us and ask for those assessed pieces.
Senator Kenny: How do you know if the stuff you're producing is any good? How much of it is produced because there is a demand for it? Somebody says, "I need to know something," or "I need to know more about something," and how much is pushed out or offered by you, "Hey, you had better pay attention because this might affect you?"

Mr. Peirce: I think it's a cycle, and it's not one or the other of those things. Both our collection of intelligence and the intelligence that we disseminate is based on the priorities set by the Government of Canada. Those are high level, but they are set by the Government of Canada and give us our guidance. Then, as an organization, we take that high-level guidance and break it into intelligence requirements. I forget what our total is right now. We have 80-odd intelligence requirements, very specific and detailed; "Collect intelligence on these issues." We use that to provide the raw intelligence that's collected and, as I said, to assess based on those priorities.

We take the time to inform government about the threat so they can make informed decisions about how to set priorities. It is a cyclical piece. We give you this intelligence. We give you this briefing that gives you some context, and then you tell us what you want to know.

We always have to be alive to the fact that we may collect intelligence that hasn't been specifically requested. We keep the flexibility to make sure we can report on emerging issues and seek feedback. We have a robust feedback mechanism to do that.

Senator Kenny: How do you evaluate the work you're doing? Who evaluates you?

Mr. Peirce: We get feedback from our clients. We seek that feedback actively. When we send out an intelligence report, there is always a request for feedback as part of that, and we do compile the feedback we receive. We're working to develop a more robust feedback mechanism.

When you go out and solicit feedback, sometimes you only hear from either end of the spectrum: The people who really like you or don't like you. We want to make sure we're getting comprehensive feedback, so we're continuing to work on developing a more robust mechanism.

The Chair: I would like to follow up in respect to what your organization does. You used the term "80 targets"?

Mr. Peirce: Eighty individuals; returnees, I believe. They're individuals who have returned to Canada, having travelled abroad for extremist purposes.

The Chair: Another agency actually informs you of those individuals; is that not correct? You are not out there finding or identifying them.

Mr. Peirce: We very much are on the front line of identifying those individuals. We are aided from a variety of sources, including the Canadian border service agency, who will share information with us. We're very much on the front line of identifying the individuals. These are individuals who have travelled from Canada.

The Chair: I know what CSIS is; I was thinking about your responsibility.

Mr. Peirce: I am CSIS.

The Chair: You are CSIS?

Mr. Peirce: I have a boss.

The Chair: I think I've got it somewhat clarified. I want to go further, and that has to do with the financing of terrorism, which we haven't touched on so far.

I have two questions: How does the glorification and financing of terrorists increase and contribute to radicalization in Canada? How serious is the question of terrorist financing in Canada, and where is that financing taking place, if it is?
Mr. Peirce: There are at least two different kinds of financing. One is financing for individuals within Canada, for example, who want to travel to engage in jihad. These are relatively small sums but very operationally important.

As you can imagine, if you see money going to an individual, it may be an indication that they’re amassing those funds for the purpose of travelling, if they’re someone who is otherwise on our radar; so tracking that kind of financing is very important.

There is financing that flows from Canada to terrorist organizations, and that kind of financing is very dependent on the kind of terrorist organization. If we look at ISIL, it is a terrorist organization that holds considerable territory; they have control over banks and oil in Iraq. As a result, they are a very well-funded terrorist organization.

We see other terrorist organizations such as al-Qaeda and the Islamic Maghreb who actively engage in kidnapping for the purpose of raising funds for their operations. We see smaller sums that flow from Canada for organizations like al-Shabaab, which is a terrorist organization active in Somalia and Kenya, in particular. We watch for the flow of funds there. There are different kinds of funding relationships, each one of them very much of concern to us.

The Chair: You cannot operate unless you have money, no matter where you are. But our focus point has to be within Canada, and where this money is being raised and the volume of money that is being raised. You’ve obviously been able to identify at least some of the sources for that financing?

Mr. Peirce: Yes.

The Chair: Perhaps you can expand on exactly what we’re speaking about and what volume of money we are speaking about.

Mr. Peirce: On the sources of financing, they are certainly varied. You have organizations that attempt to operate under cover of different purposes or individuals attempting to operate under cover of different purposes, ostensibly raising money for humanitarian purposes in Syria and Iraq, and they may well be actually funneling that money to a terrorist organization, so we see that kind of piece of work.

We have seen a recent phenomenon, essentially crowd share. The Internet age has given us the ability for people to go on and essentially put out a public message seeking funds. They won’t necessarily direct the full purpose of raising the funds. Again, they might do it under cover of humanitarian aid, but crowd share. "I want to carry out humanitarian aid in Somalia, please share funds," and they set up a website and funding flows through. It’s quite a troubling development from the Internet. You have more astute organizations that try to raise funds directly associated with terrorist organizations. One of our significant concerns is fundraising for Hezbollah in Canada, for instance.

The Chair: I want to go back. What volume of money are we speaking of in this context? Are we talking tens of thousands, hundreds of thousands or millions of dollars? What are we speaking about here, in your estimation?

Mr. Peirce: I don’t have an overall volume, and I would be loath to get into specific details in relation to specific organizations. When we’re talking about individuals, for instance, individuals who are raising money for terrorist purposes within Canada, they can be relatively moderate sums, up to $10,000 kind of thing. That’s the range you’ll normally see for individuals, particularly individuals who want to travel, for instance, up to that kind of range.

When you’re talking organizations, you are talking six-figure sums.

The Chair: Are we laying any charges?

Mr. Peirce: First of all, I have to say that’s not my end of the deal. We provide the advice, and we know that FINTRAC also provides advice, and it would be for the RCMP or local officials to lay charges.

The Chair: We’ll definitely follow up on that.
Mr. Peirce: It is a difficult area, though, because you have the fundraising, but until funds are used for something, it's very difficult to prosecute simply on the basis of the collection of funds. It's done under careful cover. I want to go and study at a madras in Yemen. Okay, on the face of it, that's what you're collecting it for, and I'm going to have a very difficult time, based on collection of intelligence, prosecuting you on that basis.

Senator Beyak: Thank you, again. I wonder if you could tell me, if I will word it a little differently, not the numbers that you're following but the actual numbers in Canada. How big is the magnitude? How big is the threat? How many individuals are radicalized, are following radical Islam? Do you have the funds to investigate the mosques and the imams who are espousing hatred towards Canada?

Mr. Peirce: In terms of the numbers, again, I will be very cautious about doing that, so I won't provide a set number for individuals. Certainly, the question of resources, I think you've heard much testimony today about the importance of prioritizing our resources. We work within the resources we have. We do shift our priorities around. We've always shifted our priorities around and shifted our resources accordingly, and at this time, we are certainly going through the process of again moving resources in response to the terrorist threat.

Senator Beyak: Thank you.

Senator Day: I have a request for a definition. You talked about the dangers of sharing raw intelligence. I've always thought of intelligence as being facts or information that has been put together and in some way looked at that is different from pure raw facts, but are you using the term "raw intelligence" just to mean raw facts?

Mr. Peirce: I will give some concrete examples of raw intelligence. Raw intelligence may be we have spoken to a human source. The human source says that person X is interested in doing something, and let's consider that terrorism-based. It may be that human source tells us that particular country is interested in collecting intelligence in a certain area. That's raw intelligence because, while we've assessed the source -- this is a long-standing source; this is a credible source; we have an assessment of our source there -- it's just an individual piece in isolation. You want to set that against our other intelligence to give a full context and assessment.

However, if we've collected that place of raw intelligence and it says that country X is looking to collect such and such information or it says that an individual is intending to carry out some conduct, we want to share that, but we want to share it saying that's just one piece. That's why I call it "raw intelligence." It has not been put together with all of the other intelligence we may have in the area, and that other intelligence adds context. It might fill out an assessment. For instance, there could be a spin on that intelligence that we see from other collection.

Senator Day: Thank you. That's helpful.

Would it be helpful in the work that you do and that your colleagues do at CSIS to have a law requiring everyone who leaves Canada to report to Canadian authorities so we have a record of everyone who has exited Canada?

Mr. Peirce: Undoubtedly, we don't have that exit information, as you know, now.

Senator Day: Yes, I understand.

Mr. Peirce: We do collect from a variety of sources and try to cover that, but certainly a law that gave us that kind of information would be helpful. That's not to comment on whether that law or however that law might be framed would be an appropriate law. I don't go into policy.

Senator Day: Is your name spelled like that as a result of you working at CSIS and that everyone who works there has a name like that, or spelled somewhat differently, so they can't find you in the phone book?
Mr. Peirce: I will say a few things first. It’s not a nom de guerre. Second, I am very well practiced in grammatical rules. It’s “I” before “E” except after “C” or in words that say “AY” as in “neighbour” and “weigh.” There are other exceptions. They include the name “Peirce.” Unfortunately, they also include the word “weird,” so you can make the connections you want to make with that.

Senator Day: You’ve been asked that question before.

Mr. Peirce: I have.

Senator Kenny: Following up on what Senator Day was asking you about, when you say you go to other sources, would that be, for example, airline travel information?

Mr. Peirce: Not necessarily airline travel information. There may be times when we can get airline travel information. We may get information because somebody may be on the specified persons list, which is part of the Passenger Protect Program, so we may get information there, but we’ll also collect information from sources in the community. We will in some instances have technical sources intercepting communications that will give an indication. We may have a technical source that allows us to intercept Internet traffic so we can see their booking their ticket online. It’s a broad range of sources.

Senator Kenny: If we could go back to the reallocation of resources. When Commissioner Paulson was here, he talked about taking a significant number of people away from, amongst other things, white-collar crime. We’ve had a director of CSIS in the past come to us and say 50 per cent of CSIS is focusing on Chinese espionage. Are we not paying any attention to the Chinese now and refocusing on the terrorist threat, or how have the resources been moved around in the organization?

Mr. Peirce: We, first of all, looked at our priorities, based on the direction from the Government of Canada, and we re-established our intelligence requirements, the tiering of them. When I say “tiering,” what happens is, as I said, you’ve got, let’s say, 80 intelligence requirements and you’re going to have maybe 15 to 20 that are tier 1. These are your highest priority. You will collect against these.

You will have a tier 2 set. These are important intelligence requirements. You will put resources to them, but you’re going to moderate those resources compared to those tier 1s.

We’ll have tier 3. Those are really ones where, if you get collection on them, possibly secondary collection, you’re going to report on them, but you’re not going to put resources necessarily.

There are four tiers. The fourth category will be areas where you say that’s a watching brief; we’re not actively collecting on that, but it’s a watching brief.

We’ve just recently looked at those tiers and said, “Do we have them right?” and adjusted them slightly. We didn’t take ones off and say, “This one, Chinese espionage, is no longer important,” and take it off and we won’t collect. We are still covering those priorities.

We did also go through the exercise, though, of looking at our investigations and, for example, looking across the country and looking at the threat that’s being investigated and saying, “Are we getting a lot out of this region on this threat?” And if not, maybe those resources don’t have to be directed in that region to that threat, so maybe we can move some of those resources on to the terrorism threat, for instance.

That’s the kind of exercise that we’ve been through, very actively looking at where are we not as efficient or not as effective, and maybe those resources can be put to a more efficient or effective use. That’s the exercise.

Senator Kenny: The committee has heard a fair amount about the relationship between CSIS and the RCMP. Could you talk to us about CSIS and the Communications Security Establishment? What sort of mechanism do you have to ensure that you’re functioning in a way that is constructive and complementary, and how do you ensure that Canadian resources are put to the best use between the two organizations?

Mr. Peirce: We have a number of mechanisms to help us in that regard. We have very close relations with the Communications Security Establishment.
Senator Kenny: They are just next door.

Mr. Peirce: They are now just next door, our new neighbours. They're keeping it down, so we're quite comfortable with that.

First of all, we have joint management team meetings where their management team sits down with our management team and we identify any issues. We identify priorities and areas where we can work together more effectively. As you can imagine, with the fact that they've moved in next door, we're very conscious about opportunities for efficiency and effectiveness, areas where we can share services with them, for example. So we have those joint management team meetings.

We have individuals from each organization seconded to the other. Sometimes it's not just knowing that they work this way and you can work with them, but you bring one of them over and you send one of your people over; and by working so closely, you get to understand the other better. We've done that and it has proven very effective for us.

We've also sat down and looked at our intelligence requirements, which I spoke of earlier, that set out our priorities. We've cross-referenced them to make sure that we have both coverage - there are no big gaps across our priorities - but also to make sure that they're rationalized against each other. You want to understand what it is they're collecting on and what you're collecting on. Sometimes they can be mutually supporting. If we can collect signals intelligence, it may aid us in our human source activity, for instance, and vice versa. You want to make sure you're well-coordinated in that way and that you're going after the same priorities. That's how we operate in that sphere.

The Chair: I would like to go into a whole different area from the point of view of CSIS and your responsibilities. Earlier today, we learned that there are 93, 95, 90 extreme travelers; 80 have returned. We've also been told — and don't quote me on this — that there are up to 145 Canadians, or dual citizenship Canadians, fighting with various terrorist organizations offshore. We've been told that there are thousands of individuals who have been identified at a lower level in respect to perhaps their involvement in the terrorist movement, either indirectly or directly.

I'd like to hear CSIS's comments in respect to the statements being made in some quarters in respect to some schools that are perhaps espousing radical Islamic views, or doctrines, in some quarters in Canada. Is that true, and do you have some concerns?

Mr. Peirce: First, one point of clarification, just because I don't want to leave any misimpression out there. When we're talking about individuals who are overseas, the 135 to 140 individuals, they are not necessarily engaged in fighting; they are engaged in supporting. It's a distinction because for the Canadian public in particular, we don't want them to think that there are 135 to 140 individuals who will come back with hardened combat abilities. That's not the case, and we don't want to leave that misimpression.

On the second part, I wasn't sure what you were referring to when you were referring to schools. The Chair: I'm referring to a certain ideology or doctrine that obviously these individuals are being exposed to, either individually or collectively. My question is: Where are they getting those teachings to be able to go to radicalization? It's one thing to talk about an isolated situation off in Quebec and another situation that happened on the Hill, but at the end of the day there seems to be at least a thread of ideology at the base of this. My question is: Are there teachings going on in Canada that are espousing that particular viewpoint, which is then transferring itself into radicalization?

Mr. Peirce: The short answer to the question is yes. There are individuals who are espousing a radical extremist view of Islam, and they are doing so specifically to radicalize individuals, often young individuals. That message is having an impact and we are, as a result, seeing people turn to a radical view of Islam. In addition, there is an enormous proliferation of extremist propaganda on the Internet, and it's a very powerful radicalizing tool.

The Chair: I want to go back to get it clarified on the record. There are actual schools or classrooms or venues that are being utilized on an ongoing basis to espouse this type of doctrine, is that correct?
Mr. Peirce: I'm not talking about specific institutions. I'm talking about individuals. I should be very clear about that. When we investigate, we investigate individuals and their activities. There may be individuals whose activities may be associated with a particular institution, but it's the individuals we investigate. For instance, we don't investigate mosques.

The Chair: The question I have is: If you have a school and a classroom and a teacher who has been identified by your organization espousing that type of doctrine, do you pass that information on to the provincial government or the authority that has the responsibility?

Mr. Peirce: If we have that kind of information.

The Chair: Have you done that?

Mr. Peirce: I can't say that we have done that with regard to schools, for instance. I can't say comprehensively "ever," but I haven't seen information specifically about a school saying: "This school has an individual in the classroom undertaking this activity." We will target individuals.

Individuals don't tend to operate in an institution quite so brazenly as that. Individuals may be associated with an institution, but they'll take students off to the side and conduct their activities in the community as opposed to in the institution. That's what we'll target.

The Chair: Colleagues, time is coming to an end here. I want to thank our witness. I believe you have been very forthright. I speak for all my colleagues when I say that we appreciate your candor. It's a very important issue for Canadians. I know many Canadians are watching this public forum. One of the reasons we're having these hearings is so we can inform Canadians of what you do, why you do it and the importance of what you do.

Mr. Peirce: Thank you very much.

The Chair: On June 19, 2014, the Senate approved the following reference for this committee: that the Standing Senate Committee on National Security and Defence be authorized to study and report on national security and defence issues in Indo-Asia Pacific relations and their implications for Canada's national security and defence policies, practices, circumstances and capabilities; and that the committee report to the Senate no later than December 31, 2015.

Joining us today to discuss the Indo-Asia Pacific the Department of Foreign Affairs, Trade and Development are David Drake, Director, General Security and Intelligence Bureau; and Peter MacArthur, Director General, South, Southeast Asia and Oceania Bureau. From National Defence and the Canadian Armed Forces is Rear-Admiral Gilles Couturier, Director General International Security Policy. Welcome to the committee.

I understand we have two opening statements, one from each department.

[French follows -- Peter MacArthur: Honorables sénateurs, je vous remercie de...]

[English follows]

Peter MacArthur, director general, Direction générale de l'Asie du Sud et du Sud-Est et de l'Océanie, Affaires étrangères, Commerce et Développement Canada: Honorables sénateurs, je vous remercie de m'avoir invité à m'adresser à vous aujourd'hui.

Je suis soucieux d'avoir la possibilité de m'entretien avec vous. Le Canada a établi près de 40 missions diplomatiques dans la région Inde-Asie-Pacifique, qui emploient près de 1 000 personnes. Le réseau diplomatique du Canada en Asie est plus puissant que dans toute autre région et croît en importance.

En faisant référence au titre de l'étude du comité, je soulévo choix important qui a été fait de reconnaître la place de l'Inde dans la sécurité régionale et mondiale. Maintenant dotée d'un gouvernement qui est axé sur les réformes et qui détient un vaste pouvoir démocratique, l'Inde pourrait être sur le point d'effectuer d'importantes réformes économiques susceptibles d'entraîner des répercussions mondiales. Le Canada et
l’Inde valorisent tous deux la liberté, le pluralisme, le respect des droits de la personne et la primauté du droit. Nos deux pays sont des démocraties parlementaires d’inspiration britannique, qui connaissent des gouvernements majoritaires et minoritaires. Nous croyons que tous les membres de la société ont un rôle à jouer pour l’avenir.

Le dialogue est la prémissed fondalementale de notre approche à l’égard de l’Asie. Quelques-uns des meilleurs exemples de transition réussie vers la démocratie au cours de la dernière génération se trouvent en Asie, c’est-à-dire la Corée du Sud, le Japon, l’Indonésie et la Mongolie. Plus tôt cette année, nous avons assisté à des élections importantes en Inde et en Indonésie, deux des trois pays démocratiques les plus peuplés du monde, ainsi que d’une partie de la démocratie en Afghanistan et, l’année dernière, au Pakistan. Parallèlement, lorsque le respect de la démocratie et des droits de la personne est mis à rude épreuve, comme en Thaïlande après le coup d’État, le Canada doit continuer d’exercer son influence et d’encourager un programme fondé sur des valeurs démocratiques. Les sociétés qui ne réussissent pas mettre en place des mécanismes de freins et de contre-poids contribuent à l’instabilité.

[Mr. MacArthur: To further Canada’s engagement in the...]

(english suit)

(Following French — Mr. MacArthur contra after... contribuent l’instabilité.)

To further Canada’s engagement in the region, the government seeks to join two vital forums: the East Asia Summit, EAS, and the ASEAN Defence Ministers’ Meeting Plus, ADMM+. The EAS likely will become an increasingly important venue for security as well as political and economic dialogue. ADMM+ is a relatively new mechanism that provides a framework for discussion and cooperation between regional militaries.

Canada is a participant in the ASEAN Regional Forum, ARF, a long-standing venue which facilitates cooperation on regional security. Canada also participates in the Shangri-La Dialogue, another important regional opportunity for security discussions in Singapore. Canada holds a number of high-level dialogues to discuss security and defence issues in the Indo-Asia Pacific region, including with regional partners such as India and Japan. In August 2014, Minister Baird announced $14 million to help address security issues of shared concern in Southeast Asia on top of $30 million that has already been announced and invested in recent years.

Projects include those to mitigate biological and nuclear threats; disrupt illicit flows while protecting legitimate trade; combat human smuggling activities; improve regional cybersecurity tools; further public-private partnerships and sound financial regulation; promote health and effective disaster response; and work with our ASEAN partners to address the foreign fighter phenomenon and radicalization. We are currently pursuing the most ambitious trade agenda in Canadian history, including with Japan and India as well as the broad Trans Pacific Partnership negotiations.

We have recently ratified the Canada-South Korea FTA and the Canada-China Foreign Investment Protection and Promotion Agreement. Energy security is a very important opportunity for Canada as Japan, South Korea, China and India are leading importers of energy, including liquefied natural gas. Canadian development programs and activities in Asia are a concrete tool to help bring security and prosperity in all its forms, including through sustainable economic development. Let me touch briefly on some particular areas of interest.

The Indian Ocean: While the rise of India has been at the forefront of geostrategic thinking for some time, India has led the way as a model in the region of a knowledge-based economy. As the world’s largest democracy, it also has the advantages that institutions of political accountability and the rule of law confer.

As the world’s fourth-largest economy, India’s relations with its close neighbours are central to regional stability. Supported by important investments in its navy, India is looking to assert itself as the dominant power in its Indian Ocean neighbourhood. However, India is also prudent in its approach to maritime disputes to its east. It is preoccupied by maintaining access to trade routes but avoids taking sides in maritime disputes. This approach has been to the benefit of regional security and many commentators agree that India-China relations are on a relatively stable footing.
Tensions in the South China Sea area reached a new high early last summer. Sovereignty over parts of the South China Sea is disputed by China, Brunei, Malaysia, Philippines and Vietnam, as well as Taiwan. The most prominent disputes concern the Spratly and Paracel Islands. Two thirds of the world's trade passes through the South China Sea. An escalation in Maritime boundary or territorial disputes between Asian countries could have disruptive effects on the global economy and threaten regional stability and global prosperity.

In East Asia, regional dynamics have also become more complex. The East China Sea has been a flash point for China and Japan. Destabilizing factors such as resurgent nationalism are stoking fears. China has become increasingly assertive in pursuing its interests, including through the establishment of an air defense identification zone which covers, in part, islands disputed with Japan. Japan is seeking a more active role for its military in defence and cooperation with allies, though it seeks to retain strict limitations on its role.

In conclusion, there is a wide recognition the balance of power in Asia is shifting. As economic growth and integration continues, all countries in the region are being forced to recalibrate their relations. Indeed, the Indo-Asia Pacific region is the new centre of global affairs and it is here that profound economic and strategic changes are unfolding.

Rear-Admiral Gilles Couturier, Director General International Security Policy, National Defence and the Canadian Armed Forces: Mr. Chair and senators, thank you very much for giving me before the committee today to speak on the Indo-Asia Pacific.

Canadians live in an uncertain world and, as I know you understand, increasing globalization has meant that developments far from our shores can have a deep impact on the safety and interests of Canadians at home and abroad. The events of last week clearly demonstrate that point.

Speaking at the Shangri-La Dialogue in 2013, the then Minister of Defence Peter MacKay stated:

Asia-Pacific security is now part of global security dynamics and however you define it ...  

... Asia-Pacific ...

... Indo-Pacific ...

... or pan-Pacific, as I like to call it from the perspective of a Pacific country.

(French follows - Mr. Couturier continuing - En bref, les préoccupations et les enjeux liés à la sécurité en Asie sont par leur ...)

(à partir de l'anglais - Mr. Couturier - from the perspective of a Pacific country.)

En bref, les préoccupations et les enjeux liés à la sécurité en Asie sont par leur nature même des enjeux et des préoccupations pour la sécurité du Canada, et la participation du ministère de la Défense dans cette région dynamique du monde vise à appuyer les objectifs du gouvernement canadien à l'échelle mondiale.

(couturier - The regional security environment in the Indo-Pacific...)

(French suit)

(Following French - Mr. Couturier continuing)

The regional security environment in the Indo-Pacific remains ever changing, uncertain and challenging. Several long-standing boundary business disputes, particularly in the maritime area, have increased tensions and are at risk of devolving into open conflict due to misunderstanding, miscalculations and the inflexibility caused by nationalistic audiences.

For example, the tension rose last spring in the South China Sea, the sea lines of communication that feed our own economy, which came under duress. On the North Korean peninsula, stability is threatened by
the erratic behaviour of the leadership and its pursuit of nuclear weapons as well as the technology to deliver them. Finally, the region is challenged by piracy, illegal migration, resource pressures and natural disasters.

As part of the Government of Canada's overall focus on the Indo-Pacific region, the Defence team is committed to defence and security cooperation aimed at maintaining peace and stability in the region to which Canada is integrally connected.

(French follows - Mr. Couturier continuing - Notre principal objectif est de favoriser un environnement de sécurité stable.)

Notre principal objectif est de favoriser un environnement de sécurité stable dans lequel les litiges sont résolus selon les normes et les lois internationales. Mais une contribution à la sécurité régionale requiert la mise au point d'une stratégie exhaustive.

(French continues - Canada is not alone and many of our friends...)

Canada is not alone and many of our friends and partners have similar concerns and are undertaking similar processes. We are sharing information with like-minded nations, such as Australia, New Zealand and the U.S., and coordinating responses to help strengthen our representative approaches.

At home, the Defence team is actively working with whole-of-government partners to explore approaches and develop plans that will take us in this direction. This was the impetus for the Asia-Pacific policy cooperation framework signed by Minister Nicholson and U.S. Secretary of Defense Hagel at the Halifax International Security Forum last fall. This framework sets the foundation for closer cooperation between our two countries, while respecting our individual national interests.

In carrying out this undertaking we are building upon existing commitments and engagements. The Canadian Armed Forces have been contributing on an ongoing basis since 1953 to the UN Command Armistice Commission in Korea. The defence team has actively been working alongside friends and partners in the region to mitigate regional security challenges through important activities such as participating in engagements with China's People Liberation Army, respecting the theme of "modest, enduring and reciprocal," and with an aim of encouraging them to take on their role as a responsible and participatory member of the global community.

We had numerous disaster relief team, or DART, deployments since 2004, the first one being in Sri Lanka for the tsunami. In Pakistan in 2005 for the earthquake and most recently in the Philippines for typhoon Haiyan. We are also demonstrating our commitment and capabilities through our participation in regional military exercises.

Indeed, after the U.S., Canada has been the largest contributor of troops to many of the exercises in the Korean peninsula such as the Ulchi Freedom Guardian in South Korea. Last summer more than 1,000 Canadian sailors, soldiers, marines and airmen deployed to the Hawaiian Islands and southern California as part of the exercise RIM of the Pacific, the world's premier combined and joint maritime exercise. Their performance in this 22-country strong exercise was absolutely stellar.

Further, the Military Training and Cooperation Program has been a valuable defence diplomacy tool, building regional capability as we strive to develop important bilateral relations within the region. Eleven Asian countries participated in the program and over the last fiscal year more than 130 officers from member countries received training sponsored by the MTCP in language, peace support, military staff and professional development programs. Canada has also sponsored several high profile seminars in Indonesia through the MTCP program.
The Defence team is focused on developing key bilateral relations, continuing participation in the ASEAN Regional Forum and exploring opportunities to contribute to the ASEAN Defence Ministers' Meeting Plus, which would give Canada a stronger voice in the region in the defence and security sphere, as you heard from my colleague from Foreign Affairs.

Multilateral dialogue tools hold great promise and opportunities to work on defence and security-related issues and strengthen cooperation in the region. At present we are striving for targeted engagement in making contributions where we believe we are adding value. This includes the areas where Canada has such a strong reputation, such as peacekeeping, counter-terrorism and of course HADR.

In sum, if the government's objectives and ambitions in the Indo-Asia Pacific region are to be fully realized, defence engagement must remain a priority within a coherent and comprehensive Canadian effort. The sense of a renewed effort speaks to a more focused priority set and achieving impact in a region of dynamic growth and complex security challenges.

French — Monsieur Couturier continuing - Dans l'ensemble, si le Canada veut réaliser ses aspirations générales dans cette région dynamique, nous devons continuer à investir dans notre sécurité et nos relations en matière de défense à long terme. Cet investissement exige des efforts soutenus et constants.

(16h00 — cam Couturier : Thank you for giving me the opportunity...)

(plus anglais)

Dans l'ensemble, si le Canada veut réaliser ses aspirations générales dans cette région dynamique, nous devons continuer à investir dans notre sécurité et nos relations en matière de défense à long terme. Cet investissement exige des efforts soutenus et constants.

(16h00 — cam Couturier : Thank you for giving me the opportunity...)

(plus anglais)

Thank you for giving me the opportunity to appear before you, and look forward to the discussion.

The Chair: I'd like to begin with Senator Mitchell.

Senator Mitchell: Thank you very much, gentlemen. This is an interesting and important topic, if not quite as urgent as the one we had earlier. We've had your testimony today, and we've had some before. I'm seeing these two lines of thought, and I can't quite figure out which way the consensus would come down. On the one hand, China, and this region in particular, is clearly an economic opportunity, and there's the risk there might be that we would miss it. On the other hand, there is this theme that there is a military threat somehow. Mitigating that, in my mind, is the fact that China holds, I think, $3 or $4 trillion worth of U.S. bonds and wouldn't want to do much to offend that economy, I would think. We actually included them in RIMPAC this year, for the first time. We're training with them. This is kind of a high-level question in the sense of which it is. Are we concerned about a war with that region, or are we concerned about missing out on the economic opportunity that's inherent in trade with that region?

Mr. MacArthur: Perhaps I could begin, Mr. Chair. I think our relations with China and North Asia need to be seen in a holistic manner. There is an economic opportunity there, and we are determined to engage with eyes wide open. There is the capacity, on parallel tracks, to maintain relations, whether it's commenting on human rights abuses or attempting to do more with China in terms of FIPA, for example, which was just ratified and allows Canadian companies to invest in China with greater predictability and transparency. I think we can walk and chew gum at the same time. These very important strategic relationships, which are multi-faceted, I would turn to my colleague about your comment on the military potential of the country.

Rear-Admiral Couturier: Like you said, we do our engaging — with the Chinese. The goal there is to share some of our own best practices and to better understand how they work as far as a military associated with their own engagement in the way they do business. We've had a least two engagements to date. In both cases, it was an exchange of ideas. They had an opportunity to look at how we operate, how we do business. One of them was on how we do human resources, and there were some significant differences in
the way we proceed in how we do business. At the same time, we had an opportunity to hear from them about how they deal with their own challenges and how they see the future developing from a human resources perspective. The goal there, without a doubt, is to get a better understanding of where they are coming from and to share some of our best practices.

The example of RIMPAC speaks volumes on where we believe the way ahead is. The best way to understand where the country comes from and to avoid any misunderstanding is to operate together. If you put this in the maritime environment, the fact that we have five ships -- but three operational ships -- deployed there gives us the opportunity to see how they react at sea and to get the commander’s appreciation that, if things were to happen, there is a way to communicate that would prevent any misunderstanding. They achieved that within the exercise of RIMPAC.

Senator Mitchell: My next question is more specifically military in the idea of the division of our resources between the east coast and west coast. I don’t know how much of this you can actually answer, but is the navy giving thought to redeploying due to reassessing priorities?

Rear-Admiral Couturier: It’s hard for me to speak for Admiral Norman. Right now, he is not my direct boss, but he could be soon. So we have to be careful of where we tread.

Having said that, we do discuss that on a regular basis amongst some of the senior naval officers. What needs to stay at the forefront is that where we’re based doesn’t really affect where we can operate. We did, over the last two years, have ships deploy from the west coast into NATO theatres of operations, and we can certainly do the opposite if necessary.

The infrastructure, as it is right now, is more favourable to the east-west split that we have as far as forces. One should not interpret that as meaning that we can’t deploy on the west coast because of the number of assets necessary. If the need or requirement’s there, there is certainly the opportunity to deploy ships from both coasts to answer the request of the government to deploy in a specific region.

Senator Stewart Olsen: Thank you, gentlemen, for coming.

Because Canada is very much focused, as a country, on the protection of democratic rights for people, I’m wondering about certain concerns that have been expressed about democracy and whether it is thriving in the region. I’m wondering if you would agree that it is a matter of concern, if so, are there areas we should be looking at? My second question to you would be: What more can Canada do to beef up making democracy more important on the agenda of these countries?

Mr. MacArthur: Very good question. Because we are a value based foreign policy, we are focused on democracy, the rule of law and human rights, particularly for women and girls, for example. This is something that we promote through our diplomatic presence around the world. I think it’s a mixed picture on democracy. There has been a setback in Thailand after the coup d’état there, which seems to be a harder coup than previous, softer coups and is something of great concern. It’s not business as usual, currently, with Thailand. You have seen statements by the minister when the coup took place. We are also concerned about human rights and democracy in Vietnam, for example.

On the other side of the coin, we see some progress in Burma, which is opening up and becoming more democratic. We expect elections in 2015, and we just opened our embassy there, our first resident embassy. The trend line is in terms of very complex, historic elections in Indonesia, India and Afghanistan, in two rounds. They are good trends. However, the elections that were held in Bangladesh were dysfunctional because the opposition party boycotted the election. It’s very much a question of governance, and we have funding called the Canada Fund for Local Initiatives. Combined with our development programming, there is funding available and being invested in trying to enable greater democratic flows. For example, in the case of Burma, we had actual practicing politicians brought to Parliament Hill to experience committee meetings, Question Period and the work of the House, and we sent parliamentarians and officers of the House into Naypyidaw, the capital of Burma, for peer-to-peer mentoring. That is designed to show to other countries, including Thailand, in this case, which has more military in its government than Burma currently does. That’s the kind of change we’re seeing.
I think Indonesia and India are showing a model to others, and it is very much a focus of foreign policy. The work of our ambassadors around the region is consistently pushing our messages and looking for progress, including through some funding programming.

Senator Stewart Olsen: Overall, you’re more encouraged than discouraged?

Mr. MacArthur: Overall more encouraged than discouraged. I think the rise of ASEAN is helpful in that regard, as is Indonesia being a model as the core, largest country of that organization.

The Chair: I trust you didn’t show them Question Period during the course of that mentoring that took place. I will go to Senator Day next.

Senator Day: ASEAN has been talking about more political integration. Has there been any advance on that? The ASEAN nations, from a military point of view, have cooperated, and Canada has been part of that for a while.

Can you tell us what’s happening in those Southeast Asian nations?

Mr. MacArthur: I can start, and my colleagues can add in if they wish. Yes, you’re quite right, senator, there is a move afoot to economically integrate the ASEAN 10. The theoretical date is the end of 2015. Most observers believe it will take longer than that, but you’re looking at a regional economic block of 600 million people, the size of the European Union. It is quite vibrant, with some of the faster growing economies in the world, the Philippines and Indonesia being examples of that. Political union will not be possible.

This is a coordinated secretariat in Jakarta. Minister Baird was the first foreign minister to meet with the Secretary-General, former Vietnamese foreign minister, in August of this year. We are keen to assist ASEAN through their connectivity agenda—not just economically, but helping them people-to-people, in justice, politics and democracy, to bring them together.

We’re watching how successful they are in doing that but there is disparity in the economic development between Singapore and Laos. Culturally, it’s not a monolith; it’s federated. Some of our capacity in federalism would be of interest to certain member countries of ASEAN such as the Philippines, for example Mindanao in the south. I will turn to my colleagues on the ARF, which is a separate institution.

Rear-Admiral Couturier: We are trying to support the progress that they’re doing and we’ve offered our services as far as the mill-to-mill aspect and both the bilateral function in a multilateral agenda. At this stage, however, there is minimum engagement from a military perspective.

Senator Day: There used to be good cooperation between China and some of the other Southeast Asian countries, particularly in trying to stop piracy near Singapore. Singapore was sort of the centre for the think tank in that regard. Since the difficulties in the South China Sea and the East China Sea, are we seeing any military cooperation between China and any of its neighbours?

Rear-Admiral Couturier: You’re correct that Singapore used to be the centre. They are still coordinating response for participating countries in the region. The Chinese are dealing not only with anti-piracy in that region but also with the anti-piracy challenges we are facing in the gulf. There are still discussions and they’re still engaged, but our appreciation of the level of cooperation that’s happening at the lower level has changed quite a bit since the recent past.

The Singaporeans are trying to bring everyone together. They are going to build an HADR centre of excellence within Singapore to support anti-piracy. By centralizing all those central committees, they hope to be able to get better interaction from all the countries.

Senator Day: As a final concluding comment, there are a good number of parliamentarians both in the Senate and House of Commons who have spent a lot of time on the ASEAN inter-parliamentary political group that we have been an active member of and the Asia-Pacific parliamentary forum. I urge you not to forget parliamentary diplomacy and the assistance that members of the House of Commons and Senate can be in that regard.
(French follows—Senator Dagenais: Merci à nos trois...).

(après anglais)

Le sénateur Dagenais: Merci à nos trois invités. J’ai deux courtes questions pour M. Couturier. J’aimerais revenir à la Thaïlande. Qu’a fait le gouvernement canadien pour promouvoir la stabilité dans cette région?

Cam Couturier: On le fait de deux façons, il y a la participation à un exercice comme RIMPAC au niveau militaire — je parle d’un engagement de militaire à militaire. Au cours de cet exercice, on a des discussions entre les officiers seniors de la région. L’officier senior chinois est venu, il y avait aussi un officier japonais dans le groupe. Cet exercice nous a permis de voir, non pas du point de vue politique, et cela ne découle pas de notre domaine, mais du point de vue militaire la façon dont on mène les opérations et les possibilités de mieux travailler ensemble pour atteindre les objectifs respectifs de nos gouvernements, sans engendrer d’aspects politiques à ce travail. C’est la raison primaire d’un exercice comme RIMPAC.

Le sénateur Dagenais: Vous avez répondu en partie à ma deuxième question qui visait à connaître un peu l’implication du gouvernement de la Thaïlande pour arriver à cette stabilité. Vous dites qu’un officier japonais et un officier chinois ont travaillé avec vous?

Cam Couturier: Plus spécifiquement, pour ce qui est de la Thaïlande, nous avons arrêté nos activités militaires en attendant de voir comment va se dérouler l’aspect politique dans la région. Nous avons un attaché qui est déployé, mais on a mis en suspens nos activités de ce côté. On s’attend a ce que, à un moment donné, il faudra réintégrer pour continuer à faire des activités très importantes pour eux.

Une des choses que l’on fait, du point de vue militaire, est d’examiner, durant les exercices que nous menons avec MTCP, les relations entre les militaires et un gouvernement civil étranger. C’est une partie du développement que nous faisons avec eux. Nous voyons ce point comme un aspect positif et une contribution quand même assez importante.

(Sen. Beyak: Mr. Couturier, could you provide the Committee...)

(english suit)

(Following French—Mr. Couturier cont’g—même assez importante.)

Senator Beyak: Rear-Admiral Couturier, could you provide the committee with the full list of the defence and security agreements being signed and the list of those being negotiated? Would you be able to give me that?

Rear-Admiral Couturier: I would have to go back and look at what those are. Of the ones that were signed, the most obvious is the one we signed during the ISIS, and that was between the minister and the secretary of defence. I will look at some of the others.

Senator Beyak: There is some concern about China’s expenditures militarily by other countries in that region. Do you see it as a problem? Is it destabilizing things in any way?

Rear-Admiral Couturier: There is certainly expansion. For example, in the submarine world — for us navy guys, it’s an important area — they’re building 3-to-1 compared to our U.S. counterparts. If you hear about the U.S. rebalancing in the region, this is an area where they are refocusing. The U.S. has sent more submarines on the west coast to try to rebalance that element. We’re monitoring and, based on what you have heard from Dr. Boutiller and others, there is not only the expansion part of China but there is also a national element. You have to consider that aspect when you analyze the growth of military hardware in all areas. We’re monitoring and are concerned to a certain extent, but at this stage we’re engaged with our allies and we are comfortable with where we are.

The Chair: Our last witness here last week, Dr. Boutiller, commented that we were late in having our presence felt in this particular area of the world.
Yet, Mr. MacArthur, you stated in your opening address that Canada maintains nearly 40 missions in the Indo-Asia Pacific region, with a staff of close to 1,000; and Canada's diplomatic network in Asia is stronger than in any other region and it is growing. Perhaps you can comment on the statement made by Dr. Boutilier?

Mr. MacArthur: Certainly, Mr. Chair. I was referring to our diplomatic footprint which was growing in places like an ASEAN ambassador's presence in Laos and Cambodia to ensure that Canadian values and foreign policy and economic interests are well understood for all ASEAN capitals. That's the work of our ambassadors and diplomatic staff. Canada's soft power has a lot to offer in that part of the world given our human rights values, our governance, which is tested, even our banking system is of interest. The robust nature of Canadian society, multiculturalism, and the way we are governed—we shouldn't underestimate that brand image in countries not just of ASEAN but in the general region. My point was that diplomatically, and that includes economic diplomacy as a subset of our diplomacy, we are much more engaged than we have been in the past.

I will give you an example. In June this year, the trade minister invited an ASEAN trade ministerial delegation to Vancouver and Toronto. Only Japan, China and the United States have done that. These were ministerial and deputy ministerial representatives of all ASEAN capitals who came to Canada. It was an eye opener for many of them. That's the kind of engagement we're trying to reverse our steady flow of ministers and officials, including our foreign and trade ministers who have been to ASEAN dialogue meetings for three successive years and have presented substance at their meetings and engaged better than ever before. That's all supported by our web of networks in the embassies and consulates across the region.

Rear-Admiral Couturier: From a budget perspective, if you look at 2007-08, we had 11 per cent of our DMTC budget going toward the Indo-Asia. Next year it will be at 30 per cent, so we certainly realize the importance of that region and we have retooled some of our resources to meet training requirements in the area that I mentioned earlier. We are seeing the importance and trying to ensure that, both from the DMTC perspective and the military-to-military aspect, we keep increasing our ability to share our own lessons learned with them.

The Chair: Turning to another area, ballistic missile defence, can we hear your comments with respect to the installation of that particular program in that part of the world?

Rear-Admiral Couturier: From a Canadian Armed Forces perspective, I will be clear what we're seeing in that region is led by the U.S. for the threat that's generated from there. From a Canadian perspective, we in the military are looking at the options in the future and how to best deal with that. That will be addressed by the government's decision in the near future, depending on whether they decide to go that route or not.

David Drake, Director, General Security and Intelligence Bureau, Foreign Affairs, Trade and Development Canada: Of course, ballistic missile defence concerns are focused primarily at North Korea, which has an extensive missile program and delivery program that I'm sure you're well aware of. Canada is very focused on this. We work within the international community to try and contain North Korea. It's problematic now because of the lack of the six-party talks, but there is significant work taking place around the world and focused on North Korea at this point in time.

Obviously, we have extensive economic sanctions placed on North Korea, including prohibition of imports and exports from North Korea, with humanitarian exceptions. North Korea has systematically ignored a whole series of UN Security Council resolutions and Canada plays a big part in trying to keep pressure on them come to the bargaining table and deal with these worrisome issues.

Senator Ngo: The question I wanted to ask was already answered, so I will turn to another one. In your presentation you say that tension in the South China Sea reached a new early last summer, and the sovereignty of the South China Sea is disputed by China, Brunei, Malaysia, Philippines and so on. The dispute concerned the Spratly and Paracel islands.

Recently, the United States has been forging a closer relationship with Vietnam in the hope of ramping up its presence against China, by lifting its ban of selling weaponry to Vietnam—. There is concern throughout the region and beyond that these hostilities could erupt because of lack of tranquility at sea. We
know that the United States has signed a military alliance with the Philippines, a military presence in South Korea, military protection in Japan, and recently selling weaponry to Vietnam. The question I'm asking is in the wake of the -- and economical exploitation by Beijing, what is Canada's position over the territory of dispute in the South China Sea, and how critical is it for Asian nations to see that Canada is committed to contributing to the peace and stability in the region?

Mr. MacArthur: Very good question there. Obviously, I think the Government of Canada's position on the South China Sea is that we are seeking a peaceful resolution under the Law of the Sea, all International law and peaceful resolution. We do not take sides, but we very much call for a cooperative approach. I know, for example, when the deputy Prime Minister and foreign minister of Vietnam were here that was the Canadian message, the need to make sure that this is done through international negotiations.

I'm happy to say there are reports of senior officials of China and ASEAN meeting currently or very soon to talk about a code of conduct for the South China Sea. So diplomatically, amongst senior officials, there is dialogue. I think ASEAN plays a key role given its weight in the region and, for example, the role of Indonesia behind the scenes seeking to ensure that things are done in an appropriate manner.

Mr. Drake: I think it's important to recognize that what you have right now is a whole series of -- and in some cases overlapping -- claims, like multiple countries. Obviously, the Chinese have the largest claim. They are also involved in the East China Sea in terms of their new air defence zone. The Chinese have put forward a dispute, but certainly they have never substantiated their claim can and as demarcated by the so-called "nine-dash" line, which covers 80 per cent of the sea. There is clearly a lot of work that needs to be done by the international community, notably by the countries themselves.

The best thing to do is call parties, as Mr. MacArthur said, to start talking according to international law, and there is not enough of that. In terms of where we need to be here, I think Canada's position is quite strong on this. We don't take a particular position vis-à-vis one country, but it is the process. It is the process of international law, which we need to focus on, and certainly Canada is a country that is highly regarded in our advice for many years.

You mentioned the South China Sea, but there is also East China Sea — a series of territorial disputes — and the way through this is by the force of international law.

The Chair: One other area before we close, I would like to follow up on Senator Beyak's question about agreements that are being negotiated or have been negotiated with the Indo-Asia region. Has either department considered moving to a strategic cooperation agreement with either Japan or India, similar to what Australia and the United States has done in the past? Do you have any comments on that?

Mr. MacArthur: I think the Canada-India relationship, particularly since the Prime Minister's visit in November 2012, has taken a certain significance and improved relations with India and presents good opportunities on a whole set of levels to do more with India.

For example, just a couple of weeks ago both the foreign and trade ministers were in India, along with the British Columbia premier. There was a massive Canadian presence, including the private sector, in the delegation. In effect, we are already conducting a very high-level, substantive relationship with India across a whole range of factors.

It wouldn't be impossible to contemplate that kind of a special relationship that's very much developing, particularly with the election of the new government under Prime Minister Modi. I think there are good opportunities for the kind of cooperation Prime Minister Modi had when he met with our ministers in New Delhi. It was a warm meeting and highly cooperative. I think there are good winning conditions there at present for that kind of development.

Rear-Admiral Couturier: With India, on the military side, we're at the early stage of engaging in some discussion.
For example, the head of our navy was recently conducting bilaterals with the head of the Indian navy, so we're certainly looking at this, but very much at the beginning of trying to reinforce that bilateral relationship.

On the Japanese side, we have a series of discussions on the bilateral element. One is called the cross-service agreement, more oriented towards a logistics element. Once this agreement is signed we believe that will be the first of others we will be able to generate to increase our cooperation with the Japanese. As I said, all services are very much engaged. There is some discussion between the Chiefs of Services regularly. In June of this year we had a discussion with their academic community on the military aspect of it where we shared some views of the world including, at the time, Ukraine and Iraq. I believe that bilateral is very strong.

The Chair: Colleagues, I see time has moved on here. I would like to thank the witnesses for taking the time to come and appear before us. You have added to the information in respect to the ongoing study we have undertaken.

I will excuse the witnesses before we go in camera.

(The committee continued in camera.)
PREVIOUS STATEMENTS FROM SECD APPEARANCE

On October 20, 2014, the CSIS Deputy Director of Operations (DDO) made an appearance at the Senate National Defence and Security Committee (SECD) to testify on matters related to terrorist threats to Canada.

Below are key statements made by the DDO at that appearance:

- **On foreign fighters:** "Canada has between 130 and probably 145 Canadians right now that are over there fighting. They're not all with ISIL. They're with other terrorist groups, such as Hezbollah, and in other parts of the country and North Africa, East Africa and West Africa. These Canadians are involved in activities overseas that they shouldn't be. The CT threat is much broader than just the ISIL group. It is something that concerns us greatly and is our number one priority." (For responsive lines, see Tab 3D).

- "The service is aware of at least 50 Canadians involved in terrorist-related activities with ISIL and other extremist groups in the region. Of these individuals, we are aware of approximately 30 in Syria alone, with the remainder located in Iraq, Turkey and associated border regions. The participation of Canadians in these conflicts is harmful to our international reputation and destabilizes regional security. Canada has an obligation to do her part to prevent such travel." (For responsive lines, see Tab 3D).

- "As the Director of CSIS noted recently, we also remain concerned over the threat posed by individuals returning to Canada after having engaged in threat-related activities abroad, whether with ISIL or other groups, like Jabhat al-Nusrah in Syria. While such individuals' experience and determination vary widely, it only takes one individual or a small group of individuals to cause great harm. We are currently aware of approximately 80 individuals in this regard, and we actively monitor them, some under judicial warrant, for any threat to public safety." (For responsive lines, see Tab 3E).

- "Do you have an estimate of how many supporters here are actively involved with those 200 or 215 identified terrorist activists? It is a good question, Senator, because you are introducing another concept here of what we don't know quite honestly. These are numbers we know. What keeps me up at night are those who haven't come across our radar screen." (For responsive lines, see Tab 3D).

- **On radicalization:** "We also remain concerned that global events could shape the threat environment in other ways detrimental to Canadian interests. For obvious reasons, CSIS remains concerned that ISIL's message and successful social media strategy could inspire radicalized individuals to undertake attacks here in Canada. Senators would be aware of such a possibility from recent arrests in Australia, where an ISIL-inspired terrorist group planned to engage in random acts of violence against innocent civilians. CSIS is actively investigating any such possibilities and will, of course, advise the appropriate parties on such matters, but I would also like to stress that, as the director has stated, CSIS has no information to indicate that a terrorist attack in Canada is imminent." (For responsive lines, see Tabs 3A and 3C).

- "We have individuals who have an expertise in radicalization, but our focus is more on targeting and ensuring that we're aware of those individuals that are problematic, engaged in threat-related activities. In terms of whether outreach impacts criminal charges or not, that's best put to the RCMP." (For responsive lines, see Tab 3C).

- "If you look at radicalization, it comes in many forms. Each individual's path to radicalization is quite different and unique. There's no one descriptor that can explain how one person went from sitting in the basement of his parents' home, surfing certain radical websites, to actually being engaged in the conflict in Syria itself. That step of radicalization and those individuals that are radicalized are quite concerning." (For responsive lines, see Tab 3C).

- **On budget allocation/resources:** "Like other agencies and departments, we work within..."
the budget that is assigned to us. We do have to prioritize. The foreign fighter threat is one that is growing. The returnees are one that does concern me a great deal. For every extremist that we prevent from going overseas to engage in extremist activity is one more individual that we have to investigate closely because they're radicalized to the point where they want to leave. Saying all of that, there is nothing more we can do with the budget we have except to prioritize internally as effectively as we can, and I think we're doing that. Our success rate has been quite good. I say that with some pride in terms of what we have been able to accomplish. I would be foolhardy to say we have all the bases covered. We do what we can with the budget we have, sir." (For responsive lines, see Tab 3I).

- "Therefore, when they do come back to Canada, obviously, we have to monitor their activities as much as we can but prioritize as well. We can't devote all of our resources to all of them all of the time. So we do have to prioritize those individuals. We do know where they are." (For responsive lines, see Tabs 3E and 3C).

- On exit information/controls: "An exit information system is not an exit control. There is no control. Canadians have every right to leave the country and enter the country again whenever they wish. Exit information is something we're lacking right now, and it's quite germane to the foreign fighter issue. We don't know when certain individuals on Canadian documentation have left the country. We just don't have that information available to us right now in terms of something that can be corroborated in terms of a passport that has been swiped on the way out of Canada." (For responsive lines, see Tab 3K).

- "Your question about passports is a valid one. In order to get back into the country, they would have had their passports. In order to leave the country, they would have had passports. It is important to note, as well, that, in terms of tracking these individuals when they leave, Canada does not have an exit information system. It is not always easy to know when these individuals have left." (For responsive lines, see Tab 3K).

- On information sharing: "I think what you're referring to, at least in the context of individuals who have travelled overseas, is the ability for other agencies with certain capabilities, particularly in a technical space, to acquire intelligence on Canadian citizens. Where that has happened and where we've had any role in it, it has been based on warranted targets that we've covered. But other agencies have the ability to target whomever they see fit, based on risks to their own countries or their own national interests. We do not have any control over that, it's based on their own laws and their own capabilities. The general rule is that Five Eyes partners will not spy on each other." (For responsive lines, see Tab 3N).

- "I'll say that what we've learned over the years in terms of improving the relationship with ourselves and the RCMP has led to a system where we will provide them lead information, because it's only natural we will be the first ones to come across that countervaillance-type information. We have a lower threshold in terms of acquiring our warrant of powers. We have a lower threshold to use those intrusive techniques that will lead to the intelligence that indicates a clear threat." (For responsive lines, see Tab 3J).
OTTAWA, Monday, October 20, 2014

The Standing Senate Committee on National Security and Defence met this day at 2 p.m. to study and report on security threats facing Canada and on national security and defence issues in Indo-Asia Pacific relations and their implications for Canada’s national security and defence policies, practices, circumstances and capabilities.

Senator Daniel Lang (Chair) in the chair.

The Chair: We have an hour for this panel. I know that we are anxious to get on with the business, so I would like to call the meeting to order.

Welcome to the Senate Standing Committee on National Security and Defence for Monday, October 20, 2014. Before we welcome our witnesses, I would like to begin by introducing the people around the table. My name is Dan Lang, senator for Yukon. To my immediate left is the clerk of the committee, Josée Thérien, and, on my right, is our Library of Parliament analyst assigned to the committee, Holly Porteous. I would like to go around the table and invite each senator to introduce themselves and state the region they represent, starting with our deputy chair, Senator Mitchell.

Senator Mitchell: Grant Mitchell, Alberta.

Senator White: Vern White, Ontario.

Senator Beyak: Senator Lynn Beyak, Ontario.


(French follows – Sen. Dagenais: Jean-Guy Dagenais, sénateur)

(après anglais)

Le sénateur Dagenais: Jean-Guy Dagenais, sénateur du Québec.

(Chair): Thank you. This afternoon, the committee will be meeting to commence...)

(anglais suit)

(following French – Sen. Dagenais — du Québec.)

The Chair: Thank you. This afternoon, the committee will be meeting to commence two new studies pertaining to our mandate of national security and defence. Before we begin our study, I wish to welcome our new deputy chair to the committee, Senator Grant Mitchell from Alberta, and two new members, Senator Carolyn Stewart Olsen and Senator Ng, who will be with us soon. I would also like to welcome back to the committee Senator Colin Kenney, who is our dean and perhaps the longest serving member of the committee. That’s the official representation on the committee.

I would also acknowledge the new chair of the Subcommittee on Veterans Affairs, Senator Joseph Day, and the new Deputy Chair, Senator Carolyn Stewart Olsen.

Also, I would be remiss if we, as a committee, did not formally acknowledge the excellent work of senators Segal, Wells and Dallaire, our previous members.
On June 19, 2014, the Senate agreed that the Senate Standing Committee on National Security and Defence be authorized to study and report on security threats facing Canada, including, but not limited to, cyber-espionage, threats to critical infrastructure, terrorist recruitment and financing and terrorist operations and prosecutions, and that the committee report to the Senate no later than December 31, 2015.

This new study will build on the work of the subcommittee on anti-terrorism, published in March 2011. In the next few weeks, we will have the deputy chair of that committee appear before us to provide an update on their report that was published back in March 2011, entitled Security, Freedom and the Complex Terrorist Threat: Positive Steps Ahead. The committee was chaired by Senator Hugh Segal and Senator Serge Joyal.

As part of our present study, we will be focusing on the threats that Canada and Canadians face from terrorism. Terrorism is not new to Canada. We have seen the terrorist attack on Air India Flight 182, which departed Canada on June 22, 1985 and exploded the next morning above the Irish waters not far from Cork, killing all 329 passengers, mostly Canadians.

This act of terror did not occur without notice or without victims. Many of our fellow citizens were left without mothers, fathers, brothers or sisters, a grandparent, an aunt or an uncle.

In 2007, Prime Minister Stephen Harper announced a public commission into the Air India tragedy, and, in 2011, the Kanishka Project was launched to help Canadians learn more about terrorism.

On September 11, 2001, many of us witnessed the 9/11 terrorist attack on the United States, which left 24 Canadians dead. On that fateful day, Canada played a vital role at NORAD, and many Canadians, from Yukon to Newfoundland and Labrador, opened their homes and hearts to those in need.

Colleagues, on our television screens, in our newspapers and on our computers, we see a daily rise in terrorism, mainly from Islamic jihadists fighting for dominance over fellow citizens. Canada has listed a number of new entities since 2006. The threat is on the rise. It is important to understand it and take appropriate action in a reasoned and well-informed manner.

One key point is that money and ideology drives terrorism. Today, to commence our look at the terrorist threat, we are pleased to have with us Gérald Cassette, Director of the Financial Transactions and Reports Analysis Centre of Canada, and Luc Beaudy, Mr. Cossette. I understand you have an opening statement. We have one hour for this panel. Please begin.

(French follows - Mr. Cossette up in full -- Honorables sénateurs, bonjour)

(après anglais)

Gérald Cassette, directeur, Centre d'analyse des opérations et déclarations financières du Canada: Honorables sénateurs, bonjour. Merci de fournir à CANAFE l'occasion de contribuer à l'étude marginale sur les menaces à la sécurité.

Avant de commencer, j'aimerais prendre quelques minutes pour vous présenter mon collègue, Luc Beaudy, gestionnaire du groupe de CANAFE qui travaille sur le renseignement destiné spécifiquement à la lutte contre le financement du terrorisme. M. Beaudy m'aitera à répondre à vos questions cet après-midi. Je peux vous assurer que nous savons aussi ouverts que possible dans nos réponses; par contre, comme vous le savez, nous ne pouvons pas fournir de l'information classifiée dans un lieu aussi public. Également, notre loi - la Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes - limite ce que nous pouvons dire au sujet de l'information que nous détenons.

Avant de répondre à vos questions, j'aimerais commencer par décrire le mandat de CANAFE et le rôle que le centre joue afin de protéger les Canadiennes et les Canadiens et l'intégrité du système financier canadien. Je me pencherai plus particulièrement sur notre contribution, en étroite collaboration avec nos partenaires du régime sous les services policiers et des organismes de sécurité nationale, afin de détecter et de combattre le financement du terrorisme.
CANAFE was created in 2000, at the moment of the adoption of the Law on the recycling of the proceeds of crime and the financing of terrorism, in order to prevent and detect the laundering of money and the financing of terrorism. Under this law, CANAFE, the financial services, the agencies of the security and national security, the prosecutors and about 31,000 companies from all over the country each play their role in creating an environment hostile to those who try to abuse our financial system and which threatens the security of Canadians and Canadians.

The legislative measures obligate the entities offering financial services, the companies of service, the casinos and other companies subject to this law to: ensure conformity, to verify the identity of the clients, to monitor business relationships, to keep certain documents and to declare certain types of financial transactions to CANAFE. In addition, the declarations of the proceeds of terrorist financing to the RCMP and to the SCRS must also be transmitted to CANAFE.

Grâce aux 20 millions de déclarations de transactions financières que nous recevons chaque année, le centre est en mesure de fournir un renseignement financier exploitable qui permet aux services de police et aux organismes de la sécurité nationale de protéger le Canada et les Canadiens et Canadiennes.

(M. Cossette : During the past fiscal year, we provided...)

(english ann.)

During the past fiscal year, we provided 1143 disclosures of actionable financial intelligence to our regime partners to assist them in their investigations of money laundering, terrorist financing and threats to the security of Canada.

Of these disclosures, 234 were specifically related to terrorist financing and threats to the security of Canada in response to information provided by our partners. This is up 50 per cent from last year and 450 per cent from 2008.

FINTRAC also produces classified strategic financial intelligence reports on suspected terrorist financing activities and trends by groups formally listed as terrorist entities by the Government of Canada.

The threat of terrorism is real, and it is not going away. A number of individuals are currently making their way through our criminal justice system for terrorist acts that they have allegedly planned to commit here in Canada. Just last month, an Ottawa resident entered a guilty plea to terrorism charges in an Ottawa court, and he received a 24-year sentence for his crimes. Over the past many months, we have also seen violent attacks in many parts of the world, a number of which involved Canadians.

The director of CSIS recently confirmed that his organization has identified more than 130 Canadians who have gone abroad in support of extremist activities. He also said that at least 80 of these individuals have subsequently returned to Canada.

Terrorist activities require funding and we know this funding is obtained from legitimate sources as well as from illegitimate ones. We also know that some of the funds that are raised to finance these violent crimes originate in Canada or transit through our country. As an example I would cite the case of Mosin Khawaja, who was found guilty of, among other charges, providing funds to facilitate terrorist activities.

With this, we have seen very clearly the devastation that terrorist groups can inflict when they have access to substantial resources.

FINTRAC disclosures, which are often based on hundreds or even thousands of financial transactions reported by Canadian businesses, help establish links between individuals and groups in Canada and abroad suspected of financing and supporting terrorist activities.

For example, at the end of the April, the RCMP integrated National Security Enforcement Teams in Ontario and Quebec recognized our contribution to a terrorist financing investigation on the International
Relief Fund for the Afflicted and Needy Canada, or IRFAN-Canada, an organization allegedly linked to the terrorist entity Hamas.

Last year, the RCMP also acknowledged FINTRAC's contribution to Project Smooth, following the arrest of two individuals for conspiring to carry out a terrorist attack against a VIA passenger train.

Given the complex and transnational nature of terrorism, we maintain very strong and productive working relationships with our police and national security partners. In order for our financial intelligence to be actionable, it must be closely aligned with our partners' priorities. We ensure this alignment through regular contact, as well as our participation in the Canadian Association of Chiefs of Police and its committees dealing with organized crime and national security.

FINTRAC also works closely with other financial intelligence units around the world in order to share intelligence and expertise, broadening our reach and analysis of international financial transactions.

Financial intelligence -- both tactical and strategic -- has become a key component of our regime partners' terrorist investigations. FINTRAC has provided timely and relevant disclosures as part of the government's broader effort to combat ISIS and others who have supported terrorists at home and abroad.

(French follows - Mr. Cossette continuing - En conclusion, Monsieur le President, le succes du regime canadien de lutte contre le terrorisme, dépend du dévouement de toutes les parties concernées, des entreprises aux particuliers, du systeme financier canadien, aux procureurs qui font condamner les criminels qui recueillent des fonds et financent le terrorisme. Ensemble, nous produisons d'importants résultats pour les Canadiens et les Canadiennes.

Monsieur le President, honorables sénateurs, je vous remercie et nous nous ferons un plaisir de répondre à vos questions.

(The Chair: Thank you very much. We certainly appreciate the presentation.)

(French suit)

(French follows - Mr. Cossette - maintenant un plaisir de répondre à vos questions.)

The Chair: Thank you very much. We certainly appreciate the presentation that you've presented to us here today.

I would like to begin with a couple of short questions. One is in reference to your statement that there were 234 disclosures specifically related to terrorist financing and threats to the security of Canada this past year.

Can you provide us with a full list of disclosures shared per year since 2006 as it relates to terrorism? Can you tell us how many were related, when it comes to terrorism, to charities and non-profit agencies?

Mr. Cossette: I don't have those numbers with me, Mr. Chair. We could provide those numbers to you and we will do that.

The Chair: I want to follow up further, colleagues, in respect to the question of charities and non-profit agencies. As has been stated, government action has been involved in respect to reviewing some of these agencies from that point of view and financing terrorism. Has your organization been involved in government action against terrorist organizations benefiting from charitable status under the Income Tax Act? Can you provide further examples of that?
Mr. Cossette: When it comes to monitoring and reporting on activities, FINTRAC does not monitor organizations or nongovernment organizations. FINTRAC monitors transactions and transaction reports that are provided to us by reporting entities.

The fusion of transactions and names, or individuals or specific organizations, happens when we do receive from our partner specific information about organizations. For instance, Mr. Chair, if I were to receive a transaction about Gerald Cassette, it doesn’t say whether I am a member of a specific organization, according to the banking transaction reports. It is the mix of the information we receive from financial institutions and what we may receive from our security partners that brings these two things together.

In answer to whether we monitor specific organizations, we do not monitor specific organizations. CSIS, the RCMP and CRA use the information we disclose and then they go after specific targets or investigations.

Senator Mitchell:

[French follows — Senator Mitchell : Merci beaucoup, Messieurs, pour votre présentation. C’était très intéressant et très bon.]

(après anglais)

Le sénateur Mitchell : Merci beaucoup, Messieurs, pour votre présentation. C’était très intéressant et très bon.

(Sen. Mitchell : I’m struck by the point you make in your presentation …)

[Following French — Senator Mitchell continuing]

I’m struck by the point you make in your presentation that you have worked and made your contribution in close cooperation with our police and national security regime partners. That is very important and very significant, and you do mention that you have provided information. What is the nature of that relationship with the CRA, CSIS and RCMP on sharing information? What are your thoughts about those organizations having direct access to your data banks in that respect?

A corollary of all of that is how exactly would you ensure proper use and proper privacy consideration protections?

Mr. Cossette: If I may, Mr. Chair, I will answer the second question first. That will explain the kind of relationship we have with our partners.

No one and no organization but FINTRAC has access to FINTRAC’s database. Our security partners do not directly access our database, be it the RCMP, CSIS or police forces. We do receive information from financial institutions according to our legislation. If we do establish that that information may be useful in the context of a money laundering or terrorism financing or a threat to Canada investigation, and if it meets that threshold, then we will communicate to the relevant partner.

It is not as if we collect the information and it sits there and people come and tap into it. We do have to establish that threshold that there is suspicion of money laundering or terrorism financing/national security before we can communicate the information to our security partners.

In terms of meeting their requirements, we do sit with them when they establish their priorities. Is it organized crime and what is under organized crime? We do that with the RCMP, for instance. We do the same with regard to CSIS. What kind of target are they after? Are there certain regions of the world that are of interest to them? We consider lists that the United Nations Security Council may have released.

We work with them at the outset to establish the priorities and then we disclose tactical information. As we disclose to them, we also ask for their feedback as to whether what we are providing is useful, relevant, timely and so on.
Senator Mitchell: One of the key elements of the usefulness of this kind of information, among other things including relevance, accuracy, predictability, and tailored to the point, is timeliness. There has been some concern in the Intelligence community about not just FINTRAC to others but about the timeliness with which information is shared. There has been a specific criticism in the case of FINTRAC - I may be wrong. Can you give us some idea about whether that criticism is legitimate and what you do to ensure either reaction to that criticism or fixing it or ensuring timeliness in the sharing of information?

Mr. Cossette: Our partners today are telling us that the information is very useful, relevant and timely. This is the feedback we get. Over the past couple of years, and Luc could expand on that if it is of interest to you, Mr. Chair, we have improved the processes that allow us to disclose much more quickly than in the past.

Over time of course, we have accumulated information that is looked at on an ongoing basis. We don't necessarily wait for requests before analyzing the information that comes in. I don't know how you call it technically, Luc, but we have a process that allows us to disclose much more quickly than we did in the past. If we have names of individuals and organizations provided to us by our partners, we may keep those files open so we don't have to start the process every time there's a request.

Senator White: Thanks for your presentation. I have an understanding around the $10,000 trigger that we would see. Is there consideration around multiple triggers? In other words, we have seen in the past where known groups that certainly were training in terrorism in other countries were moving amounts of money less than $10,000 -- $9,999 might be the number, I guess. You are saying that you don't get access to information that allows you to look for second or third triggers. Would it be helpful to you if you did? It certainly would be helpful to Canada if we did.

A story comes out of Quebec to be fair, about the amount of money that travels to one particular Caribbean island every Friday night, and it is always less than $10,000, from a movement of illegal funding. It would make sense to me that we have other potential triggers that would allow us to do this, if you don't already. I think you are telling me you don't do that now, is that correct?

Mr. Cossette: There are three things I would say in response to that question, Mr. Chair. Given the limitations provided by the $10,000, when people transact at a lower threshold, we work with the financial institutions more and more to reinforce the suspicious transaction reports, which have no threshold. If financial institutions see patterns that they consider to be abnormal given the regular behaviour of their customers, they can disclose to us. The amount of money in those cases is irrelevant. It may be $200 or $300; it doesn't really matter. Given the limitation of $10,000, we have worked with the financial institutions a lot to reinforce the capacity to produce useful suspicious transaction reports.

When we're looking at thresholds below $10,000, and it is often even more relevant in the context of authorizing financing, the issue there to be honest so far has been the capacity to process that information because then you would be talking about millions and billions and millions of transactions. Numbers and technology have to work hand in hand. We are in the process of acquiring a system that will be able to process many more transactions in the right amount of time than we can process now. Once we have acquired that capacity, the time will arrive for us to review. As we speak, the tools we have provide us with what we need.

Senator White: I appreciate that. Have you given consideration to “will fly” lists of people whose names come through banking to actually share that intelligence across the spectrum of enforcement agencies to identify them? For example, if Vern White has been identified at Toronto Pearson and has only $4,000 but happens to be noted in some of our investigations as being involved in some suspicious transactions, officials at Toronto Pearson could do something and notify our on site officials in the country of destination that the individual is travelling there.

Have you had that type of dialogue? If you can't answer me now, it's okay.

Mr. Cossette: We haven't had that type of dialogue. We do have financial institutions reporting more and more on suspicion of either money laundering or terrorism financing. The number of suspicious transactions reports has increased by 16 per cent over the past two years. We've convinced that it is because
we work with them to make sure they understand that such a report makes a difference. Recently, we have seen suspicious transactions reports being sent to FINTRAC for which there was not necessarily a request from CSIS or the RCMP. We disclose, from our perspective, to those organizations without waiting for a specific request. We do that as well.

Of course, we respond mainly to requests we receive, but there is also an attempt to be proactive, as much as we can be, in terms of disclosing information that may not be available to our partners.

Senator Stewart Olsen: I have a few questions following up with the report that banking did on FINTRAC. I have to note, Mr. Cossette, that you made several changes already that I can hear in some of the questions.

To my specific questions, how do you follow up once you report this to your various partners? Do you get a regular follow-up, perhaps quarterly, as we recommended? What happens once you have reported what you would consider to be suspicious transactions?

Mr. Cossette: We ask our partners to report to us on each transaction we send to them. We ask a certain number of questions to assess whether the information and the format are useful. We also ask what makes a difference to them in all the information we convey to them? Is it the beneficiary ownership? What is it in a suspicious transaction report or series of reports, because some of our disclosures may have hundreds of different reports, that makes a difference so we can have the feedback?

We also have an ongoing dialogue. Once in a while, we try to bring the financial institutions and the security partners together so that the financial institutions can explain how it works and what makes a difference.

A couple of weeks ago, Luc gave a presentation to a number of financial institutions on suspicious transactions reports that are useful in the context of terrorism financing. We have feedback, as much as we can get, from both the financial institutions and the partners.

Senator Stewart Olsen: Does that feedback include whether they would prosecute based on your information? Do you have that kind of feedback?

Mr. Cossette: Luc probably knows that better than I do. We're being told, for instance, "This is a name we did not have. This is a link we did not see before." The advantage we bring to the table is the horizontal view of what we see. Investigators look at their investigation. We may see something in Newfoundland that is related to Alberta that is related to Quebec, or what have you. We're told very often that this picture is new to them. They may change the focus of their investigation because of the information we provide. They may launch new investigations because of the information we provide. Sometimes they're not as specific as one would ask, in a sense that our job is to provide intelligence and their job is to investigate; so what we don't need to know, they don't tell us. That's the understanding we have with both security agencies and police forces.

I don't know if the others more you want to add.

Luc Beaupré, Manager, Terrorist Financing Intelligence Group, Financial Transactions and Reports Analysis Centre of Canada: Our job essentially is to draw the picture and point the finger toward where they need to investigate. That's their job.

The feedback we receive can be different at different stages of the investigation. At the start of an investigation and at the end the feedback is different, but it is important to have it. We collect the stats, but we also get informal feedback because we talk with the investigators. We want to make sure that our product is useful and that we're not wasting their time.

Senator Ngo: In your presentation you say that you work closely with other financial intelligence units around the world and so on. In light of the demonstrated interests in foreign intelligence services, criminal organizations, terrorist groups try to gain access to the government-held information. What is the state of
FINTRAC's cybersecurity defence? What is the state of FINTRAC's personal security, particularly in the context of insider threats and risk, potentially involving FINTRAC by a third party?

Mr. Cossette: When it comes to cybersecurity, we're of the view that we are as well protected as any of our sister organizations. We have the right system. When we're looking at the classified information, which is where we mesh together information provided by financial institutions with the information provided to our partners, this is a top secret system. It's on a separate floor; it has limited access. From an outsider threat potential, it is as well protected as any other organization.

We follow the standard. In fact, we have CSIS come once in a while to do an analysis of internal and external threats. We work with the Communications Security Establishment in order to establish our requirements when it comes to cybersecurity. We have a fairly robust regime in the sense that the Privacy Commissioner comes to our organization every two years and assesses whether the information is used for the purpose it is intended. Our legislation also has a robust framework. If people were to be found, for instance, they can be charged for up to five years and half a million dollars in penalties but moreover, we do encourage a culture of security.

To give you a specific example, tomorrow I'm launching a series of representations for all the analysts at FINTRAC, reminding them of the external threat, the internal threat, what they should and should not put on the web. We also have limited access — not technically but from a policy perspective — for instance, to social media. We do not encourage our people to use social media and at the office, they are prevented from using social media. We try as much as we can to make them understand the context they are operating in, which is a security agency.

Senator Ngo: Could you provide the committee with what security screening is practiced in FINTRAC, for example, and with what frequency?

Mr. Cossette: If you look at the security level of our employees, all our employees need top secret level security, so it's not only enhanced security; it's secret. Then there is a top secret requirement to it. And even for employees working in other departments that come to join FINTRAC, either for a short term or long-term, sometimes we redo some of the screening to ensure that they meet our own standard. From that standpoint, we're as high as the Government of Canada allows us to be.

Senator Beyak: Gentlemen, it's my understanding that since FINTRAC was established, Canada has only convicted one person of terrorism financing. Could you elaborate on that a little bit and tell me if there's a reason to your knowledge?

Mr. Cossette: I would say, Mr. Chair, this is outside of our mandate. Our contribution in that whole process is basically to receive information, process it and disclose it. What happens after that step would be much better answered by your police forces or Public Prosecution Service of Canada because, as I said, the information we provide is intelligence, not evidence, so why that evidence does not lead to convictions is difficult for me to answer.

Senator Mitchell: I'd like to pursue a point raised by Senator Ngo with respect to your relationships with international agencies that would be your counterparts. I would like to know specifically what is your mandate to develop and to deal with them. Where does that come from? And in light of the Arar case, which hangs over a lot of what you do and what this committee will be discussing, what safeguards do you have about agencies that you deal with using that information and giving it to a third party?

Mr. Cossette: First, we do not share information with counterpart organizations that don't have an MOU with us, a memorandum of understanding, which is reviewed and approved by the Minister of Finance. So we have fewer than 50 MOUs as we speak, and the MOUs request foreign countries or countries with which we're doing business to have a privacy regime similar to ours. It does not have to have the same shape, but it needs to provide the same safeguards. The second thing is that the MOUs do not oblige us to disclose, so if we would prefer not to communicate information for all kinds of reasons, there is no binding obligation to do so. We decide on our own whether the country requesting the information should get it or not.
The third thing is that we do disclose exclusive leads to other organizations, such as FINTRAC, so we have no authority, for instance, to disclose our information to the FBI in the U.S. or to any other agencies worldwide. What we can disclose, how we can disclose it is fairly well protected by the mechanisms we have. We do receive and send requests – very specific – and if there is a requirement to go above and beyond what we would provide according to our legislation, we ask the foreign country to go through our RCMP or enforcement agencies. That mechanism is well in place and is properly used.

Moreover, we do not do business with countries that are not members of the Egmont Group, which is an international group of financial intelligence units, so we know with whom we’re doing business.

Senator Mitchell: I have several more questions, but I’ll come back later. Think you said that the information you might give to your counterpart in the U.S. wouldn’t go to the FBI.

Mr. Cossette: We cannot disclose directly. We disclose exclusively to our –

Senator Mitchell: Is there any element of your MOU with your U.S. counterpart that they cannot disclose it to the FBI?

Mr. Cossette: We would ask them to ask our permission.

Senator Mitchell: That’s not binding, necessarily.

Mr. Cossette: Once they get the information, they have the information.

Senator Beyak: If your information was expected to be available or involved, was there any time, to your knowledge, that an Attorney General did not consent to that information being used to convict for terrorism financing?

Mr. Cossette: Our information is rarely used directly. Our information is used by enforcement partners either to obtain a production order, search warrant and other things. It is not evidence. It’s not like what the police do, which is build a case to demonstrate that something has occurred. We are in the intelligence business, so we signal potential things. How that information is used by the police forces is their own decision. We did have to testify in court once or twice. I think, to explain how our financial information was used, but as I said, it is part of a much larger way of working.

Senator Dagenais: Mr. Cossette, thank you for being here.

Why has it been more difficult to convict a person believed to have engaged in terrorism financing compared to money laundering?

Mr. Cossette: Once again, Mr. Chair, it’s difficult for me to assess how the judicial system works, once outside the realm of my own mandate. The only thing I would say is that terrorism, unfortunately, is international activity. International activities are always more difficult and complex in nature than national ones. I will stop here. Lawyers or prosecutors would be in a better place to explain how the system works. I’m sorry.

Senator Dagenais: I have another question. FINTRAC says it has analyzed trends in money laundering and terrorism financing. What kinds of general trends have you discerned in terrorism financing? Do specific countries, regions and other causes stand out statistically in this regard, and do certain categories of Canadian and dual nationals from specific regions figure more prominently statistically?

Mr. Cossette: If I may, Mr. Chair, I will not provide specific numbers. This is information, of course, which cannot be made public. What I would say, though, is that we are looking at money transfer from Canada to conflict zones. If you’re asking if we’re looking at what’s going on in Syria, yes, we are. If you’re asking us if we’re looking at what’s going on in Iran, yes, we are. Yes, we are looking at what’s going on in Iraq right now, to identify whether patterns that occurred before those conflicts have changed. Are there individuals or companies in Canada which used to send money to Syria, let us say, for the sake of argument, that don’t any longer because Syria falls under sanctions, but are sending the money all of a sudden to a border country with which they never did business before?
We look at these kinds of things to look at patterns. These patterns are used not only by our security partners, but they may be used by a larger number of partners, such as the Department of Foreign Affairs or the Department of Transport or even the banking system, if it may be relevant.

In that context, we look at transfer, as I said, toward conflict zones. But we do the same thing when it comes to specific groups in Canada, where their money may be going and whether these patterns are changing. We may be looking as well at money coming into Canada. Take, for instance, a sampling, a kind of transaction, and see whether, if you compare that with another group, you see the same kind of pattern. At the macro level, we do that as well, but of course we cannot disclose. Even in the communications we have with partners such as DFAIT, we cannot disclose the name of the individual, the name of the banks or that kind of information.

The Chair: I want to follow up, if I could, in respect to the question of laundering money for organized crime versus perhaps that of terrorism. Following up with the money with organized crime, you obviously have the ability, at least to identify in part, that type of criminal organization that is actually laundering money somewhere in the world; is that not correct? Through FINTRAC you at least identify in a general sense?

Mr. Cassette: We do identify groups because our enforcement partners provide us with the names and the connections between that name and the group. As I said before, if I see a transaction under my name, it doesn’t say “Gérald Cassette, member of X criminal group,” but we do receive information from our partners saying, as I said, “belongs to such a group.”

The Chair: I want to follow up with organized crime, because it has been said that perhaps in some cases organized crime is involved in one way or another in financing some of this terrorism activity. Is there any truth to that? Perhaps you could expand further on that particular question.

Mr. Cassette: The main difference between criminal organizations and terrorist organizations is that terrorists use illicit money and they acquire that illicit money the same way the organized crime does: fraud, credit card fraud and so on. So how they make money is similar to what the organized crime does.

Where it differs is that there is illicit money, proceeds of crime, but there is also legitimate money. People may contribute to terrorist organizations from their salary. So the money is not necessarily illicit; the source of that money is legitimate.

The second difference is that organized crime commits crime for profit. Terrorists collect money as a means to finance terrorist activities and terror. That’s the main difference. But the way they accumulate wealth as it pertains to illicit means are more or less the same: credit card fraud, stealing, Ponzi scheme, extortion.

Senator Day: Mr. Cassette and Mr. Beaudry, my apologies for being a wee bit late. I did have the opportunity, Mr. Cassette, to review your written comments, so I know generally what happened when I wasn’t here.

Could you tell me how many employees and how many analysts you have in your organization?

Mr. Cassette: We have about 305 employees, split in different groups. The groups which would be of interest to this committee are basically the compliance group, which is in charge of the interface with the reporting entities and then the financial analysts; the group to which Luc belongs, where they do basically the financial analysis.

Senator Day: So what you’re providing to financial intelligence to your enforcement partners, those entities you’re entitled to reveal the information to, so that is financial information you’ve received from all the financial institutions, etcetera, that has been analyzed. Are all the analysts analyzing that according to your mandate, money laundering and anti-terrorism, or do you fine-tune your analysis and different analysts look at the information from a different point of view, depending on to whom you’re giving the information and you’re passing it on to?
Mr. Cossette: Our mandate is very clear and narrow. It's about money laundering, terrorism financing/national security. In order for us to disclose information to our law enforcement and security partners, we need to reach that threshold, which means that we do receive reports from financial institutions that may never be disclosed because there is nothing in the report that shows suspicion of money laundering or terrorism financing, unless we get a specific name of a terrorist. But even then, the transaction has to suggest something, otherwise we would be disclosing everything we received.

Our legislation has been written in such a way that it has to be based on suspicion of money laundering and terrorism financing. We do not disclose on proceeds of crime. We disclose as long as it pertains to money laundering most of the time.

Senator Mitchell: I'm interested in the example you used. Mr. Cossette, of a company that may have been sending money to Syria and then, due to changes with that relationship, they're sending it to a border state, and that raises suspicions. How do you get on to that company in the first place? Are the banks letting you know or do you need a warrant to then go the next step to check them? What's the legal relationship to your being able to get that information?

Mr. Cossette: We have no investigative power. That has to be clear. Investigative powers reside with police forces. So how it works is that the legislation compels financial institutions to report on a certain number of things. Once we get the information and we establish that it's suspicious or there is a change in pattern which may suggest something, we may disclose to the police force and say, "We see here a change in patterns which suggest either money laundering or terrorism financing." The police force decides if they want to proceed. If they do, they may obtain a warrant or a production order, but we have no legal authority to do that.

We're being asked that, Mr. Chair, very often. Why don't you go back to financial institutions? Our legislation does not allow that. That's for the enforcement agencies to do. If they decide basically to pursue their investigation, then they do what they have to do.

Senator Mitchell: Do you have an opinion about whether your legislation should allow that?

Mr. Cossette: The regime allows it in the sense that the police force can do that job.

Senator Mitchell: You don't think it's something that you need to be able to do?

Mr. Cossette: I think Parliament has to decide how far we want to challenge the privacy of Canadians. Our legislation provides us with a very low threshold. If we wanted to go further, I think parliamentarians will have to assess whether privacy in this context is more important than security.

Given the fact that our threshold is low, because we receive the information, the way we may use that information is limited by our mandate in legislation.

Senator White: Thanks for your answers. They're excellent. You made a comment earlier about X criminal group or criminal organization. In the case of terrorists or terrorist organizations, we list them in this country and it's pretty easy to identify when they're sending money to a specific country. We can quickly identify whether or not they're going to a listed terrorist group. Would it help if we listed criminal organizations as well?

Hell's Angels are a criminal organization, everybody in the country knows it. Yet we still don't list them as one, even though I think we're saying it publicly today. Would that be helpful to the manner in which you provide information that the information could go back and forth if we start listing known criminal organizations that have been identified in courts a number of times, for example? How we list them is up to Parliament, I guess.

Mr. Cossette: It would not be helpful in the sense that we're tracking individual and business transactions. So even a terrorist group in Canada, Hamas or any terrorist group, unless you have names
associated with people belonging to Hamas it's impossible for us to know that they're Hamas. From that standpoint it has its limitations.

Senator White: But the fact is, with Hamas there are names attached to it. So it does help at some point. An investigative authority at least, if they're coming back and saying so-and-so belongs to Hamas, we have a couple of transactions, obviously you want to know when they're doing transactions, don't you think the next step in the criminal organization would also do it? I'm not trying to be argumentative.

Mr. Cossette: To a certain extent, Mr. Chair, that's what happens now.

Senator White: With terrorism?

Mr. Cossette: With criminal organizations as well, because the investigators may come in and say we are investigating Mr. So-and-so, who is so-and-so. That's how, at the strategic level we can track, for instance, the amount of money we may say related to the Hell's Angels or any other criminal organization.

It really depends, as Luc was saying, on the information which was provided to us on specific cases. So sometimes the information requests are very comprehensive and they tell us the whole story. Other times it's more limited.

Senator Day: I have two questions and I only have a limited amount of time, so I'm going to try to combine the questions if I can. It relates to the analysts, again.

You analyze according to your mandate, but some of the entities in Canada, in particular, may have an interest that's a little bit different because of the particular entity. What are your views with respect to your database being made available to these other entities so that they could analyze according to their particular mandate as opposed to taking the intelligence that is a result of your analysis?

One of the entities that I am thinking of is Revenue Canada. They may well be interested in tax evasion, which could easily be tied into terrorism if you wanted to take a broad perspective like you did earlier in relation to laundering.

Mr. Cossette: Mr. Chair, we already disclose to CRA. We disclose for tax evasion purposes, as long as the information which is provided to us meets two thresholds. The first is money laundering; second is tax evasion. So we disclose to CRA as we speak.

Moreover, in Budget 2014, if I'm right, or in other legislation, in fact CRA will now have access to the same international electronic fund transfer that FINTRAC accesses right now. CRA will not have access to our database. Technically the information will come from the financial institutions, one way to FINTRAC, one way to CRA, exactly the same international fund transfer. Not all the other information, but that information because it's relevant to them when it comes to tax evasion.

What may have been perceived in the past as a lack of sharing of information between our two agencies is disappearing very quickly because that capacity will be made available as of January 2015.

Senator Stewart Olsen: Just very briefly, and it's more a point of clarification. Is this information tracked two ways? For instance, can an investigative agency, say CSIS or RCMP, give FINTRAC a name or an organization and ask for information on that?

Mr. Cossette: That's what works most of the time. That's how we proceed. I don't know what the percentage of the business is.

Mr. Beaury: Approximately 80 to 85 per cent of our cases are based on information voluntarily provided by our partners, and 15 to 20 per cent of the cases are those that we proactively initiated. That's roughly, I would say, the breakdown.

Mr. Cossette: For precision, we received more than 1,300 requests from CSIS and the RCMP last year, to which we responded 1,143 times.
Senator Mitchell: I'm interested in the question of, again, the relationship with these other agencies and the sharing of information. You made the point, Mr. Cossette, which was very pertinent, that you've sped it up. You implied that you've changed the process to some extent to do that. I wonder if there's a way that you could reveal that to us.

It was suggested by the Banking Committee that actually other agencies, CBSA, CSIS, have direct access. I'm maybe rehashing that ground. Do you think it would speed it up even more and there wouldn't be too much downside if they did have direct access? Or are you a proponent of keeping the two separate and having the door they have to pass through and you have to pass through to make sure things are contained?

Mr. Cossette: When it comes to speeding up the process, I'll let Luc explain the changes we've made to our processes so it goes faster. But when it comes to direct access, there are two things.

Our legislation flows from the Criminal Code, so therefore the threshold is very low. That explains why we have no investigative powers and why police enforcement agencies need warrants and so on and so forth. If you were to give access to our database to other organizations you would need to change the nature of the relationship. The legislation has been created explicitly not to give access, given this very low threshold. That's the first issue.

The second issue is if you work to give them direct access they would need to develop their own capacity in terms of analyzing the information and making sense of it. So we have developed, since 2000, an expertise which is exclusive to us. Yes, provincial police and large municipal police forces have analytic capabilities as well, but that's what we specialize in. If you were to move that elsewhere, you would need to reproduce that same capacity in a series of organizations. The service is very much in demand, so therefore if we did not do it somebody else would have to.

Mr. Beaudry: Very succinctly, we've instructed our frontline analysts, who are reviewing all the SCRs, all the information that is coming up, with the authority to bring up to the line of management directly when she sees issues of national interest rapidly. Essentially we've cut the red tape around the review of important alerts.

When it's time to get management's approval to release the disclosure, this is something we can do within a matter of minutes. If we see it as an important aspect, we've done disclosures within an hour. It's possible to do it. So when people ask if we're timely, we pay very close attention to the issue at hand and if it requires immediate action we immediately disclose.

The Chair: I want to follow up on one other question here, and that has to do with a statement that you made in your opening remarks.

You state that, for example, at the end of April the RCMP's Integrated National Security Enforcement Teams in Ontario and Quebec recognized our contribution to a terrorist financing investigation on the International Relief Fund for the Afflicted and Needy Canada, IRFAN Canada, an organization allegedly linked to the terrorist entity Hamas.

Now, my understanding is that that particular organization was under scrutiny or investigation for a number of years. Finally, at this point in time, in April, it was finally identified and certain steps were taken.

In view of the information that you provided us today — there was, I think, 234 disclosures this past year, twice as many as the year before — I don't know how many the year before — are we going to see a further coordination of government responsibilities to ensure that if an organization such as this is utilizing their charitable status in a manner where it's financing terrorism that we're going to be able to lay charges earlier than later as opposed to this situation we're facing right here?

Mr. Cossette: The thing I can say about this, not this specific instance but the approach that is being taken when it comes to non-governmental organizations is work is being done right now under the Financial Action Task Group to better understand how non-governmental organizations are used, in fact, to channel money to terrorists or illegitimate organizations.
With regard to this specific case, it is a long story of knowing what is happening, not knowing what is happening, knowing what is happening, not knowing what is happening, and when it became clear enough then there was a possibility for the enforcement agencies to take action, but it is very difficult just at the outset to understand or, basically, to establish whether an organization does provide money to a terrorist organization.

It was possible to establish the relationship between IRFAN and Hamas, but it is not necessarily possible, given the way they hide their money sometimes, or the way they transfer the money around the world before it hits the final destination, the same way criminals do. It is a field which, in fact, is of significant interest not only to Canada, but to a number of countries, to have research work done.

The Chair: If I could, colleagues, I want to follow up on this. Is this just an example where you have a charitable organization identified with a direct link with a terrorist group, and yet we're not in a position to affect any changes in respect to what is transpiring because we haven't got enough records there on the financing from one country to another?

Mr. Cossette: In the case of IRFAN, or any organization, what you need to do is establish a relationship between this organization and the organization abroad.

The Chair: Right.

Mr. Cossette: Organizations that would like to provide money to terrorist organizations would use, more or less, the same kind of technique they use for laundering money, so it is difficult to establish the direct link between the people providing funding here and how the funding is used at the end.

In terms of terrorism, you need to establish that the fund at the other end is used for support planning and so on. It is difficult; it is more difficult than we would like it to be, but it is still difficult.

The Chair: Colleagues, we have gone over time. I want to thank our witnesses. Mr. Cossette, you have been very informative. Thank you for the time you have taken to present your information. This is part of the public conversation that we intend to have on this particular issue over the next coming months so that Canadians become aware of the threats we face and the responsibilities that government is taking on to see that they protect our peace and security.

Thank you for coming. We appreciate your work on behalf of all Canadians.

We will now continue our look at the terrorist threats to Canada. We are pleased to have with us Mr. Jeff Yaworski, Deputy Director of Operations, Canadian Security Intelligence Service. Mr. Yaworski, we appreciate your taking the time to be here with us today. I understand that you have an opening statement. Please begin.

Jeff Yaworski, Deputy Director of Operations, Canadian Security Intelligence Service: Good afternoon, honourable senators. Thank you for your invitation today to discuss terrorist threats. I will focus my remarks on the threat to Canada from terrorism and how the terrorist threat is rapidly evolving given recent world events.

As the director of CSIS stated on October 8 to a committee of the House of Commons, the threat from terrorism is real, and Canada must be vigilant in the face of it. The rise of the terrorist group known as the Islamic State in Iraq and the Levant, or ISIL, after breaking from al Qaeda over a year ago, represents a significant shift in the internal policies of global Sunni extremism and increased the complexity of the threat both internationally and to Canada.

ISIL's successes over the past year are largely due to its aggressive recruitment, fund-raising and propaganda efforts and its opportunistic territorial expansion into Iraq and Syria. Canadian interests could be affected by the region's continued slide into instability. This includes the security of our Armed Forces who are deployed and in the process of deploying to the region, the security of our regional allies and the potential for greater refugee flows and displacement of persons. CSIS will continue to appropriately advise
the government on these threats and issues just as we have in the past, for instance, on Afghanistan and the conflict in Libya.

ISIL's recruitment and propaganda efforts, alongside other extremist groups, continue to attract violent radical Muslims worldwide to join its ranks. ISIL has engaged in one of the most sophisticated and successful social media campaigns of any terrorist group to date. While some of ISIL's propaganda videos are certainly gruesome, they also work. ISIL has recruited thousands of individuals from across the West and the Middle East, particularly young disenfranchised males with a fascination and penchant for violence.

Honourable senators, as we know, Canadians are not immune from such efforts. The Service is aware of at least 50 Canadians involved in terrorist-related activities with ISIL and other extremist groups in the region. Of these individuals, we are aware of approximately 30 in Syria alone, with the remainder located in Iraq, Turkey and associated border regions. The participation of Canadians in these conflicts is harmful to our international reputation and destabilizes regional security. Canada has an obligation to do her part to prevent such travel.

As the director of CSIS noted recently, we also remain concerned over the threat posed by individuals returning to Canada after having engaged in threat-related activities abroad, whether with ISIL or other groups, like Jihadi John and Nusrah in Syria. While such individuals' experience and determination vary widely, it only takes one individual or a small group of individuals to cause great harm. We are currently aware of approximately 80 individuals in this regard, and we actively monitor them, some under judicial warrant, for any threat to public safety.

We also remain concerned that global events could shape the threat environment in other ways detrimental to Canadian interests. For obvious reasons, CSIS remains concerned that ISIL's message and successful social media strategy could inspire radicalized individuals to undertake attacks here in Canada. Senators would be aware of such a possibility from recent arrests in Australia, where an ISIL-inspired terrorist group planned to engage in random acts of violence against innocent civilians. CSIS is actively investigating any such possibilities and will, of course, advise the appropriate parties on such matters, but I would also like to stress that, as the director has stated, CSIS has no information to indicate that a terrorist attack in Canada is imminent.

In addition to domestic threats, global events increase the threat to the safety of Canadians in embassies throughout the world. CSIS works cooperatively with and provides advice to our partners at DFATD to address such threats. However, as always, I would certainly encourage Canadians to check DFATD's travel advisories before travelling internationally to make informed decisions on these matters.

Honourable senators, the dynamics between global jihadist groups is of concern for CSIS. How the competition between ISIL and al Qaeda plays out will determine much of the evolution of future threats. For instance, given the rise of ISIL, al Qaeda and its affiliates may increase their operational tempo against Western targets as a means to maintain relevance with followers who are increasingly leaving al Qaeda to join ISIL. Such a scenario is of plain concern. Conversely, one could also see a rapprochement between the two groups, which could lead to a leveraging and coordination of resources between the groups.

CSIS is working with our international partners to keep a keen eye on such developments to ensure that the Government of Canada is well advised in this increasingly complex threat environment. In that regard, we welcome the minister's announcements last week proposing various amendments to the CSIS Act, particularly by confirming our ability to operate internationally.

As the discussions over terrorism and ISIL today demonstrate, the ability of CSIS to work abroad is vital in addressing threats to Canada's national security. Without such an international presence, Canada would lack understanding of threats to the security of Canada that originate or form overseas.

Senators, I say these things to put the threat in plain sight. The men and women of CSIS are actively engaged in investigating all of these potential dangers with our partners at home and abroad.

As senators would be aware, the government recently released its public terrorist threat report, which updates the government's four-pronged strategy to prevent, detect, deny and respond to the terrorist
threat. The service’s primary role in this strategy is to detect the terrorist threat and provide the government with threat-related advice. Such a role is entirely consistent with CSIS’ mandate under its act, which is to provide advice on threats to the security of Canada to a variety of government departments and agencies.

In that regard, such advice can take many forms and can address the threat at different stages. For instance, CSIS provides screening advice to the CBSA to prevent dangerous individuals from entering Canada in the first place. For Passport Canada, we provide advice that can lead to the revocation of passports to prevent Canadians from travelling to places like Syria and Iraq to engage in armed conflict. Of course, we continue to work with our colleagues in the RCMP, who can initiate criminal investigations upon receiving a disclosure letter from CSIS. In this regard, CSIS is proud of our part in many of the successful prosecutions since the attacks of 9/11. I understand the RCMP is scheduled to appear later on this topic, and I am sure they can provide further context on these matters.

Senators, while cooperation with our government partners is essential, our work also relies on the cooperation of citizens. As I have stated before, CSIS has no information indicating an imminent threat, and I would encourage all Canadians to go about their daily lives. That said, national security is everybody’s business, and I would encourage Canadians to be vigilant and to report any potential threat to national security to CSIS or their local police or by making use of the RCMP’s national security tip line.

With that, I welcome your questions.

The Chair: Thank you very much, Mr. Yaworski. We appreciate you coming here this afternoon to discuss a very serious issue that Canadians face, and I would like to begin with the first questioner, Senator Mitchell, Deputy Chair.

Senator Mitchell: Thank you, Mr. Yaworski, for being here with us. I’m interested, as I’m sure most Canadians are, in the announcement by Public Safety Minister Blaney about changes that he’s contemplating to your ability to do what you feel you are not able to do now.

If you were him for a few moments, what changes would you want in your act or in your mandate and your authority to do what you feel you are not able to do now?

Mr. Yaworski: I have to be careful in my answer to this question, senator. As you are well aware, the bill hasn’t been introduced yet. It will be introduced this week, and I would feel much more comfortable addressing those sorts of questions after the bill is actually introduced.

There has been some speculation on the content of that bill, some speculation that perhaps is not as well-educated as it could be, and, certainly, I think those issues will be addressed in significant detail once the bill is introduced in the House of Commons.

One of the issues that does come up and that I know has already generated media attention concerns CSIS’s human sources. What I would like to say on that point is that the service relies extensively on information that is provided to us by human sources. We can’t do our job without it. They provide us with lead intelligence that helps to save Canadian lives. They’re operating against some very nefarious groups. It doesn’t take much imagination to look at what we have already seen in terms of what these groups are capable of with individuals innocent civilians. For them to discover a perceived traitor in their midst, who is providing information or intelligence to CSIS, would be extremely risky for that individual, as well as for that individual’s family.

Senator Mitchell: To get more specific, you use the number of 80 individuals, approximately, that your organization believes have returned from fighting in some sort of a terrorist organization and are now in Canada. At face value, that might be disconcerting to people. What reassurance can you give? Do they still have passports? Do they walk freely? What do you do about them? Are you watching them so that you can see if they have networks?

Mr. Yaworski: Certainly, those 80 individuals that I referred to have had different experiences over there. While you refer to fighting with these groups, that’s not fair to say for each and every one of them. Some have been involved in fundraising. Some have been used to assist with their media and their Facebook
pages. They're very media savvy, and they've been used for that purpose. Others have attended language schools. Some have attended more radical schools that we are quite concerned about, but not all of them are hardened fighters as you described it. Each of their experiences has been different.

Therefore, when they do come back to Canada, obviously, we have to monitor their activities as much as we can but prioritize as well. We can't devote all of our resources to all of them all of the time. So we do have to prioritize those individuals. We do know where they are. We share information with the RCMP wherever possible. Your question about passports is a valid one. In order to get back into the country, they would have had their passports. In order to leave the country, they would have had passports.

It is important to note, as well, that, in terms of tracking these individuals when they leave, Canada does not have an exit information system. It is not always easy to know when those individuals have left.

Senator White: Thank you very much for being here, Mr. Yaworski, and for your responses. We have heard the terminology "extremist traveller" a lot lately. I am trying to get my head around why there's been a change from jihadist to extremist traveller. Is there something that has changed, or is it just a new terminology?

Mr. Yaworski: I think it is probably more of a terminology thing than anything else. As I said in my answer to Senator Mitchell, they're not all involved in jihadist-type activity. "Jihadist" I would attribute to actually fighting and potentially seeking to be killed in combat. The experiences of others, as I have already indicated, are quite different.

Senator White: Can you walk us through your key areas of concern outside of ISIL? Before ISIL came along, I know you guys were plenty busy. Can you give us an idea of what you are busy with besides ISIL right now?

Mr. Yaworski: It's CT threats because ISIL remains the most prominent threats. If you look at radicalization, it comes in many forms. Each individual's path to radicalization is quite different and unique. There's no one descriptor that can explain how one person went from sitting in the basement of his parents' home, surfing certain radical websites, to actually being engaged in the conflict in Syria itself. That step of radicalization and those individuals that are radicalized are quite concerning.

The al Qaeda core has probably diminished in terms of importance, but its message continues to resonate throughout the Internet. In this day of the Internet, these messages are readily available, and they're influencing the next generation. It is not simply to go and fight with ISIL, which is the group today, as there are other groups.

Canada has between 130 and probably 145 Canadians right now that are over there fighting. They're not all with ISIL. They're with other terrorist groups, such as Hezbollah, and in other parts of the country and North Africa, East Africa and West Africa. These Canadians are involved in activities overseas that they shouldn't be. The CT threat is much broader than just the ISIL group. It is something that concerns us greatly and is our number one priority.

Senator Stewart Olsen: You mentioned that we have about 130 Canadians, and then you said there are about 145. Is that number to the best of your knowledge or can you share that with us?

Mr. Yaworski: On any given day, the number changes. Individuals are put on the list when we acquire additional information that confirms their identity—that confirms their nexus to Canada. Individuals come off the list when they have returned to Canada or if we believe they have been killed in action. That number is a snapshot in time. Over the past year, the number has ranged between 130 and 145.

Senator Stewart Olsen: Of the 80 Canadians that you are monitoring, you said you can't monitor them all the time. How would you say you are monitoring them? Do you pick the most dangerous? How would you monitor them? How many man-hours are involved, approximately?

Mr. Yaworski: It is difficult to attribute man-hours. I don't want to give away all of our methodology in terms of what we're doing.
Senator Stewart Olsen: I understand.

Mr. Yaworski: With a number as significant as that, we have to prioritize. The point I was trying to make, Senator Olsen, is that we have to prioritize these organizations. We have to dedicate our limited resources to those we think are the greatest threat. For some of that, we have a wide variety of techniques we can use. I spoke about human sources earlier, which are our bread and butter in terms of determining what is going on and which individuals are more radical than others. We have the capability to acquire warranted powers on those who are the most significant risk to the country in terms of the activities that we believe they're involved in. The spectrum is quite wide, but we prioritize those targets as much as we possibly can.

The Chair: If I may, I'll follow up on this with respect to your knowledge as an organization and other government departments. We know that there are up to 145 actively fighting or fundraising or doing something else in respect of terrorist groups outside this country. We have 80 who have returned and are resident in Canada, I assume they are Canadian citizens.

Mr. Yaworski: Yes.

The Chair: Do you have an estimate of how many supporters here are actively involved with those 200 or 215 identified terrorist activists? How many Canadians are involved in supporting them? They have to have family; they have to go home; they have to do something. Do you have any idea? Are we talking about 300 or 400 or 500 people?

Mr. Yaworski: It is a good question, senator, because you are introducing another concept here of what we don't know, quite honestly. These are numbers we know. What keeps me up at night are those who haven't come across our radar screen. We're very dependent domestically, obviously, on working with our close partners at CSIS and CS and with the RCMP. Overseas, where many of those threats originate, we rely very much on our close cooperation with our allies.

The threat of terrorism is not something that we can manage on its own through our own platforms. We leverage heavily our partner agencies as they do on quite frankly. We cannot do it alone and nor can they. We have many partners that help us in terms of that.

With respect to those we don't know in Canada, the support network, as you say, each day we reassess our target inventory and learn about new individuals. When we're focused on one particular target, the ripple, if you will, when you cast the stone on the pond broadens quite extensively, and there are others who are affiliated with it. Our job is to determine which of those supporters, as you have described them, warrant further targeting. We constantly reappraise our target list and ensure that resources are dedicated to those at the top of the list.

Senator Day: May I have a point of clarification, Mr. Yaworski?

Mr. Yaworski: Sure, Senator Day.

Senator Day: ISIL and ISIS: What relation, if any, do they have to one another?

Mr. Yaworski: A close relation. They're the same thing. ISIL and ISIS are one and the same -- Islamic State in the Levant or Islamic state in Syria. It is a different translation of the same group, but they are the same. They are also sometimes known simply as Islamic state.

Senator Day: Have they contacted you and said they would rather be called ISIL than ISIS?

Mr. Yaworski: No, the communication channels are not that grand.

Senator Day: Let's talk about the Integrated Terrorism Assessment Centre.

Mr. Yaworski: Yes.
Senator Day: Our information is that it brings together federal intelligence resources and various Canadian entities along with the analysts and their database. Is FINTRAC part of that group?

Mr. Yaworski: I believe FINTRAC has representation on ITAC. ITAC as you described it is exactly that -- a collective community effort that provides assessments on counterterrorism files. While it is housed in CSIS, it is an independent entity. The intent of ITAC is to bring together those agencies as well as access to their respective databases.

Senator Day: We just heard from FINTRAC, which has a good number of analysts, that they don't share their database with others, yet maybe they do share indirectly through the Inegrated Terrorism Assessment Centre. We will have to try to trace that.

Mr. Yaworski: Yes.

Senator Day: Are you aware of the analyses done and provided by FINTRAC on financial transactions that could possibly relate to terrorism? Is that information helpful to you in its existing form or do you have to analyze it more from the point of view of CSIS?

Mr. Yaworski: First, let me clarify with respect to ITAC. While their employees are members of ITAC, it is their respective employees who have access to their database. They extrapolate from those databases what is germane to whatever file they are working on. It is not as if their databases are housed in CSIS as they're completely separate.

Second, in terms of what FINTRAC has provided us, because of their access to financial institutions, FINTRAC is provided information with respect to banking transactions. Through the information that they provide to the service, we're able to make connections between individuals in Canada who are transferring funds to other parts of the world.

Senator Day: Yes.

Mr. Yaworski: We're also able to see, through our own investigations, where the recipients of that money are. In some cases, the recipients are affiliated with terrorist organizations. We can solicit information from FINTRAC directly. Also, on occasion, FINTRAC provides lead information to us for potential investigative purposes. We get both.

Certainly, in the past couple of years, the volume of information we're getting from FINTRAC is on the increase and has proven to be very valuable to our investigations.

Senator Day: How long has ITAC, with the various policing and information-gathering entities, been in operation?

Mr. Yaworski: It just celebrated its tenth anniversary. CSIS celebrated 30 years and FINTRAC has celebrated 10 years.

Senator Beyak: It's my understanding that CSIS and the RCMP participate in outreach to terrorist threats and those who would perpetrate them. Is it working in your opinion? On balance, is it interfering with the possible laying of criminal charges before they go further?

Mr. Yaworski: The service has been involved in outreach. We do meet with members of the community on a fairly regular basis, but I wouldn't say to the extent of the RCMP in terms of the work they are doing on counter and radicalization. They've devoted a lot of effort, and if the RCMP does speak to the committee, they will be able to expand more on the terms of what they're doing to learn more about radicalization and countering radicalization in its very earlier stages. I can't help but think that would be a wonderful thing.

CSIS is not in that space. We have individuals who have an expertise in radicalization, but our focus is more on targeting and ensuring that we're aware of those individuals that are problematic, engaged in threat-related activities. In terms of whether outreach impacts criminal charges or not, that's best put to the RCMP.
Senator Daganais: Thank you, Mr. Chair. My first question, how are terrorists glorified in Canada and what can be done to prevent — clarification of radicals at schools, temples, mosques or other such places?

Mr. Yaworski: It is a very good question, Senator Daganais. It is one that speaks directly to the radicalization process itself. We are concerned that certain individuals who come back after having experienced combat — in many cases from far-reaching places like Syria and Iraq currently — who have been exposed to the military aspects will have obtained training in explosives, and those who have been directly engaged in the conflict themselves do come back to Canada with additional street credibility and the ability to further radicalize others within the community.

The glorification of those individuals is something that not only happens in small circles. It is something that is a big part of the radicalization process online. ISIL itself is extremely media savvy. They have a very good media program that helps in the radicalization and they do out great effort in trying to romanticize the conflict, romanticize what is truly a bloody and gruesome activity into something that has a more romantic appeal to it.

From that point of view, they are trying to glorify what are effectively terrorists engaged in terrorist activity.

Senator Daganais: We read last week that those living around nuclear plants in Ontario were given anti-radiation tablets. Can you describe the threat to our electricity grid and our power supply from terrorists?

Mr. Yaworski: Probably not as well as I should. I can tell you that nuclear facilities themselves are extremely secure. They have their own security facilities and guards who are functioning there. Obviously if the service was to acquire information on a specific threat to a nuclear facility, we would be directly engaged with them. We have no such information at this time in terms of Canadian nuclear facilities.

There is a threat out there to them. They are a potential target, but at this point there is certainly nothing, senator, that I would say is imminent in terms of a specific threat directed against our nuclear facilities.

Senator Kenny: Welcome, Mr. Yaworski. I’m concerned about your resources. It wasn’t too long ago that Jim Judd appeared before this committee and said that 50 per cent of CSIS resources were directed at Chinese spying in this country. We have also received testimony from members of your organization that it takes between 10 and 12 personnel to plant a listening device, and as many as 75 to 80 to follow somebody surreptitiously. If you have 80 people in the country now — and I did hear you say you prioritized — it sounds like you are going to have to put a lot of focus on a relatively small number just because your resources are limited.

Mr. Yaworski: Thank you for the question, senator. I can tell you, like other agencies and departments, we work within the budget that is assigned to us. We do have to prioritize. The foreign fighter threat is one that is growing. The returns are one that does concern me a great deal.

For every extremist that we prevent from going overseas to engage in extremist activity is one more individual that we have to investigate closely because they’re radicalized to the point where they want to leave.

Saying all of that, there is nothing more that we can do with the budget we have except to prioritize internally as effectively as we can, and I think we’re doing that.

Our success rate has been quite good. I say that with some pride in terms of what we have been able to accomplish. I would be foolhardy to say we have all the bases covered. We do what we can with the budget we have, sir.

Senator Kenny: In Afghanistan, CSIS played a very significant role. Currently we have a situation where Americans are bombing targets in the Middle East and they’re using CIA and SOF to assist in targeting their
aircraft. When the time comes for Canadian aircraft to be flying, do you anticipate that role will be taken by Canadian SOF or by CSIS?

Mr. Yaworski: CSIS has not been asked to play a role yet in our combat mission in Syria. If we are, we certainly will be there. As you are well aware, senator, we have played the role, as you have described it in Afghanistan, and we continue to have a presence in Afghanistan. What we're focused on now are areas outside of the immediate conflict zone and we're covering what we can through the deployment of human sources into the area.

It is a very difficult area and the ability to get clear visibility on Canadian targets that might be there, or any other targets from an ISIL perspective, is a very difficult one.

I am speaking from a CSIS intelligence perspective, not from a military perspective. I can't answer your question on targeting. That's something best placed to the military in terms of how they're going about their targeting. I would imagine based on what I know that it is a collective effort of all those who have representation, in terms of their air forces and the specific targets that are being selected.

The Chair: I would like to ask a question in respect to more information. Do you have a list of how many Canadians or dual citizens with Canadian citizenship have been convicted of terrorism outside of Canada over the course of the last 10 years?

Mr. Yaworski: Canadians and dual Canadian citizens that have been convicted outside of Canada for terrorism I don't have that information, senator. Certainly in the last five years, that number is not a large one. We have had some success domestically in terms of the convictions we had from a counterterrorist perspective and there are cases before the courts right now of Canadians and dual citizens. But in terms of convictions overseas, senator, I don't have that information.

The Chair: Could you get us that list if there is one?

Mr. Yaworski: Certainly I can endeavor to get that.

Senator Mitchell: I would like to follow up on Senator Kenny's point about resources, because if you are prioritizing the 80, how many resources do you have for the others that you say you're not sure you even know about? I will ask a question that probably broaches policy and maybe you can't answer it. Hopefully I can ask it in a way that you will.

It does beg the question for the need of a Parliamentary oversight body that has both sides, as it were. It is not so that your community isn't just relating to a minister and a cabinet, which could do a great job, but might not have another perspective.

In your relationship with the Five Eyes – the other countries, including the U.S. and certainly the UK, have such a body – are you aware if it is useful to the intelligence communities in those countries to have that kind of oversight and body to confide policy issues, to confide budgetary issues and problems in a way that they can be dealt with in a balanced fashion?

Mr. Yaworski: Thank you for the question, senator. I can tell you that this is a policy issue for government to decide, however they decide, we will accommodate whatever that final decision ultimately is, but I'm quite confident in the role that SIRC plays in review of everything that we do. All of our investigations, all of our human resources, all of the activities of our investigators, on the street, domestically and overseas, they have access to all of that. That's not something that the Five Eyes community has access to and we rely very heavily on the advice and the questions that SIRC put to us. They keep us on our toes. They challenge us when they think it's appropriate, and we respond to their advice and counsel in terms of what things need remedying. It has made us a better organization over the past 30 years. So I'm quite confident that the review we have in place provides Canadians the assurances they require to have comfort that we do everything we do within constitutional and legal frameworks.

Senator White: Thank you for your responses. You referred to radicalization and the RCMP being at the front end or the pointy end of that stick, not CSIS. I accept that, but Ontario and Quebec and every major city
in Canada has a police service other than the RCMP that's a service of jurisdiction. Are you working with them and providing the education and the advice they need to make sure that they’re drawing on that information as well? The RCMP doesn’t have the resources any more than many do.

Mr. Yaworski: We do certainly interact with the local police forces as well as the RCMP. The RCMP has connectivity through the Canadian Association of Chiefs of Police, as you’re well aware, Senator White, and they are often the venue for that information. But to Senator Day’s question earlier, ITAL also plays a role in informing first responders on any threats of that nature. I indicated that the RCMP has the lead in terms of advanced work in countering radicalization. Public Safety is also directly involved in that space and is working on the radicalization issue as well. So it’s not just law enforcement; Public Safety has taken a lead role as well.

Senator Day: I’m going to your earlier comments and I would just like to confirm what CSIS is entitled to do internationally now. You were talking about the minister’s announcement and that you were pleased with it, and you said particularly by confirming your ability to operate internationally—So you are operating internationally now and he’s confirming it?

Mr. Yaworski: We are operating internationally. We have had that ability for the 30 years that the CSIS Act has been in place. There’s no geographic limitation on where we can investigate threats to the security of Canada. We do it both domestically and abroad. The issue that I believe the minister was referring to is it’s not as clearly articulated within the CSIS Act itself, our overseas mandate.

Senator Day: When you go on and say Canada would lack understanding on threats to the security of Canada which originate from overseas, you’re saying that would be the case if there happened to be legislation saying you couldn’t operate internationally. But you can, and you don’t lack that information now, and then the minister is just going to confirm that you can continue to do that?

Mr. Yaworski: That’s correct. Many of the threats we’re facing originate overseas. You just have to look at the recent media releases of ISIS, who have threatened Canada directly. Osama bin Laden, in his Abbottabad compound, had documentation naming Canada as a target. The threats to us are not unique to our own borders; they do originate from outside the country, and in order to acquire the intelligence, we do have to engage in overseas activities.

Senator Day: Which you’re doing?

Mr. Yaworski: Which we’re doing.

Senator Beyak: Thank you very much, Mr. Yaworski. I wonder if you would be able to tell me if we have a list or the actual number of terrorists or terrorist organizations operating in or from Canada.

Mr. Yaworski: That’s a difficult question to answer. We do have supporters, certainly, of a vast number of terrorist entities that the Canadian government has determined are worthy of a terrorist listing. That number is 53. There are 53 terrorist organizations that Canada has listed. Therefore, I think it’s safe to say that Canada is concerned about these organizations and we probably, in one shape or another, have individuals that, at the very least, support their respective causes.

Senator Mitchell: You do a good deal of work with the Five Eyes. You do need to leverage information, ours and theirs, one complementing the other. What about this question of third parties and the information, again in the context of Arab, that goes to them? Do we have control over whether or not it can go somewhere else? If not, what can we do about that and what should we do about that?

Mr. Yaworski: That’s a very good question, senator. As I said in earlier comments, we’re very reliant on the intelligence that we receive from our partners across the board. Five Eyes in particular. The service has formal arrangements with 290 separate organizations in about 150 countries, so that gives you an idea of the breadth of intelligence cooperation that we have. As indicated, Canada cannot operate on our own intelligence platform alone. We do leverage the resources of other organizations in that space.
That said, when we do share intelligence, we caveat the intelligence that we share. By "caveat," I mean there are specific directions about how our information can be used, and we do that to ensure that it's used within our own legal framework and our own constitution. When we share information, there are limits on how other agencies can use that. They cannot further disseminate that information without coming back to us and requesting our permission to do so. That's effectively the third-party rule that you're referring to, senator. They cannot pass on information without our direct consent.

Senator Mitchell: One of the concerns that was raised by the minister in his discussion of why he would be changing the act was the problem, as he puts it, I think, or officials say that judges have constrained the agency's powers in the name of preserving civil liberties. That would be a pretty important constraint in anybody's assessment.

It's a delicate issue to start addressing that balance. Could you give us some clarification of how it has been constrained and how that is, in turn, limiting your ability to do what you think you need to do?

Mr. Yaworski: On that point, senator, I'm afraid I'll have to defer to the actual introduction of the legislation. What I can say is that we respect fundamentally the decisions of the court and everything that we do must be within the framework of Canadian law and speak to Canadian values.

SIRC plays a great role in oversight and review. We do all of our investigative activities. If there are specific issues that speak to concerns of the courts, SIRC will look into those, and they have done on a regular basis. With respect to the legislative changes, I think it's only fair to wait until they're debated in Parliament.

The Chair: Colleagues, I would like to pursue a question that has to do with the legal framework that Canada presently has in place. What is actually happening day to day, which we read about, is Canadians going to, in this case, Syria, Iraq or other countries, joining terrorist groups, maybe even fundraising for terrorist groups and then coming back as a Canadian, and as far as I know they're working at Walmart now and you're watching them, the way you described it earlier.

Are there other countries where the legal framework is such that if someone leaves their country, joins a terrorist group, fights or fundraisers with a terrorist group, then comes back as a citizen of that country, they can be charged under their legal framework? Then we don't have limited resources, watching these 80 individuals who we are led to believe and have every reason to believe have been taking actions that we, as Canadians, don't agree with.

Mr. Yaworski: If I understand your question, senator, certainly other countries do have laws that are different from our own. Other western countries have a much larger problem than we do in terms of the volume, the numbers that are actually involved.

But you do touch on another issue that I think is fundamental for the discussion. We have great relationships with other countries around the world. We respect the citizens of those countries who may be travelling on their passports. So if an individual from Sweden or Norway travels to a conflict zone, is engaged in terrorist activities in support of ISIL and then decides to come to Canada, without the cooperation of those countries in Sweden and Norway who provide us lead information on that individual, we would naturally let them into the country without the requirement for a visa. So that is an additional concern, certainly, that we have, senator.

In terms of their own legal thresholds to convict these individuals, I'm not knowledgeable on the specifics of what other countries may have.

Mr. Yaworski: If I understand your question, senator, certainly other countries do have laws that are different from our own. Other western countries have a much larger problem than we do in terms of the volume, the numbers that are actually involved.

But you do touch on another issue that I think is fundamental for the discussion. We have great relationships with other countries around the world. We respect the citizens of those countries who may be travelling on their passports. So if an individual from Sweden or Norway travels to a conflict zone, is engaged in terrorist activities in support of ISIL and then decides to come to Canada, without the cooperation of those countries in Sweden and Norway who provide us lead information on that individual, we would naturally let them into the country without the requirement for a visa. So that is an additional concern, certainly, that we have, senator.

In terms of their own legal thresholds to convict these individuals, I'm not knowledgeable on the specifics of what other countries may have.

In terms of our own country, we have adopted recent legislation which makes it illegal to travel or attempt to travel to conflict zones to engage or support terrorist activity, and we have had some success to this point. I think the RCMP will be able to provide you more detail on that, but there is legislation in place currently that will help us in that space.

The Chair: This is legislation that was just recently passed?

Mr. Yaworski: Yes, the Combating Terrorism Act in July of 2013.
Senator Day: I think it would be helpful for the record if we could clarify this issue of caveats that you mentioned and leveraging, so that the record will be clear on what we’re talking about in the context of anti-terrorism and gathering information.

You indicated that whenever you share information you may put a caveat on there that the third party that you’ve passed it to not being able to pass it on to somebody else, presumably that also applies to some of the information that you receive?

Mr. Yaworski: Yes.

Senator Day: So it flows both ways?

Mr. Yaworski: It does indeed flow both ways. Certainly the third-party rule is one of the major requirements of any interaction with any other service. We’re also quite selective in what we share and who we share it with. We take into account the potential for human rights violations in a country that may receive it, and certainly with our Five Eyes partners we’re at liberty to share more information than we would with some other countries that have questionable human rights records.

Senator Day: Are there caveats on the information you receive from these major partners of ours, the Five Eyes?

Mr. Yaworski: There are caveats in some cases. There is a requirement to respect the third-party rule in all cases. Not all organizations provide the same caveats as we do on the information they share.

Senator Day: The leveraging of the information, if it has the caveat you can’t leverage. Could you explain what, in your context, leveraging would entail?

Mr. Yaworski: I should be clear on that point. We can certainly receive the information. We can use it for intelligence purposes to inform our own investigations, to advance those investigations as appropriate and we can use that intelligence to help us acquire further warranted powers, for example, should that be required. But those are in-house tools that we use the intelligence we receive to further our own investigations. We can’t take that information because we think it’s interesting and share it with another organization or another country. So that’s where the restriction is, senator, in terms of what we can do with the information.

Certainly in house, and within the circles of informing the Government of Canada, we can use it. That’s one of the purposes it was provided to us for.

Senator Day: And the term “leveraging”?

Mr. Yaworski: Leveraging is about resources and capabilities that other organizations might bring to bear on a certain target, which we don’t. Filling intelligence gaps is a better way to describe it.

Senator Day: Just so it’s clear, are you saying that you take information that you acquire from another country, one of the Five Eyes countries, and give that to some other nation in exchange for information back? Is that the leveraging that you’re talking about?

Mr. Yaworski: No, quite the opposite, senator. If information comes to us from a third party, another country, we are prevented from sharing that with an additional country. We use that information internally. We may use it to provide assessments and advice to government internally, but we cannot share other parties’ information with a third party.

Senator Day: My difficulty is I don’t understand the term “leveraging.” What are we talking about?

Mr. Yaworski: Leveraging is taking advantage of the capabilities and access that other organizations have. They may have very good coverage on one terrorist group or one particular cell which we have no knowledge of but are very interested in.
Similarly, or conversely, we may have access to a certain particular organization or a certain particular activity. We may wish to share that information with them, and in turn they share information with us that’s relevant to the threat we’re investigating.

Senator Kenny: Mr. Yaworski, it’s been widely reported that Canadians have been spied upon by other members of Five Eyes at the request of Canadian intelligence agencies. Is this possible?

Mr. Yaworski: Canadians have been spied upon by other Five Eyes partners.

Senator Kenny: At the request of Canadian intelligence agencies.

Mr. Yaworski: I think what you’re referring to, at least in the context of individuals who have travelled overseas, is the ability for other agencies with certain capabilities, particularly in a technical space, to acquire intelligence on Canadian citizens. Where that has happened and where we’ve had any role in it, it has been based on warrant targets that we have had covered. But other agencies have the ability to target, whenever they see fit, based on risks to their own countries or their own national interests. We do not have any control over that. It’s based on their own laws and their own capabilities. But the general rule is that Five Eyes partners will not spy on each other.

Senator Kenny: Would I be fair to interpret your answer as saying this is principally a communications security establishment problem?

Mr. Yaworski: I don’t think it’s a problem. I think the communications security establishment has very good relationships with their signals intelligence counterparts, particularly in the Five Eyes. It’s a cooperative relationship. It’s like us with our fellow HUMINT services. The relationships are strong and they work closely together in identifying and targeting common threats.

The Chair: I’d like to pursue a question that was earlier put by me and others, and that has to do with the 80 individuals who have left the country, have been active in a terrorism act of some kind or another, and have come back to Canada.

I asked how they could come back here and not have any charges of any kind laid against these individuals in view of the knowledge that they have. The response, if I’m not mistaken, was that under the new legislation, the Combating Terrorism Act, individuals who left the country with the intention of getting involved in terrorism could be possibly charged.

Am I correct in that? This new legislation should, at least in part, deal with these individuals if they do come back to Canada?

Mr. Yaworski: I’ll try to answer that question, senator, but I would encourage you to put those questions to the RCMP who obviously have expertise in this area.

I think one of the difficulties that they’re facing is the burden of proof, proving intent to commit an act or to join a certain group.

These individuals, when they’re about to leave the country, will not advertise where they’re going. They will not purchase a direct ticket from here to Syria. They will travel to other parts of the world where it’s very difficult to then connect the dots in terms of where they subsequently travel and when they actually end up in a conflict zone in Syria.

They obfuscate their routes. In certain cases, when they are prevented, they borrow or steal passports of other individuals to facilitate their travel. They engage in activities to hide their trails and to make it difficult to prevent their departure. When they return to Canada again, it’s one thing for us to be able to provide to the RCMP lead information saying such and such an individual was in Syria and was engaged, we believe, in operating with a terrorist group like Jaish al-Nusrah, but it’s something else for them to prove it in a court of law, and the threshold to prove that they’ve committed an act that is worthy of terrorism charges in this space has been a difficult one.
There has been some success. Certainly the new legislation that we're referring to provides an extra tool for law enforcement to use, but it's not an easy prospect to go from a willful desire to engage in activities overseas and to be able to prove that in a court of law once they return to Canada. I would encourage you to put those questions to the RCMP, sir.

Senator Kenny: I have a follow-up to that. Would it also be the case, Mr. Yaworski, that the RCMP and CSIS would in fact have different points of view on somebody coming back from time to time, and in fact, your folks might be more interested in running an agent and trying to collect more information through him, and the RCMP are really primarily interested in collecting enough evidence that they can go to court?

Mr. Yaworski: Senator Kenny, clearly there are differences in our mandates, between us and the forces. We work very cooperatively on CT issues, but to your point, absolutely. There is a difference between an intelligence investigation and a criminal investigation, which is why in the counterterrorist area we run parallel investigations. The RCMP, as you indicated, is looking to lay charges. We have an interest in developing further intelligence and perhaps recruiting that individual that you say came back to acquire additional information on where the next threat is coming from. So there are differences in our mandate, and yes, you're absolutely correct in that regard.

Senator Kenny: Chair, would you find it useful if we asked for a description of the parallel investigations?

The Chair: Go ahead and ask him.

Senator Kenny: Could you describe for the committee, if you would, how the two processes run in parallel and how you resolve issues where you disagree on whether somebody should be charged or somebody should be run?

Mr. Yaworski: The success that we've had over the past several years, but even with the cases that are before the courts right now, the VIA Act trial, for example, that I'm sure you're aware of, and other cases that we've had, the Canada Day attempt to bomb the Victoria legislature, those cases, while they're before the courts, are similar in nature, and I'm not going to get into any specifics in those cases, but generally to answer your question I'll say that what we've learned over the years is that in terms of improving the relationship with ourselves and the RCMP has led to a system where we will provide them lead information, because it's only natural we will be the first ones to come across that counterterrorism-type information. We have a lower threshold in terms of acquiring our warrant of powers. We have a lower threshold to use those intrusive techniques that will lead to the intelligence that indicates a clear threat.

At some point we will receive information that suggests this is going to proceed from an intelligence investigation to a criminal investigation because they've met that threshold. At that point, we will provide a disclosure to the RCMP, who will then initiate their own investigation, so that disclosure is relatively light in terms of content. That disclosure gives the RCMP just the bare bones of what they need to initiate their own investigation, to deploy their own resources, to deploy their own surveillance, to go up in their own Part VI applications to get their own warranted coverage. They use our lead information to advance to a point where they can initiate their own investigation, and they will take over primacy on those targets that are now being looked at from a criminal perspective.

Our parallel intelligence investigation will look at those others in the periphery, perhaps those that haven't made the top list of RCMP from a criminal threshold perspective. They're focused on those, we're looking at the others around the outer side, the perimeter, because our concern is not on the case that we've uncovered. The RCMP handles that. Our concern is on what's coming next, who else may be implicated in this. If there is an investigation over here, what's going on over there. I've tried to answer your question that way, senator.

The Chair: I want to ask one further question that the witness mentioned earlier, and that was a question of an exit information system at the borders. Perhaps you could expand on how helpful this would be for you to be able to do your job and your other departments that you work with.
Mr. Yaworski: Thank you, senator, and I did choose those words quite carefully. An exit information system is not an exit control. There is no control. Canadians have every right to leave the country and enter the country again whenever they wish.

Exit information is something we're lacking right now, and it's quite germane to the foreign fighter issue. We don't know when certain individuals on Canadian documentation have left the country. We just don't have that information available to us right now in terms of something that can be corroborated in terms of a passport that has been swiped on the way out of Canada. As a result, we have to rely on other techniques. We have to rely on other investigative methods to determine when subjects of interest to us have left the country. In many cases it's through allied reporting from a certain other country that they land in, but we do not have that exit information on the way out and, to your point, would be extremely helpful moving forward in addressing the foreign fighter phenomenon.

The Chair: Thank you very much, Mr. Yaworski. You were very fortuitous, and I felt you gave a very good presentation. This has been of benefit to us as a committee.

On June 19, 2014, the Senate approved the following reference for this committee: That the Senate Standing Committee on National Security and Defence be authorized to study and report on national security and defence issues in Indo-Asia-Pacific Relations and their implications for Canada's national security and defence policies, practices, circumstances and capabilities; and that the committee report to the Senate no later than December 31, 2015.

The Indo-Asia-Pacific is a new term for Canadians. It is important that we recognize that the region is not simply Asia, a term that is very limiting from a security and defence perspective, but rather it stretches from India across to Japan, down to Australia and New Zealand.

With us to set the stage for our study is a gentleman who is perhaps Canada's preeminent scholar and authority in this region, Dr. James A. Boutiller. Dr. Boutiller is the Special Adviser on Policy at Canada's Maritime Forces Pacific headquarters based in Esquimalt, British Columbia. Dr. Boutiller's current responsibilities include advising the Commander of Maritime Forces Pacific on matters related to foreign policy, defence and maritime security in the Asia-Pacific region.

Dr. Boutiller recently hosted the maritime security conference in Victoria, which brought together many of the nations in this region and allowed Canada to play a foremost role as a maritime nation by hosting this biannual gathering.

As an aside, Senator Kenny and I were able to attend that conference, and I want to congratulate you on a very well-run and informative conference.

Dr. Boutiller, welcome back to the committee. I understand you have an opening statement. Please begin. We have one hour for this panel.

James A. Boutiller, Adjunct Professor, Pacific Studies, University of Victoria, as an Individual: Thank you, Mr. Chair, and greetings to your fellow committee members.

I think probably the most important issue for us to wrestle with at present is the trans-Pacific relationship between Washington and Beijing. If the rise of China in the last quarter of the 20th century was the most important global phenomenon, certainly the management of the relationship between the United States and China is the most important and compelling challenge for the first quarter of this century. It's a relationship under girth, I would suggest, with profound strategic ambiguity and a lack of trust. Despite efforts at the highest level to build bridges between Washington and Beijing, there is a great deal of uncertainty as to what China's end game is.

Part of the issue is the so-called American rebalance into the Pacific. It is important to note that the Americans have been deeply engaged in the Pacific for many years indeed. What we see now in the post-Iraq, post-Afghanistan period is a reanimation of their ties and activities in the region. It is a critical development. From Beijing's perspective, however, they see all of their - that is to say, China's - activities as entirely legitimate and in response to Washington's activities in the region.
There is a sense of victimhood in China, which is a prism through which the Chinese see almost all of their actions. It's very difficult to wean them off this sort of world view. It governs all of their activities in the Western Pacific and into the Indian Ocean.

I think it is also important for us to pay passing attention — or perhaps more than passing attention — to the question of the energy and effectiveness of the Chinese economy. Some years ago, we were concerned about a China that was too powerful. Now I would suggest to you that there may be an argument for being concerned about a China that is not necessarily weak but is weakening. Certainly the level of economic activity is in a state of decline, and there is a profound array of structural challenges that face Chinese leadership.

How will these manifest themselves in terms of China's foreign policy, its interaction with other players in the region? I would suggest further that there is an architecture of containment that has begun to arise. It is informal, but it is there nonetheless, and it plays to China's sense of paranoia that surrounds the whole of China and denying China its legitimate ambitions is a structure of countries all dedicated to trying to check China's rise.

One of the sources of concern, of course, as all of you are aware, is the dramatic growth in Chinese military capability over the past quarter century. The Chinese, of course, would maintain that their defence budget, which has risen at a double-digit rate for more than two decades, is simply a reflection of comparable growth in their national GDP. The fact of the matter remains, however, that the maritime architecture of the region has changed profoundly. The Economist news magazine, for example, would suggest in a rather simplified graph that China has now surpassed the United States in terms of the number of naval hulls. That, of course, is something of a cartoon because it lacks the qualitative nuances that are critical for your consideration, but nevertheless, the dramatic appearance of an increasingly large and sophisticated Chinese navy is something that makes Washington's calculations more and more challenging.

Where do we fit in all of this as a modest, mid-level nation with modest, mid-level military assets? I would suggest to you that we are very late in the day in coming to grips with the importance of Asia. If we go back to 1983, what we see is that trans-Pacific trade exceeded trans-Atlantic trade, and that phenomenon has continued to the present day. Three and a half times greater proportion of world trade moves across the Pacific to Canada than across the Atlantic.

But for a variety of reasons, historic and structural, Canada, I would suggest to you, has ignored the new realities emerging in Asia and is coming to them at the eleventh hour. One of the big challenges for Canada is how to establish our brand, our sense of commitment to the region, because throughout much of Asia, we are, frankly, invisible. One of the things that we have to do is build up a reputation for being actually and truly committed to the region, and in the process, we have to remember that disaggregating security from trade is almost impossible in the Asian context.

So we need a great deal more focus and energy. Rhetoric alone will not sustain us, and we have to be much more strategic in terms of how we advance in a region that is vast and increasingly challenging.

Let me leave it there, Mr. Chair, and then I would be happy to entertain questions.
of the Indo-Pacific, then that clearly encompasses countries like Iran, Pakistan, Afghanistan, India and so
form.

We can see that coming out of Southwest Asia, there are certainly influences that affect Muslim states in
Southeast Asia, for example, and there are forces that stimulate radical activities in a state like Indonesia,
where 90 per cent of the population adhere to Islam. In fact, the Indonesians have acted fairly effectively
over the years to try to eliminate terrorist activity in Indonesia, but it spills over to the Southern Philippines,
and it occasionally appears in Malaysia.

It has not been an enormous threat in the way that the activities of ISIL in Iraq and Syria have been.
Islam in Indonesia is a much more relaxed and informal forum than it appears in the 16:40:00 areas of
Southwest Asia.

Terrorism is an issue. It is partly in the eyes of the beholder, as well, because in Western China, there
is a Turkmen population whose eagerness to achieve a degree of independence is a source of deep dismays
for the authorities in Beijing. That’s an area of constant tension, and unrest in Western China.

Senator Mitchell: Thank you very much, professor. We met with you some years ago when I was in
Victoria when our committee was there, and it was very impressed, as it is today.

The question I would like to get at is the nature of the threat of China, if it is a threat, or what it proposes
in the context in which you are discussing. It is known that China holds trillions of dollars of U.S. bonds,
which begs the very question: Why would China do anything to threaten the U.S. economy if the U.S. owes it
so much money? Isn’t that in itself a stabilizing factor in that relationship?

Mr. Boutiller: Well, it certainly is. I always compare it to two climbers on the north face of the Eiger.
They’re roped together, and as long as the two economies are functioning in tandem, they’re in a safe
condition. It would be catastrophic — suicidal — I would suggest — for the Chinese to begin selling off treasury
bonds on a major scale. That would, in fact, weaken fundamentally an already problematic economy in the
United States.

I don’t see that. What I do see is the Chinese are increasingly using the $4 trillion in foreign exchange to
target, by way of sovereign funds, major projects around the world. In Africa, even in places like Iceland and
Greenland, they’re the largest purchasers of land in those two north Atlantic areas.

They’re increasingly concerned about how to turn that array of foreign exchange into political
instruments, and I think your basic premise is entirely correct.

Senator Mitchell: In a sense your observation of the velocity, if I can use that word, with which their
military is being increased or enhanced is startling. At face value, that might look like a military threat to the
rest of the world or to the region. But is it also not the case that while we consider the Chinese government
to be a dictatorship and, ultimately, completely in control, it is a country of 1.4 billion people, give or take,
that’s extremely difficult to control. At the back of the leadership’s mind, is it not possible that they’re
concerned with economic pressures, with the geographic diversity, with minority groups, et cetera, and that,
in fact, they might have a stability problem within their own country and that some of that militarization is a
reflection of that and of creating jobs for a massive population that in some regions doesn’t have economic
opportunity?

Mr. Boutiller: Indeed, you have targeted many of the critical concerns for the senior leadership in
Beijing.

One of the things that is worthy of note is that a highly developed sense of nationalism prevails in
northeastern Asia, a nationalism that we might compare with the nationalism that was exhibited in Europe
on the eve of the First World War. This makes national responses increasingly emotional and sensitive. This,
of course, is also an instrument which the leadership is able to play to on occasion when it wishes to
generate, for example, anti-Japanese sentiment and so forth. But the leadership has an enormous array of
challenges.
Clearly, one of the biggest issues is the unequal distribution of wealth within the nation. In the sense that we often think of high levels of distinction between those of wealth and those without in a nation like the United States, in fact, the Gini coefficient, which measures that relationship, is significantly higher in China. So the leadership is dedicated to trying to spread the wealth, but it has not been very successful in doing that.

It is also faced with an array of fundamental issues related to the environment. The environment is, in a word, a mess, and while they're attempting to remediate it, it has become increasingly a check on economic growth.

We also see that in keeping with a long tradition in China the flats or directions that go out from Beijing are, in many cases, ignored by local party cadres in distant provinces. So they're wrestling with that challenge.

They see themselves as a nation that has now arrived after more than a century and a half of humiliation, and the growth of their military capability and, more specifically in this case, their navy, is seen as a hallmark of a nation which is now a nation of global standing. One of the critiques, of course, is that while the Chinese may wish to be seen in that way, they have failed in the eyes of many Western observers to observe international norms and to be a responsible global player.

So you are quite right in suggesting that the leadership faces an array of challenges, internal, external, and throughout the region, I would suggest, to you, that there's a profound sense of uncertainty as to what China's end game is. Virtually all the major nations have China as their number one or two trade partner, but they're all keeping their powder dry because they don't know how China is going to utilize its burgeoning military capability.

Senator White: Thanks for appearing today, Mr. Boutilier. We see Canada looking at moving more greatly into international trade and into the Asia-Pacific area. What do you see as some of the national security threats that we can expect to face?

Mr. Boutilier: It is important, among other things, to underscore the fact that the American rebalance into Asia, while frequently denominated in military terms, is, in fact, a rebalance which has a profound economic component of which the Trans-Pacific Partnership is a key element. And we, of course, are becoming partners in that trans-Pacific economic relationship.

Asia is not, in many cases, an easy world in which to do business. We find that the opaque nature of business in China, the lack of legal predictability, makes it a challenge for firms large and small to conduct operations.

Similar critiques could possibly be raised with respect to doing business in India, even though India is a good deal more open in many ways and predictable than is the case in China.

One of the challenges that we face as a nation is that very few of our companies are major companies, although there are many small companies that have expertise or products or capabilities which are very much sought after in Asia.

The big challenge, of course, is that you have got to be there. We're arriving at the eleventh hour and we're faced with some very strong competition.

I had the good fortune of addressing an audience of international barristers recently, and I said if there's one thing you take away from my presentation, it is a sense of urgency. While I would not wish to undermine the collaborative and inclusive processes to which we're dedicated here in Canada, we have to recognize that many of our competitors are moving much faster than we are in terms of trying to establish economic bridgeheads in the region.

We do have areas of expertise, whether it is in environment, air traffic, and engineering or in offshore activities and so forth that have very considerable market potential in Asia. If you were to look at the
statistics, our share of Asian trade has continued to shrink, relatively speaking. It has grown in asset terms, but, over and against many of our competitors, we are simply not holding our own.

**Senator White:** What do you see is necessary to reverse that trend?

**Mr. Boutiller:** This is a very good question. It raises some theological questions about the degree to which the government can actually create a more conducive atmosphere or environment for trade. There are some big challenges in Asia, especially in terms of distances, language capability, and the right sort of partners. Now, these sorts of concerns affect business anywhere internationally.

We have begun to turn our attention, but we continually are distracted by other developments internationally. We have to demonstrate, I think, that we are fully committed to the region, because in many quarters, we're seen as pleasant companions and colleagues, but never here, and we have not built the track record of continued commitment to the region. Of course, as I suggested earlier, security and trade are, in many cases, indistinguishable in terms of building our presence, our track record in the region. It is an area that places enormous importance on security, and it is an area in which many people who have been in the security business have moved on into senior political or advisory roles. We see that in countries like Thailand, China, and elsewhere.

It is a question of much more and much more quickly to develop a track record in the region, or we turn our back on the region and focus elsewhere. One of the issues, for the moment, is that we're technically committed to developing our priorities in Latin America, and yet, I would argue that Asian markets are a good deal more compelling in terms of their potential than the ones south of us.

**Senator Beyak:** I wonder if you could tell me, sir: We have recently heard about the South China Sea and the stable Pacific. U.S. scholar Robert Caplan writes that, for too long, the West has taken that stability for granted. Do you have any thoughts on that?

**Mr. Boutiller:** One of the ironies, I would suggest, of the Pacific arena is the fact that the dramatic growth in the Chinese economy owes a good deal to the overall stability provided by the United States Navy and the United States' presence throughout the region. Indeed, throughout the whole of the Indo-Pacific region, all of the players are eager to have Washington remain involved. They have a deep inchoate anxiety that, someday, they're going to wake up one day and find that the Americans are gone.

Leaving that aside, if we look more specifically at the South China Sea, you will see that the South China Sea is a critical connection between the Indian Ocean and the Pacific Ocean, and $5 trillion worth of trade flows through that complex, enclosed sea, coming from and going to the Indian Ocean and into the Pacific. Similarly, if we look at energy flows, which are critical to connecting those two oceans, Japan, South Korea, and China depend entirely on those flows of energy.

One of the issues for us is that ownership of islands and other geographic features in the South China Sea would normally be considered to be under the UN Convention on the Law of the Sea. The Chinese, however, I would suggest, are providing a highly aberrant interpretation of that convention, and that puts them squarely at odds with many of the other claimants. In the South China Sea, the maritime areas of a number of states overlap. The Americans have stood at arm's length in the sense that they have not supported one claimant over another, but they are increasingly concerned about peace and stability at sea.

What we saw in, not only the South China Sea but also in the East China Sea and in Northeast Asia, are ships actually firing on one another and people dying at sea. You will recall, perhaps, the tragic case, in 2010, of a South Korean corvette that was blown up by a North Korean submarine.

So this is an arena that is increasingly brittle and problematic and where the area of miscalculation is very considerable indeed. It may not happen at the level of admirals and generals, but it could very well happen at the level of local area commanders or even ship captains. So it is a concern to analysts throughout the region and beyond that various hostilities could erupt because of a lack of tranquility at sea.

**Senator Beyak:** Thank you, sir. With your knowledge of this area, would you have any advice for Canada for a strategy in that region?
Mr. Boutilier: Of course, Canada was one of the iconic founders of the UN Convention on the Law of the Sea in the late 1970s, early 1980s. Subsequent to that, for a period of almost 10 years, Canada was the co-chair of the Indonesia-Canada South China Sea Informal Working Group. That working group did not address the prickly issues of state ownership. However, they addressed an array of other issues related to fish stocks, hydrography and so forth, and, for a very modest sum of money they established Canada’s bona fides in the region as being genuinely concerned about ensuring peace and stability. We were not drawn into hard security, but we were seen throughout Southeast Asia as being friends and partners in this process.

I know for a fact, having spoken with the Indonesian co-chair of that process, who was here in Canada only a fortnight ago, that they’re very eager to reanimate that and would be delighted to see Canada deeply involved once again.

The Chair: I would like to enter the fray here with you, Mr. Boutilier, with respect to your response to Senator White with respect to Canada’s involvement and what further involvement we could have in that particular area of the world. You were saying that we’re in the 11th hour. Perhaps that may be true, but I would say that, in the last number of years, there have been some pretty significant steps taken with respect to establishing Canada’s presence, i.e. the agreement in the Philippines on defence. There was an agreement in Japan a number of years ago, and they’re negotiating still for a free-trade agreement. There’s a free trade agreement with South Korea. Our bilateral trade with Taiwan is exceeding $6 billion. That has been ever-escalating over the last number of years.

I would like to ask you, with respect to where we are today: What more should we be doing over and above the various trade agreements and defence agreements that we either have negotiated or are negotiating? Secondly, what should we be doing with respect to our navy and establishing its presence in that particular area of the world?

Mr. Boutilier: The facts that you have enumerated are compelling. However, I would suggest that they are, in many cases, products of the last half-decade and not the past 25 years. If we look at some of our competitors, like Australia, for example, one could argue, parenthetically, that the area is of even greater concern to Canberra than it is to Ottawa, but the fact of the matter remains that they have been far more aggressive, in a positive sense, in terms of forging those necessary ties.

Once again, I come back to the sense of urgency. I would suggest that, increasingly, countries that may have seemed distant or even remote to us are open for business, like South Korea, Japan, Singapore and so forth. Some of these negotiations drag on endlessly, I will be the first to admit, but we need to enhance our attention to and pressure on these agreements, which, in many cases, set the stage for many other things that follow from that.

With respect to maritime issues, clearly, our navy is small but highly professional, but the bulk of the navy, relatively speaking, is in the Atlantic. It should be noted, of course, that, were you to work on the principle of sheer distance, one can reach the northwest Indian Ocean more effectively from Halifax than one can from Esquimalt, but, if we turn to Esquimalt, we’re looking out on the world’s largest ocean and the region that is likely to be the most volatile in terms of maritime interactions.

How can we affect the course of events? Well, we can clearly do so, as I suggested with the previous question, in an informal, soft-power way. Probably, the location of our assets further forward into the Pacific, if strategic, would be one of the things that is really critical. It was certainly a lesson that the United States Navy learned in World War II that the tyranny of distance had, somehow, to be overcome.

Whether it is a case of moving some of our assets into, for example, Northeast Asian waters to work with the United States Navy or whether it is a question of moving them elsewhere, the deployment lines from the West Coast of Canada into the depths of Asia are very considerable indeed.

I think that a forward presence would probably be welcomed by our Five Eyes colleagues, who were the subject of your earlier discussions with the previous speaker. I think there are ways in which we can leverage relatively modest maritime resources by targeting them and having them in the right location. It is a question, in many cases, of symbolism, which may seem like a weak read. However, it’s critical for our Asian
colleagues that they see we're actually committed to doing something to contribute to the peace and stability in the region.

Senator Day: You made a comment early in your presentation that you think China is in a state of decline. I understood from your comment that it is a permanent state of decline as opposed to a cyclical downturn in the economy. Would you like to expand on that?

Mr. Bautlfer: I certainly wouldn't want you to go away from this interaction with the impression that China is in a state of decline. However, I would agree that what we're witnessing now is probably cyclical in terms of the downturn in the Chinese economy. We were accustomed, of course, in the 1990s and in the first decade of this century, to seeing growth rates in the 10 per cent to 12 per cent range. Now, we're probably down to 7.3 per cent to 7.4 per cent. Some analysts would suggest that going forward we may be down to 4 per cent. Others would argue that despite the one-child policy, with the sheer numbers being added—probably every 30 to 36 months China adds a population equal to Canada—you have to have an economy that's operating at 6 per cent or 7 per cent to meet the internal demand.

The Chinese leadership is faced with, as I suggested earlier, the whole array of structural issues. They are trying desperately to reform the economy. They realize that the export-led model, which was the key to their explosive growth over the past 30 years, has become, in fact, increasingly a thing of the past. Their wages are beginning to climb, and some international firms are relocating to Vietnam, Bangladesh and elsewhere in search of cheap labour.

We can also see that the Chinese are dedicated to probably the largest internal movement of people in world history with several hundred million people moving out of the countryside and into the cities of China. This, of course, has the effect of increasing the environmental costs in the sense that energy demands, pollution and so forth all begin to soar when we have enhanced urban populations.

For a variety of reasons, the Chinese are desperate to try to stimulate a new wave of economic growth predicated on domestic demand. It remains to be seen, and I am quite pessimistic about it, how quickly they can generate that transition. It's probably a 20-year phenomenon at the very least. There isn't the money in the countryside, where hundreds of millions of people still live on US$2 a day, to develop the sort of domestic consumption engine that will replace the export-led engine of the past.

We're seeing a period of consolidation, and the dramatic growth of the past may very well be a thing of the past, in the same way that it was in Japan once we got to the early 1990s. Some would suggest, by the way, that the banking system and infrastructure inventory are as over reched in China today as they are in Japan; but that remains very much to be seen.

Senator Day: I didn't appreciate that the answer would be quite that long. It was an excellent answer to a complex issue. There's a lot of reading of green tea leaves on this one. Are you aware of the Xiangshan Forum that China is hosting in November? I'm not familiar with it. It is a regional security conference. Are you familiar with that forum and should we be taking it seriously?

Mr. Bautlfer: I am aware of it. It will be from November 20-23 in Beijing. I hope to attend to get an assessment of its legitimacy and value. I was not aware of it before, to be frank with you. I was at the Academy of Military Sciences in Beijing 10 days ago, which is a think tank that advises the Central Military Commission. They invited me to attend so I'm happy to accept their invitation. I like you, I'm eager to assess the validity of this undertaking.

It should be noted that there are many security forums throughout the Asia-Pacific region in Indonesia, South Korea, Japan and so forth. I will be very interested to see how this is organized. To date, it has not been wildly impressive, but some of the plenary sessions promise to provide an interesting window on Chinese thinking.

Senator Day: I don't think this committee is planning to send anyone so we'll be interested in your comments once you've had an opportunity to attend.

Mr. Bautlfer: Absolutely, Senator Day.
Senator Mitchell: It seems, in a way, that there are two competing forces coming from your testimony. One is that we need to be more visible in China because of the economic opportunity and the other is that with their mounting military and strong nationalism there could be a military threat and we need to be repositioning perhaps naval and other assets. Aren't the two in complete conflict, in a sense? One would be intrinsically threatening while jeopardizing the opportunity in the other?

Mr. Boutiller: You could probably draw that inference from what I've suggested—that we're looking at a competitive state of affairs. First, I wouldn't want to confine myself to China alone in the sense that there are many other opportunities for international trade across Asia, whether in South Korea, the Philippines, Indonesia, and so forth. That would be my first comment.

Second, compared with the economies of many parts of the world, the Chinese economy, even in a period of slowdown, is still very muscular, especially compared with European economies currently.

Third, I would suggest that there is a good deal of anxiety about what China's endgame is. That should not prevent us for the moment from utilizing our trade opportunities, where appropriate. It may well be that this will continue for a very long time or it may be resolved. I think that the whole of the region provides potentially greater opportunity than elsewhere, and China is clearly at the centre of the economic growth throughout the region. There are still opportunities despite the anxieties. Of course, this is borne out by what I said a moment ago that China is probably the number one trade partner for almost every major power in the Indo-Asian area.

Senator Mitchell: A couple of times you mentioned other countries of economic opportunity, including Vietnam, in passing but not in that context. Vietnam is the 12th largest population in the world; and it's flexing its muscles. Having been there, I would have to conclude that the communists actually lost that war because it now has a robust capitalist economy. What are the opportunities there and should we be looking at those?

Mr. Boutiller: Vietnam has improved; I would suggest that probably about 10 years ago Vietnam was the economic poster boy of the region. More recently, its economy has slowed. One commentator said that the Vietnamese having waged war for 50 years had to learn how to wage peace. They're faced with the same challenges that sporadic communist systems encounter in making the transition from a command economy to one that's driven by the marketplace. They're eager to effect reforms. They realize that corruption is a significant issue. They have not had the sort of growth in the past couple of years that they would like, but they're increasingly looking to emulate the Chinese model. They're looking outwards in the security realm to countries like the United States and India. I think that, in time, Vietnam may hold considerable promise for international trade.

It also is an arena which is very much in need of talents in terms of engineering, offshore oil and so forth, of the sort that I enumerated earlier. It is an economy that is beginning to rise, but it's not one without problems.

The Chair: Colleagues, are there no further questions? I would like to thank Dr. Boutiller for spending his time here today with us. It was very informative.

Senator Ngo: I have a question, if we have time.

The Chair: Yes, we have time.

Senator Ngo: Thank you, professor. The Indo-Asia Pacific region is now highly militarized. Seven of the world's 10 largest standing armies are in the region, five of them including Vietnam, China, North Korea, South Korea, and they also have five of the world's declared nuclear powers; China is there. In your presentation you say that China's ambition with Bejing is aggressive in the area of South Asia, South China Sea. Recently China unilaterally declared ownership of those islands or lands in the particular dispute area, and bullying countries such as Japan, Philippines, Vietnam, and so on.

What are the security challenges posed by this level of dispute? I'm talking about military in this region.
Mr. Boutilier: Your question is an extremely sound and appropriate one. Clearly, when we look at global arms sales, for example, the Indo-Pacific region is at the top of the tables. Indeed there is an anxiety among many analysts that there's an arms race unfolding in the region, that we've moved beyond sheer modernization of navies and armies to an action/reaction model in which countries are beginning to acquire assets in response to what their neighbours are doing. You can see that, for example, between Japan and South Korea.

One of the issues of particular concern is the dramatic growth in the submarine fleets of the region. The Chinese are building submarines three or four times as fast as Americans, and we probably have some 200 submarines active throughout the region. So at the time when we turned our backs on the Atlantic thinking that the Cold War was over, we failed to appreciate the way in which new levels of instability would appear.

What's interesting, among other things, is that if you go back to 2010, Chinese hosted an international maritime conference in Qingdao, the centre of their northern fleet. Central to that was the so-called harmonious seas concept. This was the maritime equivalent of the peaceful rise of China. Then almost immediately thereafter, Chinese body language and activities took a dramatic turn. Far from harmonious seas, they in fact became increasingly bullying and aggressive in the South China Sea at the expense of nations like the Philippines and Vietnam. Some of their actions are deeply reprehensible. In the case of Vietnam, as you know, a Vietnam vessel trading hydrographic equipment had the equipment cut through by Chinese vessels twice. We can see that the Chinese have strong-armed the Filipinos when it has come to resupply of one of their atolls.

One could go on with this long and dismal catalogue. It makes you wonder what's happening internally in China. Was it a perception of a lame duck presidency under Hu Jintao? Was it the party military getting out ahead of itself? Certainly I think there is growing awareness in Southeast Asia, which has been characterized by a high degree of passivity over the past decades that this is a real threat to the sovereignty of many of the players. Even countries that were on the margins, like Malaysia, have now begun to adopt a rather anti-Chinese sentiment.

It will be very interesting to see whether the Filipino case to the International Tribunal prevails. I think it will, and this will certainly be to the detriment of China's reputation at least.

Senator Ngo: Can I follow up?

The Chair: Go ahead.

Senator Ngo: You say Canada is one of the countries that initiated the law of the sea. Since the dispute of South China Sea, we didn't say anything. What do you think Canada can do in these dispute areas with China? Are we going to, like the United States and other countries, also condone Beijing's aggressive behaviour in this dispute area because of trade? What can we do?

Mr. Boutilier: No, I don't think we should condone these actions, which are in many ways in direct contravention to the UN Convention on the Law of the Sea. One of the challenges is, if you go back to 1996 and the Chinese ratification of UNCLOS, the Chinese caveat at that ratification was half a dozen issues, which in effect meant that Chinese domestic law prevails when it comes to the application of UNCLOS. One could ask parenthetically whether the spirit of the convention has been completely undermined in the process. It's very challenging when you have a major player like China, which adopts these aberrant interpretations.

For example, for the 12 nautical miles that we all recognize internationally, the Chinese intention is to apply that same territorial authority both to the 200-mile nautical mile zone, and there are other theological issues in terms of how ships conduct themselves within that zone, whether national permission is needed from China or not. The Chinese, of course, would maintain that it is. I think it's very much in our interest to try to uphold, in any form, the integrity of UNCLOS. This is a critical issue because the Chinese approach, I would suggest, is to repeat through the aberrant interpretations frequently in the hope that these will somehow become accepted and customary. I don't think this should be permitted to happen.

Senator Ngo: Thank you, professor.
The Chain: I would like to wind up with one last question, if I could. If you could comment on this, doctor, what should be Canada's main security priorities in the Indo-Asia Pacific region? What should Canada's priorities be?

Mr. Boutiller: I think that clearly what we've got to do is work through regional organizations, and we attempted to join the ASEAN Defence Ministers' Meeting but our membership was turned down flat because the perception in the region—and this was seven years ago—was that we simply had no profile whatsoever, that we simply weren't committed to the region.

We have to work through those organizations and there's a maritime organization, the Western Pacific Naval Symposium, which brings together the heads of all navies. This is another agency through which we have to try to encourage, in whatever way we can, greater peace and stability because this is an area that is increasingly volatile and in which Chinese moves in particular are opaque. So it behooves us, I think, to be as involved as we can in the region and to try to exploit opportunities for maritime collaboration, which will in fact be confidence-building measures because it's only in this way that we can begin to break down some of the barriers that exist in terms of the narratives between some of the major players.

Senator Day: Doctor, just for the record and for your information, the Senate has participated in the ASEAN parliamentary forum for a good number of years and that may be an area where we can make some inroads, where other levels of government may not have been able to do so.

Mr. Boutiller: Absolutely. I think one of the critical issues is consistency, in the sense that if you're partaking, you have to turn up every year. This is really critical. You can't appear episodically. That's almost worse than not at all. It's essential to build relationships from which almost everything else stems in this region. I can't underscore enough the importance of relationship building in Asia.

Senator Day: I agree wholeheartedly. AIPA is the ASEAN interparliamentary group and I have attended for about 10 years in a row, so we have had representation there, not just me, but a number of parliamentarians for a good number of years. But you're absolutely right. It takes a long time in Asia to build trust.

Mr. Boutiller: Absolutely.

The Chair: Colleagues, I would like to thank Dr. Boutiller for appearing before us and giving his testimony.

You certainly bring a perspective in respect to an area that you know very well. I'm sure that we'll be calling upon your expertise at a later date as we go further into the study. Once again, thank you very much, Dr. Boutiller.

(The committee adjourned.)
On October 8, 2014, the Director of CSIS made a joint appearance with: Steven Blaney, the Minister of Public Safety and Emergency Preparedness; RCMP Commissioner Bob Paulson; and Public Safety Deputy Minister François Guimont at the House of Commons Standing Committee on Public Safety and National Security (SECU) to testify on matters related to foreign fighters/extremist travelers.

Below are key statements made at that appearance:

- **On the threat to military personnel:** “Specifically on that issue, you may remember several months ago the serviceman in Britain who was stabbed to death on the street while he was wearing his uniform. The Service obviously will look at that kind of incident – and not just the Service but ITAC also. It’s part of their job to do the terrorist assessment. And we’ll make an assessment in terms of potential threats against, in this case, military personnel. As I mentioned, the role of the Service is to advise the government. In this case, we would advise DND, and it would be up to National Defence to decide what kind of stance it had to take to mitigate that threat, whether there really was a threat, and what measures they needed to put in place.” (Director Michel Coulombe) (For responsive lines, see Tab 3B).

- **On foreign fighters:** “The Government of Canada is aware of at least 130 individuals with ties to Canada who are suspected of participating in terrorist activities. We know of about 80 who have returned to Canada.” (Minister Blaney) (For responsive lines, see Tab 3E).

- **When we’re talking about 80 returnees, we’re not talking about 80 people who fought in Iraq and Syria, and we’re not necessarily talking about people who are directly involved in planning terrorist activities. We have Canadians who are involved in terrorist activities, but those could be fundraising or propaganda. I don’t want people to believe that we have 80 returnees who were hard fighters in Iraq and Syria, because that is not the picture we have at the moment. All of them could potentially be a threat, definitely.” (Director Michel Coulombe) (For responsive lines, see Tab 3E).

- **On the number we’re quoting – at the time, 130, by the time I leave this room will change. It’s fluctuating all the time. It hasn’t increased substantially since my appearance in February. That number is the number we can confirm in a nexus to Canada, and we can confirm that the individuals are involved in terrorist-related activities. That’s the one we know. Are there some that we are not aware of? Probably. I don’t want to speculate. I’ve read in the media that it’s probably up to 300. The Service doesn’t go there. We go with facts, and the fact is that we can confirm between 130 and 145. It’s the same with the 80: that’s not speculation, that’s the one we can confirm. They were involved in terrorist-related activities overseas, they’re now back in Canada. It’s a firm number that we’re aware of. And yes, we know where they are.” (Director Michel Coulombe) (For responsive lines, see Tab 3E).

- **On preventing radicalization:** “The RCMP counterterrorism information officer initiative has seen more than 1,700 candidates participate in the program since its establishment five years ago. In the last year alone, more than 325 people have been trained by the counterterrorism team.” (Minister Blaney) (For responsive lines, see Tab 3C).

- **With our countering violent extremism program, we’re in a unique partnership with Public Safety, the CSIS, and the Toronto Police Service, who have a tremendously effective network, one that is tried and demonstrated, into all communities. So we’re overlaying this sort of approach into their existing infrastructure and we’re finding it to be..."
On exit controls: When asked by committee member Craig Scott if "Canada is considering or will need to implement an exit control system as a consequence of (UN Security Council Resolution 2178)", Minister Blaney replied: "No...Let me be very clear that we are really not contemplating exit controls...What we are contemplating is information exchange...We are committed to working with other European countries as well in sharing information, basically the information you find on a passport, which is already shared with the country where you are going. This is something we are working on." (For responsive lines, see Tabs 3C)

On the number of active investigations: "I would include CSIS in this, because we are joined at the hip in how we manage a response to the threat...the pace and tempo of operations is fairly brisk. We're operating probably about 63 active national security investigations on 90 individuals who are related to the travelling group." (Commissioner Bob Paulson) (For responsive lines, see Tabs 3B).

On funding cuts: We've (i.e. the RCMP) changed our way of managing our activities. We changed how we prioritize our federal policing model, and consequently we're able to move resources into and out of national security cases to match the tempo and pace. So the cuts have not affected our operations." (Commissioner Bob Paulson) (For responsive lines, see Tab 3J).

The role of (CSIS) is to protect us, especially against the terrorist threat. We are talking about very substantial resources...Resources are currently being redistributed. For example, most of (CSIS)'s budget covers the main priority of our strategy." (Minister Blaney) (For responsive lines, see Tab 3I).

On the passport revocation decision-making process: Are CSIS and the RCMP integrated into the decision-making process of the Passport Canada Security Bureau for passport revocation? "We do exchange information not just with Passport Canada and the RCMP, but there is that integration, coordination, and deconfliction, if not daily then at least weekly, on that very specific issue." (Director Michel Coulombe) (For responsive lines, see Tab 3N).

Is there a way for a foreign fighter to make amends and return to Canada? "As parliamentarians, it's important for us to understand the scope of the terrorist threat. We need to understand how radicalized these people are and just how far they're prepared to go...We're talking about people who are prepared to kill in order to stand up for their beliefs. We can't negotiate with terrorists. It's not complicated. There's no issue. I have a duty to do everything I can to prevent (them) from killing Canadians. It doesn't seem complicated." (Minister Blaney) (For responsive lines, see Tab 3D).

"CSIS's duty is to constantly reassess the potential threat to Canadians' safety, whether we are talking about information that exacerbates the threat or information that shows that the individual in question doesn't pose the alleged threat or no longer poses that threat." (Director Michel Coulombe) (For responsive lines, see Tab 3E).

The characterization of the threat to Canada: "The threat, as we can see, is real. The threat is there. As a country, we are constantly adjusting to the level of threat." (Minister Blaney) (For responsive lines, see Tab 3A).

Compared to the late 1990s and 2000s before 9/11, the threat is different. It's more diffuse...It develops a lot more rapidly. With the use — and the sophisticated use — of social media, for example, radicalization can happen really quickly. The development of an attack actually can also happen really rapidly. There's the movement of people. The threat is different. This phenomenon of what we call "foreign fighters," especially in the developments in Iraq and Syria, I think is real, like I've mentioned. It does pose a real threat. Again, we have no information indicating an imminent attack, but we have to remain vigilant. The threat is real." (Director Michel Coulombe) (For responsive lines, see Tab 3A).
Senate Standing Committee on National Security and Defence (SENDEF)

(41st Parliament – 2nd Session)

Membership Overview:

Committee Chair:
- Senator Daniel Lang (CPC) – Yukon

Committee Deputy Chair:
- Senator Grant Mitchell (Lib.) – Alberta

Committee Members:
- Senator Vernon White (CPC) – Ontario
- Senator Jean-Guy Dagenais (CPC) – Victoria, Québec
- Senator Carolyn Stewart Olsen (CPC) – New Brunswick
- Senator Lynn Beyak (CPC) – Ontario
- Senator Thanh Hai Ngo (CPC) – Ontario
- Senator Joseph A Day (Lib.) – Saint John-Kennebecasis - New Brunswick
- Senator Colin Kenny (Lib.) – Rideau - Ontario
Daniel Lang (CPC) – Yukon
Chair

- Served in the Yukon Legislative Assembly from 1974 to 1992
- Former Sales Associate in the Yukon Real Estate industry
- Current Vice Chairman of the Board of Governors for Yukon College
- Member of the Senate Standing Committee on Internal Economy, Budgets and Administration, and the Subcommittee on Veterans Affairs

Grant Mitchell (Lib.) – Alberta
Deputy Chair

- Deputy Chair of the Senate Committee on Energy, the Environment, and Natural Resources
- Bachelor of Arts (Honours) in Political Science from the University of Alberta and a Master of Arts in Political Studies from Queen's University
- Obtained his Chartered Financial Analyst designation in 1983
- Member of the Alberta Legislative Assembly for the riding of Edmonton-McClung (1986-1998)
- Former investment advisor with CIBC Wood Gundy
- Former Budget Analyst in the Treasury Department and Senior Intergovernmental Affairs officer in the Department of Federal and Intergovernmental Affairs
- Member of the Senate Standing Committee on Energy, the Environment and Natural Resources, and the Subcommittee on Veterans Affairs

Vernon White (CPC) – Ontario

- Former Chief of Police of the Ottawa Police Service (sworn in in 2007)
- Led the Regional Police Service in Durham, Ontario, and spent over 20 years with the Royal Canadian Mounted Police, leaving as an Assistant Commissioner
- Diploma in Business Administration from the College of Cape Breton, a Bachelor of Arts Degree in Sociology and Psychology from Acadia University, and a Masters Degree from Royal Roads University in British Columbia in Conflict Analysis and Management
- Recipient of the Commissioners Commandation, a Queen's Jubilee Medal, and a United Way Community Builder of the Year Award
- Chair of the Standing Senate Committee on Rules, Procedures and the Rights of Parliament
- Member of the Standing Senate Committee on Internal Economy, Budgets and Administration, and the Subcommittee on Veterans Affairs
Jean-Guy Dagenais (CPC) – Victoria - Québec

- Former police officer (1972 to 2011) with the Sûreté du Québec
- Former President of the Association des policières et policiers provinciaux du Québec
- Former board member of both the École nationale de police and the Canadian Police Association
- Recipient of the Officer of the Order of Merit of the Police Forces, which rewards citizens who have marked the evolution of Québec or enabled its influence in diverse fields
- Member of the Standing Senate Committee on Agriculture and Forestry, and the Standing Senate Committee on Legal and Constitutional Affairs

Carolyn Stewart Olsen (CPC) – New Brunswick

- Has extensive experience in health and politics
- Worked as a Registered Nurse for 20 years
- In 1986, named Head Nurse for the Ambulatory Care Department at Ottawa’s Grace Hospital; and later as Nursing Manager for the Emergency, Recovery Room, Ambulatory Care, and CSR departments at Carleton Place Hospital
- Served as communications assistant and Press Secretary to the Leader of the Opposition; and as Press Secretary and Director of Strategic Communication in the Office of the Prime Minister
- Member of the Standing Senate Committee on Social Affairs, Science and Technology; the Standing Senate Committee on Fisheries and Oceans; and the Subcommittee on Veteran Affairs

Lynn Beyak (CPC) – Ontario

- Small-business owner in northwestern Ontario with several years of experience in real estate, insurance, and tourism
- Has served as vice-chair of the Fort Frances-Rainy River Board of Education
- Chaired the Ontario Parent Council
- Has been a member of the board of directors of the Trillium Foundation
- Member of the Standing Senate Committee on Aboriginal Peoples, and the Standing Senate Committee on Agriculture and Forestry
Thanh Hai Ngo (CPC) - Ontario

- Appointed Citizenship Judge for Ottawa in December 2007
- Educated in France and Canada, receiving a Bachelor of Arts (Honours), from the University of Paris—la Sorbonne, and a Bachelor and a Master of Education from the University of Ottawa
- Chairperson of the Employment Insurance Board of Referees in Ottawa
- Immigrated to Canada in 1975 after fleeing communist terror in Vietnam
- Active member of various Vietnamese communities across Canada and overseas; founder and former Chairperson of the Ottawa Vietnamese Non-Profit Residence Corporation
- Co-founder of the International Committee for a Free Vietnam - Canada chapter
- President of the Vietnamese Community Association of Ottawa and Vice-President of the Canadian Assessment and Placement Centre, Employment Centre for New Immigrants
- Member of the Standing Senate Committee on Human Rights Committee; the Standing Senate Committee on Aboriginal Peoples; and the Standing Committee on Social Affairs, Science and Technology

Joseph A. Day (Lib.) - Saint John - Kennebecasis - New Brunswick

- Chair of the Senate Standing Committee for National Finance
- Law Degree and had private practice of Business Law; Patent and Trademark Agent
- Former President and CEO of the New Brunswick Forest Product Association
- Member of the Law Society of New Brunswick, the Law Society of Upper Canada, the Barreau du Québec, the Association of Professional Engineers and Geoscientists of New Brunswick, and the Laurier Club
- Former member of the now defunct Senate Special Committee on Anti-terrorism
- Chair of the Senate Subcommittee on Veterans Affairs
Colin Kenny (Lib.) – Rideau - Ontario

- From 1969 to 1979, worked in the Prime Minister's Office as Special Assistant, Director of Operations, Policy Advisor and Assistant Principal Secretary to Prime Minister
- Served as an executive with Dome Petroleum in Calgary in the early 1980s
- Served on numerous committees of special relevance to defence and national security issues
- Elected to various positions in the North Atlantic Parliamentary Assembly between 1999 and 2001
- Published on a wide range of issues including defence policy, ballistic missile defence, Canada's involvement in Afghanistan, defence procurement, strategic airlift, alternative fuels, the Arctic and offshore drilling operations, aviation security, port security, border security, and various Canadian political issues
- Became a Commissioner of the Trilateral Commission in 2009
- Became a member of the Johns Hopkins University, Atlantic Basin Initiative's Eminent Persons Group in 2012
Director
Michel Coulombe

Travel to

18-23 January 2015

Contact numbers:

Michel Coulombe
BlackBerry:  
PIN: 

Office:  
Cellular:  
Residence:  
BB:  

Office:  
Cellular:  
Residence:  
BB:  

Sunday, 18 January 2015  

Monday, 19 January 2015  

Prepared by  
14 January 2015
Tuesday, 20 January 2015

PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.

REVISED BY CSIS UNDER THE
PROTECTION ET DÉTÉRMINATION
DE LA LOI SUR L'ACCÈS
À L'INFORMATION.
Thursday, 22 January 2015

PROCESSED BY CSIS UNDER THE
PROVISIONS OF THE PRIVACY ACT AND/OR
ACCESS TO INFORMATION ACT.

RÉVISE PAR LE SCRS EN VERTUE DE LA LOI
SUR LA PROTECTION DES RENSEIGNEMENTS
PERSONNELS ET/OU DE LA LOI SUR L'ACCÈS
À L'INFORMATION.

14 January 2015

Prepared by:
End of program.
MEMORANDUM TO THE DIRECTOR

MEETING OF THE PUBLIC SERVICE
MANAGEMENT ADVISORY COMMITTEE

9:00 a.m. – 12:00 p.m.
Friday, 16 January 2015
Collaboration Boardroom, 373 Sussex Drive

You will be attending a meeting of the Public Service Management Advisory Committee (PSMAC), at which the following items will be discussed (TAB 1):

- General discussion;
- “My GCHR” Presentation;
- ADM Talent Management: New Cluster Approach (TAB 2);
- Public Service Commission (PSC) Student Employment and Graduate Recruitment Programs (TAB 3); and

BACKGROUND

At the last PSMAC meeting on 12 December 2014, members discussed a range of issues, including: the Government of Canada Business Transformation Proposal; John Doe v. Ontario (Finance); and Federal Obligations, Collaboration and Innovation: Inuit Employment under the Nunavut Land Claims Agreement.

ITEM 1: General Discussion

At the time of writing, neither topics nor documentation were provided for this item.

ITEM 2: “My GCHR” Presentation (No Documentation Provided)

Tammy Labelle, Director General of GCHR, Integrated Service Branch, Public Works and Government Services Canada (PWGSC), will provide a demonstration of the “My GCHR” system.

“My GCHR” is a Human Resources (HR) modernization initiative that aims to enhance the efficiency of HR service delivery within the federal public service. It is meant to take advantage of economies of scale by standardizing and consolidating HR processes and systems. For instance, over the next three years, the “My GCHR” program will coordinate the transition of all
departments and agencies from their existing departmental HR applications to a single government-wide instance of the PeopleSoft software. "My GCCHR" will offer a suite of common HR services to meet the provisional needs of departments and agencies looking to offer these services in a cost-effective manner.

During the discussion, it will be important for you to mention that might inadvertently imply that the Service will take part in this initiative. This is consistent with what has already been expressed at an earlier PSMAC meeting concerning workplace technology centralization by Shared Services Canada (SSC), and the letter you sent to the President of SSC.

**ITEM 3: ADM Talent Management: New Cluster Approach**

In advance of the 2015 Winter Cluster Review Discussions, Susan MacGowan, Visiting ADM, ADM Collective Management [Treasury Board Secretariat (TBS)], will seek feedback on the proposed changes to ADM Talent Management in the Public Service. These changes are the five new clusters (Security, Science, Central Agencies and Internal Services, and two Blended), as well as the renewed emphasis on succession planning.

The proposed changes are in line with the Service's direction in recent years to develop an integrated talent management program for its EX employees, including performance management, talent potential, leadership training, and succession planning.

As a separate employer, the Service is governed by its own version of many HR-related TBS policies, and is moving in the same direction as TBS in identifying critical positions that will need to be filled in the future, requiring succession planning in consequence.

The Service supports the proposed cluster approach, which, for the Security Cluster, contains a total of 78 ADMs. Both positions and employees will be evaluated in this cluster, as certain ADM positions require more experience than others. You may wish to enquire as to which of these positions are identified as being critical or essential and whose sustained vacancy would put the functioning of government at risk. While the Service is not obligated to participate in this exercise, it is valuable to align the professional development of Service executives with TBS' talent management, in the event that they desire experience in the core Public Service.

Historically, the Service has had very few executives on interchange with other government departments and most of the Service's executives are 'homegrown.' In light of the foregoing, you may wish to ask for more information about the specific requirements for ADM positions and TBS' pool of potential successors within the Security Cluster.
ITEM 4: PSC Student Employment and Graduate Recruitment Programs

Anne-Marie Robinson, President, and Gerry Thom, Vice President (both from the Public Service Commission) will seek feedback on the design of the student and graduate recruitment programs, and on the development of strategies to facilitate the use of existing program inventories.

In 2013-2014, temporary hiring of students represented 29.1% of all hires under the Public Service Employment Act. Less than 17% of the Public Service population is aged 34 or younger, a number that has been in steady decline since 2011. While student hires have increased by 8.6% in 2013-2014, the application rate of students has gone down in certain hiring programs.

The Service, as a separate employer, has crafted its own student employment program. Students must apply to the Service one year in advance for a work term and the Service must set timelines distinct from university and college calendars due to the length and intricacies of its security screening process. In the past few years, the Service has integrated new graduates through the co-op student program. In the past three years, the Service has hired 76% of its co-op students. In 2013-2014, 56 students were brought into the Service for four-month work terms.

CSIS Recruiting and Staffing has reviewed the PSC Student and Graduate Recruitment Programs and Hiring Mechanisms and determined that, due to the Service’s security parameters and processes these particular programs cannot be integrated into the Service’s hiring practices.

ITEM 5: Policy Suite Reset – Proposed Approach

Roger Scott-Douglas, Assistant Secretary for Priorities and Planning (TBS) will outline the approach to TBS’ Policy Suite Reset (PSR), including links to the Blueprint 2020 Internal Red Tape Reduction Initiative, and will set out proposed next steps for engagement.

The PSR is an all-embracing evaluation of TBS and departmental policies that pertain to a wide range of issues (e.g. finance, HR, and management) and is expected to yield a coherent, logically-grouped policy framework. By summer 2015, TBS will be interacting with departments to balance and coordinate policies common to departments as part of the PSR and to test solutions developed through the Internal Red Tape Reduction Initiative.

The Service has an interest in PSR, as it follows TBS policies as required and, otherwise, to the extent possible (e.g. in finance, corporate services and security). Moreover, CSIS went through a similar process in 2011, when it developed the CSIS Governance System (CGS) model to create a leaner and smarter internal policy suite. The Service succeeded in removing and reconciling redundancies, streamlining delegation authorities, and minimizing policy silos that had led to a cluttering of its policy suite. It also made use of web-based technology, much like TBS’ proposed reset approach. The Service experience was imparted to TBS and was well-received, with TBS intending to use it as a “touch point” when it begins engaging departments. The deck at TAB 4 reflects many of the Service’s considerations, as well as similar nomenclature, present in the briefing material shared with TBS.
As for the Internal Red Tape Reduction Initiative, its “bottom up” approach to streamlining policies in order to focus on the user reflects the solution already implemented by the Service, which, as part of the CGS, developed principles to address situations where decisions would need to be taken in the absence of an explicit policy. These principles (i.e. whether an action is lawful and authorized, necessary, proportionate, and representative of an effective and efficient use of public resources) allow for personal judgment to play a more prominent role in the policy sphere. They are applicable in real time and bridge the spirit of the Service's mission to the situation at hand, with policy being adjusted afterwards. You may wish to relay the Service's success in this regard.

The above notwithstanding, any policy reset by TBS should recognize that the Service classifies information differently than most other government agencies and departments. Clarity and consideration should be given with respect to the type of information collected or stored by other government agencies and departments that should be excluded from this policy reset so as to protect information management practices unique to the security and intelligence community.

If you require any further information, please do not hesitate to contact me.

Tom Venner
Assistant Director
Policy and Strategic Partnerships

Enclosed:
- TAB 1: Agenda
- TAB 3: Deck – Student Employment and Graduate Recruitment Programs (PSC)
Agenda / Ordre du jour

Public Service Management Advisory Committee (PSMAC) / Comité consultatif sur la gestion de la fonction publique (CCGFP)
January 16, 2015 / le 16 janvier 2015

Collaboration Boardroom, 373 Sussex Drive / Salle de conférence collaboration, 373, promenade Sussex
9:00 a.m. - 12:00 p.m. / 9h00 - 12h00

1. General Discussion / Discussion générale
   
2. My GCHR Presentation / Présentation du système Mes RHGC
   T. Labeille (PWGSC / TPSGC)
   To provide a demo of the My GCHR system, including its key functionalities / Faire une démonstration du système Mes RHGC, incluant ses fonctionnalités
des

3. ADM Talent Management: New Cluster Approach / Gestion des talents des SMA : nouvelle approche pour les examens groupés
   S. MacGowan (TBS - OCHR / SCT - BDPRH)
   To seek feedback on the proposed changes for the 2015 Winter Cluster Review discussions / Obtenir des commentaires sur les changements proposés aux Examens groupés de l'hiver 2015

4. PSC Student Employment & Graduate Recruitment Programs / Programmes de la CFP visant le recrutement de diplomés et l'emploi d'étudiants
   A.-M. Robinson / G. Thom (PSC / CFP)
   To seek feedback on student and graduate recruitment program design and develop strategies to facilitate the use of existing program inventories / Obtenir des commentaires sur la conception des programmes de recrutement d'étudiants et diplomés et élaborer des stratégies pour faciliter l'utilisation des repertoires existants

5. Policy Suite Reset – Proposed Approach / Réinitialisation de l'ensemble de politiques – Approche proposée
   R. Scott-Douglas (TBS / SCT)
   To outline the approach to TB Policy Suite Reset, including links to the Blueprint 2020 Internal Red Tape Initiative, and set out proposed next steps for engagement / Présenter l'approche de la Réinitialisation de l'ensemble des politiques du CT, incluant les liens à l'initiative de l'Objectif 2020 sur la simplification des procédures administratives internes, et établir les prochaines étapes proposées pour la mobilisation
Presentation to the
Public Service Management Advisory Committee

ADM Talent Management – New Cluster Approach

Daniel Watson, Chief Human Resources Officer
Treasury Board Secretariat

January 16, 2015
Objectives

• Discuss the evolution and future direction of ADM Talent Management.

• Provide an overview and seek comments from Deputy Ministers on the proposed changes for the 2015 Winter Cluster Review discussions.
Context

- To date, during Cluster Review meetings:
  - similar discussions and equal attention were given to all ADMs; strengths and areas to develop discussed for each ADM
  - limited discussion on potential successors for positions that may become vacant and options for individuals identified as ready for advancement/movement
- New cluster groupings by specific streams (ie. Security, science) implemented for fall discussions.
- Planning for the Winter Clusters:
  - new groupings will mean more ADMs being discussed (average of 74 per cluster);
  - need to use time efficiently;
  - opportunity to focus the conversations on succession plans for positions that may become vacant and to identify specific opportunities for ADMs ready for movement and advancement.
ADM Talent Management – progress to date

Focus on ADM Awareness and Development

Discuss strengths and opportunities for development for all ADMs

Validate talent map placements

Ad hoc discussion on critical positions to the Public Service

Preliminary discussion on Aboriginal representation at the executive levels
Evolution of ADM Talent Management meetings

Ad hoc approach to succession planning

Integrated succession planning

2014 to 2015

Bi-Annual Cluster Reviews

- Fall Clusters introduced to discuss ADM Feeder Pool
- Mandatory for EX-03s

5 - Cluster Reviews by Deputy Heads

- Security, Scientific, 2 Blended, and Central Agency
- Associate DMs invited
- Evolution of Talent Management to more integrated succession management

Prior to 2011

Individual Meetings with Deputy Heads

- 1 Security
- 8 Mix of Departments
- More ADMs known by more Deputies

2011 to 2013

9 Cluster Reviews by Deputy Heads

- More ADMs known by more Deputies
Building on learning from other organizations and literature

Research Highlights

- Business-Driven Planning
  - Identifying and developing leadership that will lead to the achievement of strategic goals
- Enterprise-wide Talent Sourcing
  - Selecting successors from across enterprise
- Talent and Succession matching
  - Talent development and succession discussions are held concurrently
- “Constructive Conflict”
  - Senior-level discussions about talent must be candid and productive

"It's not the system that counts. It's the conversation that counts"

- Michael Carey, VP of HR for Johnson and Johnson
Proposed approach to Winter Cluster discussions

1. Reasonable discussion of all ADMs, by talent map placement
   - Ready for Advancement – For what positions?
   - Ready for Movement – To where? To develop what?
   - Transition to Retirement – When? Potential successors?
   - Corporate Support – In what areas?
   - Well-placed in role / Develop in Role – One minute elevator pitch. Who could be ready for promotion if required?

2. Discuss specific requirements for ADM positions and identify pools of potential successors
   - What specific experience, knowledge, or competencies are required for these positions?
   - Timeline for projected vacancies?
   - Who has the necessary experience, skills and competencies for these positions now? And in the future?
   - What development and/or lateral move would these successors need to be ready?

3. Discuss career support for development of Aboriginal Executives
   - What specific experience, knowledge, or competencies do these Aboriginal executives need to become ADM ready in the future?
   - What will be done following the cluster discussion to support their development?
Cluster Review Take-Away
Succession Plans

Position Profile

- Title
- Level
- Key Requirements (Skills and Experience)
- Vacancy risk: Now - 1 year; 1-2 years; 2-3 years

Incumbent

Meryl Streep
- Qualifications/ skills
- Talent Map Placement
- Successor for:
  - Positions xyz

Immediate Successors

Julianne Moore
Michael Keaton
Benedict Cumberbatch

Longer-term Succession Plan

<table>
<thead>
<tr>
<th>Ready in...</th>
<th>Recommended moves for development</th>
</tr>
</thead>
<tbody>
<tr>
<td>Daniel Bruhl (2 years)</td>
<td>- Central Agency Assignment</td>
</tr>
<tr>
<td>Jake Gyllenhaal (3 Years)</td>
<td>- Position outside of functional group</td>
</tr>
<tr>
<td>Reese Witherspoon (3 years)</td>
<td>- Experience with machinery of government</td>
</tr>
</tbody>
</table>
Benefits of proposed changes

✓ ADMs continue to be known by more Deputy Heads

✓ Rather than Ad hoc succession planning, will focus on clear short and medium term succession plans for ADM level positions

✓ Ability to clearly identify positions at risk to the Public Service, if no successors are identified, and to focus our collective efforts to address these gaps

✓ Critical experiences can be incorporated into the learning plans of potential successors

✓ ADMs and feeder pool will have a better idea of what experience(s) they need to progress their career

✓ Inform future resourcing recommendations for ADM level positions
Are there other suggestions to meet your needs?

Do you support the proposed new changes?

Discussion
### CLUSTER GROUPINGS

<table>
<thead>
<tr>
<th>Security</th>
<th>Total of 78 ADMs</th>
<th>Science</th>
<th>Total of 65 ADMs</th>
<th>Central Agencies/Internal Services</th>
<th>Total of 75 ADMs</th>
</tr>
</thead>
<tbody>
<tr>
<td>CBSA</td>
<td></td>
<td>Agriculture and Agri-Food</td>
<td></td>
<td>Courts Administration Service</td>
<td></td>
</tr>
<tr>
<td>CSC</td>
<td></td>
<td>CFIA</td>
<td></td>
<td>CSPS</td>
<td></td>
</tr>
<tr>
<td>DFATD - Foreign Affairs</td>
<td></td>
<td>Canadian Nuclear Safety Commission</td>
<td></td>
<td>Department of Finance</td>
<td></td>
</tr>
<tr>
<td>FINTRAC</td>
<td></td>
<td>DFO</td>
<td></td>
<td>Justice Canada</td>
<td></td>
</tr>
<tr>
<td>National Defence</td>
<td></td>
<td>Environment Canada</td>
<td></td>
<td>PCO</td>
<td></td>
</tr>
<tr>
<td>Public Safety</td>
<td></td>
<td>Health Canada</td>
<td></td>
<td>PSC</td>
<td></td>
</tr>
<tr>
<td>RCMP</td>
<td></td>
<td>NRCan</td>
<td></td>
<td>TBS</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Public Health Agency</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Blended</th>
<th>Total of 78 ADMs</th>
<th>Blended</th>
<th>Total of 75 ADMs</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACOA</td>
<td></td>
<td>Canadian Heritage</td>
<td></td>
</tr>
<tr>
<td>AANDC</td>
<td></td>
<td>CANOR</td>
<td></td>
</tr>
<tr>
<td>DFATD - Trade</td>
<td></td>
<td>Canadian Space Agency</td>
<td></td>
</tr>
<tr>
<td>Industry Canada</td>
<td></td>
<td>CIC</td>
<td></td>
</tr>
<tr>
<td>Parks Canada</td>
<td></td>
<td>CRA</td>
<td></td>
</tr>
<tr>
<td>PWGSC</td>
<td></td>
<td>CRTC</td>
<td></td>
</tr>
<tr>
<td>Shared Services Canada</td>
<td></td>
<td>DFATD - Development</td>
<td></td>
</tr>
<tr>
<td>Stats Canada</td>
<td></td>
<td>Economic Development Agency for the Regions of Quebec</td>
<td></td>
</tr>
<tr>
<td>Transport/ Infrastructure Canada</td>
<td></td>
<td>Elections Canada</td>
<td></td>
</tr>
<tr>
<td>Veterans Affairs</td>
<td></td>
<td>Federal Economic Development Agency for Southern Ont</td>
<td></td>
</tr>
<tr>
<td>Western Economic Diversification Canada</td>
<td></td>
<td>ESDC</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ESDC - Labour</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>ESDC - Service Canada</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Immigration and Refugee Board</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Library and Archives</td>
<td></td>
</tr>
</tbody>
</table>
PSC Student Employment & Graduate Recruitment Programs

PSC PRESENTATION TO PSMAC
JANUARY 2015
Purpose

- To inform PSMAC about existing student and graduate recruitment programs and usage trends.

- To solicit feedback on student and graduate recruitment program design and opportunities for promoting existing programs.

- To gather intelligence about departmental realities and to develop strategies to facilitate their use of existing program inventories.
Hiring Activities Under the *PSEA* by Tenure (2008-2009 to 2013-2014)

In 2013-2014, temporary hiring of students represented 29.1% of all hires under the PSEA.

Sources: Public Service Commission hiring and staffing activities files; PSC Annual Report
Public Service Employee Distribution by Age Intervals (PSEA) – June 2014

Less than 17% of the PS population is aged 34 or younger; this also has been in steady decline since 2011.

Sources: Public Service Commission hiring and staffing activities files; PSC Annual Report
PSC Student and Graduate Recruitment Programs and Hiring Mechanisms

The PSC administers three programs that recruit students for temporary, part-time and summer employment:

- Federal Student Work Experience Program (FSWEP)
- Research Affiliate Program (RAP)
- Co-op and Internship Program (COOP)

The PSC administers two programs that recruit graduates for permanent employment:

- Post-Secondary Recruitment (PSR)
- Recruitment of Policy Leaders (RPL)

Other mechanisms to hire students:

- Student Bridging
- Internal and External Processes
Temporary Employment of Students

Based on 2013-2014 data, an increase in recruitment is observed with slightly greater gains for non-student hires (19.6% compared to 8.6% for student hires).

Source: Public Service Commission hiring and staffing activities files; PSC Annual Report
Student programs with greater specialization such as the Research Affiliate Program (RAP) are seeing the greatest relative growth (Annexe 1)
PSR by the numbers...
2008-2009 to 2013-2014

PSR Hires and Applications, by Fiscal Year

PSR hires are on a continued downward trend, with only 112 hires last fiscal year (Annexe 2).

Source: Public Service Resourcing System and Public Service Commission hiring and staffing activities files
- From 2008 to 2013, student hiring into permanent positions via bridging or other alternate mechanisms were on a continued downward trend but an increase was observed in 2013-2014.
- In 2013-2014, the PSC developed a new measure to estimate the proportion of indeterminate appointments made through the bridging mechanism. Using this new measure, it was estimated that at least 255 indeterminate appointments to Public Service were achieved through student bridging.

Source: Public Service Commission hiring and staffing activities files
## PSR Campaign Participation

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Departmental Career Choices</td>
<td>5</td>
<td>11</td>
<td>17 Departmental Career Choices (Annex 3)</td>
</tr>
<tr>
<td>PSC career stream inventories</td>
<td>5</td>
<td>5</td>
<td>4</td>
</tr>
<tr>
<td>Candidates</td>
<td>9,780 candidates</td>
<td>6,491 candidates</td>
<td>6,962 candidates invited to be tested</td>
</tr>
</tbody>
</table>

## Departmental Identified Needs and Appointments

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Identified Needs</td>
<td>Up to 164 positions</td>
<td>Up to 334 positions</td>
<td>Up to 227 positions</td>
</tr>
<tr>
<td>Appointments</td>
<td>254 appointments</td>
<td>112 appointments</td>
<td>Not yet available</td>
</tr>
</tbody>
</table>
OUTREACH ACTIVITIES

Internal:
- Letter to Heads of HR; HRC Updates
- National Managers Network
- Regional HR interdepartmental committees; Regional Federal Councils
- Webex sessions with HR and Hiring Managers

External:
- Attending Career Fairs and Targeted info sessions across the country
- Working in collaboration with DM champions of Universities
- Maximizing the use of social media such as Twitter, updated website info, use videos in messaging

Feedback from students:
- Are very interested in learning more about jobs in the Public Service (PS)
- Appreciate the opportunity to discuss with the PSC and federal organizations representatives
- Find it difficult to navigate the Web site and to get a job in PS
- Think that all positions within PS are bilingual
- Wish that a larger number of federal organizations would participate in Career Fairs
- Wish that all departments participating in Career Fairs would join together to display a unified brand
IT'S YOUR CAMPAIGN: YOU DECIDE...

Tailored to your needs:
- A variety of positions, groups and levels
- A variety of educational backgrounds
- A variety of experiences and skills criteria
- Possibility of EE group referrals
- Permanent and temporary hiring including casual employment

Easy to use and cost effective
- Cost of programs absorbed by PSC; no costs for departments
- Promotion of programs by PSC: will be attending over 50 career fairs
- Timely referrals: list of candidates provided within 3 to 5 days
- PSR centralized testing

Both client- and job-seeker-centric, student and graduate programs provide a quick, flexible, and cost-effective solution for your year-round hiring needs!
For Discussion

Given the low uptake by departments, are centralized recruitment programs for students and graduates still relevant or should the investment be reconsidered?

What additional strategies can the PSC use to encourage more frequent and informed use of its recruitment programs?

Are there promotion efforts that could be undertaken by the larger public service to encourage uptake (e.g. establish target in departmental HR plans)?
Annexes
## Student Employment Programs

### Activities by Fiscal Year

<table>
<thead>
<tr>
<th>Program</th>
<th>2011-2012</th>
<th>2012-2013</th>
<th>2013-2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Federal Student Work Experience Program (FSWEP)</td>
<td>Applications</td>
<td>47,343</td>
<td>45,146</td>
</tr>
<tr>
<td></td>
<td>Hires</td>
<td>8,305</td>
<td>5,835</td>
</tr>
<tr>
<td>Research Affiliate Program (RAP)</td>
<td>Applications</td>
<td>1,386</td>
<td>1,599</td>
</tr>
<tr>
<td></td>
<td>Hires</td>
<td>274</td>
<td>318</td>
</tr>
<tr>
<td>Co-operative Education and Internship Program (COOP)</td>
<td>Placements</td>
<td>4,520</td>
<td>3,408</td>
</tr>
</tbody>
</table>

While student hires have increased by 8.6% in 2013-2014, the application rate of students has gone down in FSWEP and RAP.

Source: Public Service Resourcing System and Public Service Commission hiring and staffing activities files
## Graduate Employment Programs Activities by Fiscal Year

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Hires</td>
<td>36,170</td>
<td>3,015</td>
<td>18,470</td>
</tr>
<tr>
<td>Recruitment of Policy Leaders (RPL)</td>
<td>Applications</td>
<td>1,401</td>
<td>1,504</td>
<td>1,581</td>
</tr>
<tr>
<td></td>
<td>Hires</td>
<td>18</td>
<td>11</td>
<td>7</td>
</tr>
</tbody>
</table>

Graduates application rates have fluctuated, depending on the hiring year.

Sources: Public Service Resourcing System and Public Service Commission hiring and staffing activities files; PSC Annual Report
<table>
<thead>
<tr>
<th>Department</th>
<th>Position Title</th>
<th>PSC Tests Required</th>
<th>Group &amp; Level</th>
<th>Number of applications received</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Foreign Affairs, Trade and Development Canada</td>
<td>Management Consular Officer, Policy Officer, Commerce Officer, Foreign Service Officer, International Development Officer</td>
<td>yes</td>
<td>AS-04, EC-04, CO-01, FS-01, PM-04</td>
<td>8,223</td>
</tr>
<tr>
<td>2. Citizenship and Immigration Canada</td>
<td>Foreign Service Officer (Immigration)</td>
<td>yes</td>
<td>FS-01</td>
<td>5,268</td>
</tr>
<tr>
<td>3. Canada Radio-Television and Telecommunication Commission</td>
<td>Analyst</td>
<td>yes</td>
<td>CO-01</td>
<td>1,317</td>
</tr>
<tr>
<td>4. Statistics Canada</td>
<td>Programmer, IT Application Development</td>
<td>yes</td>
<td>CS-01</td>
<td>278</td>
</tr>
<tr>
<td>Statistics Canada</td>
<td>Mathematical Statisticians</td>
<td>no</td>
<td>MA-01</td>
<td>568</td>
</tr>
<tr>
<td>Statistics Canada</td>
<td>Analyst - EC Recruitment and Development Program</td>
<td>yes</td>
<td>EC-02</td>
<td>905</td>
</tr>
<tr>
<td>5. PWGSC</td>
<td>Supply Officer Trainee</td>
<td>yes</td>
<td>PG-02</td>
<td>677</td>
</tr>
<tr>
<td>6. Treasury Board (Secretariat)</td>
<td>Financial Officer (FORD Program)</td>
<td>no</td>
<td>FI-01</td>
<td>1,267</td>
</tr>
<tr>
<td>Treasury Board (Secretariat)</td>
<td>Internal Auditor (IARD Program)</td>
<td>yes</td>
<td>AS-02</td>
<td>1,211</td>
</tr>
<tr>
<td>7. Industry Canada</td>
<td>Advanced Policy Analyst Program (APAP)</td>
<td>No</td>
<td>EC-03</td>
<td>568</td>
</tr>
<tr>
<td>8. Canada Space Agency</td>
<td>Junior Engineer</td>
<td>Yes</td>
<td>EN-ENG-02</td>
<td>392</td>
</tr>
<tr>
<td>9. Public Service Commission</td>
<td>Psychologist</td>
<td>Yes</td>
<td>PS-02</td>
<td>23</td>
</tr>
<tr>
<td>10. Canada Revenue</td>
<td>Auditor, Developmental Program</td>
<td>No</td>
<td>AU-01</td>
<td>TBD</td>
</tr>
</tbody>
</table>
## PSR - Fall 2014 Campaign (Cont’d)

### PSC Career Stream Inventories 2014

<table>
<thead>
<tr>
<th>Department</th>
<th>Position Title</th>
<th>PSC Tests Required</th>
<th>Group &amp; Level</th>
<th>Number of applications submitted</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Public Service Commission</td>
<td>Careers in Administration, Arts, Commerce and Social Sciences</td>
<td>yes</td>
<td>AS, EC, CO, IS, PE, PM</td>
<td>4,275</td>
</tr>
<tr>
<td>2. Public Service Commission</td>
<td>Careers in Information Technology (IT)</td>
<td>yes</td>
<td>CS</td>
<td>440</td>
</tr>
<tr>
<td>3. Public Service Commission</td>
<td>Careers in Pure, Natural and Applied Sciences</td>
<td>No</td>
<td>BI, PC, CH</td>
<td>757*</td>
</tr>
<tr>
<td>4. Public Service Commission</td>
<td>Careers in Health Sciences</td>
<td>No</td>
<td>NU, PS</td>
<td>425*</td>
</tr>
</tbody>
</table>

* Inventories remain open for applications until December 19, 2014.
# Student Employment Programs

## FSWEP 2014

### 4 departmental programs

<table>
<thead>
<tr>
<th>Program</th>
<th>Department</th>
</tr>
</thead>
<tbody>
<tr>
<td>Student Border Services Officer (CBSA)</td>
<td></td>
</tr>
<tr>
<td>Student Guide Program in France (VAC);</td>
<td></td>
</tr>
<tr>
<td>Great Lakes Area Summer Science Program (DFO)</td>
<td></td>
</tr>
<tr>
<td>Canadian Coast Guard - Inshore Rescue Boat Service</td>
<td></td>
</tr>
</tbody>
</table>

### 8 featured jobs

<table>
<thead>
<tr>
<th>Program</th>
<th>Department</th>
</tr>
</thead>
<tbody>
<tr>
<td>Canadian Forest Service</td>
<td></td>
</tr>
<tr>
<td>Aboriginal Student Employment Program (NRCAN)</td>
<td></td>
</tr>
<tr>
<td>Rideau Hall Visitor Services and Interpretation Program (GG)</td>
<td></td>
</tr>
<tr>
<td>Library Clerk and Reference Desk Clerk (RMC)</td>
<td></td>
</tr>
<tr>
<td>Student Guide-Interpreter (SCC)</td>
<td></td>
</tr>
<tr>
<td>Parks Canada Student Employment Program</td>
<td></td>
</tr>
<tr>
<td>Canadian Hydrographic Service - Marine Geomatics (DFO)</td>
<td></td>
</tr>
<tr>
<td>Civil Aviation Student Internship (TC)</td>
<td></td>
</tr>
<tr>
<td>Visitors Services and Interpretation Programs - Capital Heritage (PCH)</td>
<td></td>
</tr>
</tbody>
</table>
TB Policy Suite Reset:
Proposed Approach

Presentation to PSMAC
January 16, 2015

Canada
Purpose

• Recap of the October 10, 2014 PSMAC discussion

• Outline details on approach to TB Policy Suite Reset (PSR)
  - Focusing on “sieve” used to triage policy requirements

• Discuss links between PSR and BP2020 initiative

• Set out proposed next steps for engaging PSMAC and departments
Objectives of Policy Suite Reset Endorsed on October 10th

- Only essential policies, grouped logically, with clear requirements, determined by user needs (TB and DMs)
- Coherent policy requirements, within and between policies, without duplicating departmental policies (including shared service providers')
- Appropriate use of principles-based and prescriptive requirements, calibrated to risks, materiality, and need for consistency of practice
- Minimal costs for compliance and reporting and maximum use of information gathered (by TBS and depts.)
- User-centric policy suite, readily accessible to all, with supporting guidance
- Sustainable policy reviews to ensure on-going relevance and integrity
What we heard on October 10th

- Overall support for Reset, noting that it should support both agility and good management

- **Policy Considerations**
  - Rules and requirements should be “proportional to problems”
  - Requirements should be kept to a minimum, be clear and measurable, with compliance easily monitored
  - Requirements should be clear on “what” the objectives are; departments should have latitude to figure out the “how”
  - Shared accountability for enterprise-wide services should be properly set out in policy
  - Departmental policies’ relation to TB policies should be clarified and compatibility between them ensured

- **Process Considerations**
  - Ensure we build on past successes at policy reform and guard against the risk of “policy reform fatigue”
  - Auditor General should be engaged at the appropriate time
  - Close links between PSR, BP2020 and MAF should be maintained
  - Technology should be used to improve the user’s interface with policies
Policy Suite Reset – Proposed Approach

- A staged, four-step approach proposed (see details in Annex A):
  - Triaging: establishing core policy objectives and essential requirements by assessing existing requirements of all policies, directives and standards against key criteria (i.e., the “sieve”)
  - Government-wide Design: validating “essential requirements” and ensuring alignment with user’s needs and departmental policies by engaging departments and functional communities
  - User-Focussed Design: ensuring vertical and horizontal linkages among policy requirements are coherent and clear and user accessibility is maximized by designing a interactive, web-based policy suite
  - Sustainability: building in the “rules to live by” to maintain policy requirements’ integrity and relevance
Traging: TBS Review of Policy Requirements

- Determine appropriate grouping of policy instruments
- Establish core objectives for each policy
- Identify essential policy requirements using a “sieve” to assess each existing policy requirement against key criteria (e.g. uniqueness, risk, effectiveness)
- Determine whether requirements should be principles-based or more prescriptive in nature
- Identify key “vertical” and “horizontal” linkages among policy requirements across all policies using “tags”
- Identify common policy requirements (e.g., application, monitoring and reporting, consequences, etc.) and consider a stand-alone policy for these
- Develop a lexicon for key terms used across the suite
- Conduct a plain language edit to ensure clarity for users
Proposed Triage "sleve"

Current requirements in TB Policy Suite

1. Is the requirement essential for the objective and is it unique?
2. Is the requirement needed to address a material risk?
3. Can the requirement be monitored and assessed?
4. If kept, where is the requirement best placed?

Only essential policy requirements are retained

"Vertical" alignment of requirements within policy group hierarchy

Drop duplicate requirements

Demote to guidelines those requirements that can be achieved voluntarily or cannot be monitored

Drop requirements that are not essential to managing risk
Is the Policy Requirement Unique?

- Is the requirement unique to the rest of the supporting Suite and necessary to achieve the policy objective?  
  
  Consider keeping

Or

- Is it already duplicated, embedded or implied in the supporting instruments (e.g., standards/directives)?  
  
  Drop

- Is it within mandates or obligations in existing legislation or policy?  
  
  Drop
### Does the Requirement Address a Material Risk?

Is this requirement necessary to ensure...

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy/Legal/Regulatory</td>
<td>Policy, legal or regulatory obligations and provisions are implemented in a particular way and understood?</td>
</tr>
<tr>
<td>Financial Stewardship</td>
<td>Resources are managed with prudence and probity and financial controls are in place and maintained?</td>
</tr>
<tr>
<td>Stewardship of Assets and Resources</td>
<td>Assets and resources (including HR) are managed to ensure value, appropriate allocation and internal controls?</td>
</tr>
<tr>
<td>Safety and Security</td>
<td>Major supporting systems, processes and or infrastructure are protected?</td>
</tr>
<tr>
<td>Reputation and Public Trust</td>
<td>Reputation is protected and trust is enhanced?</td>
</tr>
<tr>
<td>Performance and Innovation</td>
<td>Results and outcomes are delivered efficiently and effectively and are improved to meet new challenges?</td>
</tr>
<tr>
<td>Consistency</td>
<td>Consistency across government in critical areas or defined areas of variability are understood?</td>
</tr>
</tbody>
</table>

Drop requirements that are not essential to managing material risk.
Can the Requirement be Monitored and Assessed?

**EFFECTIVENESS CRITERIA**

**Capacity**

Do TBS and Departments (including SDAs) have expertise/resources to implement/support proposed requirement effectively?

If not, can expertise/resources be developed/obtained/provided cost effectively?

**Monitor**

Can TBS adequately and cost-effectively monitor/report performance against policy? Do TBS and departments have a process for using the results of the reporting?

**Integration**

Is policy requirement adequately integrated and aligned with other requirements in other policy instruments and processes?

Demote to guidelines those requirements that can be achieved voluntarily or cannot be monitored.
Where is the requirement best placed?

- Consider where the requirement would be best placed within the policy suite architecture to ensure coherence and vertical alignment within the policy instrument:
  - **Policies** provide formal direction on what Deputies are expected to achieve.
  - **Directives/Standards** provide formal instruction on how departmental official must act, including operational or technical measures, procedures or practices for government-wide use.
  - **Guidelines** are a set of documents, databases, and tools used by specialists to improve performance and compliance (voluntary, not mandatory).
BP2020 Internal Red Tape Reduction Initiative – A User-Centric Approach

- PSMAC has recognized the need for close alignment between Policy Suite Reset and the BP2020 Internal Red Tape Reduction initiative
  - Policy Reset represents the "top down" approach to tackling administrative complexity
  - Internal Red Tape Reduction takes a "bottom up" approach

- A five-step, user-centric approach is being taken (See Annex B):
  - Explore
  - Examine areas where red tape is most frequently encountered
  - Expose
  - Establish
  - Prototype and test – and share successes or failures

- Ongoing communication with public servants through GCconnex and GCpedia
Reset & Red Tape: Complementary Timeframes

- The alignment of timeframes, combined with strong information flow between both initiatives, provides an opportunity to effect meaningful change to the administrative rules.

- By Summer 2015, Reset and Red Tape will be engaging departments (see Annex C):
  - Red Tape will be in its Establishing Phase (testing and prototyping solutions in participating departments):
    - TB policy triggers
    - Departmental policy triggers
    - Departmental processes
  - Reset will be in its Government-wide Design phase
    - Ensure "horizontal" alignment across policy suite, based on feedback from departments
    - Achieve balance and coordination between TB and departmental policies
Engagement of PSMAC

- As policy requirements are assessed, TBS policy centres will begin “government-wide design” stage and will engage functional communities in departments to discuss potential changes.
- As they are completed, TBS will share with PSMAC findings from “triage” and “government-wide design” assessment of TB policies and present proposals to change policy instruments.
- As well, over the next year, TBS will provide analysis and seek direction on broad themes that cut across all TB policy instruments, such as:
  - Governance
  - Planning
  - Reporting
  - Approach for small departments and agencies
Direction being Sought

- Do you agree with the proposed next steps for moving forward with the Policy Suite Reset?

- How else would you like to be engaged in Policy Suite Reset or BP2020 Internal Red Tape initiatives?
## Annex A - Policy Suite Reset Approach

<table>
<thead>
<tr>
<th>TRIAGE (TBS REVIEW)</th>
<th>GOVERNMENT-WIDE DESIGN</th>
<th>USER-FOCUSED DESIGN</th>
<th>RULES TO LIVE BY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Establish core policy objectives</td>
<td>Ensure &quot;horizontal&quot; alignment across policy suite, based on feedback from departments</td>
<td>Identify needs of specific users (e.g. deputy heads, functional specialists, managers)</td>
<td>Build in conditions for continuous improvement</td>
</tr>
<tr>
<td>Ensure &quot;vertical&quot; alignment within hierarchy of policies, directives, standards</td>
<td>Achieve balance and coordination between TB and departmental policies</td>
<td>Design a Policy Suite that meets the information needs of these users and is easy to navigate</td>
<td>Present proposal revised Policy Suite to Treasury Board</td>
</tr>
<tr>
<td>Identify &quot;horizontal&quot; linkages between requirements across policy suite</td>
<td>Validate essential policy requirements with functional communities and deputy heads</td>
<td>Ensure horizontal and vertical linkages among policy instruments are transparent to users</td>
<td>Establish rules to govern how TB policies will be developed and implemented in the future</td>
</tr>
<tr>
<td>Eliminate non-essential policy requirements</td>
<td>Identify appropriate responsibility for policy requirements; i.e. TBS or departments</td>
<td>Design and implement new website to ensure a user-centric Policy Suite (layered web access) with interactive component</td>
<td>Revise Policy Suite Foundation Framework documents with built-in conditions and tests</td>
</tr>
<tr>
<td>Assess every policy requirement against key criteria (e.g. uniqueness, risk, effectiveness) to identify those requirements that are essential</td>
<td>Assess collective impact of policy requirements government-wide on: - Governance - Planning - Reporting</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Develop a lexicon</td>
<td>Conduct plan language ed of policy requirements</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Conduct plan language ed of policy requirements</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### CONSTRUCTIVE ENGAGEMENT

Engagement at every stage to confirm that assessments reflect feedback and implications are understood (e.g. deputy heads, functional communities, Internal Red Tape Initiative, President, Treasury Board)
**Annex B - Internal Red Tape Reduction Approach**

<table>
<thead>
<tr>
<th>EXPLORE</th>
<th>EXAMINE</th>
<th>EXPOSE</th>
<th>ESTABLISH</th>
<th>PROTOTYPE AND TEST</th>
<th>IMPLEMENT AND SHARE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Explore some of the biggest irritants through user case stories</td>
<td>Examine areas where red tape is most pervasive</td>
<td>Expose the causes of these 3 irritants (and explain their complexity) within a small number of participating departments</td>
<td>Establish a plan of action to simplify 3 key processes where tangible results could be achieved</td>
<td>Prototype solutions to the issues identified in the plan of action with participating departments</td>
<td>Implement workable solutions and scale up</td>
</tr>
</tbody>
</table>

**OBJECTIVE**

- Engagement with all public servants
- Facilitated workshop and online discussions
- Online anonymous survey
- Database of user stories
- Develop case studies and share with TBS policy centres

**ACTIVITY & OUTPUT**

- Categorise user stories into broad themes
- Engagement with policy centres, functional communities and other networks
- Facilitated workshops
- Interim report of finding to Board of Management to identify and seek support for “deep dive” on 3 irritants
- Research and analysis of existing policy/process
- Facilitated workshops to determine root causes
- Develop alternative outcomes that favor end users
- Plan of action to simplify key processes
- Document Phase I process and final outcomes
- Present findings to Deputy Heads of participating departments and Board of Management
- Form a design team
- Develop prototypes
- Continual testing and improvement of prototypes
- Document learnings
- Implement workable solutions
- Evaluate outcomes
- Share and replicate approach across the public service

**CONSTRUCTIVE ENGAGEMENT**

Engagement and communication at every stage with public servants through GCconnex, GCpedia and in-person meetings.
Annex C: Complementary Timeframe

(See Annexes A and B for more detail on steps)
Please find attached, as promised, thoughts and reading on where the CIO reports in an organization.
February 27, 2015

To: Director

From: CIO

Subject: As promised, thoughts and readings on where CIO reports in organization

Intro

In our last bilat you raised the question of where in the organization the CIO should report, and indicated you were considering moving it into the DDA organization.

This note is a "road map" to guide you through the reading material attached. Quite a number of articles are attached, and with this memo as a guide, I do not expect you will choose to read all of them.

Note that most of the published writing on this topic is written from a private-sector perspective, so we need to translate terminology. I assume that when research refers to CIO reporting to CEO or President, that's equivalent to reporting to you, while CIO reporting to CFO or Corporate Services can be read as reporting to DDA.

Summary of Best Practice

CIOs most often report to one of CEO, CFO, or COO (Director, DDA, or DDO). Reporting to CFO was more common up to the early 2000s, when IT was considered mainly an overhead expense, but as technology became critical to the success of enterprises, it became more common for the CIO to report to the COO or the CEO, with CEO now the most common.

Surveys have indicated that organizations where CIO reports to CEO are more successful in using technology to further strategy, while those where CIO reports to CFO are more successful in minimizing the cost of IT. In organizations focused on low price, CIO should report to CFO, but in organizations focused on product differentiation or product excellence, CIO should report to CEO. I propose the latter applies to C515.

Finally, remember that CIO is responsible for IM as well as IT. IM reporting close to the head of the organization shows a stronger compliance to IM requirements (and used to be a MAF measurement, although I'm not sure if it still is).

Tour of Provided Documents

I've provided a selection of articles for your interest. I don't expect you to read all of them (perhaps not any of them). Following is a summary of the provided documents, referring to the numbers written on
4. Michael Sisco, “Report directly to the CEO to boost your IT goals and your career”
I regret this article’s unfortunate, self-serving title. It was written in 2003, when it was still most common for CIOs to report to CFOs, and was one of the early arguments that CIOs should report to CEOs instead. Reasons include:

- CEO is closer to operations
- CEO drives strategic initiatives
- CEO gives CIO more clout
- CIO becomes “operations advocate”

5. Brian Watson, CIO Insight, “Should CIOs Report to CEOs or CFOs” and attached paper by Rajiv Banker et al, “IT Orientation, CIO Reporting Structure, and Firm Performance: To Whom Should the CIO Report?”
The first article is a brief summary of the second. The second is a formal study that concludes that:

- Companies trying to compete on a “low-price” basis perform better if the CIO reports to the CFO; and
- Companies trying to compete on a “best product” or “unique products” basis perform better if the CIO reports to the CEO.

5. (b) Computerworld, Al Kuebler: “It’s the age-old question: To whom should the CIO report?”
A brief opinion piece from an IT news journalist, that CIO should report to CEO or equivalent to maintain focus on enterprise value.

5. (c) FierceCIO, David Weldon: “Woe to the CIO who reports to the CFO”
This is a summary of an interview with CIO of British Library, which is attached as a second page. British Library CIO: “IT is a strategic enabler and working for the CFO makes enablement really hard”

Articles on strategic role of CIO
I also attach a few articles that are not specifically about where the CIO reports, but about the need for the CIO to be connected to business strategy. These are both why I believe CIO should report to Director (and why I wanted CIO to remain member of Ops committee).

This paper identifies that there are 4 different roles for CIO:

- Focus on infrastructure
Sincerely,

Richard
<table>
<thead>
<tr>
<th>Dept</th>
<th>CIO</th>
<th>Title</th>
<th>Reports to</th>
<th>Equivalent</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSE</td>
<td>Fil Gagliardi</td>
<td>Deputy Chief</td>
<td>Chief</td>
<td>CIO → Director</td>
</tr>
<tr>
<td>CBSA</td>
<td>Maurice Chenier</td>
<td>VP, Sci &amp; Tech</td>
<td>President</td>
<td>(CIO + ADT) → Director</td>
</tr>
<tr>
<td>CRA</td>
<td>John Messina</td>
<td>Assistant Commissioner and CIO</td>
<td>Commissioner</td>
<td>CIO → Director</td>
</tr>
<tr>
<td>FINTRAC</td>
<td>Stéphane Cousineau</td>
<td>D/Dir and CIO</td>
<td>Director</td>
<td>CIO → Director</td>
</tr>
<tr>
<td>RCMP</td>
<td>Pierre Perron</td>
<td>Ass't Commissioner</td>
<td>Dep Comm'r, Specialized Policing</td>
<td>(CIO + ADT) → DOO</td>
</tr>
<tr>
<td>PSC</td>
<td>Christiane Poirier</td>
<td>CIO</td>
<td>Corporate Management Branch</td>
<td>CIO → DDA</td>
</tr>
<tr>
<td>CIC</td>
<td>Soyoung Park</td>
<td>CIO</td>
<td>ADM, Client Service Modernization</td>
<td>No equiv; not director.</td>
</tr>
<tr>
<td>CSC</td>
<td>Dung-Chi Tran</td>
<td>CIO</td>
<td>Senior Deputy Comm'r Transformation</td>
<td>No equiv; not director.</td>
</tr>
<tr>
<td>EC</td>
<td>Chuck Shawcross</td>
<td>ADM Service Standards &amp; Architecture &amp; CIO</td>
<td>ADM Corporate Services</td>
<td>CIO → DDA</td>
</tr>
<tr>
<td>Stats</td>
<td>Lise Duquet</td>
<td>informatics Branch</td>
<td>Corporate Services</td>
<td>CIO → DDA</td>
</tr>
<tr>
<td>DFATD</td>
<td>Martin Loken</td>
<td>CIO</td>
<td>Corp Planning &amp; CFO</td>
<td>CIO → DDA</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Company</th>
<th>CIO</th>
<th>Title</th>
<th>Reports to</th>
<th>Equivalent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco</td>
<td>Rebecca Jacoby</td>
<td>CIO &amp; Sr. VP</td>
<td>CEO</td>
<td>CIO → Director</td>
</tr>
<tr>
<td>Apple</td>
<td>Niall O'Connor</td>
<td>CIO</td>
<td>CFO</td>
<td>CIO → DDA</td>
</tr>
<tr>
<td>Walmart</td>
<td>Karenann Terrell</td>
<td>CIO</td>
<td>President</td>
<td>CIO → Director</td>
</tr>
</tbody>
</table>
A new survey from Forrester Research shows that the greatest percentage of CIOs reports to the CEO -- and that augurs well for IT.

CIOs tend to look at reporting lines like entrails or tea leaves -- a portent of how the job will play out.

A Forrester Research Inc. survey of 503 IT executives suggests the interest in chief of command is well-founded. While a CIO's reporting relationship doesn't make a radical difference in the job, says author Bobby Caillouet, it absolutely colors how IT will likely be viewed, managed and funded in your organization.

Of note, CIOs reporting to CEOs now represent by far the largest group, 34% of all respondents. At the same time, the percentage of CIOs reporting to the CFO has shrunk over the past three years, from about 25% to 18%, which is probably a good thing (read the details below and weigh).
"If you look at what the drivers are in this shift, you see an increased awareness of the value of IT and its impact on other parts of the business. The various officers in the reporting relationships, CEO, president, COO and business-unit heads, indicate that they're interested in having a more direct relationship with the technology," said Cameron, principal analyst at Cambridge, Mass.-based research firm Forrester.

So, the CIO's star is rising?

"Overall, I think this is good news," Cameron said. "The survey results are supported by data from an earlier Forrester study that strongly shows the business attitude toward IT is improving, he said.

Pro+ Features

Enjoy the benefits of Pro+ membership, learn more and join.

1. More on IT and business management

Escaping the shackles of static IT mentality

CIO to CEO: According to the report, CIOs who report to CEOs are most likely to have a centralized planning role. Interactions between IT and the business at these firms are managed "with more structure." As a result, firms where the CIO reported to the CEO were "among the strongest in

Forrester: More CIOs report to CEO than CFO

Centralized IT capabilities, such as vendor management and project or program management offices (PMOs). CIOs reporting to CEOs have the largest IT budgets when measured as a percentage of total revenue (18.8%), but they rate "only average" in terms of money spent on ongoing operations versus new investments (about 75% - 25%).

While CIOs who report to the head of IT are highly organized, they do not particularly view IT as a name changer for the business and their opinion of IT declined over the past year. They were more likely than their peers to focus on getting large projects done on time, at the expense of infrastructure service. The focus at these shops is squarely on the customer. Improving the customer experience outranked reducing costs, increasing company differentiation, supporting regulatory requirements and supporting global expansion as the most important "business driver" for next year.

CIO to CFO: True to the devilish stereotype, CIOs who report to the CFO spend more time than their peers on cost-cutting and focus the least on improving the business. They had the smallest budgets as a percentage of revenue (4.2%). They scored low on centralized vendor management and performance management, but were most likely to have strong demand management.

It reflects an increased awareness of the value of IT and the impact on other parts of the business. Bobby Cameron, principal analyst, Forrester Research Inc.

CIO to President: The 89% of CIOs reporting to the firm president were also likely to have centralized IT planning, but they were highly organized in managing internal clients, coming out second most likely to have IT marketing and above average on demand management. IT spending as percentage of revenue was average (4.4%) at these firms, but all about efficiency, not differentiation. These firms were least likely to view IT as giving them a competitive edge.

CIO to COO: Only 9% of Forrester respondents report to the COO, but this cohort appears to play an interesting role at their firms. Their bosses are the most likely to see IT as a differentiator -- and more than any other boss they believe that IT at their firms has improved over the past year. Paradoxically, these CIOs had the most centralized IT but were second least likely to play a centralized planning role. These CIOs led the pack in their focus on improving infrastructure execution quality and came out near the top on improving their firm's new IT.

CIO to business-unit head: The 3% of CIOs who report to business-unit heads have a bag of characteristics -- least likely, for example, to have centralized IT functions like service management but they score at the top on centralized PMOs and managing IT demands. They came out just below the COO group on IT being viewed as a differentiator and No. 1 on the amount of time devoted to operational excellence and improving the company with new IT.

Dig deeper on CIO career development and career paths

- How can CIOs stay relevant in a digital enterprise?
- Under-the-gun managers and other factors that kill IT innovation
- Curing the IT identity crisis starts with understanding corporate culture
- CIO of UN talks politics and the limits of big data

Let us know what you think about the story, email Linda Tucci, Senior News Writer.

Forrester: More CIOs report to CEO than CFO

Finally, Forrester found that reporting relationships varied quite a bit by industry but rarely by the size of the company. So, for example, if you’re in business services there’s a strong possibility you’ll report to the CEO (46%) or you could 30% of CIOs in retail and wholesale trades report to the CFO. The exception is in small and medium-sized businesses, Cameron said, where the reporting relationships tends to be more personality driven.

CIOs: Reporting Relationship Defines Your Job Only At The Margin

July 18, 2011

by Bobby Cameron with Alex Cullen, Brandy Worthington

Add To Reading List
Sync with our iPad app or organize favorites.

Download PDF
For individual use only.
Distribution prohibited.

WHY READ THIS REPORT

Forrester’s 2007 IT governance survey placed a bet on the business how the CIO's reporting relationship does or doesn't — impacts the way IT works and how it is perceived. We surveyed 503 senior IT decision-makers about how IT works, how it is structured, and how it is perceived. The bottom line: While there are some variations based on who the CIO has as a boss, most IT governance realities don't vary greatly based on the CIO's reporting relationship.

Tags: IT Governance, IT Organization, Management, Organization, Organizational Structure, Strategy Planning & Governance

CIO'S REPORTING RELATIONSHIP IMPACTS HOW IT BEHAVES AT THE MARGIN

Forrester’s 2007 annual governance survey of 503 IT decision-makers reveals that a CIO's reporting relationship has little, but not no, influence on the IT organization. We looked at how the CIO's reporting relationship varied by a variety of factors:

- The reporting relationships in our survey varied a lot by industry but little by size. Sometimes this was significant, as when 45% of the responding CIOs in business services reported to the CBO when one third of retail and wholesale trade reported to the CFO, but only the small and medium size businesses (SMB) have a significant variation in reporting relationship based on the size of the firm.

- IT centralization varied only slightly with the reporting relationship. This was in spite of a significant variation or centralization based on industry sector.

We found that although the reporting relationship didn't make a radical difference, it did make some difference. We found that CEOs reporting to the:

- CEO focused on the business first, using centralized management facilities. Thirty-four percent of our sample reported to their CEO — by far the largest single reporting relationship — and their approach to IT governance reflects their reporting relationship. These CIOs were the most likely to have a centralized IT planning function, and this tendency resulted in their firms being among the largest IT spenders and IT centralization management offices (PMO). CIOs reporting to their CEO had the highest IT budget as a percentage of revenue but were only average in their ratio of investments versus ongoing operations. These CIOs' companies were only the middle of the respondents in their philosophy that IT is a differentiator, and their opinions of IT that's declined over the last year. These CIOs were slightly more likely than their peers in service-oriented companies for getting large projects done on time.

- CFO spent more time reducing costs and focused on improving the business. These CIOs — 15% of our respondents — fit the cliché for IT execs reporting to CFOs. They had the smallest budget as a percentage of revenue and focused on improving business with new IT — with the largest share of their time spent on reducing costs. They were less likely to have centralized IT planning, performance management, and relationship management, but they were more likely to have demand management.

- President had the least centralized IT planning and lowest view of IT as a differentiator. Sixteen percent of our sample had CIOs reporting to their president. Because they were least likely to have centralized IT planning, they end up with fewer centralized IT management capabilities and a slower adoption of innovative R&D or centralization architecture. These CIOs didn't manage their central clients; however, they were the second most likely to have IT marketing and were above average for demand management. While they were average in IT spend as a percentage of revenue, it was all about efficiency. Their companies were the least likely to have a philosophy of IT as a differentiator.

- CDO was most likely to be seen as a differentiator, focused on improving business. Only 9% of our respondents had CIOs reporting to their CDO. They were the least centralized but the second least likely to have centralized planning. As a result, they were among the least likely to have...
centralized functions like vendor management, IT service management, and relationship management. CIOs who reported to CIOs came from companies most likely to see IT as a differentiator — and the opinion of IT at their firms had improved the most over the past year. These CIOs led the other reporting relationships in their focus on improving infrastructure execution quality and were one of the key for improving their firms with new IT.

- Business unit CIOs focused on operational excellence and improving the business. Fewer percent of the respondents' CIOs reported to business unit IT heads. For them, reducing costs and improving operational excellence decreased IT's agenda. They had average levels of centralization but were among the least likely to have centralized IT functions like service management and performance management. However, in situations where centralized centers is needed, these CIOs were among the top — for centralized PMO and IT demand management. They were second highest for seeing IT as an enabler and among the highest for new investments as a percentage of overall IT spend. Finally, they were the strongest in spending their time on operational excellence and improving the company with new IT.

![Figure 1: IMPACT ON IT MANAGEMENT STRUCTURES](https://www.forrester.com)
Centralized management: functions were most common when CIO reported to the CEO — and less common for CIOs reporting to the president.

IT-business interactions were assessed with various measures when the CIO in our survey reported to their CEO.

Relationship management by CEO

https://www.forrester.com/CIOs+Reporting+Relationship+Defines+Your+Job+Only+At...Page 3 of 6
Figure 2: IMPACT ON IT SPENDING

IT's budget was the greatest percentage of revenue for CIOs reporting to the CEO -- and the smallest when the CEO reports to the CIO. This is what the data shows in the table. The second highest IT budget as a percentage of revenue was for CIOs reporting to the CIO. This is what the data shows in the table.

The CIOs reporting to the CIOs spent the largest amount of IT budget on investment, while the CIOs reporting to the CEO spent the smallest amount of IT budget on investment.

https://www.forrester.com/CIOs+Reporting+Relationship+Defines+Your+Job+Only+At... 2015-02-25
A greater number of firms saw IT as a differentiator when the CIO reported to the CEO — and the perception of IT as a differentiator was only average when the CIO reported to the COO.

The perception of IT has improved the most over the past year for firms where the CIO reports to the CEO, and it has remained the least where the CIO reports to the COO.

Reliability of systems and network contributions were in a positive view of IT — which stood out especially for the CEO and for the IT head. Improved execution of major enterprise projects was the biggest driver of positive perceptions.

Reducing costs, improving the customer experience, and improving operational effectiveness are mentioned by the business driver for the next year. The CIO reporting to the COO, the business experience stood out higher than the key other reporting relationship. But when the CIO reports to the CEO, the importance of reducing cost and improving operational efficiency remains.

As for the top non-cost areas spent by the IT organization, improving infrastructure spending quality is tied overall — and IT spending the company with the IT CIO. IT organizations with CIOs reporting to the COO, spend more time focusing on improving the business side more IT — and things with IT CIOs reporting to the IT head on the focus of improvement. And, no initiative IT organizations where the CIO reports to the CEO spend more then any others on non-revenue costs.
SUPPLEMENTAL MATERIAL

Methodology
This report is based on data from Forrester's July 2007 North American And European Enterprise IT Management And Governance Phone Survey. Forrester conducted a phone survey of 503 North American and European IT decision-makers that are members of Global Marketست (GMI) panel. GMI weighted the data by position, company size, industry, and region to demographically balance the survey results. GMI fielded the survey from July 2007 to August 2007. For results based on a randomly chosen sample of this size (n = 503), there is 95% confidence that the results have a statistical precision of plus or minus 4.7% of what they would be if the entire population of IT decision makers had been polled. The sample used by GMI is not a random sample; while individuals have been randomly sampled from GMI's panel for this survey, they have not been randomly selected to take part in the survey panel.

In addition to sampling error, other factors need to be considered. The practical difficulties in conducting surveys, such as illegal data, and the tendency to report only positive data, can introduce bias into data. Other potential sources of error in polls are probably more serious than statistical calculations of sampling error. These other potential sources of error include question wording, question ordering, and non-response. As with all survey research, it is impossible to quantify the extent that may result from these factors without an experimental control group, so we strongly caution against using the words "margin of error" in reporting any survey data.

These statements conform to the practices of disclosure of the National Council on Public Polls.

You can find more information about the data on the Survey Data page online. From that page, you will be able to download the Survey Instrument.

ENDNOTES
8 Of the participants in our survey, 25% are the senior-most IT decision-maker in their company. 53% are executive vice-presidents in IT, and 21% report to executives in IT. In addition to the five reporting relationships featured in this document, respondents listed a variety of other categories, including general managers, public sector departmental directors, and the firm's board of directors.

https://www.forrester.com/CIOs+Reporting+Relationship+Defines+Your+Job+Only+At... 2015-02-25
Many businesses today are grappling with a proliferation of chiefs. Where there was once a vice president of marketing, there’s now a chief marketing officer. Where there was once a head of the IT department, there’s now not only a chief information officer but also a chief technology officer, a chief security officer, a chief privacy officer, and a chief knowledge officer. Armed with their important-sounding titles, all the chiefs naturally want to report directly to the CEO. But that’s not always feasible—or wise. As illustrated in this chart, companies need to make hard decisions about which positions are truly strategic.
Marc Cecere is a vice president and research manager at Giga Information Group in Cambridge, Massachusetts.
This article is about ORGANIZATIONAL STRUCTURE

FOLLOW THIS TOPIC

Comments

Leave a Comment

0 COMMENTS

JOIN THE CONVERSATION

POSTING GUIDELINES

We hope the conversations that take place on HBR.org will be energetic, constructive, and thought-provoking. To comment, readers must sign in or register. And to ensure the quality of the discussion, our moderating team will review all comments and may edit them for clarity, length, and relevance. Comments that are overly promotional, mean-spirited, or off-topic may be deleted per the moderators' judgment. All postings become the property of Harvard Business Publishing.
Memo to the CEO

Are you getting the best out of your CIO?

pwc
## Contacts

<table>
<thead>
<tr>
<th>City</th>
<th>Name</th>
<th>Title</th>
<th>Phone 1</th>
<th>Phone 2</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chicago</td>
<td>Mike Connolly</td>
<td>Senior Partner</td>
<td>+1-312-578-4580</td>
<td><a href="mailto:mike.connolly@strategyand.pwc.com">mike.connolly@strategyand.pwc.com</a></td>
<td></td>
</tr>
<tr>
<td>Frankfurt</td>
<td>Rainer Bernat</td>
<td>Partner</td>
<td>+49-69-97157-414</td>
<td><a href="mailto:rainer.bernat@strategyand.pwc.com">rainer.bernat@strategyand.pwc.com</a></td>
<td></td>
</tr>
<tr>
<td>Kuala Lumpur</td>
<td>David Hovenden</td>
<td>Partner</td>
<td>+61-2-9321-1966</td>
<td><a href="mailto:david.hovenden@strategyand.pwc.com">david.hovenden@strategyand.pwc.com</a></td>
<td></td>
</tr>
<tr>
<td>Munich</td>
<td>Nicolai Bieber</td>
<td>Principal</td>
<td>+49-89-54525-545</td>
<td><a href="mailto:nicolai.bieber@strategyand.pwc.com">nicolai.bieber@strategyand.pwc.com</a></td>
<td></td>
</tr>
<tr>
<td>London</td>
<td>Richard Bhanaop</td>
<td>Partner</td>
<td>+44-20-7393-3519</td>
<td><a href="mailto:richard.bhanaop@strategyand.pwc.com">richard.bhanaop@strategyand.pwc.com</a></td>
<td></td>
</tr>
<tr>
<td>Martin Roets</td>
<td>Principal</td>
<td></td>
<td>+44-20-7393-3394</td>
<td><a href="mailto:martin.roets@strategyand.pwc.com">martin.roets@strategyand.pwc.com</a></td>
<td></td>
</tr>
</tbody>
</table>
Richard Bhanap is a partner with Strategy&'s digital business and technology practice in London. He works with large, complex multinationals around the world to help create tight alignment between IT and the business and is often called on to coach senior business executives and CIOs through major IT-enabled business transformation journeys.

Dr. Rainer Bernmat is a partner with Strategy& based in Frankfurt. He leads the European digital business and technology practice and the German public-sector business at Strategy&. He specializes in large IT transformation programs and supports public and private institutions in leveraging innovation and modern IT to improve efficiency and effectiveness.

Martin Roets is a principal in Strategy&'s London office. He is a member of the digital business and technology team, specializing in IT strategy, operating model design, and IT and business transformation. He focuses primarily on the financial services industry.

Nicolai Bieber is a principal with Strategy& based in Munich. He specializes in IT strategies, application architectures, and large transformation programs, with a focus on the public sector, financial services, and telecommunications.

This report was originally published by Booz & Company in 2013.

Raj Muppalla, Rahul Bohra, Abhishek Pathak, Bastian Lux, and Jean-Thomas Bassette also contributed to this Perspective.
Executive summary

In an increasingly digital world, the role of the CIO is evolving rapidly. The rise of consumerization and new technologies, combined with a highly competitive environment, will pull IT further into the heart of the business agenda. More and more, CIOs will hold the key to unlocking competitive advantage and business benefits. With this shift come growing pressure and higher expectations.

As a CEO, you need to ensure that your CIO and the IT function he or she leads are best positioned to help shape and enable your business's response to these opportunities and challenges. This report, which contains a number of key insights from Strategy&'s inaugural CIO Succession Study, should provide helpful perspective on the role of the CIO.

The study, conducted during the first half of 2013, involved more than 60 CIOs from large international companies across industry sectors. Our goal was to better understand the CIO's career path, succession trends, and success factors. The study revealed some surprising and unexpected insights — a number of which are directly relevant to you as the CEO — on what the concerns and goals of CIOs are today, where to find the right people to fill the role, and how to help them and their IT departments succeed in nurturing and delivering the digital capabilities required to effectively pursue your company's business strategies and priorities.
Regardless of your industry, your company is likely to grow ever more dependent on a variety of mature and cutting-edge information technologies to connect with customers, suppliers, and employees; to stay competitive; and to succeed. Digitization is a fundamental part of the new business model, affecting supply chains and operations, marketing and sales, interactions with current and potential customers, and daily collaborations between employees. You are highly aware of the importance of the technology your company uses.

Your IT department is accountable for helping enable your broader organization embrace and exploit the potential of digitization, in close partnership with the business. Therefore, the selection of a chief information officer (CIO) to lead the IT function and help shape the business’s IT agenda has never been as critical as it is now. And it doesn’t stop there: Motivating and empowering your CIO — and creating the conditions that will allow him or her, as well as the IT department, to succeed — are equally important.

The CIO role is multifaceted and particularly challenging. Coordinating an increasingly complicated set of internal and external resources and capabilities, CIOs must ensure that the technologies and solutions that support critical business processes are constantly available. They need to oversee the development of complex new IT-enabled projects on time, on budget, and in a way that delivers the promised business value. They need to visibly contain and repeatedly attack the IT cost base. They also need to ensure that the potential impacts of new and emerging technologies and solutions are continually assessed and, when appropriate, pursued and exploited. They juggle all this while shaping and pursuing a strategic IT agenda for the business and balancing the inexorable demand for new services and solutions from every part of the organization.

Strategy& recently conducted its inaugural CIO Success(ion) study. In this study, we surveyed and interviewed CIOs from a wide range of large multinational companies, most of them headquartered in Europe, across industry sectors. Our goal was to better understand the CIO’s...
career path, succession trends, and success factors. The study revealed some unexpected insights, a number of which are of direct relevance to you as the CEO. Our findings provide a set of up-to-the-minute perspectives on what the concerns and goals of CIOs are today, where to find the right people to fill the role, and how to help them and their IT departments succeed in nurturing and delivering the digital capabilities required to effectively pursue your company's business strategies and priorities.
Where should you look for your next CIO?

The CIO Success(ion) study set out to examine where today’s CIOs came from and how they were selected and appointed.

The vast majority of CIOs are being recruited externally, our study found, the implications of which are stark for ambitious and talented members of your current IT leadership team: The odds of being promoted to the CIO role in the foreseeable future are slimmer than they may have thought — assuming, of course, that a CIO turnover even takes place. First, they are competing against their peers to be considered for the top IT job. And second, there seems to be an innate bias among organizations toward outsiders; they usually look externally for the next CIO (in a handful of cases, they consider sideways moves from other functions). The reality for current IT leaders may be even worse. Through our CIO interviews, we discovered that a number of today’s CIOs who were promoted from within had switched organizations at the level just below CIO in order to be groomed as a successor prior to their elevation (see Exhibit 1, next page).

There are several reasons that appointing a CIO from outside your company might be appealing. If your former CIO wasn’t seen as up to the task, why would you expect his or her direct reports to be much different? As the CIO of a large engineering firm explained, “A high percentage of CIOs are brought in specifically to act as change agents.” Despite this view, many CIOs we spoke with were surprised and concerned to hear how few of their peers at other companies were promoted directly into the role. One, the CIO of a global energy company, expressed the opinion that “unless we can demonstrate a clear path of senior progression within IT, our ability to attract, develop, and retain the top workforce we need to drive digitization in our business will rapidly deteriorate.” Indeed, almost every CIO we spoke to made reference to active senior-level succession planning taking place within the IT function, although many admitted that when the time came, serious consideration would probably also be given to identifying external candidates for the role.
### Exhibit 1
#### The CIO life cycle

<table>
<thead>
<tr>
<th>20%</th>
<th>The next step</th>
</tr>
</thead>
<tbody>
<tr>
<td>More than 60 percent of CIOs have bachelor's degrees or higher; only 12 percent have MBAs.</td>
<td>Almost 70 percent worked for a management consulting firm or systems integrator at some point in their career.</td>
</tr>
<tr>
<td>Almost 40 percent moved from a previous CIO position to their current role.</td>
<td>Almost half have been in their current position for more than three years.</td>
</tr>
<tr>
<td>More than 50 percent bring members of their previous teams with them to their current company.</td>
<td>Almost 60 percent expect to stay where they are for less than three years at their next organization.</td>
</tr>
<tr>
<td>Just over 50 percent began their working lives in IT.</td>
<td>Sixty percent worked in a different company in a different industry before joining their current organization.</td>
</tr>
<tr>
<td>Less than 30 percent got their current job through a headhunter.</td>
<td>The average CIO is about 48 years old, and virtually all are male.</td>
</tr>
<tr>
<td>More than 40 percent have been with their current company for more than six years.</td>
<td>A third of CIOs are forced out.</td>
</tr>
</tbody>
</table>

Source: Strategy& analysis
We offer a simple rule of thumb: If you believe IT and digitization are currently on the right path in your company, and there is broad confidence in the strategy and road map laid out by the CIO and his or her top team, looking internally for a successor should be the default plan. If, however, these conditions do not exist, consider an external successor. (You should also look within your organization to identify what allowed such a disappointing situation to develop in the first place, whether on the business side or within IT itself.)

It seems that although executive search firms continue to play an active role in finding and placing CIOs, their dominance in this space has diminished dramatically with the advent of LinkedIn and other social networking sites. According to the CIO of a leading financial-services company, "a personal referral, based on a combination of accomplishments and relationships, is increasingly the way that I get introduced to opportunities, and it's also the way I found many of my own external hires. The world is rapidly becoming a better-connected place."

Of the CIOs who do come from outside the company, the majority switched industries to take on the new role. (One exception to the industry-hopping phenomenon appears to be financial-services companies, where the majority of CIOs have worked in the industry for most, if not all, of their career.) And nearly three-quarters of today's CIOs have worked at either a management consulting firm or a systems integrator at some point in their career. This suggests that breadth of experience is valuable and that that value is recognized. "The virtue of experience as a consultant lies in the exposure to a variety of business problems, large programs, stakeholder management, and strategic thinking," the CIO of a leading industrial products company told us.
Is your current CIO likely to succeed?

To address the question of what drives success, the CIO Success(ion) study explored a number of different angles: What do today's CIOs believe the critical success factors of the role to be? On what key dimensions are CIOs and their IT functions measured by others? And on the other side of the coin, what are the primary reasons for CIO failure?

CIO folklore would have it that the quickest way to find oneself being pushed out of the job is to fail to deliver day-to-day IT services — the ability to process transactions, quickly access customer information, and even send and receive email, for example. But although the logic of this seems irrefutable, in reality we found few current CIOs whose predecessors were let go for this reason. That may be because technologies and associated solutions have matured to such an extent that major service failures are now far less common than they once were.

We did, however, find that on becoming CIO, half of our study respondents inherited, and then had to rescue or abandon, major projects. In a sizable number of cases, the failing program was what led to their predecessor's departure (see Exhibit 2, next page).

The proportion of IT projects costing more than US$1 million that fail to come in on budget and on time, or to deliver the original business promise, remains high — almost 30 percent, according to IT research firm Gartner Inc. These are typically big-ticket, multiyear, enterprise-wide programs involving new ERP, CRM, or core industry-specific solutions that promise to fundamentally change business performance and competitiveness. Unfortunately, these complex, joint IT-business projects are often allowed to deteriorate into very costly IT-driven systems implementation and replacement initiatives, which lack genuine ownership and buy-in from the business areas involved.

According to the CIO of a global consumer products company, "If you're not extremely careful with these programs, business stamina and patience run out. Just get the #@$%$!! system in once and for all so that we can pick ourselves up again and move on" becomes the dominant refrain. That's of course assuming that you can get to a working system at all." The result
Exhibit 2
Poor business partnerships and failing projects are the primary causes of CIOs’ being forced out

1. Not partnering well with the business
2. Failing IT programs
3. Top five reasons for CIO failure

Note: Reasons for failure that were not ranked in the top five include lack of innovation; not responding to new trends; being late in adopting new technologies; and ineffective outsourcing.

Source: Strategy& analysis
frequently is an expensive, shiny new IT solution that doesn't quite do what was promised, isn't well integrated into or absorbed by the business, and ultimately doesn't have much tangible impact on business performance.

Although many factors affect the success of large programs involving IT, CIOs need to ensure a strong sense of joint ownership and work in genuine partnership with business stakeholders on such journeys to ensure the successful delivery of complex IT-enabled business change. Recall that failing to establish a strong business–IT partnership was listed as the number one reason for CIO failure, followed closely by failing IT programs.

Our survey showed that although a small number of CIOs reported to a COO or other operational executive, the majority had a direct line to the CFO or CEO, in roughly equal proportion. All the CIOs we interviewed noted that the reporting line can be a critical issue, because whom they report to has a big influence on where they focus their IT organization’s energies and resources. Those reporting to the CEO suggested that they were typically encouraged to take the perspective of enterprise-wide business value — how much the IT department delivers to the business — whereas reporting to the CFO can shift the primary emphasis of IT to the cost agenda and automating operations.

According to the CIO of a major transportation company, “The cost-versus-value equation changes with reporting line. With the CEO, it’s all about focusing on strategy and value. With a CFO, the focus tends to be on costs in the back office.” The CIO of a large beverage company, who has reported to both CEOs and CFOs, noted, “My experience is that a CEO reporting line results in more ‘adult’ end-to-end business-oriented discussions with a far greater focus on value and on shaping a balanced portfolio of investments, while a CFO reporting line puts a much stronger emphasis on the ROI of individual investments and a real obsession with IT costs, sometimes leaving business value on the table.”

This suggests that reporting lines typically determine not just what people CIOs interact with, but how they think and what they concentrate their IT organizations on. How you select the right CIO and where you position that person within the senior team will depend on the nature of your company and the balance it aims to strike between cost and value. As a CEO, you need to make active choices depending on what you wish to achieve. Of course, this is not a hard-and-fast rule; there are exceptions. The CIO of another global energy company who currently reports to a CFO noted, “At the end of the day, a lot of this comes down to the nature of the relationship between the executives. If the CIO is credible [to] and accepted by the top team, and has the IT management basics like service and cost under tight control, the fact
that they report to the CFO becomes more of a convenience and doesn't have to make a lot of difference."

The IT architecture of a company — its landscape of systems and technologies — can also reflect the nature of the CIO reporting line. Companies in which the CFO has a strong influence over the IT agenda and priorities will often have powerful and well-designed transactional IT systems, such as ERP and core banking, but may be weaker in other areas, such as sales, marketing, and product development. So the choice of where the CIO role should sit organizationally should take into account the agenda you believe IT should have in your organization, today and in the future.

Just as important as the CIO's reporting line is the IT leadership team he or she builds. More than three-quarters of CIOs cited "people and skills" as a primary focus upon taking on a new position, second only to delivering major programs. The third most important focus: the IT organization itself. Several of the CIOs we interviewed pointed out that leadership was essential in this area and that they rarely brought their own people with them into new positions — at least at the start — preferring to meet the inherited team and learn their strengths and weaknesses.

Every CIO we spoke to also confirmed the importance of stakeholder management and the ability to forge strong partnerships at the junction between business and technology (see Exhibit 3, next page). "To succeed as CIO you need to communicate, communicate, communicate," said the CIO of a major logistics firm. "Reach out and get to know people. The ability to convince people is crucial, so invest time in helping stakeholders understand the business case of every IT program."

CIOs also ranked "visionary and strategic thinking" — the ability to envision how their company can benefit from technology combined with the ability to think strategically — as an exceptionally important success factor. This is becoming increasingly relevant in an era when effective use of technology is more and more closely linked to business success, and therefore is a skill that CEOs should pay particular attention to. A CIO who combines this skill with the other important success factors will likely be instrumental in your firm's ability to gain strategic advantage through technology.

Looking at how the IT organization is viewed from the outside, it is curious to see CIOs reporting that innovation appears far down on the list of measures of IT success, well below cost control, scalability, flexibility to deal with changes in the business, and quality of solutions and services. "It's a matter of pragmatism. In my view, the CIO's day job takes up most of the time," said the CIO of a leading pharmaceutical
Exhibit 3

Stakeholder management and strategic thinking top the list of success factors for CIOs.

<table>
<thead>
<tr>
<th>CIO success factors</th>
<th>Rank 1</th>
<th>Rank 2</th>
<th>Rank 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strong stakeholder management skills</td>
<td>13%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Visionary and strategic thinking</td>
<td>22%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deep understanding of the business</td>
<td>24%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>A seat at the top management table</td>
<td>9%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Oversight of all relevant resources: people, spend, etc.</td>
<td>15%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Technical background and expertise</td>
<td>9%</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: Strategy& analysis
company, “so you can leave innovation to the vendors.” The CIO of a financial-services company agreed with this view. “Don’t innovate for innovation’s sake,” he said, “but do innovate selectively, on topics like mobility and big data, taking advantage of innovation early where appropriate.”

Despite the importance CIOs place on business acumen, strategic thinking, and stakeholder management, the tension between effectively managing the cost of IT and creating business value remains their primary concern. At many companies, IT is still perceived as a cost center to be managed as efficiently as possible, and CIOs highlight cost-effectiveness as one of the primary measures of their IT departments’ success. But although cost management is a critical concern in an age when IT absorbs such a large portion of companies’ budgets, it’s not necessarily the way to get the most business value out of IT (see Exhibit 4, next page).
Exhibit 4
Cost-effectiveness remains the most important measure of success for most IT organizations

<table>
<thead>
<tr>
<th>Measure of IT function success</th>
<th>Rank 1</th>
<th>Rank 2</th>
<th>Rank 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost-effectiveness</td>
<td>22%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Flexibility and scalability</td>
<td>8%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Quality</td>
<td></td>
<td>20%</td>
<td></td>
</tr>
<tr>
<td>Innovation</td>
<td>7%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Responsiveness</td>
<td></td>
<td>11%</td>
<td></td>
</tr>
<tr>
<td>Sourcing</td>
<td></td>
<td></td>
<td>8%</td>
</tr>
</tbody>
</table>

Source: Strategy& analysis
Where do CIOs go next?

As a rule, CIOs are a restless bunch. Almost half have been in their current CIO position for three to five years, but more than 40 percent say they don’t expect to be there beyond another year or two. So if current CIOs are meeting the expectations set for them, understanding how they think and what matters to them in their careers will help you retain them.

In one sense, that should be easy. Almost 90 percent of the CIOs we surveyed said the top reason for moving to their current position was the new professional challenge involved, and more than half suggested that they were dissatisfied with their current role. Providing new business and technological problems to solve, and the support needed to solve them successfully, will certainly help provide ongoing professional challenges and keep your CIO engaged.

At the same time, a third of CIOs are forced out of the role — a finding that surprised most of the CIOs we interviewed. Half of them thought that figure was high, and was a matter of real concern. And the other half expected it to be higher, given the changing nature of the CIO role, the growing focus on digitization, and their sense that many of their current peers at other companies would struggle to be effective in the new world.

In terms of career aspirations, the majority of study participants described another, larger, more prestigious CIO position as being the obvious next step, most likely at another company. A third of participants were in their first CIO role, 25 percent were in their second, and more than 40 percent had held three or more CIO roles. The rise of the “serial CIO” is a very real phenomenon.

A small, but quite noticeable, minority of those we spoke to voiced the desire for their next role to include P&L responsibility, and a similar minority were determined to avoid such a responsibility. When considering options within their existing organization, many pointed to shared-services operations and other support functions as being obvious areas that could be put under the responsibility of the CIO in order to benefit from the service management capabilities they had built up in
the IT function, and to provide the opportunity for greater CIO scope and responsibility without their having to change organizations. Indeed, some participants have already been given responsibility for such activities. "The CIO is among the few roles with a cross-functional, cross-organizational perspective. This in conjunction with running large programs and driving change should prepare them to become COOs," said the CIO at an international retailer.

A number of CIOs raised the prospect of joining an IT solutions or services supplier — a "gamekeeper turned poacher" situation, as one CIO put it — or a consulting firm, but this is a far less common transition for CIOs.
Conclusion

The best CIOs fully understand the critical connection between IT and the business, and they're adept at managing stakeholder relationships and forging partnerships. They have an informed, even visionary, perspective on how digital technology will transform business over the next several years, and what that will mean both strategically and for day-to-day operations. They are strong and effective leaders who can coordinate well across organizational boundaries. Just as important, they are a safe pair of hands when it comes to optimizing service quality and costs, and they fully appreciate the importance of being able to do so.

There is a saying that "every organization gets the IT it deserves." In order to play a strategic role, CIOs can't go it alone. They need the support of their CEO and other top executives to maintain the necessary connections with business leaders and to ensure that all stakeholders understand their role in furthering the use of digital technology to stay competitive. It's up to you as CEO to ensure that your CIO is capable and positioned properly to shape and serve the business agenda, and to make sure that business leaders and other stakeholders are working effectively with your CIO. The stakes in the age of digitization are higher than ever, and the success of your CIO will become more and more fundamental to both your own success and that of your organization.
Report directly to the CEO to boost your IT goals and your career

By Michael Sisco, April 7, 2003, 12:00 AM PST

Traditionally, CIOs have reported to the CFO, but that's not always the best scenario for the CIO. By reporting directly to the CEO or president, CIOs can spur achievements and gain invaluable insight and career help.

Traditional corporate reporting structures tend to have the company's senior technology manager (CIO, VP of IS, CTO) report directly to the CFO. In my 20-year management career, I've reported into all different levels and believe that in today's world we need to look at a different approach.

CIOs of the corporate world should report to the CEO for many reasons, as I'll explain in this article. In fact, I feel so strongly about this need that I made it one of my stipulations when I joined my former employer as CIO.

Why the CIO usually reports to the CFO

To understand why something needs to change, you must first understand the current concept behind what's in play. The CFO is typically responsible for the corporate services organizations of a company. These include accounting, accounts payable, payroll, human resources, purchasing, and IT. This structure is especially prevalent in small- to medium-size companies.

Several reasons support this reporting structure:

- It provides a consistent management structure across all corporate services organizations that is simpler for the operations staff to work with.
- In many companies, corporate services departments are heavy users of technology, so it's a natural tendency to have IT report to the CFO.
- CFOs often want the control of IT because they are detailed types and control oriented, and their own business organizations depend heavily on technology.
- CEOs and presidents don't normally want the responsibility of IT and welcome having the CFO hold the reins. 

But while all this reasoning is logical, and most CEOs do welcome the CFO supervising the CIO, it's not always the best reporting structure for the CIO.

Making a case for reporting to the CEO

When I applied for my former CFO role, the company was trying to position itself for major growth through acquisition and had significant technology issues. What the company wanted in a CIO was someone who could turn IT support services around quickly and position the company for the acquisition efforts and planned growth.

http://www.techrepublic.com/article/report-directly-to-the-ceo-to-boost-your-it-goals-and...

2015-02-25
The opportunity was very appealing to me, and after the company met my compensation requirements, I sat down with the CEO and CFO to discuss my request to report to the CEO. I explained why I couldn’t accept the position unless the reporting structure was right for the business need and used some of the following reasoning:

- **The CEO is closer to the operations side.**
  It’s important for a CIO to be closely involved with the operations of the company. A CFO understands the financial side of the business but is not always savvy to the inner operations of the company. A CIO’s role is to help the company improve productivity and profitability through technology, and in most companies, the best opportunities to do this are within the operations staff and organization.

- **The CEO drives strategic initiatives.**
  I know that when I was part of a fast-growth company that acquired more than 35 other companies, the fact that I reported to the president made a huge difference in my early involvement with new strategies. This early involvement was critical in both my personal preparedness as well as my ability to position our IT organization for what lay ahead.

- **The CEO is usually a stronger manager.**
  This may not always be the case, but many times the CEO or president is a stronger manager than the CFO. Reporting to the strongest manager always helps you develop more skills that benefit you in your career.

- **Reporting to the CEO gives the CIO more clout.**
  There are often times when you may need to make significant changes in an organization, possibly even cultural changes. Major changes inevitably affect the employees and managers in other departments of the company. It helps to have the support of the CEO, verbally as well as in the organizational structure of the company, to show the importance of the IT department and the CIO position.

- **Most of your internal customers are operational staff.**
  When most of your technology users are part of operations, reporting to the CEO or the operations side of the business gives lots of credence to your position.

- **It helps prepare a CIO to become a CEO.**
  More and more CEOs are coming from the CIO position as companies become more technically oriented. Working directly for a strong CEO helps you develop new skills that are needed if and when you decide to seek the top position in a company.

- **It provides the CIO exposure to the board of directors.**
  This may not seem important, but it is. The higher you go in an organization, the more you need to be able to communicate at a high level and present your ideas for improvement. Bigger initiatives require more dollars and tougher cost justification. As the CIO, you are in the “big leagues” now, so you need to start getting comfortable with your board of directors.

- **The CIO should be an ‘operations advocate.’**
  When both the operations departments and the IT department report to the same executive manager, it allows differences to be managed more effectively by the senior manager. For example, because one company president acted as my mentor, rather than getting confrontational with a regional operations manager, I could use the president to position controversial issues so that IT was always viewed as an “operations advocate” or “operations partner” and not an adversary.

Position yourself as well as you can. In terms of a CIO’s career, one of the most crucial reasons I’ve outlined is that CIOs looking to move up to the CEO perch, and those in a CIO role where they’re making major decisions that affect corporate structure, need to be able to
step right into the CEO’s office.

The CIO has to be aware from the start on how to position the technology of the company to support many new initiatives the company may want to take. Having a direct relationship with the chief executive is vital.

In one of my prior CIO roles, I reported to the company president and it was by far the best move for me. Reporting to the CFO, a visionary but a poor manager, would have been very difficult in that situation. In reporting to the president, I had the support I needed, was kept informed of strategic plans, learned a lot, and was close enough to the CEO to be exposed to what went on in the CEO office.

The point is that you should try to report to the appropriate senior executive in relation to the tech leadership role you’re taking on. Considerations you want to evaluate include:

- Strategic initiatives planned by the company
- Changes you need to make and support needed
- Ability to learn from your manager
- How the position and reporting structure are viewed in the company
- Company growth (high growth means lots of change)
- Personality compatibility
- Positioning yourself for career advancement

It’s undisputed that strong CIOs normally excel no matter whom they report to because they always know how to get “early warning” news on new initiatives, and they network well within the company at all levels. Yet, if there is an opportunity to make the decision, your career and your professional achievements at the company will be greatly enhanced by reporting to someone above the CFO level.

Mike Stisco is the CEO of MDE Enterprises and has been an IT manager and CIO for more than 20 years. His company is dedicated to the training and education of IT managers to help them achieve more success. For more of Mike’s management insight, take a look at his IT Manager Development Series (http://www.mdevolution.com).

Recommended

- Why Evolve OS could win you over in the cloud race (TechRepublic)
- Gimmicks will not bring Samsung back to its pre-Apple glory
- How to turn your old glasses into

http://www.techrepublic.com/article/report-directly-to-the-ceo-to-boost-your-it-goals-and...  2015-02-25
Report directly to the CEO to boost your IT goals and your career - TechRepublic

Add your Comment

Related Ads

1. Computer Repair Technician
2. Repair Internet Explorer
3. Buy Cheap Laptops
4. Fix My Computer
5. PC Backup
6. Apple Laptop Computers
7. SQL Server Backup
8. Outlook Express Repair

Steel Entry Front Doors
verdunwindows.com

From plain & simple to Custom Doors Designs for all Budgets & Styles!

Editor's Picks

We-commerce: The sharing economy's uncertain path

'PayPal Mafia' redefined success in Silicon Valley

http://www.techrepublic.com/article/report-directly-to-the-ceo-to-boost-your-it-goals-and
Should CIOs Report to CEOs or CFOs?

By Brian P. Watson | Posted 01-21-2008

Should CIOs Report to CEOs or CFOs?

Should CIOs report to CEOs or CFOs?

Conventional wisdom says it depends on a company's strategy. Rajiv Banker, professor of accounting and IT at Temple University's Fox School of Business, says that conventional reporting models don't always produce the expected results.

He spoke recently with online editor Brian P. Watson about his research into the misperceptions surrounding those reporting structures.

**CIO Insight:** What situations indicate that the CIO should report to the CEO?

Banker: The kinds of companies with that kind of reporting tend to strive for competitive advantage by differentiating their products and services. To do so, you need to have your organization focused on innovation-- innovation in technology, introducing new products, increasing the value proposition. The CIO has to constantly think about potential new IT that can widen that advantage.

But we’ve seen research that shows the CIO isn’t involved in strategic planning. Shouldn’t he or she be, in this scenario?

More and more companies recognize that IT plays a strategically vital role. But just because IT can play a strategic role does not necessarily mean the CIO is the one who leads the strategic change.

Very often, [the CIO’s] strategic role is supportive. For example, for companies with market-based strategies, aiming to deliver to customers, the strategy will perhaps be driven more by the marketing organization. IT will then follow up to make sure that strategy is delivered.

When a CIO reports to the CEO, is there a tendency to let costs get out of control, because of investing more in emerging technologies or riskier projects with a potentially higher return?

That's exactly right, if that's the way your organization has chosen to compete. On the other hand, if it's not, taking that sort of risk may be out of line, and the CIO can get in trouble.

That can be averted by having the CFO supervise the decisions the CIO is making. That's the value of having that reporting relationship. It makes you more conservative.

What are the pros and cons of reporting to a CFO?

We tend to hear it's best for CIOs to report to CFOs because it forces them to have a narrower financial mindset or focus on quantifying the success of their technologies. This might not be the case.

The challenge for management is not so much to find innovative ways to deliver value to customers, but rather, [to discover] how they can do so at lower cost. The kinds of technologies used in such cases are not necessarily at the cutting edge or experimental, but are proven ways to use information systems to eliminate waste and increase efficiency. Having that financial focus actually helps the strategic goals of the company.

That's the key part here: The role of the CIO should be to support whatever might be the strategic positioning of the company.

Page 2: The Path to Success

The Path to Success

When should a CIO report to the COO?

Reporting to the COO is typically seen when a company is interested in having IT play a supporting role, ensuring that operations are conducted efficiently. But we've only seen a few examples, far fewer than reporting to the CEO or CFO.

Do these different reporting structures create different kinds of CIOs?

There are two very different types of CIOs: the ones very connected to technology and R&D, and the kind you want in a firm pursuing a differentiation strategy, where the CIO has more of a financial background.

What it underscores is the need to recognize that, when you talk about the COO, it doesn't always mean the same thing. It depends on the type of business. That means you have to weigh the needs of the company.

We see this to be a lot more confusing and complex, or even challenging, but we try to extend both these types of characteristics in the same persons in the same organizations. That's not quite the case. There are two different tracks.

Do you find that one kind of CIO tends to last longer or fare better than the other?

That was a bit of a surprise. People tend to be of the general belief that CIOs are better off in a company with [an overall] differentiation strategy, because they get to be more creative, apply their specialized technology experience, and have a greater role in strategic planning.

We find that it's not the case. It's true for companies with a product differentiation strategy, but not true for companies getting a competitive advantage through their cost structure.
IT Orientation, CIO Reporting Structure, and Firm Performance: To Whom Should the CIO Report?

Rajiv Banker - Nan Hu - Paul A. Pavlou

University of California, Riverside - Singapore Management University

ABSTRACT

Twenty years after the introduction of the CIO position, the IS literature has yet to prescribe the ideal CIO reporting structure. To address this void, this study proposes a contingency model in which the CIO reporting structure depends on the firm's competitive firm IT orientation. We introduce Sales over Assets as a success measure for firms employing IT for strategic differentiation. Also, Operating Income over Sales is introduced as a performance measure for firms leveraging IT for operational excellence. Following the strategy-structure paradigm, this study hypothesizes that firms with higher Sales over Assets will have their CIO reporting to the highest executive (CEO), while firms with higher Operating Income over Sales will have their CIO report to a lower-rank executive (CFO). In addition, following the alignment paradigm, we hypothesize that only firms with either (i) a superior Sales over Assets and a CIO-CEO reporting structure, or (ii) a superior Operating Income over Sales and a CIO-CFO reporting structure will have superior performance over time than the other configurations. Secondary data from 700 firms support the proposed hypotheses, validating the strategy-structure and the alignment theories. The paper concludes by discussing the ideal CIO reporting structure and its performance implications.

1. RESEARCH MOTIVATION

The CIO position has emerged in the early 80s (Synnott and Gruber 1981) in response to rapidly-changing technology, frequent changes in consumer preferences that require market orientation and data mining tools, increased business competition that requires new delivery channels and services, enhanced user sophistication who demand greater functionality, and the emergence of the ‘information economy’ (Benjamin et al. 1985; Fleming, 2002). Since its inception, the CIO position has gradually become more strategic in nature as IT has been increasingly playing a greater role in the firm’s success (Lankit 2001; O’Donnell 2001; Lasker and Norton 1996). IS researchers have focused on prescribing several means (e.g., business background, communication skills, service orientation) by which CIOs could become more important (e.g., Rockart 1982). Today’s CIOs have many roles, such as from new product development, knowledge management, business process reengineering, regulatory compliance, and IT maintenance.

The CIO’s role varies dramatically among firms (Gottschalk 1999). A key distinction of primary concern to the CIOs is one between a strategic (IT as a competitive weapon) versus an operational (IT for cost-effectiveness) role of IT (Watson 1990). This distinction is herein proposed to influence the decision of the firm’s IT structure in regards to CIO reporting (CEO Vs CFO).

Despite the important role of the CIO reporting structure on firm strategy and performance, the literature has yet to address the links between IT structure, strategy, and performance. This is what this study aims to do by shedding light on two research questions:

- How does a firm’s IT orientation determine its CIO reporting structure (CEO Vs CFO)?
- Does an alignment between IT orientation and CIO reporting structure influence firm performance?

2. LITERATURE REVIEW

2.1 CIO Roles & Reporting Structure

There are two broad categories that describe the CIO’s role (Stephens et al. 1992; Vizard 2000):

First, a strategic role where the CIO is involved in strategic planning, participates in strategic policy committees, stimulates new business opportunities, and influences the firm’s decision making (Gottschalk 2002). This CIO role is associated with a leadership role, increased staff orientation, and corporate responsibility for information resource policy and strategy (Rockart et al. 1982). Such strategic CIOs help align IT with firm strategy and lead IT-enabled strategic projects.
Second, an operational or supporting role that the CIO is responsible for IT implementation, managing the IT infrastructure, and providing functional IT support in a cost-effective way. This more traditional focuses on managing 'must-do' IT projects with clear payback (Caldwell et al. 1996).

A key element of a firm's IT structure is the CIO reporting structure. Whether the CIO reports to the CEO (one level down) or CFO (two levels down) is a well-accepted measure of the relative power and importance of the CIO in the firm (Applegate and Elam 1992). For the CIO, the CFO is often seen as an adversary or obstacle due to the difficulty of CIO to show returns on IT investments (Slater 2002).

3. CONCEPTUAL DEVELOPMENT

3.1 Firm IT Orientation

The strategy-structure paradigm (Chandler 1962) has long advocated the need to match a firm's strategy with its structure. Since a firm's competitive strategy largely depends on IT (Bakos and Treacy 1986), following the strategy-structure paradigm, the IS literature has suggested that a firm's competitive strategy is related to its IT structure (Tavares and 1989).

Without loss of generality, firms have two key types of IT orientation: strategic vs operational. Firms with a strategic IT orientation focus view IT as a competitive weapon and an enabler of new business opportunities. Firms with an operational IT orientation focus on cutting operating expenses and emphasizing strict IT spending, allowing business needs to drive IT decisions (and not vice versa). To capture the relative importance of IT in the firm, we propose Sales over Assets as a success measure for firms employing IT for strategic differentiation. On the other hand, Operating Income over Sales is proposed as a performance measure for firms leveraging IT for operational excellence.

3.2 CIO Reporting Structure

The CIO reporting structure depends on how critical is IT to the firm's strategy, and the culture of the firm in terms of IT (Benjamin et al. 1995). We propose that firms with a strategic IT orientation tend to have their CIO report directly to the CFO, whereas in firms where IT has an operational role, the CIO tends to report to the CEO.

A CIO-CEO reporting structure is associated with emphasis on new product development, business process reengineering efforts, market orientation, and knowledge management. Firms whose CIO has a strategic role often have a formal IT strategy, an IS strategic orientation, greater IS planning success, and greater IS maturity. A CIO-CEO reporting structure is often the result that IT plays an important role in managing knowledge, and the need for the CIO to implement knowledge management systems (Lasker and Norton 1999). Firms whose CIOs report to the CEO tend to leverage IT for growth and competitive advantage (Caldwell et al. 1999).

A CIO-CFO reporting structure helps bring portfolio management and cost discipline to IT spending, it focuses IT initiatives on business needs, and ensures adequate IT resources dedicated to financial reporting and analysis systems (OptimizeMag, 2003). This reporting structure emphasizes efficiency, infrastructure maintenance, and regulatory compliance.

In summary, reporting to the CEO is an IT structure for firms who view IT as a source of competitive advantage, while firms whose CIO report to the CFO see IT as a way to cut operating expenses (Caldwell et al. 1998).

H1: Firms with a strategic IT orientation (high Sales over Assets) have their CIO reporting to the CEO.

H2: Firms with an operational IT orientation (high Operating Income over Sales) have their CIO report to the CFO.

3.3 Strategy-Structure Alignment & Firm Performance

Alignment or 'contingency-fit', rooted in the information processing view (Galbraith 1977), is conceptualized as the degree of ideal configuration among relevant factors (Venkatraman 1989). Following this contingency view, the success of any CIO reporting structure depends upon the firm's IT orientation (strategic or operational) since the relationship between the CIO and other C-level executives (CEO or CFO) may influence the success of IT in the firm (Peery et al. 1992; Jarvenpaa and Ives 1991).
Direct CEO reporting improves the similarity of IT perceptions between the CIO and CEO ("shared vision for IT") (Tai and Phelps 2000) and the CIO-CEO relationship and communication (Gottshalk 1999; Raghunatham 1992), which would be particularly valuable for firms that emphasize a strategic IT role. A direct CIO-CEO reporting also facilitates IT implementation (Gottshalk 1999), which in turn elevates the attention to the strategic role of IT and the CIO's influence on the CEO (Slofstra 2001). On the other hand, firms where IT has a supporting role must emphasize strict IT spending and focus on low-risk projects where IT can result in further efficiency improvements.

Summarizing these arguments, we expect to have two ideal profiles:

H3: Firms with either (i) a strategic IT orientation and a CIO-CEO reporting structure, or (ii) an operational IT orientation and a CIO-CFO reporting structure will have superior performance over time.

4. RESEARCH METHODOLOGY & RESULTS

To test the proposed hypotheses, secondary data from 70 Fortune 2000 firms were collected.

Sales over Assets: A strategic IT orientation is operationalized with superior sales over assets. The reliability (Cronbach's alpha) of this variable was .80.

Operating Income over Sales: An operational IT orientation is operationalized with superior operating income over sales. This variable's reliability was .99.

The dichotomous nature of the CIO reporting structure allowed us to use a logistic regression analysis using the following equation over a 5-year period:

\[
\text{Report to CEO} = \alpha_1 \times \text{Average Operating Income/Sales} + \alpha_2 \times \text{Average Sales/Assets}
\]

The results of the logistic regression model are shown in Table 1, which validate H1 and H2.

<table>
<thead>
<tr>
<th>Logistic Regression Factor</th>
<th>Coefficient</th>
<th>p-value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average Operating Income/Sales Over 5 Years</td>
<td>2.2248</td>
<td>0.0662</td>
</tr>
<tr>
<td>Average Sales/Assets Over 5 Years</td>
<td>-0.3244</td>
<td>0.0030</td>
</tr>
</tbody>
</table>

5. DISCUSSION

5.1 Key Findings

The results suggest that a firm's IT orientation determines its CIO reporting structure. Firms with superior sales over assets tend to have their CIO report directly to their CEO. On the other hand, firms with higher average operating income over sales have their CIO reporting to the CFO. In turn, the alignment between IT orientation and CIO reporting structure influence firm performance. More specifically, firms with a strategic IT orientation (high sales over assets) that have their CIO report to the CEO have superior performance over time. Similarly, firms with an operational IT orientation (operating income over sales) and a CIO-CFO reporting structure also have a superior performance compared with firms that have other IT orientation-reporting structure configuration (i.e., operational IT orientation with CIO-CEO reporting and strategic IT orientation with CIO-CFO reporting structure). In sum, the results confirm both the strategy-structure paradigm (Chandler 1962) and also the strategy-structure alignment perspective (Galbraith 1977, Venkatraman 1989), and shed light on the ideal CIO reporting structure.

5.2 Theoretical and Managerial Implications

The study has implications for the nature of CIO reporting structure and its implications for firm performance. From a descriptive perspective, the study reveals how a firm's IT orientation (as reflected by key accounting factors) predicts to whom the CIO reports to (CEO Vs CFO). From a prescriptive standpoint, the study sheds light on the ideal CIO reporting structure depending on a firm's IT orientation. This finding can help managers design their CIO's reporting structure based on how their firm views IT.
5.3 Limitations and Suggestions for Future Research

Economic conditions influence the role of the CIO and her importance in the firm. Recessions are associated with an emphasis on cost reduction and reduced IT spending (reduced importance of the CIO), while economic expansions emphasize new IT-enabled initiatives (enhanced CIO role). Even if the longitudinal results may have captured changes in economic conditions, future research could examine the role of economic conditions (among other factors) that may shape the ideal CIO reporting structure.

REFERENCES

### Appendix 1. Cumulative Results for Sales Over Assets (SALE/ASSET)

<table>
<thead>
<tr>
<th></th>
<th>Value</th>
<th>P-Value</th>
<th>Test (P-Value)</th>
<th>Test (P-Value)</th>
<th>Test (P-Value)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>bothCEO</td>
<td></td>
<td>bothCEO=bothCFO</td>
<td>bothCFO=DIFFCFO</td>
<td>bothCEO=DIFFCFO</td>
</tr>
<tr>
<td>Average</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SALE/ASSET (T+1, T+2)</td>
<td>-1.10322</td>
<td>0.0001</td>
<td>0.0003</td>
<td>0.0004</td>
<td>0.0005</td>
</tr>
<tr>
<td></td>
<td>bothCFO</td>
<td>0.09161</td>
<td>0.4011</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>DiffCFO</td>
<td>-0.85894</td>
<td>0.0001</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Average</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SALE/ASSET (T+1, T+2, T+3)</td>
<td>-0.75827</td>
<td>0.0001</td>
<td>0.0020</td>
<td>0.0240</td>
<td>0.0006</td>
</tr>
<tr>
<td></td>
<td>bothCFO</td>
<td>0.17812</td>
<td>0.2868</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>DiffCFO</td>
<td>-0.51308</td>
<td>0.0016</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Average</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SALE/ASSET (T+1, T+2, T+3, T+4)</td>
<td>-0.67401</td>
<td>0.0001</td>
<td>0.0005</td>
<td>0.0123</td>
<td>0.0005</td>
</tr>
<tr>
<td></td>
<td>bothCFO</td>
<td>0.24150</td>
<td>0.2073</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>DiffCFO</td>
<td>-0.42585</td>
<td>0.0032</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Appendix 2. Cumulative Results for Operating Income Over Sales (OPIS)

<table>
<thead>
<tr>
<th></th>
<th>Value</th>
<th>P-Value</th>
<th>Test (P-Value)</th>
<th>Test (P-Value)</th>
<th>Test (P-Value)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>bothCEO</td>
<td></td>
<td>bothCEO=bothCFO</td>
<td>bothCFO=DIFFCFO</td>
<td>bothCEO=DIFFCFO</td>
</tr>
<tr>
<td>Average</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OPIS (T+1, T+2)</td>
<td>0.01138</td>
<td>0.1333</td>
<td>0.0975</td>
<td>0.1676</td>
<td>0.0001</td>
</tr>
<tr>
<td></td>
<td>bothCFO</td>
<td>-0.04381</td>
<td>0.0272</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>DiffCFO</td>
<td>-0.01509</td>
<td>0.00795</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Average</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OPIS (T+1, T+2, T+3)</td>
<td>0.01598</td>
<td>0.0738</td>
<td>0.0001</td>
<td>0.0234</td>
<td>0.0001</td>
</tr>
<tr>
<td></td>
<td>bothCFO</td>
<td>-0.05122</td>
<td>0.0041</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>DiffCFO</td>
<td>-0.01286</td>
<td>0.1183</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Average</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OPIS (T+1, T+2, T+3, T+4)</td>
<td>0.02643</td>
<td>0.0047</td>
<td>0.0001</td>
<td>0.0091</td>
<td>0.0001</td>
</tr>
<tr>
<td></td>
<td>bothCFO</td>
<td>-0.04282</td>
<td>0.0091</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>DiffCFO</td>
<td>-0.0020</td>
<td>0.4550</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Where:
- bothCEO: Both CEO (Actual and Predicate)
- bothCFO: Both CFO (Actual and Predicate)
- DiffCFO: Actual CFO but predicate CEO
It's the age-old question: To whom should the CIO report?

Imagine if the strategic engine of the enterprise didn't report to the CEO

By Al Kuebler

The question has been batted back and forth for nearly as long as there have been CIOs: To whom should they report? I won't keep you in suspense as to where I stand: CIOs hold a C-level position, and as such they should report to the strategic leader, meaning either the CEO or the COO.

Why do I believe this? I have several reasons, and none of them has anything to do with status. The simplest is this: Because information technology is the most powerful competitive enabler available to most businesses, its leader should not be relegated to reporting to someone who may have other priorities than the organization's strategic performance.

There are some exceptions to this, and I'll get to them. But first, let me articulate the primary reasons why having the CIO report directly to the CEO is the best arrangement.

1. CFOs have totally different priorities.

CFOs are, by nature, risk-averse. They are charged with protecting the financial well-being of the organization. Their charter is to question expenditures, ensure that proper controls are in place and ascertain that investments realize the expected returns. Their focus is on the short term, and their priority is process. CIOs, on the other hand, must be risk takers. After all, every strategic system development project is risky — it has never been done before in the company and will have long-term impact. CIOs have to focus on the long term, since most significant IT developments span many years. Their priority is introducing beneficial change, not maintaining a consistent process. When a CIO reports to the CFO, the IT function ends up operating much more conservatively than it should. That might be OK for certain companies, on a temporary basis, and in the course of my career as a CIO, I had some productive working relationships with CFOs that I reported
to. Nonetheless, I think that the days when this sort of relationship could really work are gone. Quite frankly, a conservative IT function is not going to help most companies to confront the increasingly intense competitive environment out there.

2. The CEO needs to know what IT can do for the company.

Strategic IT projects can have an enormous impact on the future of a company. That makes the IT function so central to the company's competitiveness that it's essential for the CEO to have a working knowledge of the process of IT project creation. This is too important to be blunted by intermediaries. A CEO needs a CIO who can function as a partner, giving the CEO enough familiarity with the process of IT project creation so that the CEO can make sure that the company's strategy is being properly addressed by the IT function.

3. CIOs need to be deeply involved in business operations.

The officers who are closest to the operations side of the business are the CEO and COO. Most CEOs today want their CIO to help the business compete profitably through technology, and they recognize that the CIO can better do this when enmeshed in the inner operations of the lines of business. A CIO reporting to the CFO or CAO misses out on working closely with people who are savvy about those things.

4. CIOs need credence in the eyes of users.

Most internal IT customers are part of the operational staff. A CIO who is positioned on the same side of the org chart as them has more credence.

5. Reporting to the CEO provides enterprisewide purview.

Because IT is the strategic engine of the business, its priorities must be set with the participation of all parts of the organization. When the CIO reports to the CEO, the other C-level executives understand that relationship.

6. Reporting to the CEO gives the CIO more influence.

Influence should not be confused with status. Status resides inside people's heads, but influence has real practical value. A CIO might need to make significant organizational changes, possibly even cultural changes. Anything that affects the status quo is likely to meet major resistance, and a CIO who is working hand in hand with the CEO is better
able to carry out initiatives effectively. When everyone knows that the CIO reports to the CEO, they perceive that the CEO accords the IT function and the CIO position a great deal of importance. And when any part of the business has a problem with what IT is doing, the CIO can set up a meeting with the CEO quickly.

7. No one but the CEO is going to adequately support the research the CEO wants the CIO to deliver.

Increasingly, CEOs want their CIOs to help lead the business to better ways of doing things through new ideas and technologies. But it's unlikely that any other C-level officer is going to fully recognize how vitally important researching emerging technologies is, and they certainly would be slow to come up with the necessary funding.

When Is a CIO Not a CIO?

Case closed? Actually, no. There are instances when a CIO shouldn't be in a close relationship with the CEO and should instead report to someone else. What this comes down to is the qualifications of the CIO, plus the CEO's definition of a C-level position. In other words, there are CIOs who hold the title but aren't really considered to function at the C level.

A C-level CIO is not just technically competent. Such CIOs are also proactive in their technical competence, display business leadership abilities and are skilled in collaboration, communication and persuasion. They know how to create relationships out of a community of interest in profitably growing the business, and they are able to jump-start initiatives to move the business to higher competitive levels. In other words, they have considerable business acumen and are able to talk about their specialty in the business and stockholder terms that their peers understand.

CIOs who lack these skills -- who cannot clearly articulate how the IT function benefits business results by avoiding cost, improving service and increasing revenue -- should report to an executive other than the CEO. CIOs just don't belong on that level of management if they are unable to convert strategic and business direction into IT actions. These CIOs are really technology-focused IT managers who do not understand all aspects of the business value proposition. They cannot be expected to fully develop the initiatives the organization needs to derive from its IT function, and frankly, I've found that such technology-focused IT managers will not take such initiatives in any case.
It's the age-old question: To whom should the CIO report? | Computerworld

The trend today seems to be toward more and more CIOs who truly belong on the C level, with some of them holding broad general business management positions. Some examples: The CIO of one of the largest IT equipment suppliers also directs his firm's supply chain; the CIO for a major airline is responsible for all marketing activities; the CIO for a major parcel-delivery company is also responsible for route acquisition and optimization.

What they all have in common, besides a deep understanding of the business and how to communicate in business terms, is that they all report to their CEO.

Al Kuebler was CIO for AT&T Universal Card, Los Angeles County, Alcatel and McGraw-Hill and director of process engineering at Citicorp. He also directed the consulting activity for CSC Europe. He is now a consultant on general management and IT issues. He is the author of the book Technical Impact: Making Your Information Technology Effective, and Keeping It That Way, from which this article was adapted. He can be reached at ak@technicalimpact.com.

Follow everything from Computerworld

From CIO: 8 Free Online Courses to Grow Your Tech Skills

YOU MIGHT LIKE

Why Google wants to replace Gmail

Unique Method Regrows Lost Hair (Do This D...)

Microsoft tells Windows 10 users to uninstall Office

http://www.computerworld.com/article/3507512/it-management/its-the-age-old-question... 2015-02-26
News Scan: Woe to the CIO who reports to the CFO; Most firms unprepared for cloud challenges; more

September 29, 2014 | By David Weldon

>> CIOs shouldn't report to CFOs, says IT exec

Chief information officers can report to a variety of executive leaders, but if they report to CFOs, they are at a disadvantage. That is the take of Richard Boulderstone, the chief digital officer at the British Library. According to an article at CIO UK, "IT is a strategic enabler and working for the CFO makes enablement really hard." Boulderstone was quoted as saying. Boulderstone became the first CDO at the British Library in May 2013, after having been the head of IT since 2002. Commenting on the difference between his previous role and his new role, Boulderstone said "I have a small team to coordinate the digital efforts of the organization and it is liberating as I'm not from IT and it allows me to get more done."

(Read more on CIOs and CFOs: The technology CEO, IT's best friend / CFOs coulda, shoulda been IT's top advocates)

>> Many firms unprepared for cloud, data challenges

Many organizations like to talk the talk when it comes to cloud computing, but few are doing a good job of walking the walk. That is the conclusion of a new survey from IBM, which was cited in an article at CIO Insight. The report, entitled "The IT Infrastructure Conversation: New Content, New Participants, New tone," finds that "senior executives recognize IT's role as a business and revenue driver. And most plan to increase their infrastructure investments. However, only a small number of IT departments are working in tandem with line-of-business leaders to tackle tech infrastructure challenges." In contrast, those companies that are doing a good job of adopting cloud technology "are more likely to outperform their peers on several business outcomes."

(Read more on cloud adoption: iCloud Drive available for Windows ahead of the Mac / 6 new IT rules you need to fill)

>> Enterprise mobility solutions market growing at 24% rate

Thanks to the growing adoption of bring-your-own-device programs, the global enterprise mobility management, or EMM, market is expected to reach $15.7 billion in value by 2018. That represents a compound annual growth rate of 22.4 percent, says an article at Cloud Services World, citing new
research from Kable. "Of the various EMM solutions, the mobile application platform management, or MAMP, segment accounted for the largest share (48 percent) of the overall EMM market in 2013." The article notes that the development in the fields of machine to machine and wearables technologies are also impacting organizations, forcing many to deploy robust EMM solutions to manage a wide variety of devices and applications.

(Read more on enterprise mobility: Infographic: Mobile security risks and responses / Infographic: 95% of enterprise allow BYOD in some form)

>> CompTIA expanding efforts with Canadian IT industry

Information technology trade association CompTIA has announced that it is "expanding its engagement with manufacturers, distributors, solution providers and other organizations active in Canada's vibrant IT industry." The CompTIA Canadian IT Business Community launched with some 60 Canadian business owners, executives and leaders in attendance at a special event in Toronto. In announcing the initiative, CompTIA said "the community's new name better reflects the broader make-up of community participants ... We're offering companies in Canada's IT sector a forum for networking; a place to learn and share industry best practices; and a think tank to collectively discuss and address industry issues."

(Read more on CompTIA: Industry group urges renewed ban on internet taxes / IT talent shortage troubling for firms)

Tech leaders cannot enable if they report to CFOs

British Library Chief Digital Officer sees working for finance as a barrier to business outcomes

By Mark Chillingworth | 26 September 2014 | CIO UK

CIOs working for the CFO cannot position technology as a strategic enabler within the organisation says the new COO at The British Library, Richard Boulderstone.

Boulderstone became the first COO at the British Library in May 2013 having been head of IT since 2002.

"IT is a strategic enabler and working for the CFO makes enablement really hard," he said in a CIO UK profile of his new role.

"IT gets a bad press though as too many people trying to serve customers don’t see the point of technology, so I see the COO role as one of connecting technology with the rest of the organisation. As IT you are seen as a cost centre, barrier or having resource issues," he said of his previous role and career in IT.

"I have a small team to coordinate the digital effects of the organisation and it is liberating as I’m not from IT and it allows me to get more done."

News
Board politics

By Mark Chillingworth | Follow 26 September 2014 | CIO UK

Recommended Articles

CIOs have gotta have faith - Mike Altendorf

Three roles that CIOs will be asked to take on next - CEB

Brightside Group appoints insurance
CIO James Fairhurst

Five years ago, Chief Information Officers (CIOs) were on top of the world. These executives played mission-critical roles in driving multi-million dollar projects that delivered massive change. However, a global recession and the inability of CIOs to deliver on business value have tarnished their status. Today's CIOs are under pressure to deliver on requests for innovation, cost reduction, connectivity, and a growing demand for business intelligence.

Just as previous technology and business shifts have changed the role of the CIO, the new, more consumer-oriented business models of the social revolution will favor a new breed of business and technology leader. These leaders will have to navigate myriad converging and disruptive technologies, align new initiatives to both business value and technology feasibility, and identify strategies to leverage existing investments to fund innovation.
Consequently, the role of the CIO will evolve. Many next-generation technology leaders will still come from traditional tech backgrounds, but business leaders with a technology bent will also have a shot. As overall business strategy planning ties closer to IT strategy, four personas of the next-generation CIO will emerge:

1. Chief "Infrastructure" Officers focus on cost reduction, and account for 65% to 70% of the overall IT budget. Most of this CIO persona's projects prioritize keeping the lights on and managing legacy environments. Disruptive technologies such as virtualization and cloud will play a key role in cost reduction. These infrastructure officers tend to focus on the technology side and internal-facing activities.

2. Chief "Integration" Officers connect internal and external ecosystems. With 5% to 10% of the overall budget, this CEO persona must bring together a hodge-podge of business processes, data, systems, and connection points with legacy systems and newer cloud-based approaches. Projects touch external systems and often address post-merger integration environments. These integrators tend to focus on the technology side and both internal and external activities.

3. Chief "Intelligence" Officers empower the business with actionable insights. Representing between 10% and 15% of the overall budget, this CIO persona must improve business-user access to information. A key theme includes placing the right data to the right person at the right time on the right interface. These intelligence officers tend to focus on the business side and internal facing activities.

4. Chief "Innovation" Officers identify disruptive technologies for pilot projects. Investing 5% to 10% of the overall budget, this CIO persona must drive innovation on a shoestring. Typically from business backgrounds, these leaders move fast, fail fast, and move on. They tend to focus on the business side and external activities.
Most of today’s CIOs fit squarely in the Chief Infrastructure Officer persona, dedicating their time and resources struggling to keep the lights on. Shifting into the Chief Integration Officer role will be a smooth transition for most of them, but only a few with a business bent will grow into the Chief Innovation Officer role. On the flip side, many business leaders with a technology bent will evolve into the Chief Innovation Officer and Chief Intelligence Officer roles.

Among the companies we study, we’re seeing three different approaches to accommodating the different CIO personas:

1. One CIO can deliver on all four roles this by upgrading his or her skill sets.
2. A shadow CIO-like organization could emerge on the business side to fill the roles of Chief Intelligence and Chief Innovation Officer.
3. A CIO could have lieutenants charged with one or more of these functions.

R "Ray" Wang is Principal Analyst and CEO at Constellation Research.

This article is about SOCIAL PLATFORMS

+ FOLLOW THIS TOPIC

Related Topics: TECHNOLOGY

Comments

Leave a Comment

0 COMMENTS

JOIN THE CONVERSATION

POSTING GUIDELINES

We hope the conversations that take place on HBR.org will be energetic, constructive, and thought-provoking. To comment, readers must sign in or register. And to ensure the quality of the discussion, our moderating team will review all comments and may edit them for clarity, length, and relevance. Comments that are overly promotional, mean-spirited, or off-topic may be deleted per the moderators’ judgment. All postings become the property of Harvard Business Publishing.
IT Cannot Be Only the CIO's Responsibility

by Donald A. Marchand and Joe Peppard

JULY 19, 2013

IT is not something that can be managed from a box on the organizational chart. Unfortunately, this is not the view in most C-suites. Just look at what most do: They appoint a CIO and give him or her a budget and a mandate to get on with it! Why? As one CEO said to us: “I just want to forget about IT and concentrate on my core business.”

Of course, this response would be fine if the challenge were merely to deploy technology (on time and to budget) and ensure it continues to function properly for as long as required. It would also mean that outsourcing to a proven tech provider would be a legitimate response to perceived problems with IT (get someone with more experience and knowledge to run it for you). Or that the cloud is the remedy for IT's perceived inability to deliver, its inflexibility, tardiness, and questionable return. (By portraying IT as a utility like water and electricity, with apps on demand, a pay-as-you use model, and unparalleled scalability, what could be more attractive?)

The reality is somewhat different. This approach may work for business functions like manufacturing or logistics, but it definitely won't work for IT.
For one thing, what a manufacturing director is and is not responsible for is very clear. So what can a CIO be held responsible for? Technology? This only results in technology being deployed on time and to budget and works. What about being held to account for the benefits and value from IT spend?

This raises the fundamental question as to whether a CIO can really be held accountable for something that will only emerge when their colleagues step up to the plate. For example, successfully deploying CRM software on time and to budget will deliver little unless sales, customer services, and fulfillment processes are redesigned, staff trained to have the right conversations with customers, data quality improves, and marketers build the right competencies to use all the data that will now be available to them.

Let's say that a company's sourcing strategy calls it to move all IT requirements to best-of-breed cloud-based providers. Infrastructure and IT-based services will now be provisioned and delivered directly from the cloud. The question is, will problems with IT go away, particularly the challenges around delivering business value? Of course not! Why? Because the problems with enterprise IT have generally nothing to do with IT. They never have!

What the cloud does is make the technology-supply side more efficient and perhaps more agile. It may make costs more predictable and shift investments from CapEx to OpEx. It may even lead to access to leading-edge technologies. But these are generally not where the challenges lie when we look at the situation in most companies regarding return from IT spend.

The reality is that the organization still requires a strategy for information and systems. It still needs to make choices around process standardization and the extent of digitization, define the degree of integration required, and think about innovation...
opportunities enabled by IT, whether they be process innovation, business model innovation, management innovation, or innovation in the customer experience. And the organization still needs to prioritize IT spend, run programs and projects, manage the IT investment portfolio, orchestrate the organizational change to deliver expected business benefits, and make sense of information.

Accountability for some of these areas reside with the CEO and the other members of the C-suite (we are assuming CIO is a member of the c-suite), for others with LOB manager, and some will be shared. What is clear is that they are not the sole responsibility of the CIO. All members of the C-suite needs to recognize and embrace their fundamental roles.

What is therefore required is strong governance of IT. Be clear about the decisions concerning IT that need to be made, who gets to make them, how they are made, and the supporting management processes, structures, information, and tools needed to ensure that they are effectively implemented, complied with, and are achieving the desired levels of performance. Unfortunately, we have found that the focus of governance around IT continues to be on the more operational IT issues of delivering technology capabilities and IT services.

The basic requirement for success with enterprise IT has changed little over the decade. There is no magic bullet. The bottom line is that executives need to get their hands dirty and actively engage with their CIO and IT. Decisions about IT today really have little to do with technology!
• The CIO In Crisis: What You Told Us
• How to Compete When IT Is Abundant

Donald A. Marchand is a professor of strategy execution and information management at IMD in Lausanne, Switzerland. Joe Peppard is a professor of information systems at Cranfield University’s School of Management in the United Kingdom.
Enterprise IT is in crisis — no doubt about it. Our research, conducted in partnership with Harvard Business Review, The Economist, CEB (formerly the Corporate Executive Board), Intel, and TNS Global, finds that corporate leadership has lost confidence in the CIO as a strategic partner and views IT as a commodity rather than a difference-maker.

Clearly the roles of CIO and the IT organization need reinvention — and that's the conversation we've been having over the last few months in webinars and posts. (See also here, here, and here.) This conversation has generated a lot of interesting conversation via blog comments, emails, and face-to-face interactions at conferences and meetings and has revealed a few more insights that should factor into our evolving thinking.

CIOs need to understand business better, but the C-suite should understand technology's potential better. While the CIO needs to understand the business to add value, equally true is that senior leadership and the board of directors don’t understand how to incorporate technology in their strategy, and some don’t even see the need to do so. As gerajohm commented, “The best executives I have met have had
a great understanding of how to use technology to gain competitive advantage and improve operations. They also worked with the CIO to help them to understand the business. They worked together to identify the technologies that could improve the company's competitive advantage versus technologies that were needed to support the business. Once this was done, the executive leadership and CIO focused on implementing technologies that improve the company's competitive advantage."

**Every other function of the organization is as out of touch as IT.** Victorio M. commented, "Reading this post is both humorous and disheartening. Humorous because, as a Human Resources practitioner, I hear similar calls for change within my profession. So it's not just us! Yet it's disheartening because it's yet another organizational function that appears to not be able to keep up with the pace of business, staying stuck in a transactional, as opposed to strategic, frame of mind."

The Management Innovation Exchange is currently running a competition to "hack" the human resources function to enable organizational adaptability. As real space and cyberspace merge, do financial practices like budgeting provide value over their costs of time, money, effort, agility? All the parts of the organization have to come together and build a common language to discuss their markets and their enterprise. They need to have a common appreciation of each other's purpose. The CIO must step up and mentor the C-suite on the potentials, possibilities, threats and opportunities of information technology, but likewise, the HR lead needs to discuss the impact of a free-agent workforce, the head of legal needs to discuss the impacts of open innovation and IP sharing, and so on.

**As IT steps up as mentor, it needs to mature as well.** IT needs to step up, but collaboratively — not as the smartest guys in the room. One commentator said, "About 10 years ago, IT people suddenly became business process experts. Strategy in IT is one thing, but the process experts suddenly began giving advice about areas in which they were not experts and honestly felt they should lead strategic planning for..."
the entire organization." If IT and the CIO come to the party talking like engineers, only offer convergent lines of thought (analytical, rational, quantitative, sequential, constraint driven, objective and detailed focus) and don't offer a more holistic, shaded divergent thinking point of view (creative, intuitive, qualitative, subjective, possibility driven, holistic with conceptual abstractions), then they have missed the point.

**CEOs sense the problem perhaps more than CIOs do.** This is a totally unscientific finding, but it is what I experienced during the two weeks of article-writing and the culminating webinar, in which I engaged directly or indirectly with a large number of CIOs, IT managers and CEOs. There were a significantly larger number of CIO/IT conversations that took place in conference or meeting situations, and the CEOs generally self-selected by reaching out to discuss or gather more information. Unless I pointed out the topic, many of the IT people were generally unaware or just tangentially aware. The CEOs were actively aware, concerned, looking at alternatives such as chief digital officers, or creating "not-so-shadow" IT organizations under the CMO. Few of the conversations originated with IT people, unless they were already engaged in trying to address the issues (another self-selection bias?). A number of the conversations started with the assumption that social engagement, collaboration and analytics were not part of IT, but the responsibility of marketing.

**The bifurcation of IT and business is a myth.** There have been two paths of discussion around this. One is the concept of alignment. The other is the idea that as IT socially enables companies, the actual concept of management and how we organize and structure work as practiced today begins to disappear. There were numerous discussions around COBIT and ITIL — popular IT process- and service-management frameworks — and there is a lot that COBIT in particular offers. But too often, it turns alignment into supplication or worse, subservience. The CIO must understand and execute on the differences among leadership, governance, and managing. The CIO
must lead by showing the way IT can impact the organization both positively and negatively, sometime leading by how technology is applied in IT itself, then influence and guide the organization in making the right decisions. Then the CIO must direct and restrain the use of technology - how it is developed, sourced and applied in the best interests of the organization and its stakeholders with appropriate governance mechanisms. Lastly, the CIO must execute by managing the procurement, provisioning, monitoring and management of the delivery and application of IT to serve the organization. Several discussions focused in on understanding the difference between delivering IT and applying IT. If you are delivering IT, then you are a surrogate IT company that might not be aligned with the enterprise. If you are applying IT to the business, then by definition you have to be aligned with the business, or fail.

**Multiple roles, one company versus one role, multiple companies.** Historically, people got to the C-suite by progressing up the career ladder in one discipline, moving among multiple companies until they made it to an executive role in finance, sales, etc. Now, however, the model is changing. In successful companies, top executives rotate among multiple disciplines in increasing levels of responsibility until they advance to the C-suite. Leaders then have a multi-disciplinary understanding of the organization, rather than an exclusive, deep knowledge of just one area. And as we are learning, good leaders do not have to be discipline-specific if they engender trust and responsibility in their organization. Many CEOs expect their next CIO to come from marketing instead of their or another IT shop.

I started looking into the role of the CIO with the assumption that the onus was on CIOs to step up IT's game to enable their enterprise to succeed in the future. One observation from all this is that there is an endemic problem across the C-suite: there
has been such a long-standing culture of domain and functional specialization focused on efficiency that the overall gestalt of the business and its efficacy at creating and maintaining a customer has been lost.

But that doesn’t relieve CIOs of their responsibility to change IT to enable the business to better change. For aspiring CIOs, the best thing for your career is to leave IT and move to other departments — even if it involves taking a step back. Preferably, these roles need to be part of the value chain, facing either customers or partners, and eventually both. Then, step back into IT. This idea could be true for all departments — for instance, new business managers should come from outside the business function to encourage a holistic view of the business.

For existing CIOs, ask yourself a few questions. Are you generating customer value? Are you (or do you have the potential to be) the best in the world at what you are doing? Are you required to do what you are doing? Using the answers to those questions, what do you need to stop doing, start doing or do differently? Where are you spending your time interacting and relating to the rest of the organization? What resources should you have and how should you allocate them? What activities consume most of your efforts and what outcomes are you expecting from them? And lastly, what are you really focusing on and what questions are really driving you?

The point of all this is to pose these questions to everyone in the C-suite — not necessarily to be answered, but to start the collaborative, co-creative process to discover the answers and to continue the conversation.

Reinventing Corporate IT
An HBR Insight Center

- How to Compete When IT Is Abundant
- Can UX Save Enterprise IT?

- The Metamorphosis of the CIO
- Shadow IT Is Out of the Closet

Jim Stikeleather serves as Executive Strategist, Innovation for Dell Services, the IT services arm of Dell, where he leads a team of information technology and business experts who identify, evaluate and assess the potential of new technologies, business models and processes to address evolving business, economic and social trends.
We hope the conversations that take place on HBR.org will be energetic, constructive, and thought-provoking. To comment, readers must sign in or register. And to ensure the quality of the discussion, our moderating team will review all comments and may edit them for clarity, length, and relevance. Comments that are overly promotional, mean-spirited, or off-topic may be deleted per the moderators' judgment. All postings become the property of Harvard Business Publishing.
Why CIOs should be business-strategy partners | McKinsey & Company

Insights & Publications

Latest thinking | Industries | Functions | Regions | Themes

Anise
Why CIOs should be business-strategy partners

Our latest survey of business and IT executives finds that IT performance matters across the board when CIOs are involved in shaping business strategy.

February 2015 The Forum on Technology Strategy - McKinsey Insights

Performance issues and misaligned priorities

When CIOs play an active role in business strategy, IT performance on a wide range of functional and business needs improves. But at McKinsey, we've found that IT leaders are deeply involved in helping shape the strategic agenda and confidence in IT's ability to support growth and future business goals is strong. Moreover, IT and business executives disagreed strongly on the importance of IT performance, a situation that has grown in importance since the previous survey. The results suggest that the gap to capture more value in strategy discussions could deliver business benefits and address widespread concerns over IT effectiveness.

Exhibit 1

<table>
<thead>
<tr>
<th>IT organizations' effectiveness of functional processes</th>
</tr>
</thead>
<tbody>
<tr>
<td>% of IT respondents, n = 365</td>
</tr>
<tr>
<td>---------------------------------</td>
</tr>
<tr>
<td>Managing IT infrastructure</td>
</tr>
<tr>
<td>Governing IT performance</td>
</tr>
<tr>
<td>Implementing strategic approach to sourcing</td>
</tr>
<tr>
<td>Driving technology enablement to innovation in business processes and operations</td>
</tr>
<tr>
<td>Actively managing IT organization's health and culture (not only its performance)</td>
</tr>
<tr>
<td>Targeting places in organization where IT can add the most value</td>
</tr>
</tbody>
</table>

Stay connected

http://www.mckinsey.com/insights/business_technology/why_cios_should_be_business-s... 2015-02-25
Exhibit 2

As new technologies emerge, change on IT's top priority - particularly on costs and information.

% of respondents, by function

<table>
<thead>
<tr>
<th>Current IT priorities at respondents' organisations</th>
<th>IT executives, n = 363</th>
<th>Non-IT executives, n = 360</th>
</tr>
</thead>
<tbody>
<tr>
<td>Improving effectiveness of business processes</td>
<td>62</td>
<td>65</td>
</tr>
<tr>
<td>Improving cost efficiency of business processes</td>
<td>44</td>
<td>47</td>
</tr>
<tr>
<td>Reducing IT costs</td>
<td>13</td>
<td>16</td>
</tr>
<tr>
<td>Providing managers with information to support planning and decision making</td>
<td>38</td>
<td>54</td>
</tr>
<tr>
<td>Creating new business products or services</td>
<td>34</td>
<td>37</td>
</tr>
<tr>
<td>Managing data</td>
<td>25</td>
<td>22</td>
</tr>
<tr>
<td>Ensuring compliance with regulations</td>
<td>21</td>
<td>50</td>
</tr>
<tr>
<td>Entering new markets</td>
<td>11</td>
<td>13</td>
</tr>
</tbody>
</table>

*Respondents who answered "don't know" are not shown.

When asked about IT spending for 2015, IT executives are more likely than their business peers to expect that their budgets for both operating expenses and new investments will shrink (Exhibit 3).

Exhibit 3

When asked about IT spending for 2015, IT executives are more likely than their business peers to expect that their budgets for both operating expenses and new investments will shrink (Exhibit 3).

http://www.mckinsey.com/insights/business_technology/why_cios_should_be_business-s... 2015-02-25
Hail to the chief

Despite dominant assumptions of IT effectiveness, CIOs now signal a new era of higher performance. IT organizations active CIOs involvement in the business. Where respondents say their CIOs are very or extremely involved in shaping enterprise-wide strategy, they report much higher IT effectiveness than other processes whose CIOs are less involved.

What's more, both IT and non-IT executives recognize that between CIO involvement and performance, the strategy asked each group to rate IT effectiveness in separate dimensions. The differences are especially stark regarding IT's ability to generate new organizational capability, according to IT executives, and to perform with the business to develop new capabilities, according to business respondents (Exhibit 4). As expected with the most involved CIOs, executives also show much higher than others to use IT facilities, business activities, including new market entry and the creation of new products.

Exhibit 4

<table>
<thead>
<tr>
<th>% of respondents</th>
<th>IT Executives</th>
<th>Non-IT Executives</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>n = 383</td>
<td>i = 380</td>
</tr>
<tr>
<td>Managing IT infrastructure</td>
<td>35</td>
<td>24</td>
</tr>
<tr>
<td>Actively managing IT organizational health and culture just its performance</td>
<td>47</td>
<td>42</td>
</tr>
<tr>
<td>Driving technology advancement or innovation in business processes and operations</td>
<td>58</td>
<td>45</td>
</tr>
<tr>
<td>Governing IT performance</td>
<td>27</td>
<td>21</td>
</tr>
<tr>
<td>Targeting processes in organization where IT can add the most value</td>
<td>33</td>
<td>25</td>
</tr>
<tr>
<td>Implementing innovation ideas developed by frontline staff or middle management</td>
<td>15</td>
<td>21</td>
</tr>
</tbody>
</table>

CIOs very or extremely involved in shaping business strategy
CIOs somewhat or not at all involved in shaping business strategy
Unfortunately, CIOs don't play this role at influential business executives at many organizations. The results show that just over half of all respondents say their CIOs are on their organizations' most senior teams, and only one-third of their CIOs are extremely involved in shaping the overall business strategy and agenda.

The CIO's impact on functional performance is underappreciated further by the fact that roughly one-sixth of respondents (15% of IT respondents and 38% of all executives) believe that at least one out of the top five IT management issues are the most significant to their organization.

**Continuing talent and organizational health challenges**

Executives continue to rate the overall quality of IT talent as a priority, but not as improving the function's performance. Better talent is cited second, just behind better functional accountability for IT-related projects and more effective technology. (Exhibit 5)

But talent challenges remain difficult. Many of the respondents cited attracting IT talent as a significant challenge for their organization (Exhibit 3), even when respondents indicated that they have enough IT talent to meet the demands of their businesses.

**Exhibit 5**

<table>
<thead>
<tr>
<th>Initiative that would be most important to improving IT performance</th>
<th>2013 (n = 728)</th>
<th>2014 (n = 973)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Improve the business's accountability for IT-related projects</td>
<td>45</td>
<td>45</td>
</tr>
<tr>
<td>Improve overall level of talent and capabilities of IT staff</td>
<td>33</td>
<td>44</td>
</tr>
<tr>
<td>Increase IT budgets and technology spending</td>
<td>22</td>
<td>25</td>
</tr>
<tr>
<td>Replace IT management with new leadership</td>
<td>20</td>
<td>18</td>
</tr>
<tr>
<td>Otherwise some or all problem areas to external providers</td>
<td>17</td>
<td>17</td>
</tr>
<tr>
<td>Committee and board accountability for IT group</td>
<td>15</td>
<td>11</td>
</tr>
<tr>
<td>Eliminate any internal IT group beyond basic services</td>
<td>14</td>
<td>12</td>
</tr>
</tbody>
</table>

*The percentages do not add up to 100 because of rounding.*

Not surprisingly, the most recent results suggest a notable rise in the need for data-analysts-related talent. The current survey (2015-02-25) shows a significant increase in the demand for these roles, with nearly twice the demand for data scientists and nearly four times the demand for data engineers.

**Exhibit 6**

*The data for this exhibit is from the latest talent baselines survey. The data is as of 2014.*

http://www.mckinsey.com/insights/business_technology/why_cios_should_be_business-s... 2015-02-25
Why CFOs should be business-strategy partners

CFOs can help drive business strategy in three main ways:

1. They are instrumental in shaping business strategy.
2. They contribute to overall business strategy.
3. They help cultivate a distinctive recruiting engine.

Looking ahead,

- drowned by the CIO's role. The survey results suggest that companies should adjust
  their approach to hiring and retaining their CIOs and other technology leaders by a more
  meaningful role in shaping business strategy. This means shifting away from a CIO
  with a supplier mindset who provides a cost-effective utility and toward a
  leadership that is integrated into the organization's overall business strategy and
  contributes positively to innovation and business growth. Some ways to
  enhance such changes include:

  - Aligning with the business strategy:
  - Establishing clear partnerships between the IT and corporate-strategy functions:
  - Holding both business and IT leaders accountable for key results.

- Draining IT's business strategy. Before they can contribute to overall business strategy,
  many CIOs and IT leaders may need to improve their understanding of the business.
  To achieve this, IT leaders who have both business and technology knowledge can
  participate more effectively in different roles, foster partnerships, and
  knowledge exchange among senior business leaders and strong IT leaders, and
  recruit business-owners with IT backgrounds into IT.

- Build a distinctive recruiting engine. Respondents note the growing importance of
  the recruiting function in a driver of better IT talent. In one experience, hiring new
  talent is often left to the IT function's HR team. This may not work and ownership
  should be with IT leadership. Leaders must provide HR with input on the most
  critical elements of a role's requirements, the necessary capabilities, the criteria for
  evaluating candidates, and sources of talent, and most importantly, a forecast of
  their talent needs six to 12 months ahead. This will allow for a more targeted and
  proactive talent acquisition process.

--

http://www.mckinsey.com/insights/business_technology/why_cios_should_be_business-strateg... 2015-02-25
About the authors
Patricia Zerwas, a partner in McKinsey & Co.'s New York office, and Ed Bylsma III, a director in the firm's Atlanta office, discuss
why CIOs should be business-strategy partners.

Related articles
Driving the top line with technology: An interview with the CIO of Coca-Cola
Above, 2013 – Ed Bylsma III is reshaping his CIO role at The Coca-Cola Company, accelerating its use of technology innovations to operationalize, market, and sell its

How CIOs can lead their company's information business
April 2013 — In data-driven companies, CIOs and other chief data officers should think big and help accelerate bold changes throughout the enterprise.

IT under pressure: McKinsey Global Survey results
March 2014 — Recognition of IT's strategic importance is growing, but so is dissatisfaction with its effectiveness. According among chief information officers on business and technology strategy, showed

Developing talent for large IT projects
April 2014 — Good program managers are hard to find. Here's how organizations can attract and develop their own leaders.

About Insights & Publications
The views and opinions expressed in this publication are those of the authors and do not necessarily reflect those of McKinsey & Co.
WHY READ THIS REPORT

In 2015, digital disruption will change the nature of competition, forcing firms to obsess about creating superior digital experiences across the entire customer lifecycle. Many CIOs have the technical expertise and cross-functional business acumen to help drive this level of innovation, but they are too often still seen as nothing more than the leader of a cost center. In 2015, CIOs will finally connect their teams’ technical and business know-how to the CEO’s focus on company growth and customer obsession by accelerating their firm's Business Technology (BT) agenda and establishing themselves as a key business leader. It can and will be a self-fulfilling prophecy, with not all CFOs up to the challenge. In this report, Forrester predicts three key things that successful CIOs will do in 2015 to lead their firms’ digital transformation.


CIOs DRIVE CUSTOMER OBSESSION INTO TECHNOLOGY MANAGEMENT

In 2015, companies that successfully harness digital technology to advantage will serve customers better by delivering a seamless, connected customer experience to their users in a way that is intuitive and convenient. Many CIOs have the technical acumen to help drive this level of innovation, but they are too often still seen as nothing more than the leader of a cost center. In 2015, CIOs will finally connect their teams’ technical and business know-how to the CEO’s focus on company growth and customer obsession.

Prediction No. 1: CIOs Accelerate The Business Technology Agenda

Accelerating digital business opportunities at scale will drive the majority of CIOs to focus more investments on their firm’s BT agenda — the build-out of access to and delivery of digital services. This is happening because CIOs have the technical expertise and cross-functional business acumen to help drive this level of innovation. In 2015, CIOs will:

• Spend the majority of their new project budget on BT. In 2015, BT agenda technologies will cost less than half of new project purchases, with overall spending rising by 20% or more per year. (Note: “BT” refers to IT/IT initiatives like cloud, mobile, data, social, and customer experience that is a part of the customer lifecycle, and “CIO” includes all levels of the BT agenda, while CIOs in education, healthcare, telecommunications, and transportation will struggle to devote enough spending to BT: see endnote 1).

• Embrace customer-focused governance models for the BT agenda. Customer demands require more accountability and rapid delivery improvements — work that is understood only when a problem is felt by the customer before it is not delivered. Funding BT delivery of this variable work cannot be determined — or predicted — in advance. Many governance models will become more useful in the short run. CIOs will carefully monitor the impact of their BT agenda on the business and customer. And as the evolution of cloud continues, CIOs will measure the impact on the customer — and not the execution of some new technology — at the closest level of detail (see endnote 3).

• Boost software engineering skills to improve brand experience. To build the software that drives customer interactions, connected products, and mobile services, CIOs will make customer experience the design point in the development, with Agile development, modular architecture, and software-driven release and configuration management that support continuous delivery (see endnote 4). In 2015, CIOs will increase their investment in the required skills and tools, and a growing number of them will create separate software engineering teams with the senior skills and tools of mobile commercial software firms.
- Embrace hybrid cloud architectures to drive simplicity and time to benefit. The BT agenda focuses on systems for engaging with customers. As a result, in 2015, the overwhelming majority of CIOs will accelerate the standardization and simplification of systems of record, moving non-differentiating processes to commercial cloud providers. Some of these systems will be incrementally delivered, but more will be provided by external suppliers. For example, global utilities replace 100% of their non-core IT infrastructure with cloud-based, open, and agnostic cloud providers such as Microsoft Azure and IBM Bluemix.

- Cut through organizational silos with service orchestration. Individual functions like marketing, manufacturing, and final sales are becoming more intimately connected across all digital technologies and processes. As brands evolve, the CIO is increasingly expected to deliver integrated end-to-end experiences, and the CIO will incrementally integrate cloud services with existing on-premises solutions.

Prediction No. 2: CIOs Unlock Data-Driven Business Opportunities

Success at the age of the customer is predicated on the ability to transform disparate sources of data into an end-to-end view of customer behavior. CIOs are in the best position to aggregate and orchestrate a broad data strategy for the business — including data protection. In 2015, CIOs will:

- Transform data into a product of service that drives new revenue. In 2015, CIOs will move existing internal data that they already control with the fast-growing array of external, third-party data on social media, social media, and mobile service and location-based data to help create new data services, resulting in new sources of revenue. CIO-led companies will increasingly generate data that drives John Deere’s FarmSight business. Similarly, CIOs will leverage insights into customer behavior that help to identify new markets.

- Run point on raising data security and privacy issues. With a data-driven economy to flood consumers, data security and privacy concerns will rise dramatically in 2015. CIOs will lead the effort but will need to partner with external tech management to ensure that it is a top enterprise business issue. Relatedly, privacy questions regarding ownership of data are attracting more attention. In 2015, CIOs will work with business peers to positively manage data’s security and privacy impacts on their firm’s behavior and brand.

- Stretch their data strategy and orchestration skills. In 2015, the strategic focus on data opportunities will shift from the self-reliance for the CIO’s organization. Consulting and integration planning, and architecture, vendor management, and security skills will become more critical than traditional data configuration and system maintenance skills. This is due in part to increased use of software-as-a-service and greater consideration of infrastructure. But this also reflects the important role of innovation, growth, and data protection.

Prediction No. 3: CIOs Make CDOs Unnecessary

2015 will be a defining year for the CIO’s career. As businesses pursue digital transformation and customer obsession, their CIOs will build their reputation as a digital innovation leader. In 2015, CIOs will:

- Turn fledging relationships with CDOs into functional partnerships. As CDOs begin to understand the impact of the age of the customer, they will expect CIOs to work side by side with other business leaders to leverage data — especially customer marketing offices (CMOs) — in leading the transformation of digital business. CDOs and CIOs will increasingly be forced to work together and lead transformation efforts.

- Become leaders of digital change — or be marginalized. Somewhere lies the key to change in increasingly distributed and independent technology for the enterprise. Field-level, data-driven innovation that drives a coherent, cross-channel digital experience is crucial to succeeding in today’s markets. Although some firms have appointed a chief digital officer (CDO), most CIOs will need to move into a role that supports this effort. In 2015, the CDO role will be even more critical as the CIO’s role becomes more relevant. The CDO role will become more relevant in 2015, and this will be the year that the CDO role becomes more critical. The CDO role will become even more critical in 2015, as the CIO’s role becomes more relevant. The CDO role will become even more critical in 2015, as the CIO’s role becomes more relevant.

- Embrace hybrid cloud architectures to drive simplicity and time to benefit. The BT agenda focuses on systems for engaging with customers. As a result, in 2015, the overwhelming majority of CIOs will accelerate the standardization and simplification of systems of record, moving non-differentiating processes to commercial cloud providers. Some of these systems will be incrementally delivered, but more will be provided by external suppliers. For example, global utilities replace 100% of their non-core IT infrastructure with cloud-based, open, and agnostic cloud providers such as Microsoft Azure and IBM Bluemix.

ENDNOTES

2. Forrester's US tech market outlook for 2014 and 2015 provided general guidance for US CIOs. But every firm operates in a specific industry. So, in this report, we provide our outlook for tech budget spending for our 23 industry groups. This report will help CIOs understand the tech spending prospects in their industry and what they need to do to keep up with agile competitors, especially in their pursuit of the business technology (BT) agenda or realigned strategy, serving, and retaining customers. See the October 12, 2014 "US Tech Spending by Industry, 2014-16" report. 

3. Forrester developed its IT Balanced Scorecard for CIOs almost a decade ago, based on the original Balanced Scorecard framework proposed by Robert S. Kaplan and David P. Norton. Over the years, we have worked with hundreds of CIOs to apply the IT Balanced Scorecard to measure and benchmark IT value and performance. But as we enter the age of the customer, where powerful customers are disrupting every industry, companies will have to change how they develop, market, sell, and deliver products and services to their customers and through their partners. CIOs and their teams are crucial for these strategic responses and will have to focus on transformation and performance with these new trends to go beyond their traditional IT agenda to include business technology (BT) — technology, systems, and processes to serve, serve, and retain customers. This research introduces Forrester's new Tech Management Balanced Scorecard, which incorporates both the IT and BT agendas for CIOs. See the May 6, 2014, "Forrester's New Tech Management Balanced Scorecard" report. 

4. Application delivery in the modern age no longer plays a supporting role. It is the center stage. Business success in the age of the customer means mastering modern application delivery. Speed in developing and delivering innovation applications is becoming essential to the success of businesses in any industry. These applications are not the enterprise apps of old, back office support functions focused on cost savings and operational support. They are how customer-facing, multichannel, interconnected revenue engines evolve as fast as organizations can keep up. Forrester's modern application delivery playbook charts the course toward mastery of delivering modern applications. It is an evolution and extension of earlier research on Agile and Lean methodologies and application life-cycle management, picking up where line-of-business left off in guide organizations toward developing and delivering market-leading applications. See the March 4, 2014, "Modern Application Delivery: Drives Digital Business Success" report. 

5. Digitally empowered customers are redefining how businesses work, forcing firms to become digital businesses that leverage digital technologies across the ecosystem. Working in this fast-paced digital era requires CIOs to adopt a new approach. Traditional solutions fail to support the urgent changes that customers demand and can't keep up with the complicated complexity of customer journeys from multiple channels and across multiple organizations. This report looks at the emerging use of customer business services (CBSes) to bridge this complexity. A CBS is a discrete business service that is managed to continuously provide a specific outcome and that can be composed into customer journey-moment solutions by the speediest of digital technologies like mobile, Web, and call center. The success of the CBS model is as much about addressing the business challenge of cross-organizational work as it is about the technologies and development methodologies used to build CBSes. See the August 7, 2014, "Bridge Complex Customer Journeys With Continuous Business Services" report. 

6. A small number of strategic roles can turn the culture, systems, and processes of the tech management organization toward improving customer experiences. These include: relationship managers, architects, program/roadmap managers, vendor managers, user experience designers, data experts, and business process designers. See the November 7, 2014, "Five New Skills for Technology Management" report. 

Attached, for your information, is the agenda for the Management Development Program (MDP) Workshop which will take place from February 12 to 13 in the Conference Centre. During this workshop, certificates will be presented to the first cohort of graduates from the MDP. A list of graduates is attached along with a sample certificate.

In addition, suggested topics are included to help guide your and the Director’s address to workshop participants.

Regrets.

JAN 3 2015
ADH,

Attached, for your information, is the agenda for the Management Development Program (MDP) Workshop which will take place from February 12 to 13 in the Conference Centre. During this workshop, certificates will be presented to the first cohort of graduates from the MDP. A list of graduates is attached along with a sample certificate.

In addition, suggestion topics are included to help guide your, and the Director’s address to workshop participants.

Regards,

CCM# EXE14-
MANAGEMENT DEVELOPMENT PROGRAM (MDP)
Workshop 2015
"Towards an Engaged Workforce"

NHQ Conference Centre

Agenda

Thursday, February 12, 2015

8:00 to 8:30  Arrival and registration of participants
8:30 to 8:45  Words of welcome — DDG, LD, Employee Development

<table>
<thead>
<tr>
<th>OBJECTIVES</th>
<th>EXPECTED RESULTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>* Provide an update on the challenges and priorities facing the Service.</td>
<td>* Develop a better understanding of the Service's mission and mandate, the current challenges it faces, and the key priorities going forward.</td>
</tr>
<tr>
<td>* Support the professional development of Service employees participating in the MDP.</td>
<td>* Acquisition of knowledge and expertise in key aspects of leadership and management.</td>
</tr>
<tr>
<td>* Create opportunities for networking and dialogue.</td>
<td>* Develop a sense of belonging to the MDP community and enhance the collective leadership ability of MDP participants.</td>
</tr>
</tbody>
</table>

8:45 to 9:15  Opening remarks — ADH, John Gillies
9:15 to 10:45 "Innovation in the Service”. A panel presentation and discussion — ADE, CIO &

10:45 to 11:00  Break
11:00 to 12:00 “Understanding Human Resources Services”. A panel presentation and discussion — DG, HRS & DDG, TR
12:00 to 12:45  Lunch
MANAGEMENT DEVELOPMENT PROGRAM (MDP)
Workshop 2015
"Towards an Engaged Workforce"

NHQ Conference Centre

Agenda

Thursday, February 12, 2015

12:45 to 2:15 Simultaneous workshops – Participants attend one of two professional development workshops where they will learn useful tools and strategies applicable to their work environments.

<table>
<thead>
<tr>
<th>Workshop A</th>
<th>Workshop B</th>
</tr>
</thead>
<tbody>
<tr>
<td>Difficult conversations</td>
<td>Change Management</td>
</tr>
<tr>
<td>Leaders: ICMS</td>
<td></td>
</tr>
</tbody>
</table>

2:15 to 2:30 Break

2:30 to 4:00 Simultaneous workshops – Participants attend a second workshop as outlined above.

<table>
<thead>
<tr>
<th>Workshop A</th>
<th>Workshop B</th>
</tr>
</thead>
<tbody>
<tr>
<td>Difficult conversations</td>
<td>Change Management</td>
</tr>
<tr>
<td>Leaders: ICMS</td>
<td></td>
</tr>
</tbody>
</table>

4:00 to 4:30 Individual reflection and discussion on question, “What have I learned today?”

4:30 to 5:00 Presentation of ideas to ADH Gillies. Discussion facilitated by

End of Day
MANAGEMENT DEVELOPMENT PROGRAM (MDP)
Workshop 2015
“Towards an Engaged Workforce”
NHQ Conference Centre

Agenda

Friday, February 13, 2015

8:15 to 8:30 Recap of Day 1 and Overview of Day 2
8:30 to 9:00 “A View from the Bridge” – Michel Coulombe, Director
9:00 to 12:00 “A Path to Wake Up, Grow Up and Show Up”. A presentation in plenary.

<table>
<thead>
<tr>
<th>Workshop</th>
</tr>
</thead>
<tbody>
<tr>
<td>Presentation and discussion</td>
</tr>
<tr>
<td>Leader</td>
</tr>
</tbody>
</table>

12:00 to 12:30 Lunch
12:30 to 1:30 “Employee engagement” A presentation in plenary – DDG, IAB
1:30 to 2:30 “What to expect as an Executive”, Panel presentation and discussion.
2:30 to 2:45 Break
2:45 to 3:15 Individual reflection and discussion on question, “What am I going to do differently as a result of this workshop?”
3:15 to 4:00 Presentation of ideas to Director Coulombe. Discussion facilitated by

| Evaluation |

4:00 to 4:15
4:15 to 5:15 Graduation Ceremony for first graduates of the MDP. Meet and greet with the Director and members of the Executive Committee.
Atelier Programme de perfectionnement en gestion (PPG)

Background :
Les thèmes de l'ordre du jour furent développés en lien avec les priorités stratégiques et les attentes des participants face à cet atelier. Les participants du programme désirent profiter de l'atelier pour réseauter et pouvoir apprendre des expériences des autres gestionnaires.

Le portrait actuel du PPG
68 participants
45 AR (66% des participants sont des agents de renseignements)
28 Femmes & 40 Hommes

Suggestions :
• MDP is a 5-year program in which activities aim to develop key competencies in leadership but participants remain responsible for their own development
• Highlight the importance & efficiency of mentoring as a learning activity: more than 75% of MDPers are paired with an EX, the others will be paired shortly

Veuillez prendre note que nous avons effectué un sondage auprès de notre clientèle PPG, savoir ce qu'ils s'attendaient sur cet atelier. Certaines de ces questions ont été soulevées et seront possiblement posées lors de cet atelier.
• Postes réservés seulement pour les participants du programme pour les affectations ou transfert
• Opportunité de détachement : est-ce qu'il y a une possibilité d'en avoir davantage ?
• L'importance des critères linguistiques: pourquoi que nous n'exigeons pas les mêmes critères linguistiques, CEB, pour tous les superviseurs dans l'organisation ?

Directeur

Suggestion de points à couvrir pour votre présentation :
• Les attentes du Service envers les futurs leaders : l'importance de leur rôle dans le développement de la relève.
• Période de probation pour les cadres : un mécanisme pour le développement des cadres qui s'inscrit dans la modernisation, EX Performance Agreement. SVP prendre note que les participants du programme ont reçu l'information par courriel à ce sujet.

Questions soulevées par les participants du programme lors de notre sondage :
• Les impacts suite aux réorganisations récentes tant au niveau des Directions, Sections ou Régions.
• Défis dans la livraison de notre mandat dans le contexte fiscal actuel.
• Mise à jour des défis et priorités auxquels fait face le Service.
MANAGEMENT DEVELOPMENT PROGRAM (MDP)
Workshop 2015
"Towards an Engaged Workforce"

NHQ Conference Centre

Agenda
February 13, 2015

4:15 to 5:15 Graduation Ceremony for first graduates of the MDP.
Le présent atteste que

Nom

a réussi le

Programme de perfectionnement

en gestion (PPG)

Sous-directeur général, AP, Perfectionnement des employés
This is to certify that

Name

has successfully completed the Management Development Program (MDP)

Deputy Director General, Employee Development
This is to certify that

Name

has successfully completed the
Management Development Program (MDP)

February 13, 2015

Deputy Director General, LD, Employee Development
Management Development Program (MDP)
Workshop 2015
"Towards an Engaged Workforce"

NHQ Conference Centre

Agenda

Thursday, February 12, 2015

8:00 to 8:30  Arrival and registration of participants
8:30 to 8:45  Words of welcome — DDG, LD, Employee Development

<table>
<thead>
<tr>
<th>OBJECTIVES</th>
<th>EXPECTED RESULTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Provide an update on the challenges and priorities facing the Service.</td>
<td>• Develop a better understanding of the Service’s mission and mandate, the current challenges it faces, and the key priorities going forward.</td>
</tr>
<tr>
<td>• Support the professional development of Service employees participating in the MDP.</td>
<td>• Acquisition of knowledge and expertise in key aspects of leadership and management.</td>
</tr>
<tr>
<td>• Create opportunities for networking and dialogue.</td>
<td>• Develop a sense of belonging to the MDP community and enhance the collective leadership ability of MDP participants.</td>
</tr>
</tbody>
</table>

8:45 to 9:15  Opening remarks — John Gillies, ADH
9:15 to 10:45  "Innovation in the Service", A panel presentation and discussion — John Cousineau, ADF, Richard McDonald, CIO &
10:45 to 11:00  Break
11:00 to 12:00  "Understanding Human Resources Services", A panel presentation and discussion — DDG, HRS &
12:00 to 12:45  Lunch
MEMORANDUM TO THE DIRECTOR

MINISTERIAL BRIEFING
25 February 2015, 16:00-16:45

- At the first of a new series of monthly bilateral meetings with the Minister you may wish to raise the following items: the proposed overall approach to Ministerial Direction, CSIS’ duty of candour and the EX conference [TAB 1].
- The note also provides additional information with regard to SIRC’s jurisdiction to consider allegations raising issues of law including those pertaining to the Charter.

1. Renewal of Ministerial Direction:

2. Duty of Candour:
SIRC later issued a report in September 2010 saying they had the right to rule on Charter issues.

Implications:
3. Executive Conference: A letter seeking Ministerial support for a CSIS executive conference will be transmitted to the Minister's office shortly [TAB 5]. The letter will identify the costs [TAB 6].

As a result, the Service is seeking Ministerial authorization to hold an executive conference in 2015. In order to continue to respect fiscal constraints, the conference would be held at the facility, be shorter in duration (1.5 days), and no outside speakers would attend. The cost estimate for this year's conference is approximately — which includes all meals, accommodations, and travel. A memorandum seeking the Minister’s approval will be conveyed to the Minister’s office.

As always, please do not hesitate to contact me should you require further information.

__________________________
Tom Venner
Assistant Director Policy and Strategic Partnership

Enclosures:
Tab 1: Agenda
Tab 2: Proposed Framework for Renewal of Ministerial Direction
Tab 3: October 2014 Memo to Minister on SIRC Annual Report
Tab 4: CSIS letter to PCO on Duty of Candour
Tab 5: Draft Memo to Minister on Ex Conference
Tab 6: Cost Breakdown for Ex Conference
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.
MEETING WITH PUBLIC SAFETY MINISTER

FEBRUARY 25, 2015

AGENDA ITEMS

1. Overall Approach to Ministerial Direction flowing from new legislation (further to SraPol briefing on February 23, 2015)

2. SiRC (duty of candour) (further to PMO / PCO questions and Service response)

3. CSIS Executive Conference 2015
ISSUE:

Though CSIS publicly agreed with the recommendations published in the Security Intelligence Review Committee’s 2013-2014 Annual Report regarding two separate investigations into the revocation of Security Clearances, the cases raise a number of questions regarding the Service’s role in SIRC’s investigation of complaints.

BACKGROUND:

On December 10, 2013, SIRC issued a classified report in a complaint regarding the revocation of a Security Clearance that caused a loss of employment. SIRC upheld the decision and dismissed the complaint. However, SIRC indicated that CSIS’ duty of disclosure extends beyond producing documents for review and includes proactively presenting the most relevant pieces of evidence to the Committee member, and criticized the Service for not having done so in this case.

On January 21, 2014, SIRC issued its final report in a complaint regarding the revocation of a secret clearance and reliability status. The report concluded that “there were reasonable grounds under the Policy on Personnel Security for the revocation of the Complainant’s security clearance.” The complaint was dismissed.

The report was, however, extremely critical of how the Service dealt with information regarding a whose reliability was in question. The Member said that:

- the Committee was seriously misled on this matter as the Service’s report that discredits the allegation against the complainant was not presented to the Committee;
- the Service demonstrated a lack of candour with respect to the information presented in this report to the Committee;
- the Service did not demonstrate an acceptable level of disclosure when it failed to provide the Committee with this report, but rather argued that the report was available at the Service.

The report made two recommendations:

1) That the Service provide the Committee with a detailed update on all the changes and initiatives applicable to security clearance assessments undertaken pursuant to the 2009 DDO Directional Statement on rigour (this has been sent to SIRC);

2) That the Service issue a policy directive to all personnel about the importance of the duty of proactive candour in proceedings before the Committee.

In a letter dated 7 March 2014, CSIS advised SIRC that it accepted the recommendations and provided to SIRC a detailed description of the relevant initiatives. Further, on 17 July 2014, CSIS issued a notice to all CSIS Employees regarding the duty of candour, this in relation to criticisms levied by both SIRC and the Federal Court.
DISCUSSION:

The issue of ‘duty of disclosure to the Committee,’ also raised in the context of another complaint summarized in the annual report, raises a fundamental question regarding the Service’s role in a SIRC investigation in which it must both support SIRC and defend itself.

In accordance with standard procedures, CSIS identifies documents containing the individual’s name or file number and prepares a package for disclosure to SIRC. The disclosure package is made available to SIRC counsel on Service premises. In addition to reviewing the disclosure provided by CSIS, while on the premises, SIRC counsel has direct access to CSIS reporting and may request additional documents. In parallel, CSIS prepares its own defence, generally also on the basis of the same documents disclosed to SIRC.

It appears, however, that SIRC is relying on the Service’s review and exhibits without informing the Service of what it believes are the relevant issues or conducting its own independent investigation to determine what is relevant. This is evidenced by the following statement: “The Service’s duty of disclosure to the Committee goes beyond producing documents for the Committee’s review. It also includes the duty to present the most relevant pieces of evidence proactively before any Presiding Member.”

NEXT STEPS:

The Service is of the view that successful resolution would include either of the following approaches, wherein SIRC reads everything that is disclosed by the Service early in the process, or identifies additional issues it wishes to investigate along the period of the review so that relevant Service information may be provided to SIRC.

SIRC’s 2013-2014 Annual Report provides an opportunity to clarify the issues of the Service’s duty of disclosure, and is the subject of ongoing discussions with SIRC.
MÉMOIRE AU MINISTRE

RAPPORT ANNUEL DU COMITÉ DE SURVEILLANCE DES ACTIVITÉS DE RENSEIGNEMENT DE SÉCURITÉ DE 2013-2014

SOMMAIRE

• Le Comité de surveillance des activités de renseignement de sécurité (CSARS) vous a récemment présenté son Rapport annuel de 2013-2014, lequel renferme des résumés non classifiés des études des activités du Service canadien du renseignement de sécurité (SCRS) ainsi que les conclusions d’enquêtes menées à la suite de plaintes formulées contre le SCRS.

CONTEXTE

En vertu de l'article 53 de la Loi sur le SCRS, le CSARS vous présente un Rapport annuel des activités qu’il a menées lors du dernier exercice. Vous êtes tenu de présenter le rapport au Parlement dans un délai de quinze jours de séance.


ANALYSE

En prenant à sa charge certaines fonctions de l’ancien Inspecteur général du SCRS en 2012, le CSARS a signalé l’éventuelle difficulté de conserver une relation d’indépendance nécessaire et
de vous informer au sujet du rendement du Service, y compris grâce au processus de certification annuel. Dans son rapport de cette année, le CSARS mentionne que contrairement à ses premières préoccupations, ses relations plus fréquentes avec vous et le Ministère ont renforcé son rôle et, par extension, la reddition de comptes au sein du système. Une fois de plus, le CSARS souligne les défis que représente l'examen général des activités relatives à la sécurité nationale du Canada et mentionne qu'il a présenté sa propre proposition en vue d'un vaste examen indépendant en vertu duquel il pourrait examiner les activités d'autres ministères lorsqu'elles se rapportent au SCRS.

Le CSARS affirme qu'il est entièrement satisfait du rapport du directeur du SCRS pour 2013-2014, précisant que les activités décrites dans le document « sont conformes à la Loi sur le SCRS et aux directives ministérielles, et constituent un exercice raisonnable et nécessaire des pouvoirs du Service. » Il ajoute également que les activités décrites dans le rapport du directeur correspondent aux tâches et aux fonctions énoncées aux articles 12 à 20 de la Loi sur le SCRS. Le CSARS suggère toutefois que les opérations à l'étranger du Service et les enquêtes réalisées en vertu de l'article 16 auraient dû être décrites avec plus de minutie.

Le Service a indiqué au CSARS que le lecteur trouvera beaucoup d'informations sur les opérations à l'étranger et les enquêtes réalisées en vertu de l'article 16 à travers le rapport du directeur. Le rapport est organisé en fonction des priorités du gouvernement du Canada en matière de renseignement. En structurant le rapport selon les secteurs d'activité, les régions géographiques ou les articles de la Loi sur le SCRS, le Service aurait de la difficulté à résumer ses activités de manière pertinente et cohérente. En outre, le Service a précisé que certaines activités relatives à l'article 16 peuvent ne pas être signalées en termes explicites étant donné des chevauchements fréquents avec des exigences de l'article 12.

Dans la plupart de ses études, le CSARS est satisfait de la façon dont le SCRS a mené ses activités en fonction de son mandat. Il souligne toutefois deux études qui ont soulevé des points qu'il a jugés si importants qu'il vous a envoyé directement des rapports, conformément à l'article 54 de la Loi sur le SCRS. Le premier point traite des changements dans l'utilisation, par le Service, d'informations recueillies à des fins de filtrage de sécurité.

Le second point qui a donné lieu à un rapport (article 54) traite du soutien aux opérations et de son utilisation à l'étranger, en portant particulièrement attention à la gestion du programme d'armes à feu du SCRS et à sa reddition de comptes. Vous vous rappellerez qu'en mai 2014, je vous avais signalé cette étude du CSARS. J'avais expliqué la politique et le cadre décisionnel du Service et mis en évidence les cas où le ministre avait été informé à ce sujet.
Le CSARS déclare qu'il a éprouvé des difficultés dans son travail avec le SCRS, en mentionnant notamment lorsqu'il a fallu obtenir l'ensemble des informations, mais le SCRS a œuvré avec diligence pour entretenir sa relation de travail efficace avec le CSARS et s'efforcera de poursuivre cette collaboration au cours de l'année. Jusqu'à présent, le Service a répondu à presque toutes les recommandations du CSARS. Le Service cherchera également à donner suite à certaines recommandations, au besoin, dans son attachement à une culture d'amélioration de l'organisation, et toute question se rapportant aux communications qui émanera de la publication du rapport sera traitée rapidement selon les mécanismes et procédures en place. L'addition des réponses du Service dans le rapport du CSARS (rendue possible par un nouvel outil de suivi développé conjointement par le Service et le CSARS) est certainement une nouveauté utile.

Comme toujours, n'hésitez pas à communiquer avec moi si vous souhaitez obtenir de plus amples informations.

Michel Coulombe

Pièce jointe
Annexe : Sommaire des études du CSARS, 2013-2014

c.c. Conseiller à la sécurité nationale
Sous-ministre, Sécurité publique

Le présent document peut faire l'objet d'une exception aux termes de la Loi sur l'accès à l'information ou de la Loi sur la protection des renseignements personnels. On pourra également s'opposer à la communication des informations ou des renseignements qu'il contient en vertu de la Loi sur la preuve au Canada. Ces informations ou renseignements ne doivent être ni communiqués ni utilisés comme preuve sans consultation préalable du Service canadien du renseignement de sécurité.
EX CONFERENCE 2015 (Exec attending)
Complex

<table>
<thead>
<tr>
<th>CONFERENCE FEES</th>
<th>Nights / days</th>
<th>Price/Night</th>
<th>EX TOTAL</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hotel Rooms</td>
<td>2</td>
<td>$167.00</td>
<td>$334.00</td>
<td>max. within budget</td>
</tr>
<tr>
<td>Meals included for travelers (Breakfast, lunch</td>
<td>2</td>
<td>$10.50</td>
<td>$21.00</td>
<td>meals included</td>
</tr>
<tr>
<td>Meals included for travelers (Breakfast, dinner)</td>
<td>5</td>
<td>$17.25</td>
<td>$86.25</td>
<td>per person</td>
</tr>
<tr>
<td>Meals included for travelers (Breakfast, dinner, lunch)</td>
<td>3</td>
<td>$50.50</td>
<td>$151.50</td>
<td>per person</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Meal Breaks</th>
<th>Nights / days</th>
<th>Price</th>
<th>EX TOTAL</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Morning coffee break</td>
<td>2</td>
<td>$360.00</td>
<td>$720.00</td>
<td>per person</td>
</tr>
<tr>
<td>Lunch break</td>
<td>2</td>
<td>$30.00</td>
<td>$60.00</td>
<td>per person</td>
</tr>
<tr>
<td>Afternoon coffee break</td>
<td>2</td>
<td>$160.00</td>
<td>$320.00</td>
<td>per person</td>
</tr>
<tr>
<td>Dinner for Tuesday</td>
<td>5</td>
<td>$50.00</td>
<td>$250.00</td>
<td>per person</td>
</tr>
</tbody>
</table>

| Guest Speakers | No fees |

<table>
<thead>
<tr>
<th>TRAVEL COSTS FOR EX IN REGIONS / POSTS</th>
<th>Business</th>
<th>Executive</th>
<th>Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vancouver</td>
<td>Business</td>
<td>$5</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Executive</td>
<td>$5</td>
<td></td>
</tr>
<tr>
<td></td>
<td>$5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Edmonton</td>
<td>Business</td>
<td>$5</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Executive</td>
<td>$5</td>
<td></td>
</tr>
<tr>
<td></td>
<td>$5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Paris</td>
<td>Business</td>
<td>$5</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Executive</td>
<td>$5</td>
<td></td>
</tr>
<tr>
<td></td>
<td>$5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>London</td>
<td>Business</td>
<td>$5</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Executive</td>
<td>$5</td>
<td></td>
</tr>
<tr>
<td></td>
<td>$5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Toronto</td>
<td>Business</td>
<td>$5</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Executive</td>
<td>$5</td>
<td></td>
</tr>
<tr>
<td></td>
<td>$5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Halifax</td>
<td>Business</td>
<td>$5</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Executive</td>
<td>$5</td>
<td></td>
</tr>
<tr>
<td></td>
<td>$5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Washington</td>
<td>Business</td>
<td>$5</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Executive</td>
<td>$5</td>
<td></td>
</tr>
<tr>
<td></td>
<td>$5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Quebec</td>
<td>Business</td>
<td>$5</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Executive</td>
<td>$5</td>
<td></td>
</tr>
<tr>
<td></td>
<td>$5</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Notes:**

- **Cost of Hotel is an estimate at $199 per night.**
- **Meals included are estimated at $20 per person.**
- **The meal break estimates are based on the cost of $15 per person.**
TO: DIRECTOR
FROM: ADH

BRIEFING NOTE

SUBJECT: OFFICE OF THE CHIEF HUMAN RESOURCES OFFICER (OCHRO), FALL CLUSTER TALENT MANAGEMENT REVIEW MEETING

INFORMATION:

The Office of the Chief Human Resources Officer (OCHRO), Treasury Board Secretariat (TBS), has invited you to participate in a Deputy Head cluster review discussion on talent management that will take place at 269 Laurier Avenue, 10th Floor, on Monday, March 2, 2015. The meetings have been organized by functional community groupings, where possible. There will be five Cluster Review groupings: Security, Science, Central Services, and two Blended groups. These groupings were piloted during the Fall 2014 Cluster Reviews and were well received. In addition, Associate Deputy Ministers are invited to attend an alternate cluster grouping as an observer.

As discussed and supported by Public Service Management Advisory Committee (PSMAC) on January 16, 2015, the format of the Winter Cluster Reviews will be modified to enable more emphasis on ADM's where clear actions are needed and a tailored discussion on ADM succession management.

The March 2 discussion with the Security Group will be chaired by Mr. Daniel Watson, Chief Human Resources Officer, TBS. The meeting itself is expected to last 6 hours. Also invited are Deputy Heads from Public Safety Canada (PS), Correctional Service Canada (CSC), Canada Border Services Agency (CBSA), Department of National Defence (DND), Royal Canadian Mounted Police (RCMP), and the Communication Security Establishment of Canada (CSEC).

A copy of the draft agenda is attached for your reference. As well, upon arrival at the meeting, you will receive a preloaded tablet, for your use during the meeting, with a copy of the ADM Community Dashboard, ADM Demographic Overview, ADM Talent Map Placement, ADM profiles, and the Succession Planning Document.
Due to the sensitive nature of the ADM Feeder Pool list and the ADM Areas to Develop list, OCHRO will hand deliver these documents to you, for our eyes only, in advance of the meeting. This information will also support in your preparation for the scheduled meeting.

**CSIS INVOLVEMENT:**

The meeting will begin with a brief overview of the ADM community, followed by three main areas of discussion:

In the first part of the meeting, the key objective will remain the same as previous years: to have ADMs known by more Deputy Heads. However, this year’s discussion will be organized by talent map placement meaning that all ADMs with the same talent map placement will be discussed at the same time (Ready for Advancement first, followed by Ready for Movement, then Corporate Support and finally, Well-Placed in Role or Develop in Current Role). Note that she is in a secondment position with CBSA.

In the afternoon, the meeting will shift to discussion of ADM Succession Management. For the Security Clusters, to build on the discussions in the Fall, conversation will start with the core national security positions. For the Service, the DDO, ADO, ADT, ADS, ADI, ADC, ADP and EX DIR (ITAC) positions have been identified. Deputy Heads will be asked to identify potential successors by referring to the following questions:

- What are the key characteristics for the position? (two or three)
- What are the names (if any) of people within their organization who could take on these jobs now? What about within 2 years?
- Are there individuals from other organizations who could be a good fit?
- In what timeframe would they be ready?
- If they are not ready now, what do they need to develop to become ready?

As requested, a brief description of the roles of certain key senior EX positions is listed in Appendix A.

The last portion of the meeting will be a discussion on next steps to support the development of Aboriginal Executives who have longer-term potential to become ADMs. The group will briefly review the individuals identified during the Fall Cluster Reviews and signal if there are other individuals to add to the list.
Appendix A. Brief Description of Roles of Key Senior EX Positions

ADT

The ADT provides leadership of the overall CSIS technology portfolio and incorporates operational and business insight to transform the Service’s technological activities and assets - with the goal of continuously improving business operations.

Key responsibilities include oversight for:

- activities related to information and telecommunications systems, records management, and client services,
- scientific and technological capabilities
- a diverse range of specialized functions
  each of which assist the Service in carrying out its mandate.

Key attributes for the role include:

- Extensive knowledge of applied technology best practices in a security environment,
- Demonstrated experience leading transformational change,
- Demonstrated leadership competencies including strategic thinking, engagement, people management, financial management, and action management.

ADS

The ADS supports the Deputy Director, Operations (DDO) with the overall management of the Service’s national security screening program.

Key responsibilities include oversight for:

- strategic guidance in regards to ADM-level engagement internally and externally with partner departments and agencies, including Canada Border Services Agency (CBSA) and Citizenship and Immigration Canada (CIC),
- representing the program at the operational level and providing detailed and strategic advice on deployment of the screening program’s resources and potential re-allocations, and
- providing advice with respect to wider Government of Canada legislation and policy developments, as required.

Key attributes for the role include:

- Extensive knowledge of national security screening policies and procedures.
- Demonstrated experience managing partnerships and relationships across government, and
- Demonstrated leadership competencies including strategic thinking, engagement, people management, financial management, and action management.

**EX DIR (ITAC)**

The main role of the EX DIR (ITAC) is to oversee the production of accurate, relevant and timely threat assessments on terrorism.

Key responsibilities include oversight for:

- managing the Integrated Terrorism Assessment Centre (ITAC), a community-based organization located at CSIS national headquarters in Ottawa, that is staffed by representatives from the following federal organizations: Public Safety Canada, the Canada Border Service Agency, Communications Security Establishment Canada, the Department of National Defence, Transport Canada, the Correctional Service of Canada, the Financial Transactions and Reports Analysis Centre of Canada, Public Works and Government Services Canada, the Royal Canadian Mounted Police, the Canada Revenue Agency and the Canadian Security Intelligence Service.

Key attributes for the role include:

- Extensive knowledge of the intelligence and security environment,
- Demonstrated experience managing partnerships and relationships, and
- Demonstrated leadership competencies including strategic thinking, engagement, people management, financial management, and action management.

**ADP**

The ADP supports the Director and, through him, the Minister, in their accountability for the overall operational activities of the Service and provides strategic policy advice to the Director and Executive.

Key responsibilities include oversight for:

- all external and internal communications requirements and programs of the Service,
- ensuring the Service is in a constant state of operational preparedness and prepared to respond to, and recover from, an emergency or critical incident,
- acting as the Service's liaison with the Security Intelligence Review Committee (SIRC) and the Office of the Inspector General (IG),
- civil and criminal litigation case management, including those related to the Immigration and Refugee Protection Action (IRPA) and the Access to Information and Privacy Act (ATIP),
- coordinating and supporting the development of Service policies and procedures, and domestic arrangements (Memoranda of Understanding),
- the overall coordination and development of most strategic-level policy issues within the Service, and
- managing foreign relations matters, including visits from foreign agencies to CSIS, travel abroad by CSIS Executives, arrangements with foreign partners, agency profiles and précis, conscious relationships and official passports/visas for CSIS employees.

Key attributes for the role include:

- Extensive knowledge of the intelligence and security environment, the Government of Canada machinery and policy community,
- Demonstrated experience managing partnerships and relationships, and
- Demonstrated leadership competencies including strategic thinking, engagement, people management, financial management, and action management.
WINTER CLUSTER REVIEWS  
SAFETY AND SECURITY CLUSTER  

March 2, 2015  
Duration: 10:00 am – 4:00 pm  
269 Laurier Avenue West, 10th floor, Executive Boardroom

PARTICIPANTS
CHAIRPERSON
- Daniel Watson, Chief Human Resources Officer, Treasury Board of Canada Secretariat

CLUSTER PARTICIPANTS
- Luc Portelance, President, Canada Border Services Agency
- Michel Coulombe, Director, Canadian Security Intelligence Service
- Greta Bossenmaier, Chief, Communications Security Establishment Canada
- Don Head, Commissioner, Correctional Service Canada (absent)
- Gérald Cossette, Director, Financial Transactions and Reports Analysis Centre of Canada (absent)
- Christine Hogan, Deputy Minister of International Trade, Foreign Affairs, Trade and Development Canada
- John Forster, Deputy Minister, National Defence
- Richard Fadden, National Security Advisor, Privy Council Office - National Security Advisor Office
- François Guimont, Deputy Minister, Public Safety Canada
- Bob Paulson, Commissioner, Royal Canadian Mounted Police (absent)

SUPPORT
- Coleen Volk, Deputy Secretary to the Cabinet, Privy Council Office
- Janine Sherman, Assistant Secretary to the Cabinet, Secretariat of Senior Personnel, Privy Council Office
- Susan MacGowan, Visiting ADM, Treasury Board of Canada Secretariat (absent)
- Réa McKay, Senior Director, ADM Collective Management, Treasury Board of Canada Secretariat
- Nadine Lemery, Manager, ADM Collective Management Operations, Treasury Board of Canada Secretariat
<table>
<thead>
<tr>
<th>Time</th>
<th>Agenda Item</th>
<th>Speaker</th>
</tr>
</thead>
<tbody>
<tr>
<td>10:00am-10:05am</td>
<td>A. Introduction: Objectives and Approach</td>
<td>D. Watson</td>
</tr>
<tr>
<td>10:05am-10:15am</td>
<td>B. ADM Demographic Overview</td>
<td>D. Watson</td>
</tr>
<tr>
<td></td>
<td>The Chief Human Resources Officer will provide an overview of the ADM Community as a whole, as well as highlight the key findings for the Cluster.</td>
<td></td>
</tr>
<tr>
<td>10:15am-12:45pm</td>
<td>C. Overview of the ADM Community</td>
<td>Deputy Heads</td>
</tr>
<tr>
<td></td>
<td>Deputy Heads will discuss the ADMs based on their Talent Map Placement, addressing each ADM's strengths, areas for development, and progress since last year as well as specific questions tailored to each Talent Map Placement:</td>
<td>Moderator: D. Watson</td>
</tr>
<tr>
<td></td>
<td>• Ready for Advancement — For what types of positions?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Ready for Movement — To where? To develop what?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Corporate Support — What type of support?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Well-Placed &amp; Develop in Role — Who is ready for promotion, if required?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Transition to Retirement — When?</td>
<td></td>
</tr>
<tr>
<td>12:45pm-1:15pm</td>
<td>Working Lunch</td>
<td>Deputy Heads</td>
</tr>
<tr>
<td>1:15pm-3:30pm</td>
<td>D. ADM Succession Management</td>
<td>Deputy Heads</td>
</tr>
<tr>
<td></td>
<td>Deputy Heads will discuss the specific characteristics for their ADM positions and identify pools of potential successors:</td>
<td>Moderator: D. Watson</td>
</tr>
<tr>
<td>3:30pm-3:55pm</td>
<td>E. Discussion on Under Represented Groups – Aboriginal Executives</td>
<td>Deputy Heads</td>
</tr>
<tr>
<td></td>
<td>Deputy Heads will discuss next steps in supporting the development of Aboriginal Executives, particularly those with potential to reach the ADM level.</td>
<td>Moderator: D. Watson</td>
</tr>
<tr>
<td>3:55pm-4:00pm</td>
<td>F. Wrap Up and Next Steps</td>
<td>D. Watson</td>
</tr>
</tbody>
</table>
BACKGROUND NOTE: BILL C-44

NOTE: The following information is for background.
MEMORANDUM TO THE MINISTER

REQUEST FOR APPROVAL OF THE CONFERENCE 
FOR CSIS EXECUTIVES

ISSUE:
The Canadian Security Intelligence Service (CSIS) requests approval for the Conference for CSIS Executives.

BACKGROUND:
In the past, the Service has held an annual conference for all CSIS Executives that brings together managers from across Canada and its international posts to re-establish corporate links, to communicate and discuss corporate priorities and to participate in annual planning and strategic discussions. This conference is critical for Service cohesiveness given the geographic dispersion of the Executive cadre.

By bringing together our Executives we are able to ensure a shared vision going forward, a common understanding of key initiatives and future plans, while reinforcing consistent management perspectives and practices. Again this year, there are many important corporate issues to address, such as particularly in light of events over the past few months. Past conferences have proven very effective in addressing these types of issues. The conference will be held taking advantage of this space while removing our Executives from the CSIS building to allow everyone to focus without the competing demands of daily business.

DISCUSSION:
The Service did not hold an annual executive conference this past year as we decided to try a bi-annual conference approach as a cost saving measure. While no firm conclusion has been reached about the bi-annual approach, not having an executive conference last year has served to highlight the view of gathering our Executives together. Accordingly we are seeking your

Unofficial English version
Accompanies official French Memorandum,
signed by Director of CSIS
support to hold an executive conference. We have changed the proposed approach for the 2015 conference, eliminating outside speakers, and reducing the length of the event, all in the interest of reducing costs.

The conference also offers us the opportunity to achieve efficiencies by organizing a number of other essential meetings that otherwise we would have to hold at other times (for example, Regional Director General’s Meeting).

The cost estimate for this year’s conference is which includes meals, accommodations, and travel. Great care was taken during the planning phase to ensure expenses were contained.

If you agree, we recommend that this year’s conference be held for 1.5 days. Each year we endeavour to limit costs, and the Service ensures that alcohol is not paid for with public funds.

RECOMMENDATION:

It is recommended that the Request for the Conference for CSIS Executives be approved.

If approved, the Minister is required to sign this Memorandum.

As always, please do not hesitate to contact me should you require further information.

Michel Coulombe

☐ I approve
☐ I do not approve

The Honorable Steven Blaney, P.C., M.P.
Minister of Public Safety and Emergency Preparedness

Date

Enclosure (1)

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

Unofficial English version
Accompanies official French Memorandum, signed by Director of CSIS
Evidence Act. The information or intelligence must not be disclosed or used as evidence without prior consultation with the Canadian Security Intelligence Service.