

Court File No. T-1492-17

**FEDERAL COURT**

**BETWEEN:**

**BRITISH COLUMBIA CIVIL LIBERTIES ASSOCIATION**

Applicant

- and -

**ATTORNEY GENERAL OF CANADA**

Respondent

---

**CERTIFIED TRIBUNAL RECORD**  
**Volume XVIII**

---

TOP SECRET (with attach)

T-1492-17

**FEDERAL COURT**

BETWEEN:

**BRITISH COLUMBIA CIVIL LIBERTIES ASSOCIATION**

Applicant

- and -

**ATTORNEY GENERAL OF CANADA**

Respondent

---

**CERTIFICATE**


(Rule 318 of the *Federal Courts Rules*)

---

I, Josée Décosse, Registrar at the Security Intelligence Review Committee, hereby certify that the attached list of documents with the Addendum formed part of SIRC's record in preparing its report, dated May 30, 2017, in the matter of a complaint filed by the Applicant pursuant to section 41 of the *Canadian Security Intelligence Service Act* (File no. 1500-481), which is at issue in these proceedings.

This Certificate and the attached list were prepared in accordance with this Honourable Court's Order dated January 26, 2018 and Direction dated November 19, 2018 with respect to the transmission of the Certified Tribunal Record.

Dated at OTTAWA, this November 27, 2018.

  
\_\_\_\_\_  
Josée Décosse  
Registrar



## LIST OF DOCUMENTS (WITH ADDENDUM) IN 1178-17/2 FILE

TOP SECRET

Document # and page #	TITLE	DATE	DOCUMENT WITHHELD
	<b>CORRESPONDENCE PART I</b>		
1 pp. 1-42	Complaint submitted by Champ & Associates on behalf of BCCLA, against CSIS pursuant to section 41 of the CSIS Act	February 06, 2014	N/A
2 pp. 43-44	Letter to Paul Champ informing him of the procedures regarding a complaint under section 41 (1) of the CSIS Act	February 14, 2014	N/A
3 pp. 45	Letter to Paul Champ concerning the complaint of BCCLA and requesting an update on whether his client has received a response from the Director	March 18, 2014	N/A
4 pp. 46-48	Fax from Paul Champ further to SIRC's letter of March, informing SIRC that CSIS has failed to provide any substantive response to his complaint	March 20, 2014	N/A
5 pp. 49-50	Letter from Paul Champ further to SIRC's letter of March, informing SIRC that CSIS has failed to provide any substantive response to his complaint	March 20, 2014	N/A
6 pp. 51-52	Letter to Paul Champ providing him with the opportunity to make additional representations regarding SIRC's jurisdiction	March 28, 2014	N/A
7 pp. 53-158	Letter to [REDACTED] informing him of the complaint by BBCLA, providing CSIS with the opportunity to make representation on SIRC's jurisdiction.	March 28, 2014	N/A
8 pp. 159-161	Fax from Paul Champ making representations on SIRC's jurisdiction.	April 4, 2014	N/A
9 pp. 162	Letter from Stephanie Dion informing us that CSIS does not wish to make any representations on SIRC's jurisdiction at this point.	April 7, 2014	N/A
10 pp. 163-164	Letter to P. Champ informing him that on May 27, 14, the SIRC determined that it does have the jurisdiction to investigate	June 2, 2014	N/A
11 pp. 165	Letter to S. Dion informing her that on May 27, 14, the SIRC determined that it does have the jurisdiction to investigate	June 2, 2014	N/A
12 pp. 166	Letter from Paul Champ requesting information from CSIS is not productive and that he prefers to request a summons for a CSIS witness	June 24, 2014	N/A
13 pp. 167	Letter to Paul Champ informing him that the above-noted matter has been assigned to Hon. Y. Fortier	September 8, 2014	N/A
14 pp. 168	Letter to Paul Champ informing him that procedural issues or requests can be raised with the presiding member at the pre-hearing conference.	July 4, 2014	N/A
15 pp. 169	Letter to Stephanie Dion informing her that the above-noted matter has been assigned to Hon. Y. Fortier	September 8, 2014	N/A

## LIST OF DOCUMENTS (WITH ADDENDUM) IN 1178-17/2 FILE

TOP SECRET

16 pp. 170-171	Letter from Stephanie Dion making suggestions that certain issues be investigated as part of the complaint by BCCLA.	September 24, 2014	N/A
17 pp. 172-174	Fax from Paul Champ further to letter dated Sept. 8, 2014, object to appointment of the Hon. Yves Fortier.	September 25, 2014	N/A
18 pp. 175-177	Letter from Clayton C. Ruby saying that he's against the appointment of Yves Fortier to lead the investigation	October 7, 2014	N/A
19 pp. 178-179	Letter to Paul Champ giving him instruction regarding the file.	October 8, 2014	N/A
20 pp. 180-182	Fax from Paul Champ further to the presiding member's direction dated Oct. 8, 2014, regarding the complaint's conflict of interest concerns	October 29, 2014	N/A
21 pp. 183-185	E-mail from Sylvie Roussel to Yves Fortier.	November 5, 2014	Solicitor-Client Privilege
22 pp. 186-187	E-mail from Yves Fortier to Sylvie Roussel.	November 24, 2014	Solicitor-Client Privilege
23 pp. 188	E-mail from Sylvie Roussel to Yves Fortier.	November 24, 2014	Solicitor-Client Privilege
24 pp. 189-191	E-mail from Sylvie Roussel to Yves Fortier concerning modifications to a letter enclosing letter from Paul Champ	October 28, 2014	Solicitor-Client Privilege
25 pp. 192	Letter to Paul Champ on behalf of the Hon. Yves Fortier informing him that he has never occupied any position with TransCanada nor Enbridge	November 25, 2014	N/A
26 pp. 193-194	Fax from Paul Champ letting know that BCCLA is prepared to proceed before Hon. Fortier.	December 09, 2014	N/A
27 pp. 195-196	E-mail from Nathalie Theriault to Yves Fortier enclosing a fax from Paul Champ	December 15, 2014	N/A
28 pp. 197	E-mail from Sylvie Roussel to Michael Doucet entitled "Récusation".	December 15, 2014	Solicitor-Client Privilege
29 pp. 198-218	Letter from Paul Champ to inquire as to the status of the complaint BCCLA + encl. additional records disclosed under the Access to Information Act.	March 25, 2015	N/A
30 pp. 219-326	Registrar's Binder - British Columbia Civil Liberties Association (BCCLA) - 05-20-2015	May 20, 2015	Solicitor-Client Privilege
31 pp. 327	Memo to file regarding BCCLA PHC dates.	March 30, 2015	N/A
32 pp. 328-329	Letter from Stephanie Dion, Counsel for CSIS, concerning a complaint against CSIS Pursuant to section 41 of the CSIS Act.	July 8, 2015	N/A

## LIST OF DOCUMENTS (WITH ADDENDUM) IN 1178-17/2 FILE

TOP SECRET

33 pp. 330	Memo to File concerning Pre-hearing conference for BCCLA	April 8, 2015	N/A
34 pp. 331	Memo to File regarding BCCLA response to Champ letter and ex-parte pre-hearing conference.	April 9, 2015	N/A
35 pp. 332-333	E-mail exchange with Stephanie Dion, Counsel for CSIS.		N/A
36 pp. 334-335	E-mail exchange with the Honourable Yves Fortier concerning pre-hearing conference.		Deliberative Privilege
37 pp. 336-346	Letter from Paul Champ in a complaint by BCCLA + encl. copy of a letter to SIRC copies of Memorandum to the Director		N/A
38 pp. 347	E-mail exchange with court reporter Noel Keeley.		N/A
39 pp. 348	E-mail from Stephanie Dion, Counsel for CSIS.		N/A
40 pp. 349-350	Letter from St��phanie Dion, counsel for CSIS, concerning a complaint against CSIS pursuant to section 41 of the CSIS Act.		N/A
41 pp. 351-352	E-mail exchange with Paul Champ concerning location of hearing.		N/A
42 pp. 353-354	Operator Assisted Service confirmation for teleconference.		N/A
43 pp. 355-356	E-mail from St��phanie Dion, counsel for CSIS, regarding witnesses for the in camera portion of hearing.		N/A
44 pp. 357	E-mail to The Honourable Yves Fortier concerning BCCLA pre-hearing conference.		Deliberative Privilege
45 pp. 358	E-mail exchange with The Honourable Yves Fortier concerning documentation related to BCCLA.		Deliberative Privilege
46 pp. 359-369	Memorandum to Yves Fortier + encl. copies of 7 letters and redacted copies of SIRC Study 2008-02 and 2012-02		Deliberative + Solicitor-Client Privilege
47 pp. 370	E-mail from Noel Keeley to confirm his attendance for May 20, 2015 pre-hearing conference.		N/A
48 pp. 371	E-mail from Paul Champ concerning hearing in BCCLA Complaint.		N/A

## LIST OF DOCUMENTS (WITH ADDENDUM) IN 1178-17/2 FILE

TOP SECRET

49 pp. 372-374	Letter to Paul Champ + encl. agenda for the pre-hearing conference of May 20, 2015.		N/A
50 pp. 375	Letter to St�phanie Dion, Counsel for CSIS + encl. agenda for the pre-hearing conference of May 20, 2015.		N/A
51 pp. 376	E-mail to the Honourable Yves Fortier concerning teleconference of May 20, 2015.		Solicitor-Client Privilege
52 pp. 377-378	E-mail to the Honourable Yves Fortier concerning a letter to be prepared after teleconference of May 20, 2015.		Solicitor-Client Privilege
53 pp. 379-381	Letter to Mr. Paul Champ and same letter to Ms. Stephanie Dion, counsel for CSIS concerning pre-hearing conference to be held on May 20, 2015.		N/A
54 pp. 382-393	E-mail to the Honourable Yves Fortier + encl. Pre-hearing speaking notes, Agenda and letter dated May 15, 2015		Solicitor-Client Privilege
55 pp. 394-404	E-mail to Sylvie Roussel + encl. Vetted speaking notes, vetted agenda and vetted letter dated May 15, 2015.		Solicitor-Client Privilege
56 pp. 405-406	E-mail from the Honourable Yves Fortier concerning notes for the pre-hearing conference for BCCLA complaint.		Solicitor-Client Privilege
57 pp. 407	E-mail to Karolyne Ch�n��r concerning copies of studies to be prepared for the Honourable Yves Fortier.		Solicitor-Client Privilege
58 pp. 408	E-mail exchange with Paul Champ concerning a letter dated May 15, 2015.		N/A
59 pp. 409-413	Memo to file and Memorandum concerning the Use of Vancouver Hearing Facilities.		N/A
60 pp. 414	E-mail concerning arrangements for the hearings of August 13 and 14, 2015.		N/A
61 pp. 415	E-mail to Stephanie Dion, Counsel for CSIS concerning hearings of August 13 and 14, 2015.		N/A
62 pp. 416	E-mail to Paul Champ concerning hearings of August 13 and 14, 2015.		N/A
63 pp. 417	E-mail to Noel Keeley concerning pre-hearing conference transcripts.		N/A
64 pp. 418	E-mail to Melissa Netley concerning hearing room request for Vancouver Federal Court.		N/A
65 pp. 419-423	E-mail exchange with Melissa Netley concerning hearing room request for Vancouver Federal Court + encl. memo to visiting Boards.		N/A

## LIST OF DOCUMENTS (WITH ADDENDUM) IN 1178-17/2 FILE

TOP SECRET

66 pp. 424	E-mail exchange with Melissa Netley concerning hearing room request for Vancouver Federal Court.		N/A
67 pp. 425	E-mail to Melissa Netley concerning hearing to be held in Vancouver Federal Court.		N/A
68 pp. 426-430	E-mail to Melissa Netley + encl. signed contract for Vancouver Federal Court hearing.		N/A
69 pp. 431-434	Letter to Stéphanie Dion, Counsel for CSIS + encl. Pre-hearing transcript (copy 4 of 6) and c.c. to ER&L (copy 5 of 6 and CD).		N/A
70 pp. 435	E-mail from Melissa Netley concerning media policy of the Vancouver Federal Court,		N/A
71 pp. 436-437	E-mail exchange with Melissa Netley concerning media during hearing to be held in Vancouver Federal Court.		N/A
72 pp. 438	E-mail to Noel Keeley concerning upcoming hearings.		N/A
73 pp. 439	E-mail from Melissa Netley concerning hearing to be held in Vancouver Federal Court.		N/A
74 pp. 440-441	E-mail exchange with the Honourable Yves Fortier concerning Hearing to be held in Vancouver Federal Court.		N/A
75 pp. 442-443	Letter to Stéphanie Dion, Counsel for CSIS, concerning hearing in Vancouver.		N/A
76 pp. 444-445	Letter to Paul Champ concerning hearing in Vancouver.		N/A
77 pp. 446-447	Senior Counsel notes to file.		N/A
78 pp. 448-449	Letter from Stéphanie Dion, Counsel at CSIS, concerning witness for the in camera hearing of August 13 and 14.		N/A
79 pp. 450-468	E-mail exchange with Paul Champ + encl. Will Say statements for five of the six witnesses.		N/A
80 pp. 469	E-mail exchange with the Honourable Yves Fortier concerning witnesses Will Says and extension request from the complainant's counsel		Deliberative Privilege
81 pp. 470	E-mail exchange with Stephanie Dion, Counsel for CSIS concerning an extension of time request and witness information.		N/A
82 pp. 471	E-mail to Paul Champ concerning the last Will Say to be filed.		N/A

## LIST OF DOCUMENTS (WITH ADDENDUM) IN 1178-17/2 FILE

TOP SECRET

83 pp. 472-474	E-mail exchange with Stephanie Dion, Counsel for CSIS, concerning transcript of the May 20, 2015 pre-hearing conference.		N/A
84 pp. 475-477	Letter to Paul Champ + encl. Transcript of Pre-hearing teleconference held on May 20, 2015 (Copy 6 of 6).		N/A
85 pp. 478-486	E-mail from Paul Champ + encl. two additional Will Says for hearing of August.		N/A
86 pp. 487	E-mail to Paul Champ concerning a complaint pursuant to section 41 of the CSIS Act.		N/A
87 pp. 488-490	Memo to Chantelle Bowers concerning the transition of the file.		Solicitor-Client Privilege
88 pp. 491	Letter to Stephanie Dion, Counsel for CSIS + encl. copy of letter dated June 18, 2015 and copy of letter dated June 26, 2015 with ex parte witnesses Will Says (For the Complainant).		N/A
89 pp. 492	Memo to file BCCLA-Aug 12th court; CSIS extension request.		N/A
90 pp. 493	Letter from Paul Champ + encl. 5 copies of the complainant's Book of documents (in two volumes)		N/A
91 pp. 494-497	Letter from Stephanie Dion, Counsel for CSIS concerning Topics that will be addressed in the Ex Parte.		N/A
92 pp. 498	E-mail exchange with Stephanie Dion, Counsel for CSIS, concerning Ex Parte hearing.		N/A
93 pp. 499	E-mail exchange with the Honourable Yves Fortier concerning hearing in Vancouver.		N/A
94 pp. 500-504	Letter to Stéphanie Dion + encl. Complainant's book of documents vol. 1 and 2 (copy 4 of 5 - c.c. to ER&L with copy 5 of 5)		N/A
95 pp. 505	E-mail exchange with the Honourable Yves Fortier concerning an extension of time request by the Service to produce their Book of documents.		N/A
96 pp. 506	E-mail to Stephanie Dion, Counsel for CSIS, concerning extension of time to produce their Book of documents.		N/A
<b>CORRESPONDENCE PART II</b>			
1 pp. 507	E-mail exchange with Melissa Netley concerning Contract for Vancouver Federal Court.		N/A
2 pp. 508	E-mail exchange with Melissa Netley concerning hearing in Vancouver.		N/A

## LIST OF DOCUMENTS (WITH ADDENDUM) IN 1178-17/2 FILE

TOP SECRET

3 pp. 510	E-mail to Paul Champ concerning date modification for hearing in August.		N/A
4 pp. 511	E-mail to Stephanie Dion, Counsel for CSIS, concerning date modification for hearing in August.		N/A
5 pp. 512	E-mail to Noel Keeley concerning date modification for hearing in August.		N/A
6 pp. 513-514	E-mail exchange with Julie Gordon concerning date modification and accommodation for hearing in August.		N/A
7 pp. 515-522	Contract and E-mail exchange with Julie Gordon of Vancouver Federal Court.		N/A
8 pp. 523	E-mail from Cynthia Bouchard to Diane Marion concerning hearing in Vancouver.		N/A
9 pp. 524-525	E-mail from Paul Champ + encl. letter from Paul Champ to Shayna Stawicki dated July 14, 2015.		N/A
10 pp. 526-527	E-mail exchange with Paul Champ concerning documentation to be provided by CSIS and to update the file.		N/A
11 pp. 528-537	Letter from Stephanie Dion, Counsel for CSIS + encl. 5 copies of CSIS unclassified Book of documents.		N/A
12 pp. 538-539	E-mail exchange with Paul Champ concerning CSIS Book of documents.		N/A
13 pp. 540-541	E-mail exchange with the Honourable Yves Fortier concerning a case management conference.		Deliberative Privilege
14 pp. 542-543	Letter to Paul Champ + encl. copy 5 of 5 of CSIS Book of documents.		N/A
15 pp. 544	E-mail exchange with the Honourable Yves Fortier concerning Case management teleconference.		Deliberative Privilege
16 pp. 545-546	E-mail exchange with Stephanie Dion, Counsel for CSIS, concerning a case management conference to be held on July 24th.		N/A
17 pp. 547-548	E-mail exchange with Paul Champ concerning case management teleconference.		N/A
18 pp. 549-550	E-mail exchange with the Honourable Yves Fortier concerning transcript of May 20, 2015 pre-hearing conference.		Deliberative Privilege
19 pp. 551-553	Letter to the Honourable Yves Fortier + encl. Transcript of pre-hearing conference of May 20, 2015 (copy 2 of 5).		N/A



## LIST OF DOCUMENTS (WITH ADDENDUM) IN 1178-17/2 FILE

TOP SECRET

20 pp. 554	Email exchange with Honourable Yves Fortier concerning Witness Question.		Deliberative Privilege
21 pp. 555	Email to Stephanie Dion concerning Witness Enquiry.		N/A
22 pp. 556	Letter from Paul Champ + encl. Form 1803 Summons to Witness & Complainant's Supplementary Book of Documentation.		N/A
23 pp. 557-558	Email exchange with the Honourable Yves Fortier concerning Summons for Witness.		Deliberative Privilege
24 pp. 559-560	Email exchange with the Honourable Yves Fortier concerning Complainant's Supplementary Book of Documents.		Deliberative Privilege
25 pp. 561-562	E-mail exchange with Melissa Netley concerning hearing in Vancouver.		N/A
26 pp. 563-564	Email exchange with Paul Champ concerning the order of Witnesses.		N/A
27 pp. 565-566	E-mail exchange with Melissa Netley concerning security concerns for hearing in Vancouver.		N/A
28 pp. 567	E-mail to Paul Champ concerning Complainant's Supplementary Book of Documents.		N/A
29 pp. 568-569	Letter to Stephanie Dion with enclosed copy of Complainant's Supplementary Book of Documents for the hearing scheduled August 12-14, 2015.		N/A
30 pp. 570-573	Letter to Paul Champ with encl. Summons to Witness.		N/A
31 pp. 574-575	Letter to Stephanie Dion with enclosed copy of transcript of the case management teleconference held on July 24, 2015.		N/A
32 pp. 576-577	Letter to Stephanie Dion with enclosed copy of redacted transcript of the case management teleconference held on July 24, 2015.		N/A
33 pp. 578	Email exchange with Stephanie Dion concerning redacted transcript of the case management teleconference held on July 24, 2015.		N/A
34 pp. 580-581	E-mail exchange with Stephanie Dion concerning Complainant's Supplementary Book of Documents.		N/A
35 pp. 582-584	Letter to Paul Champ with enclosed redacted copy of transcript of the case management teleconference held on July 24, 2015.		N/A
36 pp. 585	E-mail exchange with the Honourable Yves Fortier concerning date for the ex parte hearing.		Solicitor-Client Privilege



## LIST OF DOCUMENTS (WITH ADDENDUM) IN 1178-17/2 FILE

TOP SECRET

37 pp. 586-587	Memo to file concerning Whitaker's affidavit.		N/A
38 pp. 588	Memo to file.		Solicitor-Client Privilege
39 pp. 589	Memo to file concerning ex parte.		N/A
40 pp. 590-591	Letter to Stephanie Dion, Counsel for CSIS + encl. transcript (copy 4 of 6, copy 5 of 6 to ER&L+ CD) of the in camera hearing.		N/A
41 pp. 592	E-mail exchange with Stephanie Dion, Counsel for CSIS concerning extension request made by the Complainant's Counsel.		N/A
42 pp. 593	E-mail exchange with Paul Champ concerning extension request.		N/A
43 pp. 594-595	E-mail + encl. letter from Paul Champ concerning Reg Whitaker affidavit.		N/A
44 pp. 596-640	E-mail from Paul Champ and response + encl. Affidavit of Reg Whitaker.		N/A
45 pp. 641-644	Letter to Stephanie Dion, Counsel for CSIS + encl. Affidavit of Reg Whitaker.		N/A
46 pp. 645-652	Letter from St��phanie Dion, Counsel for CSIS + encl. redactions in the transcript of the hearing held on August 12 and 13, 2015.		N/A
47 pp. 653	Email from Shayna Stawicki. Transcript volume 2 has a new non classified version.		N/A
48 pp. 654-656	Letter to Stephanie Dion, Counsel for CSIS + encl. redacted copy of transcript (volume 2) of the in camera hearing held on August 12-13, 2015.		N/A
49 pp. 657-659	Letter to Paul Champ + encl. redacted copies of transcripts volume 1 and 2 (copy 6 of 6) of the in camera hearing held on August 12-13, 2015.		N/A
50 pp. 660-662	Letter from Stephanie Dion, Counsel for CSIS concerning cross-examination of a witness.		N/A
51 pp. 663	Memo to file concerning cross-examination of the 7th witness.		N/A
52 pp. 664	Memo to file concerning ex parte hearing dates.		N/A
53 pp. 665	Note to file concerning ex parte hearing.		N/A

## LIST OF DOCUMENTS (WITH ADDENDUM) IN 1178-17/2 FILE

TOP SECRET

54 pp. 666	E-mail from Stéphanie Dion, Counsel for CSIS, concerning availability for ex parte hearing.		N/A
55 pp. 667	E-mail exchange concerning an E-mail from CSIS related to their availability for ex parte hearing.		Deliberative Privilege
56 pp. 668-670	E-mail exchange with the Honourable Yves Fortier related to Teleconference follow-up.		N/A
57 pp. 671	Memo to File related to October 27, 2015 teleconference with the Honourable Yves Fortier.		Solicitor-Client Privilege
58 pp. 672	Memo to File related to BCCLA Ex parte.		Solicitor-Client Privilege
59 pp. 673	Letter from Stéphanie Dion, Counsel for CSIS related to the ex parte hearing.		N/A
60 pp. 674	E-mail exchange with Stéphanie Dion, Counsel for CSIS, related to additional documents that have been uploaded into SIRC's Ringtail case		N/A
61 pp. 675-676	E-mail exchange with [REDACTED] to set up a briefing.		N/A
62 pp. 677-679	Letter from Stéphanie Dion, Counsel for CSIS + encl. SIRC Complaint Worksheet.		N/A
63 pp. 680	Letter from Stéphanie Dion, Counsel for CSIS + encl. summaries of anticipated evidence of [REDACTED]		N/A
64 pp. 681	Letter to Paul Champ regarding ex parte questions		N/A
65 pp. 682	E-mail exchange with Chantelle Bowers related to BCCLA Hearing.		Solicitor-Client Privilege
66 pp. 683	Letter to Stéphanie Dion confirming ex parte hearing		N/A
67 pp. 684-685	E-mail exchange with [REDACTED] related to documentation to be filed.		N/A
68 pp. 686	Letter from Stéphanie Dion, Counsel for CSIS + encl. 5 copies each of CSIS's Books of documents (Volumes 1A, 1B, 1C, 2 and 3).		N/A
69 pp. 687-688	FW: 1500-481: Ex parte questions overdue		Solicitor-Client Privilege
70 pp. 689	E-mail to Paul Champ related to Ex Parte questions.		N/A

## LIST OF DOCUMENTS (WITH ADDENDUM) IN 1178-17/2 FILE

TOP SECRET

71 pp. 690	E-mail to the Honourable Yves Fortier related to Ex Parte questions.		Deliberative Privilege
72 pp. 691	E-mail from the Honourable Yves Fortier related to Ex Parte questions.		Deliberative Privilege
73 pp. 692	Memo to file related to a teleconference with the Honourable Yves Fortier.		Deliberative Privilege
74 pp. 693-694	Letter from Stéphanie Dion, Counsel for CSIS [REDACTED]		N/A
75 pp. 695-696	Memo to file.		Deliberative Privilege
76 pp. 697	Memo to file related to [REDACTED] and add witness.		Deliberative Privilege
77 pp. 698	E-mail to Stéphanie Dion, Counsel for CSIS to advise that the new documents sent to SIRC on February 2, 2016 as been entered as Exhibit CSIS 9A		N/A
78 pp. 699-701	Letter to Stéphanie Dion + encl. in camera/ex parte transcript.		N/A
79 pp. 702-703	E-mail exchange with the Honourable Yves Fortier related to file dates for hearing.		Deliberative Privilege
80 pp. 704	Memo to file related to last witness hearing dates.		Deliberative Privilege
81 pp. 705	E-mail from Stéphanie Dion, Counsel for CSIS about witness availability for March 23, 2016.		N/A
82 pp. 706	E-mail to Stéphanie Dion, Counsel for CSIS related to hearing of March 23, 2016.		N/A
83 pp. 707-708	E-mail exchange with the Honourable Yves Fortier related to the date of the ex parte hearing.		Deliberative Privilege
84 pp. 709	E-mail exchange with Stéphanie Dion, Counsel for CSIS related to the new date for the ex parte hearing.		N/A
85 pp. 710	Letter to Stéphanie Dion confirming in camera / ex parte hearing.		N/A
86 pp. 711	Internal e-mail related to willsays.		Solicitor-Client Privilege
87 pp. 712-713	Letter to [REDACTED] + encl. electronic in camera ex parte transcript.		N/A

88 pp. 714-716	Letter from Stéphanie Dion, Counsel for CSIS + encl. the Summary of anticipated evidence of [REDACTED]		N/A
	<b>CORRESPONDENCE PART III</b>		
1 pp. 717-723	Letter to Stéphanie Dion + encl. ex parte transcript.		N/A
2 pp. 724	Internal email related to a letter to be sent to CSIS with the summary of evidence (SOE).		Solicitor-Client Privilege
3 pp. 725-728	Letter to Stéphanie Dion + encl. copy of Summary of evidence (SOE) for vetting.		N/A
4 pp. 729	Email exchange with Stéphanie Dion, Counsel for CSIS related to the Summary of Evidence.		N/A
5 pp. 730-732	Letter from Stéphanie Dion, Counsel for CSIS, related to the wording of the Summary of evidence (SOE).		N/A
6 pp. 733-734	Email exchange with the Honourable Yves Fortier related to a teleconference about the Summary of Evidence (SOE).		Deliberative Privilege
7 pp. 735	Memo to file related to a teleconference with the Honourable Yves Fortier about Summary of evidence (SOE) vetting.		Deliberative Privilege
8 pp. 736-741	Summary of Evidence (SOE)		N/A
9 pp. 742-748	Letter to Stéphanie Dion + encl copy of Summary of evidence (SOE) for vetting.		N/A
10 pp. 749-750	Email exchange with Stéphanie Dion, Counsel for CSIS, related to the Summary of evidence (SOE) to be sent out to the Complainant's Counsel.		N/A
11 pp. 751	Internal email exchange related to the Summary of evidence to be sent out to the complainant's Counsel.		Solicitor-Client Privilege
12 pp. 752	Email to Stéphanie Dion, Counsel for CSIS, related to the Summary of evidence (SOE) sent to the complainant's counsel.		N/A
13 pp. 753-758	Vetted Summary of Evidence (SOE)		N/A
14 pp. 759-760	Letter to Paul Champ + encl. a copy of the vetted statement of evidence (SOE).		N/A
15 pp. 761	Letter to Stéphanie Dion regarding final submissions.		N/A

## LIST OF DOCUMENTS (WITH ADDENDUM) IN 1178-17/2 FILE

TOP SECRET

16 pp. 762-763	Fax from Bijon Roy + attached letter to request an extension of time to file the complainant's final written representations.		N/A
17 pp. 764-765	Email exchange with the Honourable Yves Fortier related to an extension request from the complainant's counsel to file final submissions.		Deliberative Privilege
18 pp. 766-767	Email exchange with Stephanie Dion, counsel for CSIS related to an extension request from the complainant's counsel to file final submissions.		N/A
19 pp. 768	Email to Bijon Roy to advise him that his extension request has been granted by the presiding member.		N/A
20 pp. 769-770	Email from Paul Champ + attached letter related to final submissions.		N/A
21 pp. 771	Letter from Paul Champ + encl. final submissions and book of authorities.		N/A
22 pp. 772	Email to Paul Champ to acknowledge receipt of his email and attached letter dated September 19, 2016.		N/A
23 pp. 773-775	Letter to Stephanie Dion + encl. final submissions and book of authorities.		N/A
24 pp. 776-777	Email exchange with Stephanie Dion, counsel for CSIS related to final submissions from the complainant's counsel.		N/A
25 pp. 778	Email exchange with the Honourable Yves Fortier related to the complainant's submissions.		Solicitor-Client Privilege
26 pp. 779	Letter from St��phanie Dion, counsel for CSIS + encl. 5 copies each of CSIS's classified, unclassified final submissions and Book of authorities.		N/A
27 pp. 780	Email from Stephanie Dion, counsel for CSIS related to submissions.		N/A
28 pp. 781	Email exchange with the Honourable Yves Fortier related to submissions from CSIS.		Solicitor-Client Privilege
29 pp. 782-788	Letter to Paul Champ + encl. final submissions.		N/A
30 pp. 789	Email to Stephanie Dion, counsel for CSIS, on the complainant's final rebuttal submissions.		N/A
31 pp. 790	Email to Bijon Roy to acknowledge receipt of his email and rebuttal submissions of the complainant.		N/A
32 pp. 791-799	Email from Paul Champ + encl. copy of letter and complainant's final rebuttal submissions.		N/A

## LIST OF DOCUMENTS (WITH ADDENDUM) IN 1178-17/2 FILE

TOP SECRET

33 pp. 800	Letter from Bijon Roy + encl. 5 copies of complainant's final rebuttal submissions.		N/A
34 pp. 801-807	Complainant's rebuttal submissions.		N/A
35 pp. 808	Letter to Bijon Roy & Paul Champ regarding final submissions.		N/A
36 pp. 809-816	Letter to Stephanie Dion regarding Final Submission.		N/A
37 pp. 817	Internal email exchange related to the complainant's final rebuttal submissions.		Deliberative + Solicitor-Client Privilege
38 pp. 818	Email exchange with the Honourable Yves Fortier related to the status of a complaint file.		Deliberative + Solicitor-Client Privilege
39 pp. 819-820	Email from Linda Tucci, Executive assistant to the Honourable Yves Fortier related to a conference call to be scheduled.		Deliberative + Solicitor-Client Privilege
40 pp. 821-822	Email exchange with Linda Tucci, executive assistant to the Honourable Yves Fortier to confirm a conference call.		Deliberative + Solicitor-Client Privilege
41 pp. 823	Memo to file related to a conference call with the Honourable Yves Fortier.		Deliberative + Solicitor-Client Privilege
42 pp. 824-826	(TS) Letter from Stephanie Dion, counsel for CSIS, about the Service's position with respect to paragraph 17 of the Respondent's Rebuttal submissions.		N/A
43 pp. 827-828	(Protected) Letter from Stephanie Dion, counsel for CSIS, about the Service's position with respect to paragraph 17 of the Respondent's Rebuttal submissions.		N/A
44 pp. 829	Letter to Paul Champ Re : final rebuttal submissions		N/A
45 pp. 830-886	BCCLA Final Report- Signed by Fortier on May 30, 2017 CLASSIFIED		N/A
46 pp. 887-890	Email from Bijon Roy RE: Response to December 23, 2016 letter		N/A

## LIST OF DOCUMENTS (WITH ADDENDUM) IN 1178-17/2 FILE

TOP SECRET

47 pp. 891-894	Email to Yves Fortier RE: correspondance received by Bijon Roy		Solicitor-Client Privilege
48 pp. 895-898	Letter to Stephanie Dion regarding Final correspondence.		N/A
49 pp. 899	Internal email exchange related to the status of the file.		Solicitor-Client Privilege
50 pp. 900	Internal email related to a meeting in Montreal with the Honourable Yves Fortier about a complaint file.		Solicitor-Client Privilege
51 pp. 901-903	Internal email exchange related to a meeting to be held in Montreal with the Honourable Yves Fortier in a complaint file.		Deliberative + Solicitor-Client Privilege
52 pp. 904	Email exchange with the Honourable Yves Fortier related to a meeting to be held in Montreal in a complaint file.		Deliberative + Solicitor-Client Privilege
53 pp. 905-906	Email exchange with the Honourable Yves Fortier related to a meeting to be held in Montreal in a complaint file.		Deliberative + Solicitor-Client Privilege
54 pp. 907	Memo to file. Status Check.		Deliberative + Solicitor-Client Privilege
55 pp. 908	Memo related to the final report modifications.		Deliberative + Solicitor-Client Privilege
56 pp. 909-910	Email exchange related to changes in the Final Report.		Deliberative + Solicitor-Client Privilege
57 pp. 911	Email related to the procedure for the footnotes for the Final Report.		Deliberative + Solicitor-Client Privilege
58 pp. 912	Letter to Stephanie Dion encl final report for vetting		N/A
59 pp. 913-915	Email exchange related to the preparation of the Final Report.		Solicitor-Client Privilege



## LIST OF DOCUMENTS (WITH ADDENDUM) IN 1178-17/2 FILE

TOP SECRET

60 pp. 916-917	Letter to Paul Champ Re status of final report		N/A
61 pp. 918-977	Letter enclosing CSIS's proposed redactions of the report		N/A
62 pp. 978-980	Internal email exchange regarding a telephone meeting between the counsel and the member.		Deliberative + Solicitor-Client Privilege
63 pp. 981-983	Email exchange regarding a meeting between SIRC and Justice.		N/A
64 pp. 984	Email to Stéphanie Dion (Justice) related to Chantelle's meeting.		N/A
65 pp. 985	Letter from Stephanie Dion related to the review of vetting for national security concerns of the Final Report.		N/A
66 pp. 986-987	Email exchange regarding the process of completing the review of the proposed redactions to the final report.		N/A
67 pp. 988	Letter to Paul Champ & Bijon Roy + encl. final report BCCLA		N/A
68 pp. 989	Letter to Minister Ralph Goodale encl Final Report		N/A
69 pp. 990	Letter to Director of CSIS David Vigneault encl final report		N/A
70 pp. 991-1047	Final Report - Declassified.		N/A
71 pp. 1048	Letter to Bijon Roy - Counsels response - Final report remains as is		N/A
	<b>TRANSCRIPTS</b>		
	Transcript of In Camera/Ex Parte Hearing held on Thursday, January 28, 2016.	January 28, 2016	N/A
	Transcript of Ex Parte/In Camera hearing (no. 2), held on Tuesday, March 22, 2016.	March 22, 2016.	N/A
	Transcript of Pre-hearing Teleconference held on Wednesday May 20, 2015,	May 20, 2015,	N/A
	Transcript of Case Management Conference held on Friday July 24, 2015,	July 24, 2015,	N/A
	Redacted Transcript of the Case Management Teleconference held on July 24, 2015	July 24, 2015	N/A
	Transcript (Volume 1) of In Camera Hearing, held on Wednesday, August 12, 2015, at Vancouver BC.	August 12, 2015	N/A



## LIST OF DOCUMENTS (WITH ADDENDUM) IN 1178-17/2 FILE

TOP SECRET

Transcript (Volume 2) of In Camera Hearing, held on Thursday, August 13, 2015, at Vancouver BC.	August 13, 2015	N/A
Redacted Transcript (Volume 2) of In Camera Hearing, held on Thursday, August 13, 2015, at Vancouver, BC	August 13, 2015	N/A
<b>BOOK OF DOCUMENTS</b>		
CSIS's Book of Documents vol. 5 - Ex parte hearing.	January 28, 2016	N/A
	February 4, 2016	N/A
Complainant's Book of Documents Volume I of II.	July 8, 2015	N/A
Complainant's Book of Documents Volume II of II.	July 8, 2015	N/A
CSIS Book of Documents - In Camera hearing.	July 17, 2015	N/A
Complainant's Supplementary Book of Documents.	August 5, 2015	N/A
SIRC Book of documents.	August 12, 2015	N/A
CSIS's Book of Documents vol. 1A - Ex Parte hearing.	December 4, 2015	N/A
CSIS's Book of Documents vol. 1B - Ex Parte hearing.	December 4, 2015	N/A
CSIS's Book of Documents vol. 1C - Ex Parte hearing.	December 4, 2015	N/A
CSIS's Book of Documents vol. 2 - Ex Parte hearing.	December 4, 2015	N/A
CSIS's Book of Documents vol. 3 - Ex Parte hearing.	December 4, 2015	N/A
CSIS's Book of authorities.	October 17, 2016	N/A
Respondent's classified (Top secret) submissions.	October 17, 2016	N/A
Respondent's (Protected B) submissions.	October 17, 2016	N/A
Complainant's book of authorities.	September 20, 2016	N/A
Complainant's final submissions.	September 20, 2016	N/A
<b>ADDENDUM</b>		
CSIS's Book of Documents vol. 4 - Ex parte hearing.	December 4, 2015	N/A

Revised 2018-11-21

TOP SECRET INFORMATION  
Ex Parte/In Camera Hearing  
File No. 1500-481

THE SECURITY INTELLIGENCE REVIEW COMMITTEE  
COMITÉ DE SURVEILLANCE DES ACTIVITÉS DE RENSEIGNEMENT  
DE SÉCURITÉ

CASE NO. 146

IN THE MATTER of a Complaint filed by The British  
Columbia Civil Liberties Association, pursuant to  
Section 41 of the *Canadian Security Intelligence*  
*Service Act, R.S.C. 1985, c. C-23*

BETWEEN:

British Columbia Civil Liberties Association  
Complainant

- and -

THE CANADIAN SECURITY INTELLIGENCE SERVICE  
Respondent

Transcript of *Ex Parte/In Camera* Hearing (No. 2), held  
on Tuesday, March 22, 2016, at Ottawa, Ontario,  
commencing at 4 p.m.

BEFORE: The Honourable L. Yves Fortier, P.C., C.C.,  
O.Q., Q.C., Presiding Member

(Volume 4A - *Ex Parte*)

Official Court Reporters: Keeley Reporting Services  
Inc.:  
Per: N.C. Keeley, C.S.R.

APPEARANCES

C. Bowers for SIRC  
S. Dion for CSIS

---

Also in Attendance:

[REDACTED] ER&L Representative  
S. Stawicki Hearings Registrar  
Noel C. Keeley, C.S.R. Court Stenographer

---

WITNESSES:

[REDACTED] for CSIS

---

INDEX

WITNESSES:

PAGE NO.

                    Called and Affirmed:

6

Ex.-in-Ch. By Ms. Dion

8

Ex. By Ms. Bowers

29

Ex. By Mr. Fortier (Presiding Member)

47

Redir. by Ms. Dion

52

Preliminary/Procedural Matters:

2

EXHIBITS

NUMBERED/DESCRIPTION:

PAGE NO.

None Filed

UNDERTAKINGS

NUMBERED/DESCRIPTION:

PAGE NO.

None Noted:

1 TOP SECRET:

2 Ex Parte/In Camera Hearing

3 Volume 4A:

4 --- The Hon. L. Yves Fortier, P.C., C.C., O.Q., Q.C.,

5 Presiding Member

6 --- Upon commencing at Ottawa, Ontario, on Tuesday,  
7 March 22, 2016, at 4 p.m.:

8 Preliminary/Procedural Matters:

9 THE PRESIDING MEMBER: Good afternoon,  
10 everyone. We meet yet again. Thank you for being here  
11 today.

12 I am responsible for the fact that we  
13 have an additional witness, someone from the Service  
14 that I felt should be invited to provide evidence in  
15 this File, someone who was not preaching from  
16 Headquarters about what the Service was doing or was  
17 not doing but, rather, someone who had experience on  
18 the ground in B.C., and I am grateful to the Service  
19 for having made this Witness available.

20 (To Ms. Dion): I understand the name  
21 of the Witness is [REDACTED]

22 MS. DION: That's correct, Mr.  
23 Fortier.

24 THE PRESIDING MEMBER: At this time,  
25 we will go through the usual formalities, in accordance

1 with the Outline that Shayna prepares for me, starting  
2 with a reminder to everyone that Subsection 48(1) of  
3 the *CSIS* Act provides that every Investigation of a  
4 Complaint by the Committee "shall be conducted in  
5 private". As such, for reasons of security and  
6 confidentiality, no electronic devices are allowed in  
7 this Hearing Room. This includes cellular telephones,  
8 laptops, tablets, et cetera.

9 I am sure that is well understood by  
10 all of those in attendance here today.

11 I welcome all of you to this Hearing.

12 For the record, I am Yves Fortier, and  
13 I am a Member of the Security Intelligence Review  
14 Committee. I have been selected as the Presiding  
15 Member in the Investigation of the Complaint filed by  
16 the British Columbia Civil Liberties Association, the  
17 BCCLA.

18 For the record, that is Committee File  
19 Number 1500-481, and Committee Case Number 146.

20 We are continuing today the *Ex Parte*  
21 portion of the Hearing.

22 Being veterans of these processes --  
23 not in age but in experience -- you are all aware of  
24 the purpose of an *Ex Parte* Hearing, which is to hear  
25 classified evidence.

1                   These *Ex Parte* Proceedings, as is the  
2 case today, are conducted in the absence of the  
3 Complainant.

4                   The *In Camera* portion of the Hearing,  
5 conducted in the presence of the Complainant, was  
6 conducted last August in Vancouver, on August 12 and  
7 13, 2015, and the first portion of the *Ex Parte* portion  
8 of the Hearing took place a couple of months ago now,  
9 on January 28, 2016.

10                  I have accompanying me today Madam  
11 Chantelle Bowers, Counsel to the Committee; Madam  
12 Shayna Stawicki, the Registrar for the Committee; and,  
13 in the booth behind me, our ever-devoted Court  
14 Reporter, Mr. Noel Keeley.

15                  At this point, I will ask those in  
16 attendance on behalf of the Service to identify  
17 themselves for the record, starting with Madam Dion...

18                  MADAM DION: Yes. Good afternoon, Mr.  
19 Fortier. I am Stéphanie Dion, Counsel for the Canadian  
20 Security Intelligence Service.

21                  [REDACTED]: And I am [REDACTED]  
22 [REDACTED] from ER&L.

23                  THE PRESIDING MEMBER: Thank you.  
24 Maître Dion, I understand you have identified, at my  
25 request, one witness who is going to testify today.

1 MS. DION: That's correct, Mr.  
2 Fortier.

3 THE PRESIDING MEMBER: And how long do  
4 you expect to be in presenting the Witness's testimony?

5 I think you know the matters that I am  
6 preoccupied with and what it is I am after in terms of  
7 this additional evidence.

8 How long do you think you will be in  
9 presenting this evidence?

10 MS. DION: Mr. Fortier, let me say at  
11 the outset that we feel we have provided the evidence  
12 that was necessary to address this Complaint. However,  
13 that being said, we are happy to put [REDACTED] on the  
14 Witness Stand today to testify from a B.C. perspective.

15 I have about ten minutes of questions  
16 for him, following which he will be available to answer  
17 any questions the Committee may have of him in respect  
18 of this Investigation. But my examination of him will  
19 be fairly short.

20 THE PRESIDING MEMBER: Very well.  
21 Thank you, maître Dion.

22 I know that you, Madam Bowers, will  
23 have questions for the Witness and that you may be a  
24 little longer than ten minutes.

25 MS. BOWERS: Yes. Thank you.



1 THE PRESIDING MEMBER: And I, too, may  
2 have some questions for the Witness.

3 With that, we will have [REDACTED]  
4 brought into the Hearing Room...

5 THE REGISTRAR: Yes.

6 --- [REDACTED] Called to the Witness Table)

7 THE PRESIDING MEMBER: Good afternoon,  
8 [REDACTED]

9 At this point, I will ask the  
10 Registrar to swear you in...

11 THE REGISTRAR: Good afternoon, Sir.

12 Do you solemnly affirm that the  
13 evidence you are about to give to the Committee shall  
14 be the truth, the whole truth, and nothing but the  
15 truth?

16 THE WITNESS: I do.

17 [REDACTED] Called and Affirmed:

18 THE REGISTRAR: For the record, would  
19 you please state your full name, spelling your last  
20 name...

21 THE WITNESS: [REDACTED] The  
22 last name is spelled: [REDACTED]

23 THE REGISTRAR: Thank you.

24 Secondly, I would like to read to you  
25 Section 51 of the *Canadian Security Intelligence*

1 Service Act, which provides protection to witnesses  
2 appearing before the Committee.

3 It reads as follows:

4 "Except in a prosecution of a  
5 person for an offence under  
6 section 133 of the Criminal Code  
7 (false statements in extra-  
8 judicial proceedings) in respect  
9 of a statement made under this  
10 Act, evidence given by a person  
11 in proceedings under this Part  
12 and evidence of the existence of  
13 the proceedings are inadmissible  
14 against that person in a court or  
15 in any other proceedings."

16 Do you understand?

17 THE WITNESS: Pretty much. Yes, I do.

18 THE REGISTRAR: Thank you. You may be  
19 seated.

20 THE PRESIDING MEMBER: Good afternoon  
21 again, [REDACTED]

22 You will be questioned initially by  
23 Counsel for the Service, Madam Dion.

24 Madam Dion, your witness...

25 MS. DION: Thank you, Mr. Fortier.

1 Examination-in-Chief by Ms. Dion:

2 Q. Good afternoon, [REDACTED] Thank  
3 you for being here today.

4 I will ask you to start by giving the  
5 Committee an overview of your employment with the  
6 Service?

7 A. Yes. I began my career in 1995,  
8 [REDACTED]

9 One of the happiest days of my life  
10 was when I was told that I was going to start as an  
11 Intelligence Officer with CSIS.

12 [REDACTED]  
13 [REDACTED]  
14 In 1998, I was transferred to B.C.  
15 Region, [REDACTED]

16 [REDACTED]  
17 [REDACTED]  
18 [REDACTED]  
19 [REDACTED]  
20 [REDACTED]  
21 [REDACTED]  
22 [REDACTED]  
23 [REDACTED]  
24 [REDACTED]  
25 [REDACTED]

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25

[REDACTED]

[REDACTED] So, in 2008, we came back to Vancouver,  
where I started as the [REDACTED]  
[REDACTED]

I remained there up until [REDACTED]  
2010, [REDACTED] 2010, I was transferred to  
[REDACTED] as the Head of that  
Unit.

Under that Unit, there are multiple  
responsibilities, [REDACTED]  
[REDACTED]

THE PRESIDING MEMBER: To be more  
precise insofar as your work in the B.C. Region is  
concerned, you were there from 1998 to 2004?

THE WITNESS: Correct.

THE PRESIDING MEMBER: And then in  
2008 ---

When in 2008 did you arrive back in  
B.C. Region?

1 THE WITNESS: I arrived, I believe it  
2 was, [REDACTED] 2008, [REDACTED]  
3 [REDACTED]  
4 [REDACTED]

5 But, that was in Vancouver.

6 THE PRESIDING MEMBER: And you stayed  
7 in Vancouver until 2010?

8 THE WITNESS: No.

9 THE PRESIDING MEMBER: "No".

10 I would like you to be more precise,  
11 then, in terms of the dates.

12 THE WITNESS: Okay. Sorry.

13 I transferred to Vancouver in 2008,  
14 and I have been there ever since.

15 THE PRESIDING MEMBER: You have been  
16 there since?

17 THE WITNESS: Correct.

18 THE PRESIDING MEMBER: Okay. I had  
19 misunderstood you, then. I thought you said that in  
20 [REDACTED] 2010, you were transferred ---

21 Your responsibilities were different?

22 THE WITNESS: That is correct.

23 THE PRESIDING MEMBER: So you have  
24 been in Vancouver with B.C.R. since 2008?

25 THE WITNESS: Correct.

1 THE PRESIDING MEMBER: Okay. Thank  
2 you.

3 THE WITNESS: Where was I...?

4 THE PRESIDING MEMBER: [REDACTED]  
5 [REDACTED]

6 --- (Laughter)

7 THE WITNESS: [REDACTED]  
8 [REDACTED]

9 --- (Laughter)

10 So for now, that would be a bad thing!

11 --- (Laughter)

12 THE PRESIDING MEMBER: Okay. Thank  
13 you.

14 THE WITNESS: So I was the Head of  
15 the...

16 We'll call it the "Domestic Desk", for  
17 ease of reference.

18 I was there until, I believe it was,

19 [REDACTED] 2013, [REDACTED]  
20 [REDACTED]  
21 [REDACTED]  
22 [REDACTED]  
23 [REDACTED]  
24 [REDACTED]  
25 [REDACTED]

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25

[REDACTED]

THE PRESIDING MEMBER: You were Head of the Domestic Desk in Vancouver from when to when?

THE WITNESS: From [REDACTED] 2010 to [REDACTED] 2013.

THE PRESIDING MEMBER: Thank you.

Go ahead, Madam Dion...

MS. DION: Thank you.

Q. When you were the Head of the Domestic Desk, what were some of your responsibilities and the roles that you played as the Head?

A. At the time, we were responsible for overseeing, obviously, the Investigations that fell under our remit. But in terms of tactical day-to-day responsibilities, I had Intelligence Officers under my employ. So a typical day would see an Intelligence Officer coming to me and saying they want to debrief a source. They would give me their Game Plan, their location and when the Interview would be, along with the Interview objectives, and I would give them my blessing. I would add some input, if I had any to give. I would approve Reports as submitted by my Intelligence Officers once the Operational Reports are created following the Source Debriefs.

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25

[REDACTED]

I would be responsible for at least initiating the dialogue with my Chief to put into place Warrant Powers against a Target, if we felt that that was necessary.

In general, I think that's it.

THE PRESIDING MEMBER: Who was the Regional Director for B.C. prior to this new Director "Bob" taking office [REDACTED]

THE WITNESS: Roughly, yes.

The Director-General of the Region?

THE PRESIDING MEMBER: The Director-General.

THE WITNESS: Yes. [REDACTED]

[REDACTED]

THE PRESIDING MEMBER: [REDACTED]

Could you spell that for me?

THE WITNESS: Hopefully, you won't ask me to spell the [REDACTED] part!

The [REDACTED] part, I believe, is spelled [REDACTED]



1 THE PRESIDING MEMBER: That one I can  
2 do myself!

3 [REDACTED]  
4 THE WITNESS: [REDACTED]  
5 [REDACTED]

6 Oh, oh...

7 THE PRESIDING MEMBER: And he was  
8 there, more or less, from when to when?

9 --- (A Short Pause)

10 THE WITNESS: If I can backtrack, I  
11 know for certain that on my arrival in 2008, the  
12 Director-General was [REDACTED] and he  
13 was there, for certain, [REDACTED]  
14 [REDACTED]

15 So I am going to say that [REDACTED]  
16 [REDACTED]

17 THE PRESIDING MEMBER: Just in rough  
18 terms. I am not going to hold you to precise dates.

19 THE WITNESS: [REDACTED] I  
20 would say.

21 THE PRESIDING MEMBER: Okay. Thank  
22 you.

23 MS. DION:

24 Q. You have talked about your  
25 responsibilities as the Head of the Unit; you have

1       talked [REDACTED], about debriefing Human  
2       Sources, and about Warrant Powers.

3                       What would happen if an I.O. wanted to  
4       conduct a Community Interview? Would that go through  
5       you?

6                       A. Yes. Absolutely. It would have  
7       to go through me, yes.

8                       Q. And how many Heads were there for  
9       that particular Unit, the Domestic Desk?

10                      A. [REDACTED]

11                      Q. [REDACTED]

12                      A. [REDACTED]

13                      Q. in your experience, how frequently  
14       does B.C.R., or B.C. Region, conduct Community  
15       Interviews under [REDACTED]

16                      A. [REDACTED]

17 [REDACTED]  
18 [REDACTED]  
19 [REDACTED]  
20 [REDACTED]  
21 [REDACTED]  
22 [REDACTED]  
23                      There is recognition in Headquarters  
24       and at the Regional level that it is a sensitive  
25       Investigation.

1                   When knocking on doors, there is the  
2 risk that it might have some kind of impact on the  
3 civil liberties of individuals, at least perceptually.  
4 The perception may be: *Well, why are we knocking on*  
5 *the door of a [REDACTED]?* Are we  
6 *investigating [REDACTED]?* Why are we knocking  
7 *on the doors of [REDACTED]?* Are they going to  
8 *think that we are investigating [REDACTED]?*

9                   So we had to be very, very careful  
10 when we actually made the decision to go out and do an  
11 Interview, unlike other Investigations, because there  
12 is so much more involved.

13                   THE PRESIDING MEMBER: What is your  
14 shorthand for "Interview"? What was the term that you  
15 used?

16 [REDACTED]

17 THE WITNESS: For the [REDACTED]

18 THE PRESIDING MEMBER: Yes.

19 THE WITNESS: Sorry. That is

20 [REDACTED]  
21 [REDACTED]  
22 [REDACTED]

23 THE PRESIDING MEMBER: So the initials  
24 stand for [REDACTED]

1 THE WITNESS: [REDACTED]  
2 [REDACTED]

3 THE PRESIDING MEMBER: [REDACTED]  
4 [REDACTED]

5 Okay. That is the [REDACTED]

6 MS. DION: [REDACTED]

7 That is something that we covered in  
8 the last Hearing, Mr. Fortier, and that is why I didn't  
9 define the term.

10 If you turn to CSIS-5A, which is  
11 Volume 2, at Tab 3, you will see the [REDACTED] that  
12 we had talked about, which is [REDACTED]  
13 [REDACTED] and in parentheses it is referred to  
14 as [REDACTED]

15 THE PRESIDING MEMBER: Okay. Thank  
16 you.

17 I can't say that I have total recall;  
18 however, it is coming back to me somewhat at this  
19 point.

20 MS. DION: I apologize.

21 THE PRESIDING MEMBER: No, no.

22 (To the Witness): So that is the  
23 [REDACTED]

24 Okay. I have it now. Thank you.  
25 Please continue...

1 THE WITNESS: [REDACTED]  
2 [REDACTED]  
3 [REDACTED]

4 THE PRESIDING MEMBER: Yes. Okay.

5 Thank you.

6 THE WITNESS: [REDACTED]  
7 [REDACTED]  
8 [REDACTED]

9 The decision was made to be very, very careful when we  
10 did go out into the Community.

11 [REDACTED]  
12 [REDACTED]  
13 [REDACTED]  
14 [REDACTED]  
15 [REDACTED]  
16 [REDACTED]  
17 [REDACTED]  
18 THE PRESIDING MEMBER: Thank you.

19 MS. DION:

20 Q. And you understand, [REDACTED]

21 that you are here in the context of a Complaint that  
22 has been filed by the BCCLA alleging that the Service  
23 investigated or monitored individuals linked to a list  
24 of Groups for their opposition to the Northern Gateway  
25 Pipeline.

1 I believe you have the Complaint  
2 Letter in your hand.

3 Is that what you are bringing out?

4 A. Correct, yes.

5 Q. As a Service employee in the B.C.  
6 Region for -- and correct me if I am wrong -- for  
7 fifteen years, how would you respond to these  
8 allegations?

9 A. I guess I would have a short  
10 response and a long response, at your leisure. The  
11 short one is ---

12 THE PRESIDING MEMBER: Give us both.

13 THE WITNESS: All right.

14 The short answer is: No. We're not  
15 in the business of investigating Environmentalists  
16 because they are advocating for an Environmental Cause,  
17 period.

18 The longer one...?

19 THE PRESIDING MEMBER: Yes. Please.

20 --- (A Short Pause)

21 THE WITNESS: I don't know where to  
22 begin.

23 First, as the Supervisor of the  
24 Domestic Unit, I am aware of all actions taken under my  
25 remit.

1 THE PRESIDING MEMBER: Right.

2 THE WITNESS: I have never heard of

3 [REDACTED]  
4 [REDACTED]

5 The other ones, I am aware of through  
6 the Press or through incidental [REDACTED]

7 [REDACTED]  
8 [REDACTED]  
9 [REDACTED]  
10 [REDACTED]  
11 [REDACTED]  
12 [REDACTED]  
13 [REDACTED]  
14 [REDACTED]

15 To take a step back, there are a lot  
16 of mechanisms in place to ensure that we wouldn't be  
17 involved in investigating such Groups. On the macro  
18 level, there is just the Law itself.

19 It is against the Law, against the  
20 CSIS Act, to investigate lawful advocacy, protest or  
21 dissent, unless it is tied directly to a threat.

22 Below that, there are our own  
23 Policies. There are Policies in this regard both in  
24 terms of Human Source Policies [REDACTED]

25 [REDACTED] what one is allowed and not allowed to do with

1 a Source [REDACTED]

2 [REDACTED] There are Policies under the Targeting  
3 aspects limiting, again, our actions in that regard.  
4 There are Directional Statements coming from our  
5 Headquarters. In at least one case that I can  
6 remember, we had a Directional Statement explicitly  
7 saying: *Given the nature of this sensitive*  
8 *Investigation, care must be taken when dealing with*  
9 *Sources and Contacts in this File.*

10 Something like that.

11 And then below that, there is a bit of  
12 a Corporate and Political risk issue, in that we are  
13 always aware of the impact that our Investigations  
14 might have on the perceptions of others, and that is  
15 one of the reasons, as I mentioned before, why we are  
16 so careful in carrying out Interviews.

17 And all of that, combined, mitigates  
18 against our targeting such Groups.

19 If you look at ---

20 I don't know whether it is in that  
21 Binder.

22 [REDACTED]  
23 [REDACTED]  
24 [REDACTED]



1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25

[REDACTED]

THE PRESIDING MEMBER:

[REDACTED]

THE WITNESS:

[REDACTED]

--- (A Short Pause)

What else can I say...?

We've had opportunities to ---

I will give you an example.

[REDACTED]

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25

[REDACTED]

because

that is not what we are about. We are only interested  
in our Targets.

--- (A Short Pause)

I will leave it at that.

1 THE PRESIDING MEMBER: When you say,  
2 in your Summary of Evidence -- which you have signed --  
3 that between 2010 and 2013, you were Supervisor for the  
4 Unit responsible for [REDACTED]

5 THE WITNESS: [REDACTED]  
6 yes.

7 THE PRESIDING MEMBER: Yes.  
8 Could you please tell me what [REDACTED]  
9 [REDACTED] encompasses?

10 THE WITNESS: Okay. That issue would  
11 involve [REDACTED]

12 Well, actually, not even necessarily  
13 so.

14 [REDACTED]  
15 [REDACTED]  
16 and who are willing to use serious violence towards  
17 achieving that end.

18 [REDACTED]  
19 [REDACTED]  
20 [REDACTED]  
21 [REDACTED]  
22 So, to identify such activities and  
23 the people involved in such activities: support  
24 networks; intentions.

25 THE PRESIDING MEMBER: Okay.

1                   We are talking here about events in  
2 British Columbia, one of the many Provinces in Canada  
3 where there is a lot of resource development, to use  
4 shorthand.

5                   You are, and were, familiar with the  
6 Northern Gateway Pipeline Project, I am sure...

7                   THE WITNESS: Correct.

8                   THE PRESIDING MEMBER: What does that  
9 connote in your mind now when you recollect the events  
10 of 2011, 2012, 2013, when there were what I will call  
11 "manifestations" against the Northern Gateway Pipeline  
12 Project?

13                   What does that bring to your mind?  
14 For example, does it bring [REDACTED] to your  
15 mind? Does it bring the British Columbia Civil  
16 Liberties Association to your mind?

17                   THE WITNESS: To your first question,  
18 [REDACTED] at the time the Northern  
19 Gateway Pipeline Project came up, my first thought was:

20 [REDACTED]  
21 [REDACTED]  
22                   In terms of the Protesters, yes, it  
23 seemed to be a natural protest against resource  
24 development in British Columbia.

1                   That happens. There is no surprise in  
2                   that regard. We didn't expect anything but. There are  
3                   no surprises there.

4                   In my mind, what I was looking for  
5                   was: [REDACTED]

10                  Those were my thoughts at the time.

11                  THE PRESIDING MEMBER: Okay. Thank  
12                  you.

13                  I will let Madam Dion continue with  
14                  her questions.

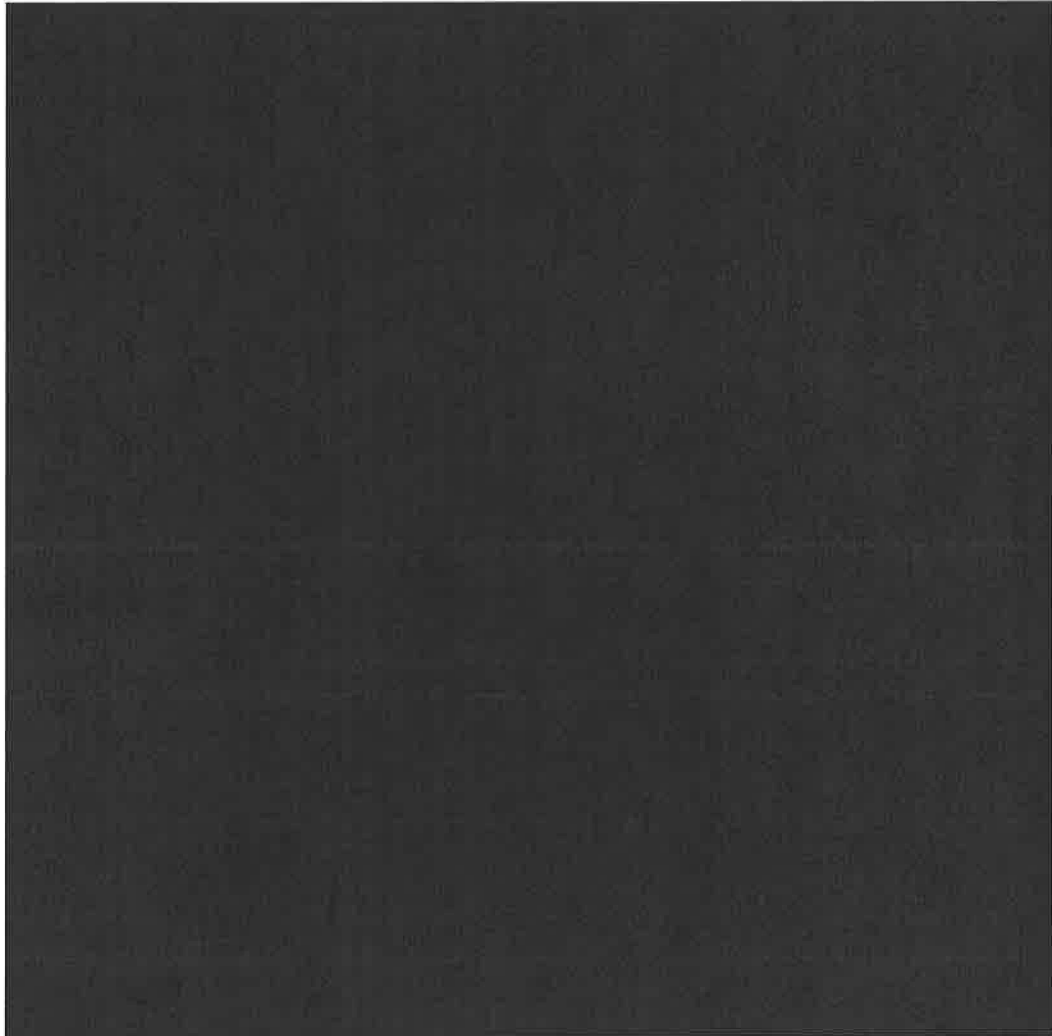
15                  (To maître Dion): My apologies for  
16                  the interruption, Madam Dion. I will defer any further  
17                  questions until later.

18                  MS. DION: Thank you, Mr. Fortier.

19                  Q. Going back to the example that you  
20                  used earlier with regard to [REDACTED]

21 [REDACTED]  
22 [REDACTED]  
23                  In the example that you used, you  
24                  talked about the safeguards that were taken in that  
25                  specific case.

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25



I always thought DND was an  
Organization of acronyms. I never realized that we  
are, too!



1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25

[REDACTED]

Q. I believe you may have answered this; however, to ensure that it is clear, do you recall any of the members of the Groups mentioned in this Letter being interviewed by the Service?

A. [REDACTED]

Q. [REDACTED]

A. [REDACTED]

[REDACTED]

Q. Okay. Thank you.

Do you remember, in the time that you were the Head of the Unit, any activity conducted by the Service that, in your view, could have [REDACTED]

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25

[REDACTED]

A. I don't see how.

MS. DION: Those are all of the questions I have. Thank you.

THE PRESIDING MEMBER: Thank you, Madam Dion.

Madam Bowers, any questions for the Witness?

MS. BOWERS: Yes. Thank you, Mr. Fortier.

(To the Witness): Thank you, [REDACTED] for being here today.

My questions, in large part, have been addressed in the questions put to you by maître Dion, and particularly so in the last couple of questions she posed to you. However, I am going to go over a couple of these areas with you, if I may.

THE WITNESS: Um-umm.

Examination by Ms. Bowers:

Q. Your testimony is that [REDACTED]

[REDACTED]



1 I appreciate that you have told us  
2 that you weren't aware of some of them.

3 The Groups in question are LeadNow,  
4 ForestEthics Advocacy Association, Council of  
5 Canadians, Dogwood Initiative, EcoSociety, Sierra Club,  
6 and Idle No More.

7 [REDACTED]  
8 [REDACTED]  
9 [REDACTED]  
10 A. If I may clarify, I know

11 [REDACTED]  
12 [REDACTED] but through the course of our  
13 investigations, incidentally, some Reporting [REDACTED]  
14 [REDACTED] might come up [REDACTED]  
15 [REDACTED]

16 Is that good?

17 Q. So your testimony is that [REDACTED]  
18 [REDACTED]  
19 [REDACTED]

20 A. Correct.

21 Q. [REDACTED]  
22 [REDACTED]  
23 [REDACTED]  
24 [REDACTED]  
25 [REDACTED]

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24

A.

Correct.

Q. And this is in relation to activities in respect of the Northern Gateway Pipeline Project.

A. Correct. Yes.

Q. Are you aware as to whether or not the Service had collected information, to put it that way, related to individuals and/or groups that were opposed to the Northern Gateway Pipeline Project and then giving that information to someone else, such as the National Energy Board or some non-Governmental entities?

Do you know, in your experience, whether the Service had provided information that could have been gleaned in the course of its investigations to other entities?

The example I have already given to you is the National Energy Board. But there could be other non-Governmental entities involved, such as entities within the Petroleum Industry, for example.

A. Right. That is correct.

1 I will insert a bit of a caveat here:  
2 We did have Contacts in the Petroleum Industry, with

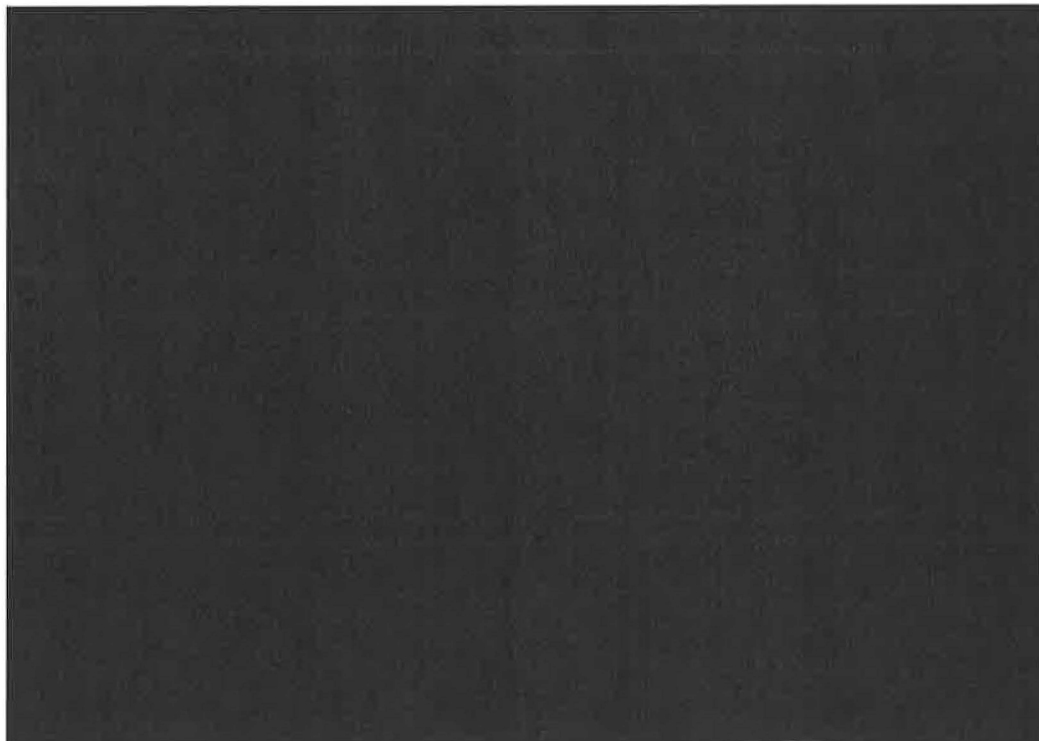


7 Q.



8 A.

9 We are always looking for triggers or  
10 flash points in terms of where violence could erupt in  
11 relation to our Targets.



1 [REDACTED]  
2 [REDACTED]  
3 [REDACTED]  
4 So that is the purpose of such  
5 Contacts.

6 And in the course of that process, the  
7 information is pretty much one-way: it is them to us.  
8 But, of course, they are always going to ask: "*What*  
9 *have you heard?*"

10 And beyond maybe a little bit of open  
11 information passing on the general scenario, the "lay-  
12 of-the-land" type of information, that would be it.

13 But the information flow was pretty  
14 much one-way.

15 Q. Okay. Thank you.

16 I am going to refer you to a Letter,  
17 [REDACTED] and I am going to ask you whether you are  
18 familiar with this Letter.

19 It is an Open Letter that was written  
20 by The Honourable Joe Oliver, who was the then Minister  
21 of Natural Resources. It is dated January 9<sup>th</sup>, 2012.

22 --- (Document Produced to the Witness)

23 THE PRESIDING MEMBER: Do you have the  
24 Letter before you?

25 THE WITNESS: Yes.

1 MS. BOWERS: Does my friend have a  
2 copy?

3 MS. DION: Yes. Thank you.

4 THE PRESIDING MEMBER: It is Exhibit 7  
5 in Complainant's Book, Exhibit C-3.

6 MS. BOWERS: That's correct. The  
7 Complainant's Supplementary Book of Documents.

8 THE WITNESS ((To the Presiding  
9 Member): Can I borrow your glasses!?

10 THE PRESIDING MEMBER: No! I wouldn't  
11 be able to read it myself!

12 --- (Laughter)

13 I am sure that if you need ---

14 THE WITNESS: I can get it.

15 MS. BOWERS:

16 Q. Just to give you a bit of context,  
17 [REDACTED] the Complainant referred to this Letter a  
18 couple of times during the course of the *In Camera*  
19 Hearing that took place in Vancouver in August of 2015.

20 I am going to read for you a portion  
21 of the Letter, starting with "Unfortunately", which you  
22 will find in the middle of the Letter.

23 It reads:

24 "Unfortunately, there are  
25 environmental and other radical

1 groups that would seek to block  
2 this opportunity to diversify our  
3 trade. Their goal is to stop any  
4 major project, no matter what the  
5 cost to Canadian families and lost  
6 jobs and economic growth. No  
7 forestry. No mining. No oil. No  
8 gas. No more hydroelectric dams.  
9 "These groups threaten to hijack  
10 our Regulatory system to achieve  
11 their radical ideological agenda.  
12 They seek to exploit any loophole  
13 they can find, stacking public  
14 hearings with bodies to ensure that  
15 delays kill good projects. They  
16 use funding from foreign special-  
17 interest groups to undermine  
18 Canada's national economic  
19 interests. They attract jet-  
20 setting celebrities with some of  
21 the largest personal carbon  
22 footprints in the world to lecture  
23 Canadians not to develop our  
24 natural resources. Finally, if all  
25 other avenues have failed, they

1                   will take a quintessential American  
2                   approach: Sue everyone and anyone  
3                   to delay the project even further.  
4                   They do this because they know it  
5                   can work. It works because it helps  
6                   them to achieve their ultimate  
7                   objective: delay a project to the  
8                   point it becomes economically  
9                   unviable." (As Read)

10                   Have you seen this Letter before this  
11                   particular point? Do you recall seeing it, reading it?

12                   A. No.

13                   Q. Okay. So, would you know ---

14                   THE PRESIDING MEMBER: I didn't hear  
15                   your answer...

16                   THE WITNESS: "No". Sorry.

17                   MS. BOWERS:

18                   Q. Would you know, [REDACTED] whether  
19                   the Service itself, CSIS, did anything, if at all, to  
20                   appease the concerns of Leaders of the various  
21                   Environmental Organizations that were claiming to be  
22                   affected by this Letter? Do you know whether the  
23                   Service responded to this Letter or acknowledged this  
24                   Letter in any way?

25                   A. I have no knowledge of that.

1 Q. Okay. That's fine. Thank you.

2 You might be aware, however, or  
3 perhaps you can assume, that some of the Organizations  
4 that I listed earlier were upset with this Letter, were  
5 concerned with this Letter, and felt that they  
6 themselves were being targeted, if you will, as a  
7 result of this Letter going out into the public domain.

8 To that extent, what I want to do --  
9 and I will direct the Tribunal and my friend to the  
10 Transcript of the Open Hearing, dated August 13, 2015,  
11 at Vancouver, and specifically to Page 133.

12 I will ask the Registrar to provide  
13 that reference to the Witness...

14 --- (Document Produced to the Witness)

15 THE WITNESS: Thank you.

16 MS. BOWERS:

17 Q. I will take you directly to Page  
18 133 of the Transcript of August 13<sup>th</sup>, 2015. This is  
19 testimony of an individual by the name of Jamie Biggar,  
20 who was the Campaigns Director of LeadNow.

21 A. Okay.

22 Q. There were questions put to him by  
23 his Counsel. I am going to pose a question to you at  
24 the end of this reference. But before doing so, I want  
25 to provide you with the context.



1 I will read the passage in question  
2 into the record, both for your benefit and for the  
3 benefit of my friend.

4 A. Okay.

5 Q. The portion of the Transcript that  
6 I want to refer you to is at Line 19 on Page 133, the  
7 Answer given by Mr. Biggar ---

8 In fact, let's start with the question  
9 that was posed to him.

10 I apologize.

11 (Reading):

12 "Q. Okay. Can you tell us what  
13 LeadNow's initial response or view  
14 was on the Stories or revelations  
15 that were coming out?"

16 And this in the News, and so forth.

17 And then Mr. Biggar responds:

18 "A. ...I think there was a  
19 perception amongst our Staff Team  
20 and amongst Volunteers and folks in  
21 our Community who we were speaking  
22 with that we were part of a  
23 community of people that was being  
24 targeted.

25 "There was a feeling of being

1 targeted and kind of put on an  
2 'Enemy List'.

3 "With the rhetoric from Mr. Oliver  
4 and with the follow-up revelations  
5 about the surveillance of this  
6 Workshop, it created a sense for us  
7 that we ---

8 "We simply couldn't even know the  
9 size and the scope of surveillance  
10 or intelligence gathering that was  
11 being conducted on the LeadNow  
12 Community Members or on our Staff  
13 or our Organization.

14 "We were alarmed by that.

15 "And with that situated then within  
16 the further context of ---"

17 And he goes on:

18 "So, first there was Minister  
19 Oliver's comments, followed by the  
20 revelations that we were being  
21 surveilled, and then, finally, in  
22 this year, Bill C-51 and the  
23 expansion of the definition of the  
24 kinds of activities that could be  
25 considered threats, particularly

1 including economic threats."

2 And then lastly:

3 "In the context of all of that, we  
4 have really seen kind of a growing  
5 concern on the part of our  
6 Community that it may be that they  
7 are being targeted or watched by  
8 the Government in different ways,  
9 and we are very concerned about  
10 that." (As Read)

11 I know that earlier you testified that

12 [REDACTED]  
13 But that is a telling comment from the Witness at the  
14 time, and I am just curious as to whether you have any  
15 comment or opinion on that, or whether you can shed any  
16 light at all on that from the Service's perspective.

17 A. I will acknowledge that there is a  
18 perception out there that CSIS is the arm of the  
19 Government in monitoring people involved in peaceful  
20 advocacy/protest, as it sounds like these folks were  
21 doing.

22 I understand the alarm. I fully  
23 understand it. And that is of concern, especially  
24 since this country is based on democracy and the  
25 ability to protest and to speak one's mind.

1 I don't know.

2 My thoughts, without repeating what I  
3 said earlier...

4 --- (A Short Pause)

5 You know, I look at his comments in  
6 the Letter...

7 "These groups threaten to hijack  
8 our regulatory system to achieve  
9 their radical ideological agenda.  
10 They seek to exploit any loophole  
11 they can find, stacking public  
12 hearings ---" (As Read)

13 I assume that is the Joint Review  
14 Panel/NEB Hearings.

15 --- (A Short Pause)

16 I don't know. I don't see Briefing  
17 Notes to the Minister.

18 It just couldn't have come from CSIS.

19  
20  
21  
22  
23  
24  
25

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25

[REDACTED]

which is why, from a Regional  
B.C. perspective, we just weren't interested in NEB  
Hearings going on in B.C. [REDACTED]

I don't know if that is an answer to  
your question, but that is my reaction to this.

Q. Let me ask you the question more  
directly.

You do not find the concerns, while  
you understand them, to be founded; that they are  
unfounded?

A. Oh, they are absolutely unfounded.  
Yes.

Q. Okay.

One other reference, if I may -- and  
it is in a similar context. It is found a few pages on  
in the same Transcript.

I direct you to Page 164 of this same  
Transcript -- and again, I have chosen just a couple of  
references on which to get your insight.

In this particular context, it is  
testimony from Ms. Caitlyn Vernon.

1 She is the Campaigns Director of the  
2 Sierra Club.

3 A. Okay.

4 Q. At the bottom of Page 164, Line  
5 21, it reads:

6 "Q. Ms. Vernon, there were some  
7 Stories in the Press in late 2013  
8 indicating that certain groups  
9 involved in or opposed to Northern  
10 Gateway Pipeline Project were being  
11 monitored or surveilled by the RCMP  
12 and CSIS.

13 "Were you aware of those Stories?"

14 (As Read)

15 And so forth. And she says:

16 "A. Yes."

17 And then I take you to Page 166 ---

18 The Question was:

19 "Q. ...What impact did those  
20 Stories have on Sierra Club BC, its  
21 Staff and its Supporters and  
22 Volunteers?"

23 And at Page 166, Line 6, her Answer

24 was:

25 "A. ...You know: We are operating

1                   within the bounds of the law. We  
2                   are operating within the Charitable  
3                   Guidelines. We are not doing  
4                   anything wrong. And yet we feel  
5                   like we're being put to this level  
6                   of scrutiny. We feel like we are  
7                   being painted, somehow, as less-  
8                   than-honest, even though we are  
9                   entirely operating above-board and  
10                  within the law.

11                 "Concerns have been expressed  
12                 about: What does this mean for  
13                 people's job prospects, if they  
14                 want to meet a Security Clearance  
15                 for some kind of a job or they want  
16                 to work for the Federal Government  
17                 in the future?

18                 "What does this mean for the  
19                 ability of Sierra Club BC Staff to  
20                 cross the Border, for example?"

21                 Those are some of the concerns that  
22                 were being raised: a "chilling effect", basically, is  
23                 a common theme that we heard from some of the  
24                 Witnesses; that they were essentially being, while not  
25                 targeted, perhaps part of a collateral damage effect,

1 if you will.

2 I am just wondering whether you have  
3 any comment on that, on this "collateral damage  
4 effect".

5 Is there any validity to that concern?

6 A. I don't see any validity to that  
7 concern. Just looking at the "crossing the Border"  
8 aspect, if, incidentally -- and I can't remember  
9 anything in this regard off the top of mind.

10  
11  
12  
13  
14  
15  
16

17 The only way that that could impact  
18 the Border is if we decided to

19  
20  
21  
22

23 That is not what we have done, nor is  
24 it something that we would do, unless we got to the  
25 point where we subsequently identified that the person



1 in question was involved in a direct threat to the  
2 national security of Canada, in which event we would  
3 open up an Investigation on that individual.

4 [REDACTED]  
5 [REDACTED]  
6 [REDACTED]  
7 [REDACTED]  
8 But in the context we have here, I  
9 would say "no". It wouldn't be an issue.

10 And I am not in Security Screening;  
11 but I find it inconceivable that someone's Security  
12 Clearance would be denied based on the fact that they  
13 just happen to be [REDACTED]  
14 [REDACTED]  
15 [REDACTED]  
16 [REDACTED]

17 I am no expert on Security Screening,  
18 but I can't see that happening -- unless they lied  
19 during their Security Screening Interview, and then who  
20 knows. But...

21 MS. BOWERS: I have no further  
22 questions.

23 Thank you, [REDACTED]

24 THE PRESIDING MEMBER: Thank you,  
25 Madam Bowers

Examination by the Presiding Member (Mr. Fortier):

The Letter from The Honourable Joe Oliver which Ms. Bowers questioned you about is dated January 9, 2012 ---

And I am sure you knew at that time that Mr. Oliver was the Minister of Natural Resources in the Federal Cabinet.

You said you hadn't seen that Letter. But had you heard of that Letter during the month of January of 2012?

THE WITNESS: I can't remember. It is not pinging to my mind, this Letter.

THE PRESIDING MEMBER: Obviously, it struck you ---

Even without glasses, you picked up on that sentence: "*These Groups threaten to hijack our regulatory system to achieve their radical ideological agenda.*"

This is not something that was discussed in the Offices of CSIS, B.C. Region, at the time?

THE WITNESS: The NEB Hearings and the ---

THE PRESIDING MEMBER: Well, the NEB Hearings and these accusations -- and not even veiled

1       accusations -- by the Head of the Ministry of Natural  
2       Resources.

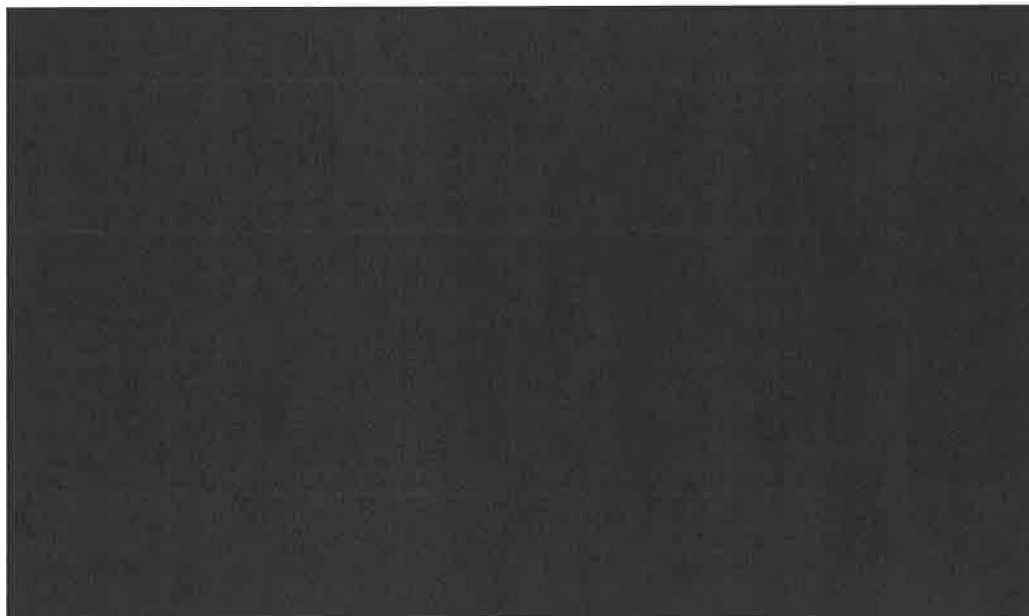
3                       Was this something that was being  
4       discussed ---

5                       THE WITNESS:   Just the issue itself of  
6       the "hijacking"?

7                       THE PRESIDING MEMBER:   Yes.

8                       THE WITNESS:   Like I mentioned before,

9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19



20                      THE PRESIDING MEMBER:   Okay.   Thank  
21       you.

22                      In terms of your remit ---

23                      What was the remit of the Service at  
24       that time vis-à-vis the Protests against the building  
25       of the Northern Gateway Pipeline?

1 THE WITNESS: Nothing to do with us,  
2 unless there were activities regarding [REDACTED]

3 [REDACTED]  
4 THE PRESIDING MEMBER: So, there was  
5 no ---

6 THE WITNESS: [REDACTED]  
7 [REDACTED]  
8 [REDACTED]  
9 [REDACTED]

10 Remember, "Gateway" was an idea at the  
11 time. There was nothing on the ground. It was just a  
12 Hearing.

13 [REDACTED]  
14 [REDACTED]  
15 That was ---

16 If I remember at the time, that was  
17 the mindset.

18 THE PRESIDING MEMBER: But there were  
19 Protests during the Hearings.

20 THE WITNESS: Yes.

21 THE PRESIDING MEMBER: That, you do  
22 recall?

23 THE WITNESS: Yes. I definitely  
24 remember the Media Reports, the one in Bella Bella, and  
25 some others.

1 Yes, I would have read that in the  
2 Newspapers, for sure.

3 THE PRESIDING MEMBER: And at that  
4 time, did you see any mention of the British Columbia  
5 Civil Liberties Association playing a role in these  
6 Protests?

7 --- (A Short Pause)

8 THE WITNESS: Against the NEB, the  
9 Northern Gateway Pipeline ---

10 THE PRESIDING MEMBER: During the  
11 Hearings, yes.

12 --- (A Short Pause)

13 THE WITNESS: No, I don't remember  
14 that.

15 THE PRESIDING MEMBER: When the  
16 Complaint was filed ---

17 And you know that there was a  
18 Complaint filed by ---

19 THE WITNESS: Yes.

20 THE PRESIDING MEMBER: That is why we  
21 are here.

22 You were in Vancouver at the time the  
23 Complaint was filed.

24 Did you think at the time that the  
25 BCCLA had valid reason for lodging a Complaint?

1 Did you know what the nature of the  
2 Complaint was? Were you informed as to the nature of  
3 the Complaint, as a member of the Service in Vancouver  
4 at that time?

5 THE WITNESS: I do remember initially  
6 seeing it, and I can't remember whether it was in my  
7 capacity as Acting Chief or if it was when I was Head.

8 But I do remember seeing an e-mail  
9 saying: "This is the Complaint. Does B.C. Region have  
10 any information on this issue?"

11 I remember that my thought at the time  
12 was: [REDACTED]

13 THE PRESIDING MEMBER: I'm sorry...?

14 THE WITNESS: [REDACTED]  
15 [REDACTED]

16 THE PRESIDING MEMBER: Yes. Okay.

17 --- (A Short Pause)

18 I don't have any further questions.

19 Thank you, [REDACTED]

20 Madam Dion, do you have any questions  
21 arising from the questions that Madam Bowers and I have  
22 posed?

23 MS. DION: Maybe just one quick  
24 question, if I may...

25 THE PRESIDING MEMBER: Sure.

Re-Examination by Ms. Dion:

Q. With regard to Minister Oliver's Letter -- Mr. Oliver, the Minister of Natural Resources at the time -- was he speaking on behalf of CSIS, to your knowledge?

A. No.

This sounds like a "political" statement, not a statement made by the Security Intelligence Service.

Q. And with regard to the Transcript excerpts that my friend read to you in the context of these Stories that were written by a Journalist, does the Service have any bearing on, or say in, what Journalists write in Newspapers or books or articles?

THE PRESIDING MEMBER: Of course they do!

--- (Laughter)

MS. DION: It seems like an obvious question, but...

THE PRESIDING MEMBER: No, no, no. I apologize. I am not making light of your question. I think it is a fair question.

THE WITNESS: No, not directly. Obviously, they will always go to the Communications Branch and ask for a comment. But to my understanding,

1 all things being equal, [REDACTED]

2 [REDACTED]

3

So the answer is "no".

4

MS. DION:

5

Q. Can you just explain, briefly, why

6 [REDACTED]

7 [REDACTED]

8 [REDACTED]

9

A. I will caveat my answer by

10

pointing out that I am not with the Communications

11

Branch and, as such, am not up-to-speed on their exact

12

M.O.; however, all things being equal, [REDACTED]

13 [REDACTED]

14 [REDACTED]

15 [REDACTED]

16 [REDACTED]

17 [REDACTED]

18 [REDACTED]

19 [REDACTED]

20 [REDACTED]

21 [REDACTED]

22 [REDACTED]

23 [REDACTED]

24 [REDACTED]

25 [REDACTED]



1 [REDACTED]  
2 [REDACTED]  
3 [REDACTED]  
4 [REDACTED]  
5 That is my general understanding as to  
6 why that policy exists.

7 MS. DION: Thank you. I have no  
8 further questions.

9 THE PRESIDING MEMBER: Thank you,  
10 Madam Dion.

11 Any questions arising, Madam Bowers?

12 MS. BOWERS: No. Thank you very much.

13 THE PRESIDING MEMBER: [REDACTED] I am  
14 responsible for your coming here to testify today, and  
15 I appreciate the fact that you have done so and have  
16 answered the questions that were put to you. You are  
17 now free to go back to Vancouver and [REDACTED]  
18 Travel well and safely.

19 THE WITNESS: Thank you very much.  
20 --- (The Witness Stood Down and Withdrew from the  
21 Hearing Room)

22 THE PRESIDING MEMBER: Madam Dion, I  
23 am grateful to you and to the Service for having made  
24 [REDACTED] available today. It was important for me to  
25 hear his evidence, and I have now done so.

1 I want to thank you again for your  
2 contribution and cooperation throughout this process.  
3 I also extend my thanks to Madam Bowers and Shayna, our  
4 Registrar.

5 Copies of the Transcript will be made  
6 available in due course.

7 We have had the *In Camera* portion of  
8 this Hearing, as well as the earlier *Ex Parte* portion,  
9 and now this additional Session to hear further *Ex*  
10 *Parte* evidence. In all, we have had three different  
11 Sessions.

12 We will be in touch with the Parties  
13 insofar as "Next Steps" are concerned.

14 With that, I will close today's  
15 Hearing.

16 MS. DION: Thank you.

17 MS. BOWERS: Thank you, Mr. Fortier.

18  
19 Certified Correct:

20 

21 Noel C. Keeley, C.S.R.  
22

2015 11 19

## Energy and Utilities Sector Classified Briefing – Threat Update

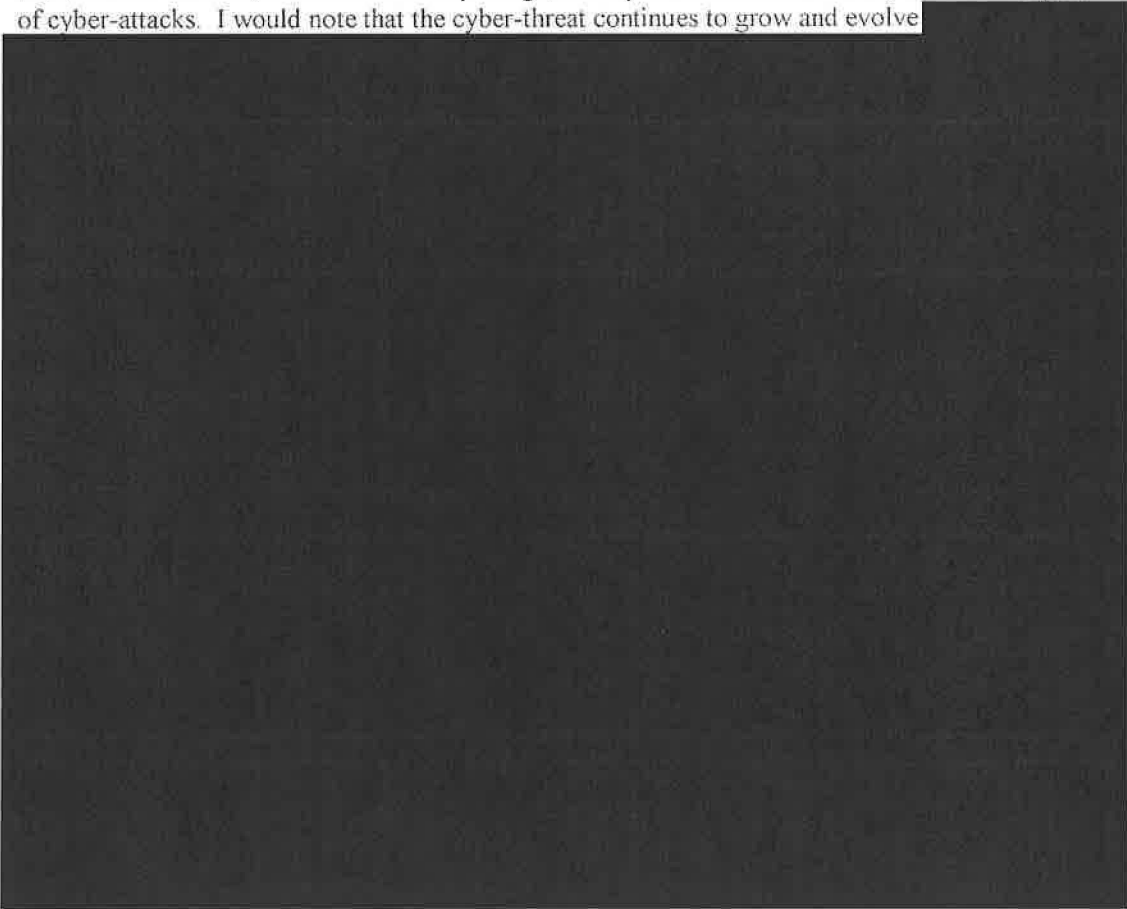
## SPEAKING NOTES

The Threat Environment

I am again pleased to be invited to the Energy Sector Classified Briefing to provide this update on threats to the energy and utilities critical infrastructure sector since I spoke to you last May.

As this will be my 4<sup>th</sup> address to this group, and I want to recall the broad themes of my earlier briefings.

My first briefing to you in 2014, provided an overview of the threats to the critical infrastructure sector from terrorism, extremism and espionage, but my focus was on the many recent examples of cyber-attacks. I would note that the cyber-threat continues to grow and evolve



- 1 -

2015 11 19

The takeaway from that briefing for you in the critical infrastructure sector is that the potential for such an attack in Canada continues to pose a serious and credible risk.

(1) The Cyber Threat

Every Classified Briefing devotes some discussion to cyber threats and I can tell you, the threat is not declining. I want to give you a clear picture of the nature of the threat. As you are well aware, the cyber threat to critical infrastructure is two-fold: (1) firstly the threat of cyber-attack and hacking on industrial control system hardware and software – so-called SCADA attacks, and (2) secondly, the threat of cyber-espionage, exfiltration of data and loss of proprietary information from corporate systems as well as cyber-attacks on your employees and breaches of confidentiality.

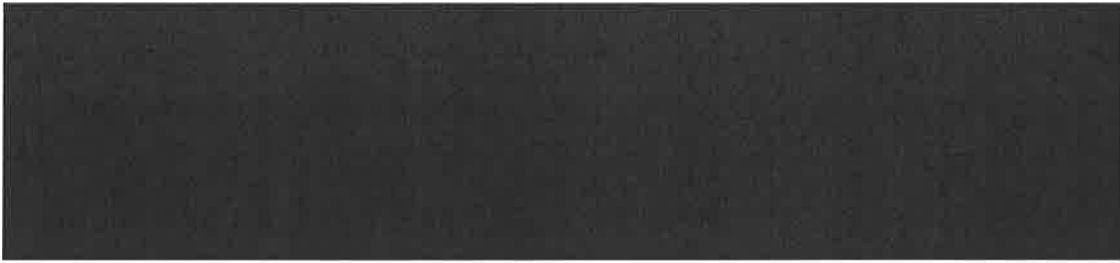
Industrial Control Systems

We also expect that the number of [REDACTED] actors that pose a cyber-threat to Canada and other nations' public and private sectors will increase and that the tools and techniques used to mount cyber campaigns will evolve quickly and become more efficient, posing additional national security challenges. [REDACTED]

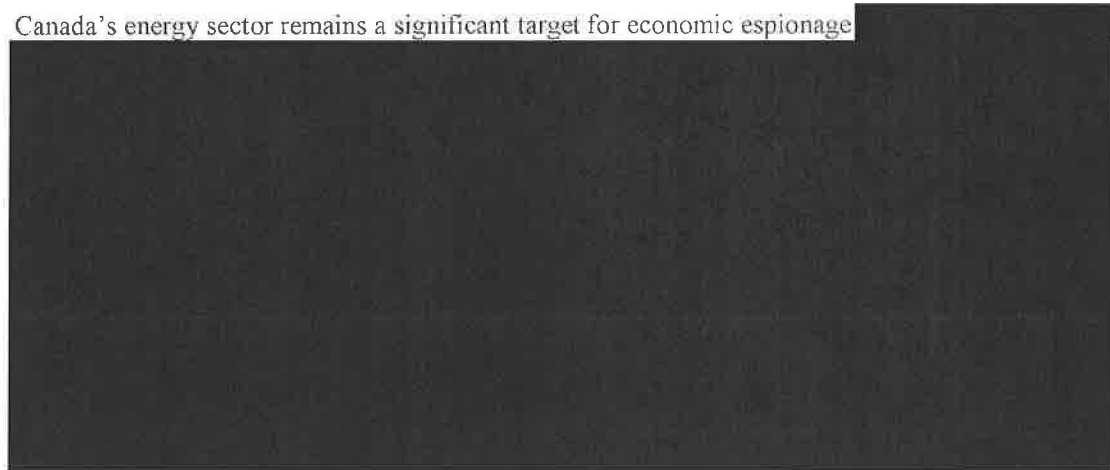
Indeed, a report by the Industrial Control System Cyber Emergency Response Team (ICS-CERT) [REDACTED] reports that industrial control systems were hit by cyber-attacks at least 245 times over a 12-month period from 2013 to 2014. Almost a third of the affected industries were in the energy sector. [REDACTED]

- 2 -

2015 11 19

Cyber Espionage

Canada's energy sector remains a significant target for economic espionage

(2) Home-Made Explosives and Improvised Explosive Devices

Our intelligence does not indicate any let-up or easing of the terrorist threat at home or abroad. Obviously, the threat in Canada is not as great as in the Middle East, but I can confirm that CSIS investigations related to terrorism in Canada are active and ongoing. They are not diminishing.

As I mentioned previously, domestic extremists of various ideologies have been responsible for 10 bombings in Canada since 2004, including:

- Royal Bank of Canada bombing, Ottawa (2010)
- 6 EnCana Bombings (2008-2009)
- 3 bombings claimed by *Initiative de Résistance Internationaliste*:
  - Hydro-Québec transmission tower (2004)
  - Vehicle of spokesperson of Canadian Petroleum Producers Institute (2006)
  - Canadian Forces Recruitment Centre (2010)



- 3 -



2015 11 19

Here I will again remind you, as I do at every briefing, that CSIS does not investigate lawful protest or activism. However, the Service believes there is potential for serious politically or ideologically motivated violence associated with [REDACTED]

There is no question your industry sector's focus on security and resilience is the correct one. But it is also indisputable that your industry's assets will remain vulnerable to improvised explosive devices, [REDACTED]

I have previously spoken about the importance of the internet and social media to the terrorist threat. That trend very much applies to explosives and bomb-making. There is an abundance of information and step-by-step instructions on the internet to assist would-be extremists in producing powerful explosives and assembling bombs. The wide availability of this information considerably increases the risk.

#### Comments about ISIL's attacks [REDACTED]

Over the last few years, it has been difficult to assess the terrorist capabilities of the Islamic State (ISIL). While it was successful in capturing and holding territory in Syria, it had been unable to threaten interests beyond its borders.

Initially, the view was that ISIL had no particular aspirations to execute spectacular attacks outside its borders. Then, some argued that Al Qaeda was more sophisticated than ISIL, and therefore continued to pose a greater threat. Finally, the focus shifted to so-called lone wolf attacks, an area in which everyone could agree that ISIL excels. [REDACTED]

- 4 -

2015 11 19

[REDACTED] Therefore, the potential for such an attack in Canada continued to pose a serious and credible risk.

Now, in a few short weeks, ISIL has validated that assessment in an unambiguous manner. It has claimed responsibility for the October bombing of a Russian passenger plane that killed 224. The group is also believed to have killed 44 people in a suicide bombing in Beirut just days ago. And after Friday night's coordinated attacks in Paris – in which three teams using guns and suicide belts killed at least 129 people – ISIL again claimed responsibility. In the months preceding all of this, ISIL had struck repeatedly, in scores of small and large attacks, including a synchronized suicide bombing in Sana'a, Yemen, that killed more than 140 in March.

[REDACTED]

The message for this group is that spectacular terrorism no longer requires spectacular resources. A few patient and disciplined people along with some careful planning can wreak tremendous havoc.

**Concluding Remarks Emphasizing the Importance of Cooperation**

Canada energy infrastructure remains vulnerable to targeting by terrorists and extremists focused on destruction, and to cyber-attacks [REDACTED]

As I have mentioned every time I addressed this classified briefing, the detection and disruption of terrorist and cyber-attacks is not solely the responsibility of CSIS. [REDACTED]

As always, I encourage further discussion on these issues throughout the day, or subsequently with your contacts at our regional offices.

- 5 -

2015 05 21

**Energy and Utilities Sector Classified Briefing – Threat Update****SPEAKING NOTES****The Threat Environment**

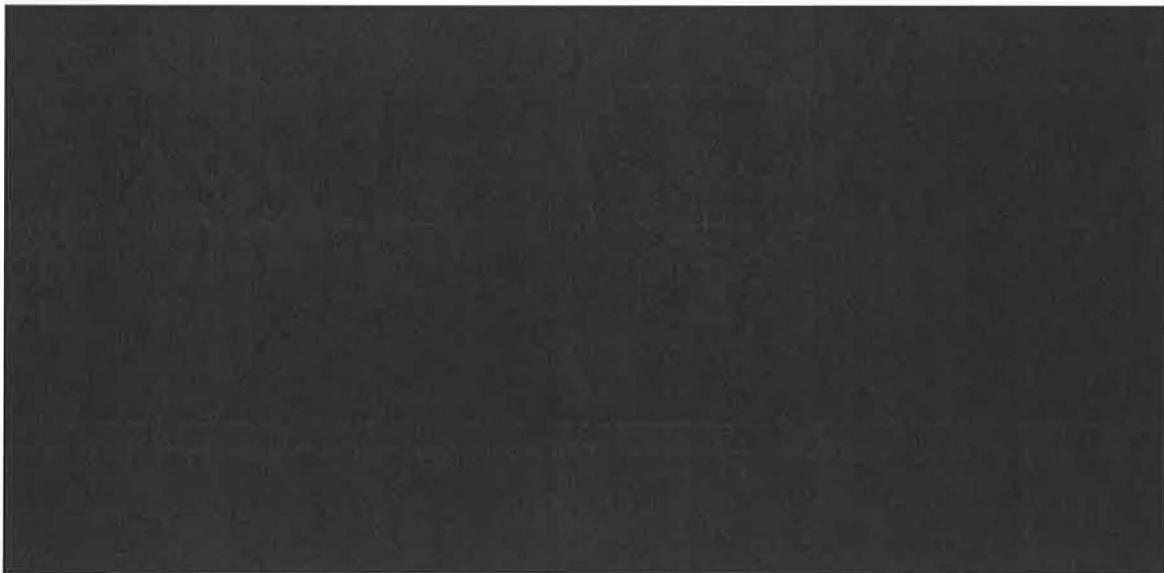
I am pleased to provide this update on threats to the energy and utilities critical infrastructure sector since I spoke to you at the last classified briefing in November 2014.

As you already know, but it bears repeating, CSIS investigates a range of national security threats, including terrorism, extremism, sabotage, espionage, clandestine foreign influenced activities, nuclear proliferation and malicious cyber activities. Each of these categories includes threats that are relevant to critical energy infrastructure.

As always, I encourage further discussion throughout the day on any of these issues, or subsequently with your contacts at our regional offices.

**Terrorism: Global trends in 2015**

As I noted last November, Islam-inspired terrorism continues to be the most serious threat to national security and a priority for the Service. This threat continues to evolve with individuals travelling to, and returning from conflict zones such as Syria, Iraq and Africa.



1



2015 05 21

[REDACTED]

The Service is trying to better understand those who mobilize to violence. While this work is ongoing, there are some interesting preliminary results.

[REDACTED]

2015 05 21

#### 4. The importance of social media

Extremist messages and ideas continue to inspire in the virtual realm.

Groups such as ISIL use social media not only to radicalize individuals, but also to mobilize them to violence.

#### 5. The impact of ISIL

ISIL now dominates the Canadian terrorist threat spectrum:

- as a direct threat to our military forces operating in Iraq;
- as recruiter of Canadians to fight in Iraq and Syria; and
- as inspiration for possible attacks in Canada.

Canadian extremists have joined ISIL and aspire to do so. Canadian's were likely attracted to ISIL's extremist world view, propagated by a sophisticated media campaign. And once Canadians arrive in the region, it is relatively easy for them to join the group. The emotional pull of ISIL's caliphate, and its winning streak, seems to have played an important role in mobilizing both male and female extremists to travel to Syria.

ISIL's operational capabilities are significantly enhanced by its ability fund itself, including proceeds from seized oil production, which allows it to purchase weapons and acquire the training and expertise it needs to carry out attacks in Iraq and Syria, and potentially beyond in North Africa. This revenue also enables the group to disperse funds to like-minded terrorist organizations, including those with attack aspirations against the West, which could significantly increase the terrorist threat to Canada and our allies.

#### 6. The global AQ network

AQ Core continues to command the loyalty of key Islamist extremist ideologues and several affiliate organizations. Despite a let-up in counter-terrorism pressure on AQ in Pakistan, attack planning against North America remains a high priority, and AQ has encouraged both its affiliates and associated Islamist extremist groups to carry out attacks in the West.

Although AQ Core has not attacked the West since the 2005 bombing of the London Underground, several attempts have been discovered and disrupted. This demonstrates an ongoing intent and capacity for serious violence, and that AQ continues to actively target Canadian interests.

2015 05 21

## 7. Domestic extremism

[REDACTED] Although small in number, domestic extremists have caused significant property damage over the past decade, primarily to energy infrastructure and banks. [REDACTED]

## 8. Heightened risk for energy infrastructure

The rapid rise of ISIL and the recent attacks in Canada increase the security threat to the energy infrastructure sector. Deadly attacks motivated by Islamist extremism and conflict overseas cannot be ruled out in Canada. The attack and hostage-taking at the gas plant in Algeria provides a vivid example of how motivated and trained Islamist terrorists – including at least two Canadians in that attack – can quickly overcome perimeter security and threaten energy facilities and personnel.

## 9. Importance of Cooperation

The challenge for Canada and our allies is to monitor and disrupt the flow of aspiring jihadists to areas of conflict and training camps where they will gain experience and contacts that increase their capacity to advance terrorist plots should they survive and return.

As I always mention at every classified briefing, the detection and disruption of terrorist activities is not solely the responsibility of CSIS. The Service's longstanding partnership with the energy sector provides a secure channel to share information relevant to the terrorist threat.

[REDACTED]

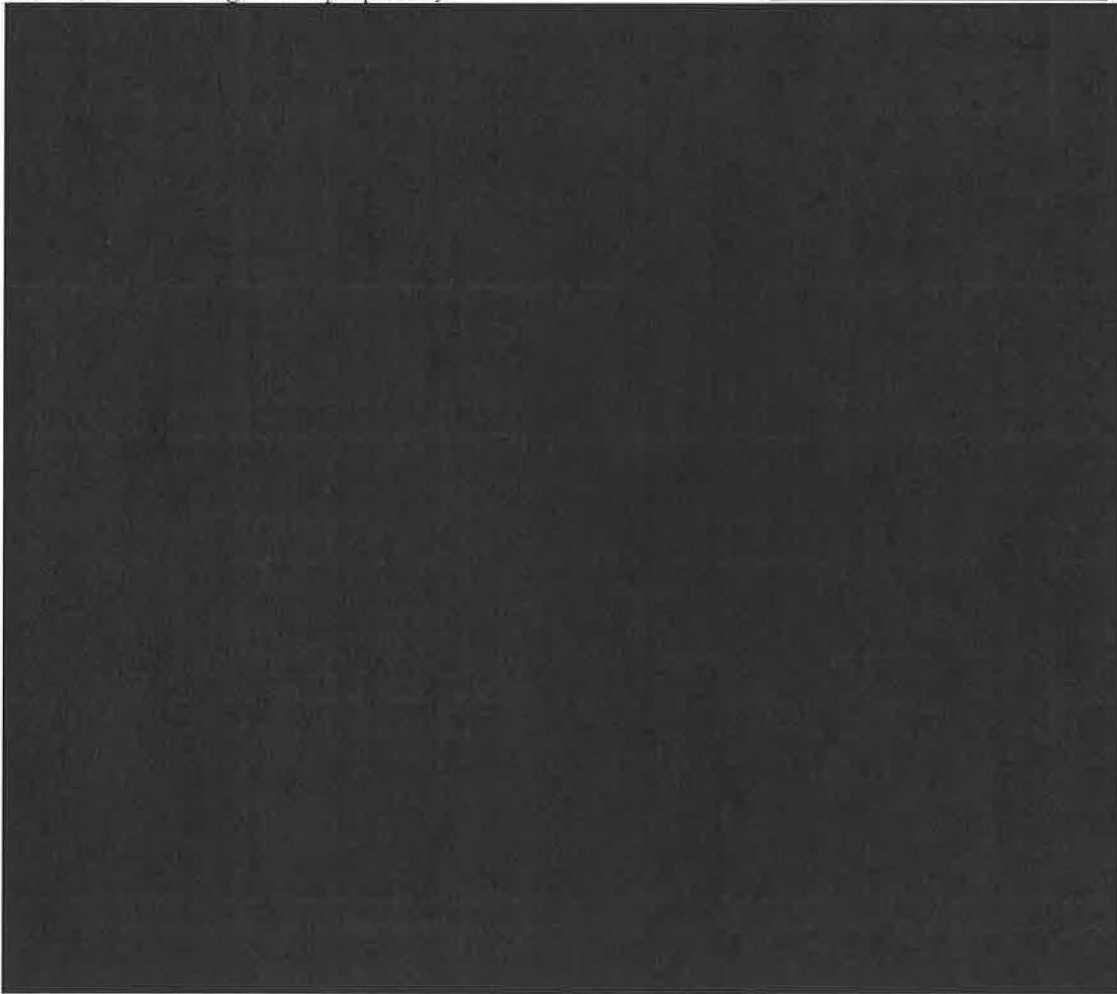
2015 05 21

Espionage, Economic Security and Foreign Interference

The energy sector remains a significant target for economic espionage – focussed primarily on resource extraction, energy infrastructure, advanced technology and know-how.

**10. Technology and Economic Interests at Risk**

Canada has always been a target for traditional espionage activities, many of which focus on advanced technologies and proprietary information and know-how. [REDACTED]



2015 05 21

## 12. Technology inventory

Not all of your technology is secret. Most of it may even be for sale. But when it comes to espionage, it is important to be able to distinguish sensitive proprietary technology from older, less-current technology. You have to know what the really secret technology is and be prepared to protect it.



### Cyber Threats

I have only a few words on strategic cyber threats, about which you will hear more later.



We expect that the number of non-state actors with the means to pose a cyber-threat to Canada and other nations' public and private sectors will increase and that the tools and techniques used to mount cyber campaigns will quickly evolve and become more efficient, posing additional national security challenges.

### Concluding Remarks

Canada energy infrastructure remains vulnerable to targeting by terrorists and extremists focused on destruction, and to espionage by foreign states seeking information, advanced technology and know-how to advance their own interests.

I reiterate again that critical infrastructure owners and operators are important partners for CSIS and the RCMP, and we will continue to work closely with you.

TOP SECRET – CEO


File No.: 2800-170  
(TD R522)

**CSIS ACTIVITIES RELATED TO DOMESTIC  
INVESTIGATIONS AND EMERGING THREATS**

**(SIRC STUDY 2012-02)**

**Security Intelligence Review Committee  
March 8, 2013**

**TABLE OF CONTENTS**

<b>1</b>	<b>INTRODUCTION .....</b>	<b>3</b>
<b>2</b>	<b>METHODOLOGY .....</b>	<b>4</b>
<b>3</b>	<b>DOMESTIC EXTREMISM .....</b>	<b>5</b>
	3.1 High Profile Events of 2010 .....	5
	3.2 Post Event Recalibration .....	6
		
<b>4</b>	<b>INTELLIGENCE REQUIREMENTS AND SETTING PRIORITIES .....</b>	<b>10</b>
<b>5</b>	<b>ISSUES FOR CONSIDERATION .....</b>	<b>11</b>
	5.1 Domain Awareness: Maintaining Knowledge of a Cyclical Threat Environment .....	11
	5.2 The Importance of Liaison .....	12
<b>6</b>	<b>REASONABLE INVESTIGATION .....</b>	<b>14</b>
<b>7</b>	<b>CONCLUSION .....</b>	<b>16</b>

## 1 INTRODUCTION

For most of its history, CSIS has run successful, [REDACTED] investigations into domestic threat-related activities [REDACTED]

[REDACTED] collection authority against a threat to the security of Canada as defined under the CSIS Act. They may target groups, organization, individuals, issues or events. [REDACTED]

[REDACTED] Nationally, CSIS is still collecting on domestic extremism in regions where such threats exist [REDACTED]

Overall, SIRC is in agreement with CSIS, [REDACTED] to cover domestic threats, and with the perspective that, in general, the actual threat arises from issues or events. Although [REDACTED] the investigations may present some challenges, SIRC believes that increased liaison with law enforcement provides assurance that CSIS will be apprised should criminal behaviour drift into the realm of threats to national security. This information can also assist the Service in its function of providing accurate reporting to Government of Canada clients.

March 8, 2013

Page 3 of 16




## 2 METHODOLOGY

This review examined CSIS's activities related to their domestic investigations and emerging threats. SIRC examined corporate, operational and policy documents and reviewed [REDACTED] operational messages and [REDACTED] files. In addition, SIRC held briefings with CSIS Headquarters (HQ) staff representing the [REDACTED] Branch and the Intelligence Assessments Branch (IAB) and completed an on-site visit [REDACTED] to meet with management and regional intelligence officers.

The core review period was from January 1, 2010 to December 31, 2011, [REDACTED]  
[REDACTED]

### 3 DOMESTIC EXTREMISM

CSIS characterizes domestic extremism as the willingness of individuals or groups in Canada to use violence or the threat of violence for political and/or ideological purposes. This often includes those groups or individuals who use serious violence or acts of sabotage to further their environmental, anti-capitalist, anti-globalization, and animal rights objectives.



In recent years, the high level of threat associated with all these investigations has been re-assessed.




#### 3.1 High Profile Events of 2010

In the years leading up to 2010, the Vancouver Olympics and the G20/G8 meetings in Ontario



The biggest threat to the events was assessed to be violence associated with



March 8, 2013

Page 5 of 16

[REDACTED]

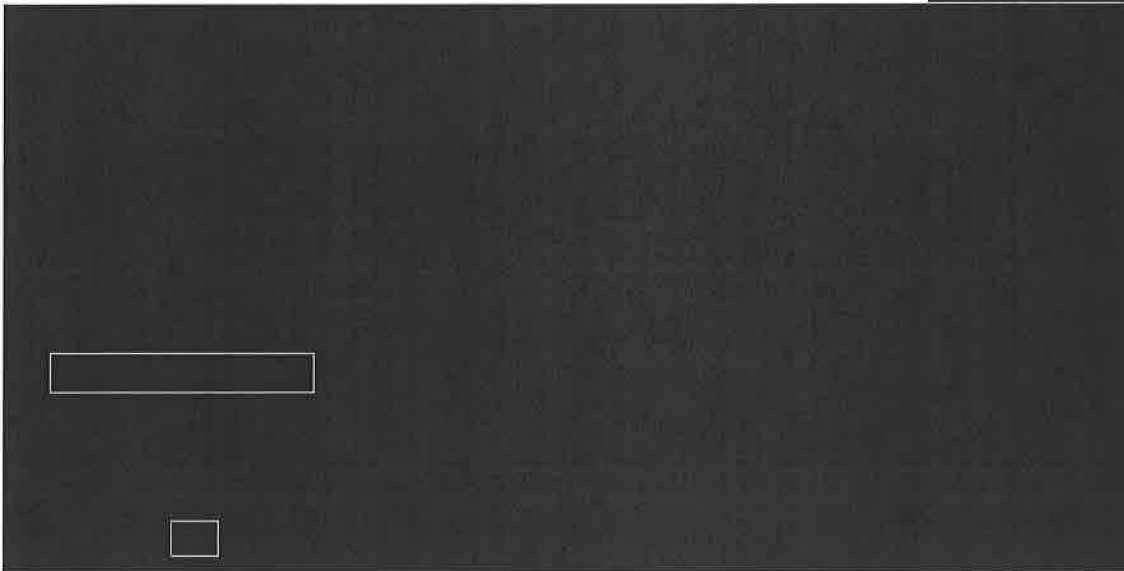
The Vancouver Olympic Games were ultimately relatively peaceful in spite of some very vocal opposition. [REDACTED] A very strong pro-Olympic reaction to the opposition was apparent -- in fact there were even counter-protests organized. [REDACTED]

The G-20 Summit in Toronto was not as tranquil. [REDACTED]

[REDACTED] Moreover, although there was a substantial amount of vandalism targeting banks and downtown Toronto businesses, [REDACTED]

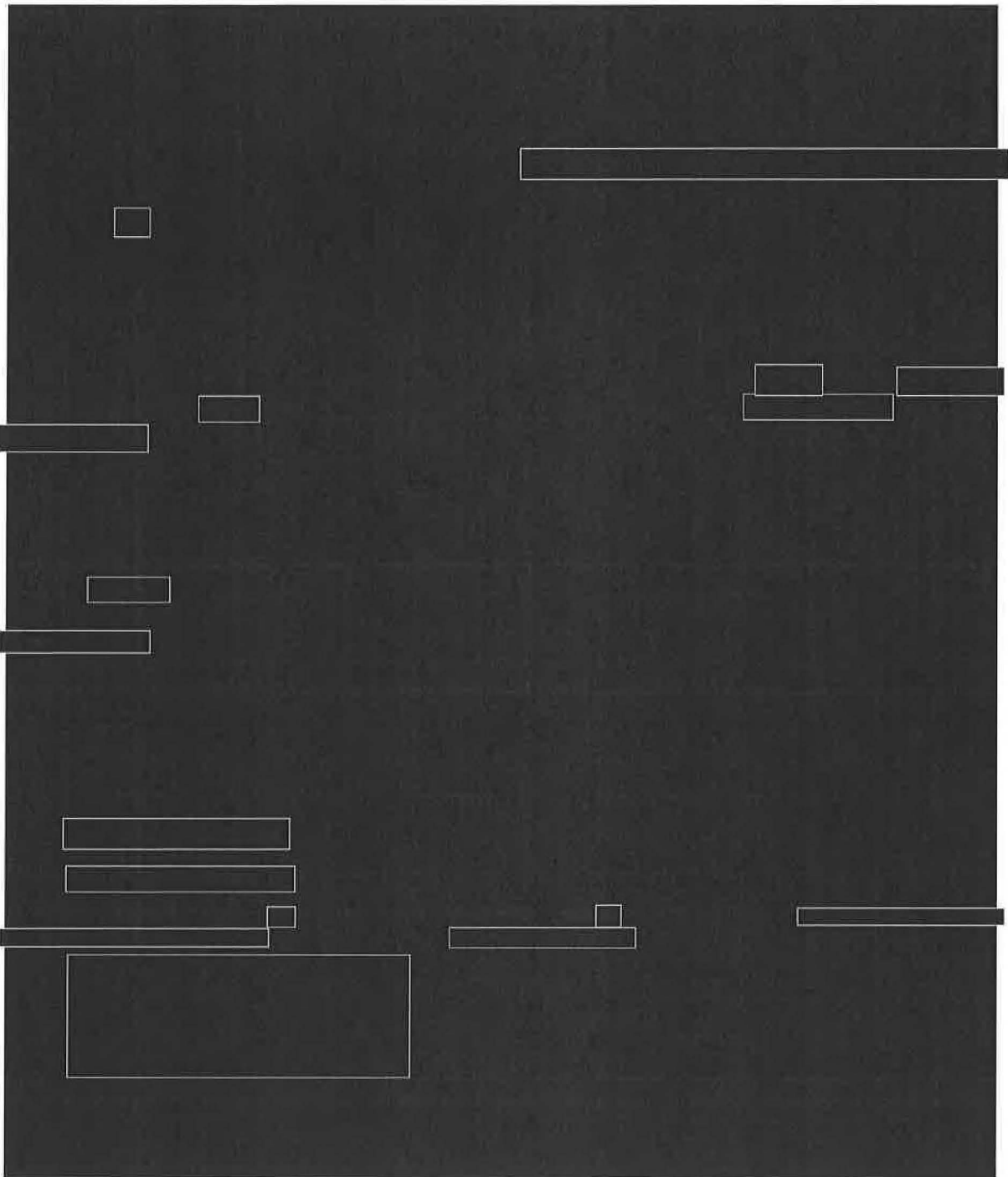
### 3.2 Post Event Recalibration

With the conclusion of the Vancouver Olympics and the G8/G20 Summits, [REDACTED]



March 8, 2013

Page 6 of 16



March 8, 2013

Page 7 of 16

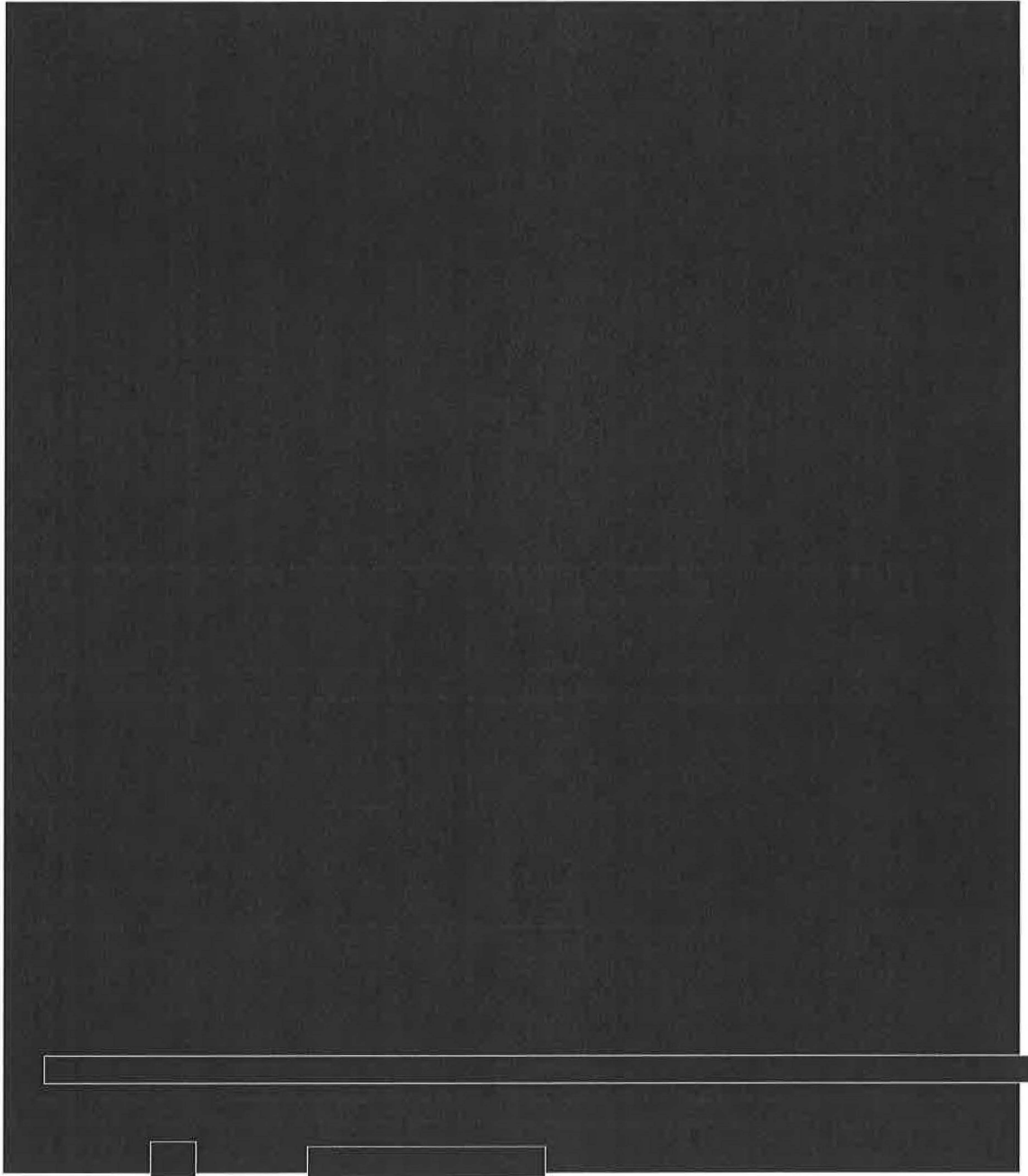
[Redacted]

Tab/Onglet 10

Page 736

7 of 16

AGC1061



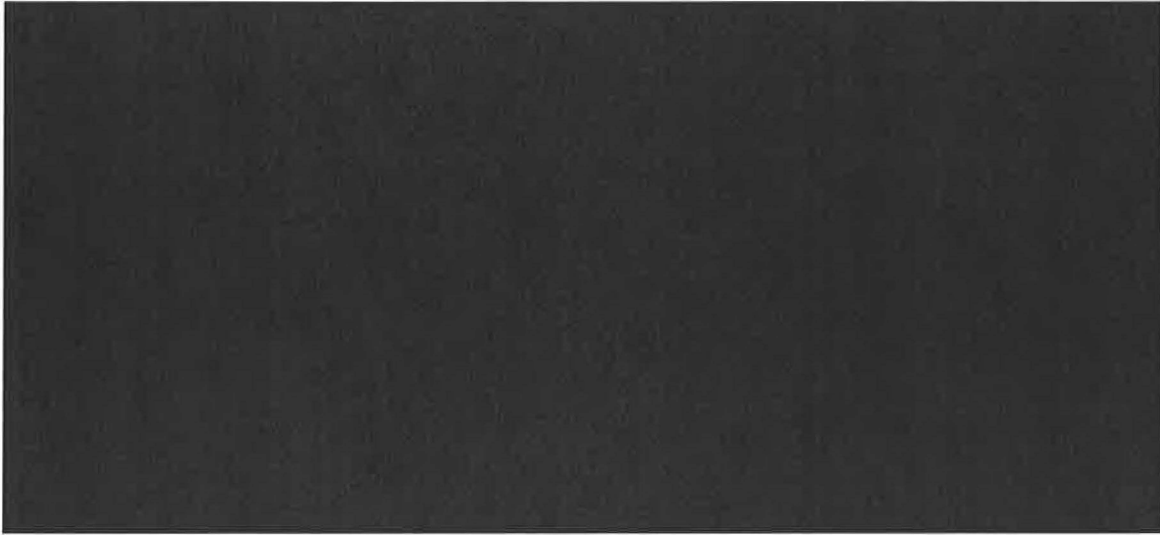
March 8, 2013

Page 8 of 16

[Redacted]

Tab/Onglet 10

Page 737



[Redacted]

March 8, 2013

Page 9 of 16

[Redacted]

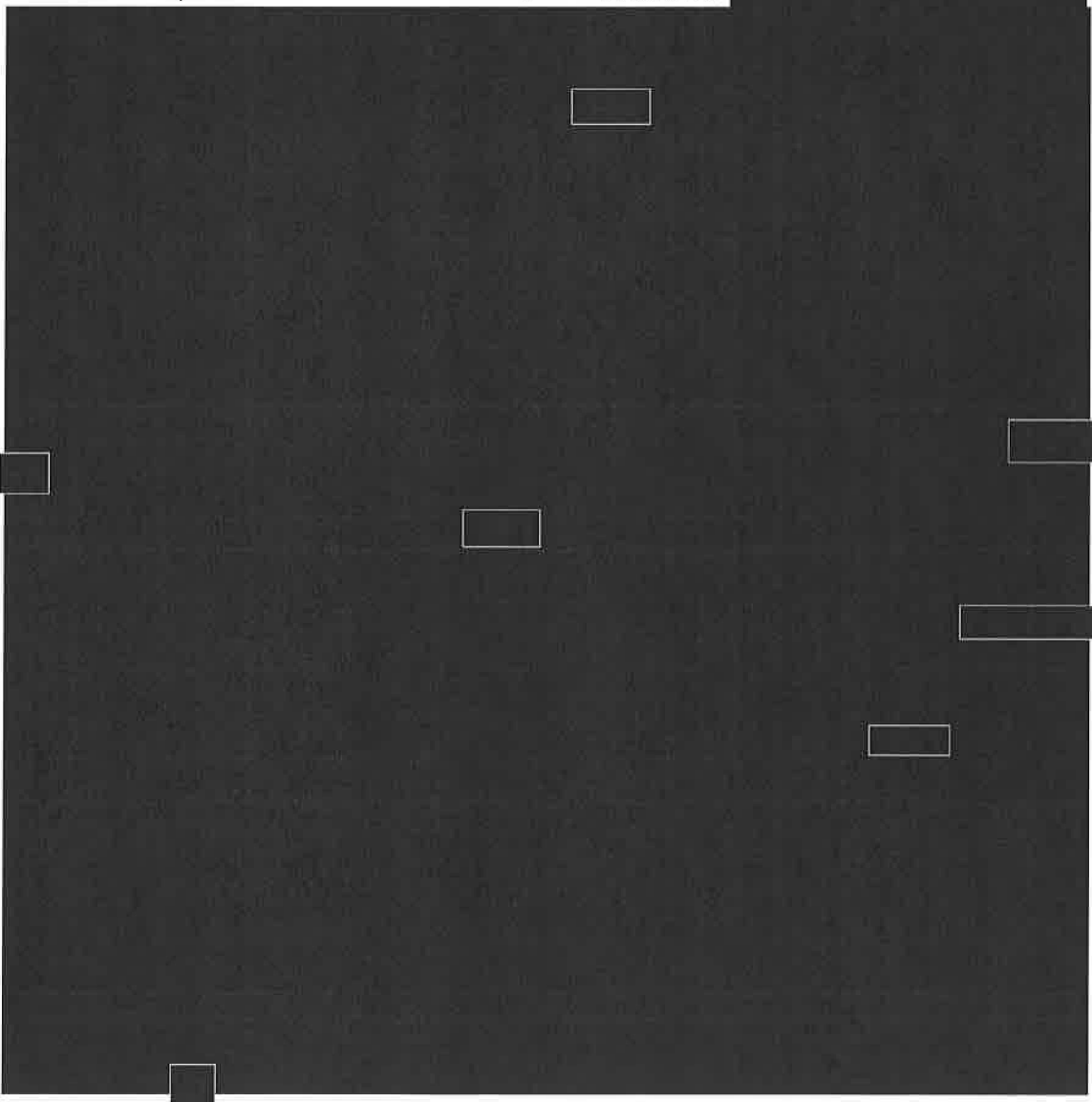
Tab/Onglet 10

Page 738

#### 4 INTELLIGENCE REQUIREMENTS AND SETTING PRIORITIES

[REDACTED] the Intelligence Assessments Branch (IAB) released the Intelligence Requirement Document [REDACTED] Intelligence Requirements (IRs) are subjects of interest [REDACTED]

[REDACTED] The IRs are prioritized from one to four: Tier 1 IRs are the highest priority for the Service and predominate in terms of resource commitment. [REDACTED]



March 8, 2013

Page 10 of 16

## 5 ISSUES FOR CONSIDERATION

### 5.1 Domain Awareness: Maintaining Knowledge of a Cyclical Threat Environment

[REDACTED]

[REDACTED] These all require some degree of monitoring, or what IAB referred to as "domain awareness", in part to ascertain potential triggers and flashpoints, and in part to ensure that CSIS is aware of what is happening should a threat arise. The Service must be prepared to answer to the Government of Canada's inquiries [REDACTED]

[REDACTED]

[REDACTED] when an event happens the Government of Canada expects to be briefed quickly and accurately by the Service.

[REDACTED]

March 8, 2013

Page 11 of 16

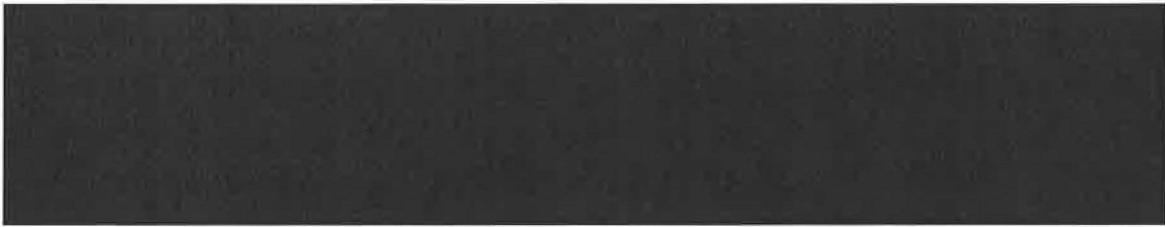


## 5.2 The Importance of Liaison

[REDACTED] liaison with law enforcement becomes of central importance.

Law enforcement agencies can be a source of information, [REDACTED]

[REDACTED] Law enforcement officials, however, may be aware of those involved in criminal activity who may at some point pose a threat according to CSIS's mandate. All the Directional Statements issued for the collection of information [REDACTED] highlight the need for liaison and SIRC saw examples of fruitful liaison with law enforcement, both in older areas where the Service no longer had investigations and with emerging issues.<sup>29</sup>



SIRC found that liaison with law enforcement agencies [redacted] is an effective use of resources. [redacted]

[redacted] it is an appropriate means of gaining information and staying abreast of potential threats.



March 8, 2013

Page 13 of 16



## 6 REASONABLE INVESTIGATION

During the review process, SIRC examined [REDACTED] operational reporting to ensure that investigations were handled in an appropriate and reasonable manner -- i.e. adherence to internal policy and the CSIS mandate. SIRC also wanted to ensure that the Service stopped investigating those many targets who had been terminated after the 2010 events.

[REDACTED] not to report on activities relating to legitimate protest and dissent, and that the Service was only interested in threat-related activities. **SIRC found that activities related to legitimate protest and dissent were not investigated and that detailed operational reporting on former targets ceased.**

Although there was no indication that CSIS was investigating those who were involved in legitimate activities, there was an instance where operational reporting was distorted to indicate a person was advocating the use of extreme violence to further a cause. [REDACTED]

[REDACTED]

SIRC believes this does not indicate a general misunderstanding at CSIS of [REDACTED] but rather a case of careless reporting. SIRC was pleased to see that after its request for any other information the Service may have in their possession to indicate the support of [REDACTED] the entry was amended in operational reporting [REDACTED]

[REDACTED]

[REDACTED]

March 8, 2013

Page 15 of 16

## 7 CONCLUSION

[REDACTED]

Overall, SIRC agrees with the direction that CSIS is taking with regards to domestic extremism. [REDACTED]

**SIRC found that CSIS moved quickly to terminate investigation of those individuals who were no longer considered threats after the major events of 2010 and would encourage the Service to be as vigilant regarding future events or issues.**

The Government's need for information on threats that are mainly dormant until an event or an issue arises, contributes to the need for the Service to continue to maintain "domain awareness". CSIS must ensure that by maintaining a presence that they do not intrude on legitimate forms of protest and dissent. [REDACTED]

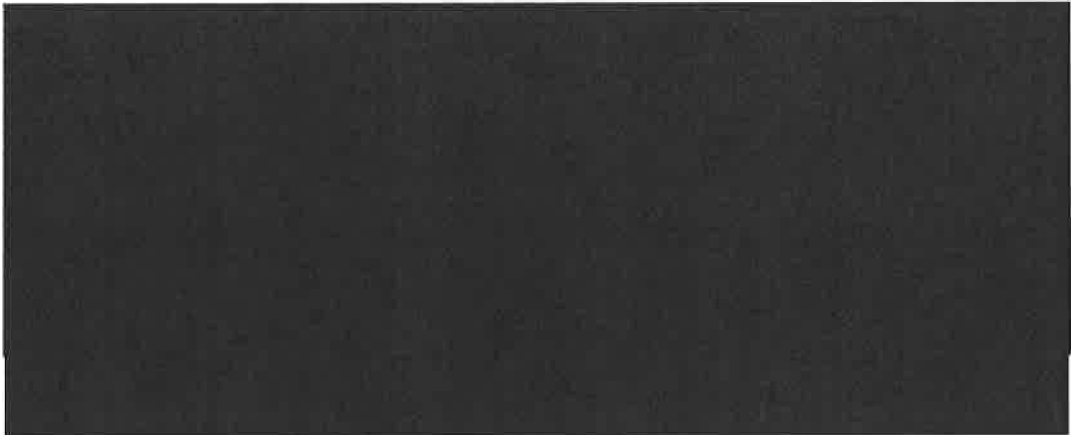
[REDACTED] SIRC encourages the direction the Service is taking [REDACTED] liaising with their domestic partners.

These relationships ultimately help provide information [REDACTED] and help CSIS advise its Government clients when the time arises.

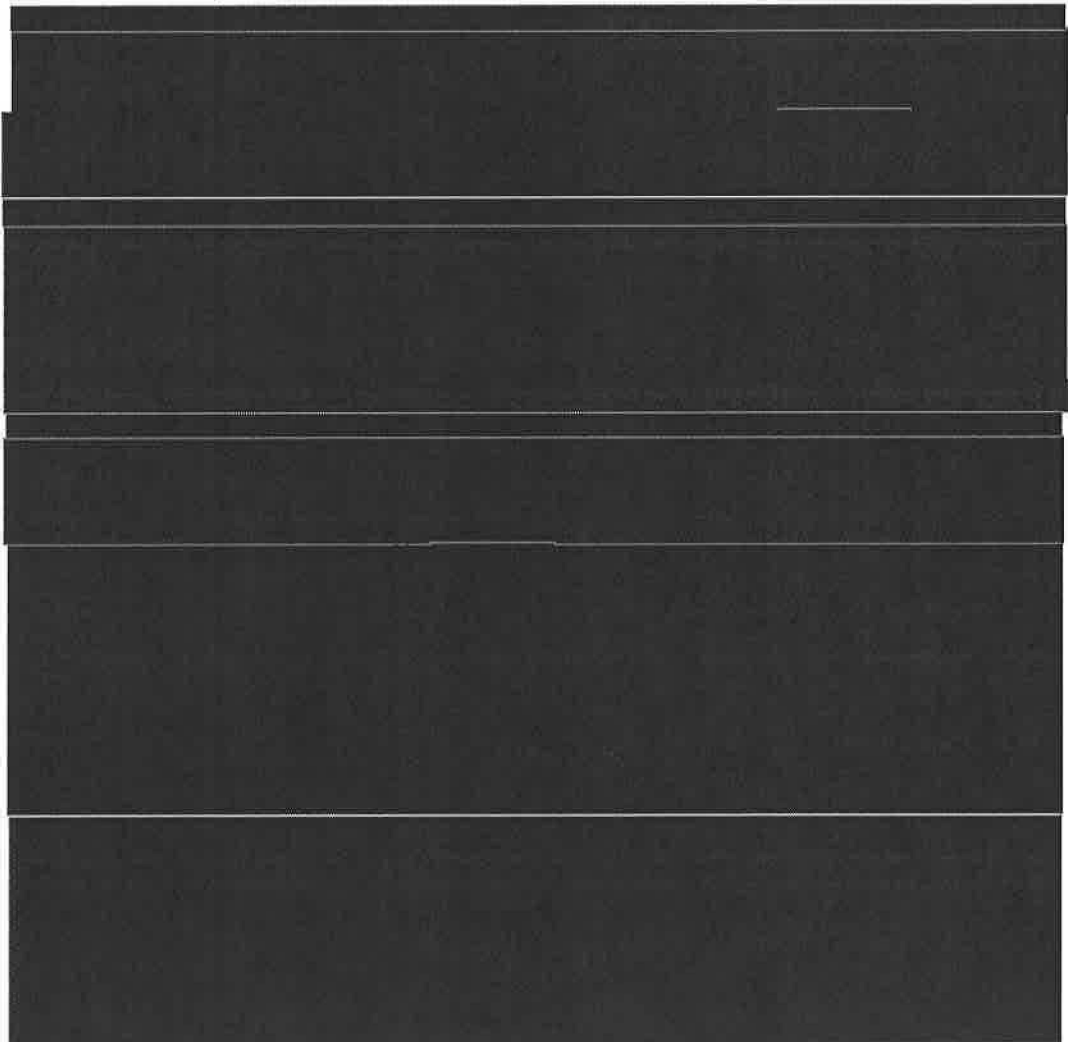
DATE  
20130125

RE / OBJET:

SYNOPSIS / SOMMAIRE:

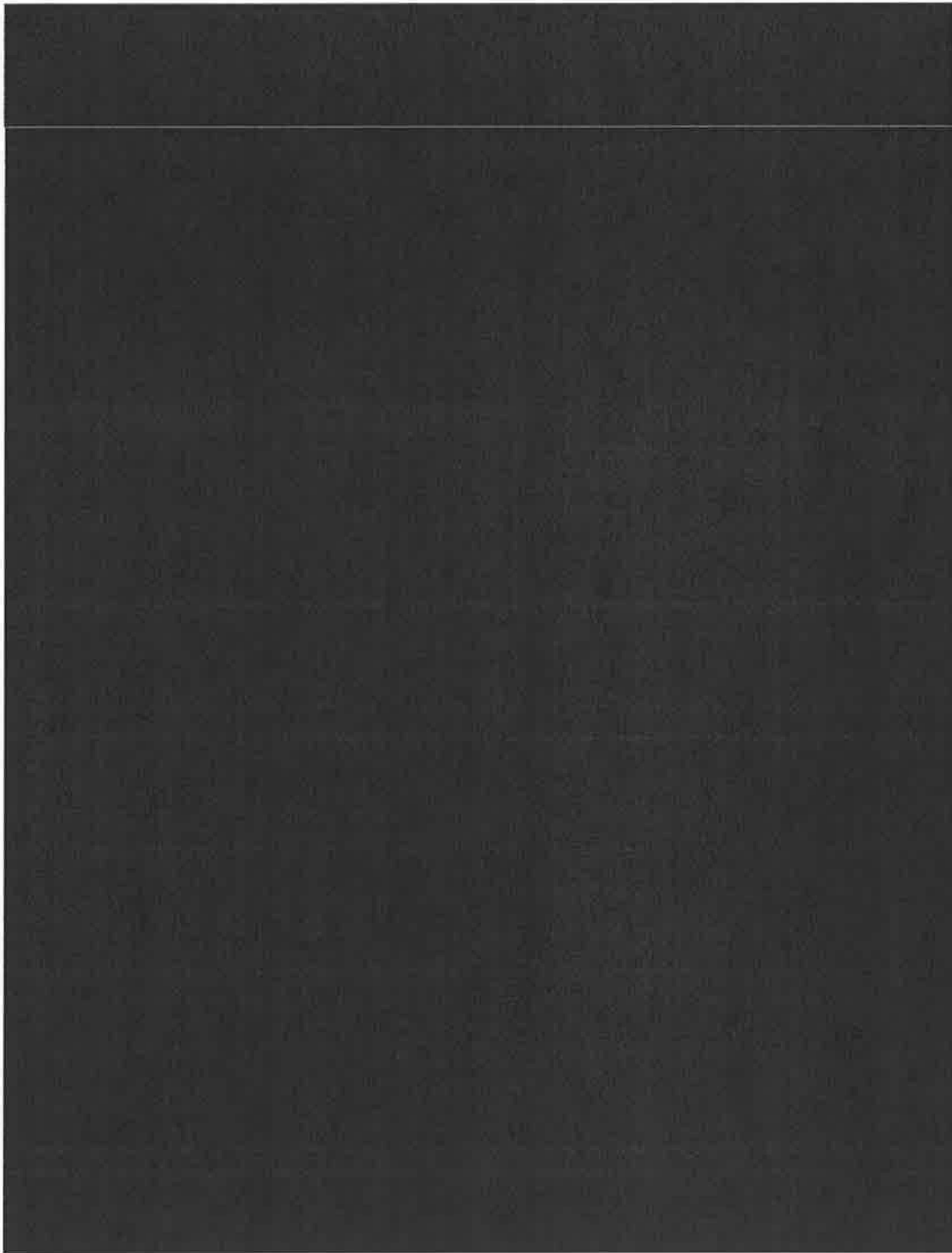


INFORMATION / RENSEIGNEMENTS:



[REDACTED]







Information  
Access to Information  
Intelligence  
Security

Services  
Government  
Intelligence  
Security

Our file: [REDACTED]  
Your file: DC7040-12-212 / MA

Protected

Ms. Andrée Morissette  
A/Director  
Access to Information and Privacy  
Natural Resources Canada  
580 Booth Street, 11th Floor  
Ottawa, Ontario K1A 0E4

NOV 29 2012

Dear Ms. Morissette:

This refers to your consultation letter of October 16, 2012 together with attachments, requesting recommendations for exemption under the *Access to Information Act* pursuant to a request for "I am requesting a list of attendees of the Classified Briefings for Energy Sector Stakeholders from May 1st to the present".

We recommend that the information highlighted in **GREY** in the attached records be exempted

[REDACTED]

It is CSIS practice not to enter section numbers for exemptions next to the deleted portions on pages released to the applicant. Therefore, for national security reasons, please ensure that these section numbers are not included on any of the released documents.

Should you disagree with our recommended exemptions, please advise us to that effect prior to the release of these documents.

Please direct any queries to [REDACTED]

Thank you for consulting with us on this matter.

Yours truly,

[REDACTED]

Coordinator  
Access to Information  
and Privacy

Attachments

Canada

P.O. Box 9732, Station C, Ottawa, Ontario K1G 4G4 C.P. 9732, Succursale C, Ottawa, Ontario K1G 4G4  
Tel: (613) 231-0107 1-877-995-9903 Fax: (613) 842-1271

Tab/Onglet 7

Page 505

**CLASSIFIED BRIEFING FOR ENERGY SECTOR STAKEHOLDERS**  
**SEANCE DE DEBREFFAGE CLASSIFIEE POUR LES PARTIES INTERESSEES A L'ENERGIE**

WEDNESDAY, MAY 18, 2011

Invitees / Participants

**NRCAN:**

Kwamena, Felix  
Anka, Gary  
Lightfoot, Phil  
Morin, Guy  
Desforges, Benoit  
Zrudlo, Lisa  
Entwistle, Sandra

**OUTSIDE INVITEES:**

[REDACTED]  
Alder, Roberts RCMP  
Alves de Jesus, Tiago RCMP  
[REDACTED]  
Athanasilades, John, Sgl RCMP

[REDACTED]  
Bruce, Shelly Canadian Security Establishment  
[REDACTED]

Chorney, David Saskatchewan Research Council  
Coady, Theresa Public Safety Canada  
[REDACTED]

Corcoran, Steve RCMP  
[REDACTED]

Elliott, Wes NEB

CONSULT

000001  
000001

Tab/Onglet 7

Page 506

**CLASSIFIED BRIEFING FOR ENERGY SECTOR STAKEHOLDERS**  
**SEANCE DE DÉBREFFAGE CLASSIFIÉE POUR LES PARTIES INTÉRESSÉES À L'ÉNERGIE**

[REDACTED]  
Gagnon, Jerome Ministry of Public Security Quebec  
[REDACTED]

Garber, Rick DRDC  
Gendron, Angela Carleton University  
Grant, Ian CNSC  
Greenley, Catherine RCMP  
[REDACTED] CSIS

Head, Tim RCMP  
[REDACTED]

King, Reg RCMP  
[REDACTED]

Landra, Keith CNSOPB  
[REDACTED]

[REDACTED] CSIS  
Lapointe, Sandy NEB  
[REDACTED]

Leafloor, Bob Industry Canada  
[REDACTED]

[REDACTED] CSIS  
Legault, Nicole Transport Canada  
LeMay, Robert NEB  
[REDACTED]

McGraw, Shawna New Brunswick Government  
McKelvey, Dale CNSC  
McNaughton, Devin Government of Alberta  
McPherson, Carrie Ann RCMP  
[REDACTED]

Messier, Maxime OND  
[REDACTED]

CONSULT [REDACTED]

000002  
000002

**CLASSIFIED BRIEFING FOR ENERGY SECTOR STAKEHOLDERS**  
**SÉANCE DE DÉBREFFAGE CLASSIFIÉE POUR LES PARTIES INTÉRESSÉES À L'ÉNERGIE**

[REDACTED]  
Nicol, Wendy

RCMP

CSIS

CSIS

O'Hayon, Greg

RCMP

O'Neill, Tim

RCMP

[REDACTED]  
CSIS

Pika, Howard

CNLOPB

Pinka, Stuart

CNLOPB

Poloz, Adriana

RCMP

[REDACTED]  
CSIS

Ruelokke, Max

CNLOPB

Rudner, Martin

Carleton University

CSIS

Saad, Ziad

CEPA

Schramm, Laurier

Saskatchewan Research Council

Scratch, David

CNSOPB

Smith, Maggie (formerly Lackey)

Industry Canada

Stanley, Hal

CNLOPB

Stock, Gordon

Office the Auditor General

[REDACTED]  
CSIS

[REDACTED]  
CSIS a

Therrien, Josée

RCMP

CONSULT

000003  
000003

Tab/Onglet 7

Page 508

**CLASSIFIED BRIEFING FOR ENERGY SECTOR STAKEHOLDERS**  
**SEANCE DE DÉBREFFAGE CLASSIFIÉE POUR LES PARTIES INTÉRESSÉES À L'ÉNERGIE**

[REDACTED]

Way, Fred CNLOPB

[REDACTED]

Węgrzycka, Barbara RCMP

[REDACTED]

Wong, Suki Public Safety Canada

[REDACTED]

Yuen, Wo Saskatchewan Research Council

Zimmer, Jeff Saskatchewan Research Council

[REDACTED]  
[REDACTED]

[REDACTED]

CONSULT

000004  
000004

[REDACTED]

Tab/Onglet 7

Page 509

CLASSIFIED BRIEFING FOR ENERGY SECTOR STAKEHOLDERS  
SÉANCE DE DÉBRIFFAGE CLASSIFIÉE POUR LES PARTIES INTÉRESSÉES À L'ÉNERGIE

THURSDAY, NOVEMBER 17, 2011

Invitees / Participants



Dr. Tiago Alves de Jesus  
Royal Canadian Mounted Police

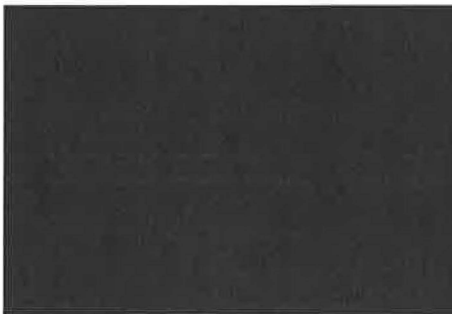
Windy Anderson  
Public Safety Canada

Gary Anka  
NRCan

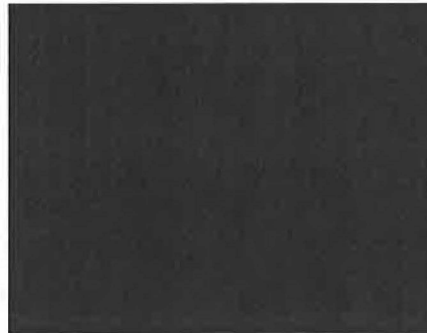
Sgt. John Anthanasiades  
Royal Canadian Mounted Police



Cpt. Hakim Bellal  
Royal Canadian Mounted Police



Mylene Bouzigon  
Canadian Security Intelligence Service



Jeffrey Burton  
NRCan

Luc Cadieux  
Department of Justice Canada

Michelle Cameron  
Royal Canadian Mounted Police



Canadian Security Intelligence Service



Gina Carletti  
Scotiabank



CONSULT

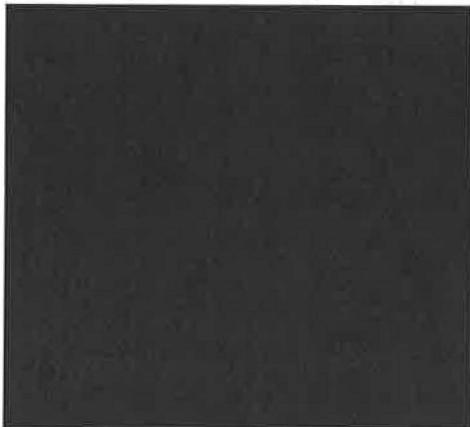
Natural Resources  
Canada

Resources naturelles  
Canada

Canada

000005  
000005

**CLASSIFIED BRIEFING FOR ENERGY SECTOR STAKEHOLDERS**  
**SEANCE DE DÉBREFFAGE CLASSIFIÉE POUR LES PARTIES INTÉRESSÉES À L'ÉNERGIE**



Mark Freiman  
Lerners LLP



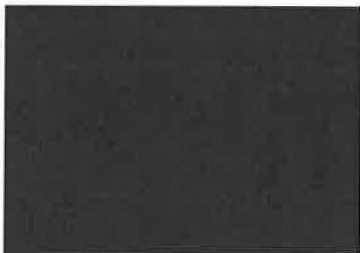
Rick Garber  
Defence Research and Development Canada

Angela Gendron  
Carleton University, CCISS

Tim Gray  
Defence Research and Development Canada

Connie Delisle  
Privy Council Office

Benoit Desforges  
NRCan



Barry Dubreuil  
Atomic Energy of Canada Limited

Wes Elliot  
National Energy Board

Allan Ferguson  
Department of Justice Canada

Noel Flatters  
Royal Canadian Mounted Police

Stephen Fourney  
Public Safety Canada



Canadian Security Intelligence Service

Sandro Hervato  
Industry Canada



Natural Resources  
Canada

Ressources naturelles  
Canada

Canada

000006  
000006



**CLASSIFIED BRIEFING FOR ENERGY SECTOR STAKEHOLDERS**  
**SÉANCE DE DÉBRIFFAGE CLASSIFIÉE POUR LES PARTIES INTÉRESSÉES À L'ÉNERGIE**

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

LAB CSIS

[REDACTED]

[REDACTED]

Canadian Security Intelligence Service

[REDACTED]

Felix Kwamena  
NRCan

Cst. Nancy Lambert  
Royal Canadian Mounted Police

[REDACTED]

Yves Lanthier  
Privy Council Office

[REDACTED]

Canadian Security Intelligence Service

Sandy Lapointe  
National Energy Board

[REDACTED]



Natural Resources  
Canada

Ressources naturelles  
Canada

[REDACTED]

Bob Leafloor  
Industry Canada

[REDACTED]

Nicole Legault  
Transport Canada

[REDACTED]

[REDACTED]

Canadian Security Intelligence Service

[REDACTED]

Jeff McCarthy  
Government of New Brunswick

[REDACTED]

Mark McGowan  
Royal Canadian mounted Police

[REDACTED]

Devin McNaughton  
Government of Alberta

[REDACTED]

Maxime Messier  
Canadian Forces

Canada

000007  
000007

**CLASSIFIED BRIEFING FOR ENERGY SECTOR STAKEHOLDERS**  
**SÉANCE DE DÉBREFFAGE CLASSIFIÉE POUR LES PARTIES INTÉRESSÉES À L'ÉNERGIE**

Gilles Michaud  
Royal Canadian Mounted Police



Guy Morin  
NRCan

Victor Munro  
Royal Canadian Mounted Police



Rob Murray  
Bank of Canada



Canadian Security Intelligence Service



Wendy Nicol  
Royal Canadian Mounted Police



Steven Nordin  
Atomic Energy of Canada Limited

Gerard Normand  
Department of National Defence

John O'Dacre  
Canadian Nuclear Safety Commission  
Greg O'Hayon  
Royal Canadian Mounted Police



National Security Intelligence Service



Canadian Security Intelligence Service

Howard Pike  
Canada-Newfoundland and Labrador Offshore  
Petroleum Board



Isabelle Rivard  
Privy Council Office

Dr. Martin Rudner  
Carleton University



Laurier Schramm  
Saskatchewan Research Council

David Scratch  
Canada-Nova Scotia Offshore Petroleum Board



Natural Resources

Resources naturelles  
Canada



Canada

000008  
000008

CLASSIFIED BRIEFING FOR ENERGY SECTOR STAKEHOLDERS  
SÉANCE DE DÉBREFFAGE CLASSIFIÉE POUR LES PARTIES INTÉRESSÉES À L'ÉNERGIE

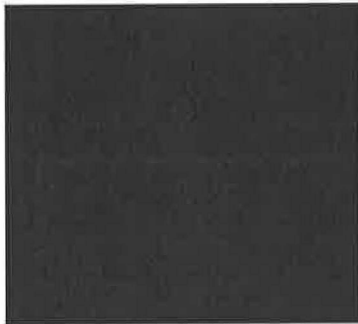
Patrick Smyth  
National Energy Board



Rose Stricker  
Royal Canadian Mounted Police



Paul Thompson  
NB Power Nuclear



Leigh Wolfrom  
Finance Canada

Edward Wood  
Office of the Auditor General of Canada



Natural Resources  
Canada

Resources naturelles  
Canada

Canada

000009  
000009

**CLASSIFIED BRIEFING FOR ENERGY SECTOR STAKEHOLDERS**  
**SÉANCE DE DÉBREFFAGE CLASSIFIÉE POUR LES PARTIES INTÉRESSÉES À L'ÉNERGIE**

**THURSDAY, MAY 24, 2012**

**Invitees / Participants**

[REDACTED]  
Dr. Tiago Alves de Jesus  
Royal Canadian Mounted Police

Michael Baudette  
Canadian Nuclear Safety Commission

[REDACTED]  
Dan Bond  
Royal Canadian Mounted Police

[REDACTED]  
John Brayman  
NRCan

Christine Breton  
Royal Canadian Mounted Police

[REDACTED]  
Ted Broadherst  
Royal Canadian Mounted Police

Charmaine Bulger  
Royal Canadian Mounted Police

Jeffrey Burton  
NRCan

Ric Cameron  
NERC

[REDACTED]  
Canadian Security Intelligence Service

[REDACTED]  
Daniel Chicoyne  
Canada-Newfoundland and Labrador Offshore  
Petroleum Board

[REDACTED]  
Steve Corcoran  
Royal Canadian Mounted Police

CONSULT

Natural Resources  
Canada

Ressources naturelles  
Canada

Canada

000010  
000010

**CLASSIFIED BRIEFING FOR ENERGY SECTOR STAKEHOLDERS**  
**SÉANCE DE DÉBREFFAGE CLASSIFIÉE POUR LES PARTIES INTÉRESSÉES À L'ÉNERGIE**

David Ott  
Public Safety Canada

Mario Deschênes  
NRCan

Benoît Desforges  
NRCan

Connie Deslisle  
Privy Council Office



Keith Durace  
Royal Canadian Mounted Police

Wes Elliot  
National Energy Board

Scott Foster  
Royal Canadian Mounted Police

Stephen Fournay  
Public Safety Canada



Rick Garber  
Defence Research and Development Canada

Angela Gendron  
Carleton University, CCISS

Jean Goulet  
Office of the Auditor General



Canadian Security Intelligence Service



Canadian Security Intelligence Service

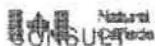
Ross Johnson  
Capital Power Corporation

Canadian Security Intelligence Service



Canadian Security Intelligence Service

Valentine Konza  
NRCan



Natural Resources  
Canada

Ressources naturelles  
Canada

Canada

000011  
000011

**CLASSIFIED BRIEFING FOR ENERGY SECTOR STAKEHOLDERS**  
**SÉANCE DE DÉBRIEFAGE CLASSIFIÉE POUR LES PARTIES INTÉRESSÉES À L'ÉNERGIE**

Felix Kwamena  
NRCan



Canadian Security Intelligence Service



Bob Leafloor  
Industry Canada



André Levesque  
Privy Council Office



Brittany McBain  
Royal Canadian Mounted Police



Barry McLean  
Canadian Nuclear Safety Commission



Maxime Messier  
Department of National Defence

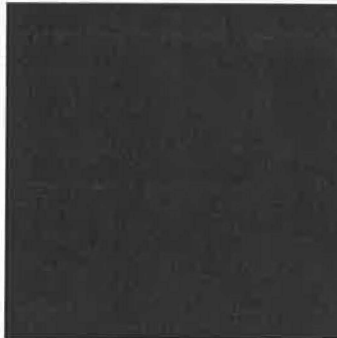
Adam Mohamed  
NRCan



Canadian Security Intelligence Service

Victor Munro  
Royal Canadian Mounted Police

Nicole Murphy  
Royal Canadian Mounted Police



Canadian Security Intelligence Service

Steven Nordin  
Atomic Energy of Canada Limited

Greg O'Hayon  
Royal Canadian Mounted Police

Deborah O'Neil  
Royal Canadian Mounted Police

Tim O'Neil  
Royal Canadian Mounted Police



Natural Resources  
Canada

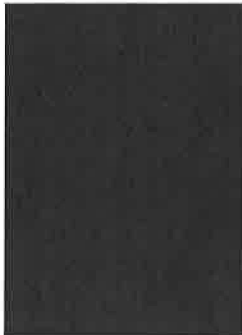
Resources naturelles  
Canada



Canada

000012  
000012

**CLASSIFIED BRIEFING FOR ENERGY SECTOR STAKEHOLDERS**  
**SÉANCE DE DÉBREFFAGE CLASSIFIÉE POUR LES PARTIES INTÉRESSÉES À L'ÉNERGIE**



Dr. Martin Rudner  
Carleton University



Laurier Schramm  
Saskatchewan Research Council

David Scratch  
Canada-Nova Scotia Offshore Petroleum Board



Canadian Security Intelligence Service

Patrick Smyth  
National Energy Board



Canadian Security Intelligence Service



Canadian Security Intelligence Service



Canadian Security Intelligence Service



Canadian Security Intelligence Service

Edward Wood  
Office of the Auditor General of Canada

Robert Zawerbny  
Royal Canadian Mounted Police

Lisa Zrudlo  
NRCan



Natural Resources  
Canada

Resources naturelles  
Canada

Canada

000013  
000013



Natural Resources  
Canada

Ressources naturelles  
Canada

ATIP Secretariat  
550 Booth Street, 11<sup>th</sup> Floor  
Ottawa, ON N1A 0E4  
Facsimile: (613) 993-6693

Secrétariat de l'ATIP  
550, rue Booth, 11<sup>e</sup> étage  
Ottawa, ON N1A 0E4  
Télécopieur: (613) 993-6693

Our file: DC7040-12-212 - MA

October 16, 2012

Ms. [REDACTED]  
Access to Information and Privacy Coordinator  
Canadian Security Intelligence Service  
P.O. Box 9732,  
Station T  
Ottawa ON K1G 4G4

Dear Ms. [REDACTED],

I am writing to inform you that this Department has received a request pursuant to the *Access to Information Act*. The request reads as follows:

(Clarified August 31, 2012)

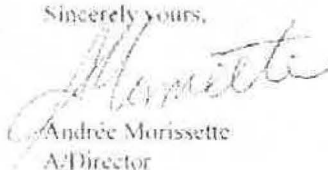
"I am requesting a list of attendees of the Classified Briefings for Energy Sector Stakeholders from May 1st 2011 to the present."

The attached documents, which are relevant to the request, are of interest to your organization. We are seeking your views in regards to disclosure.

Should you feel that all or portions of the documents be withheld, please indicate the section of the *Act* and the specific injury that would result from disclosure. In order to comply with the statutory period for response as set out in the *Act*, a reply by November 5, 2012 would be appreciated. Please forward your views in writing to our address noted above.

Should you have any questions, please do not hesitate to contact Marcia Anderson at (613) 992-1056 or by e-mail at [manderso@nrcan-mecan.gc.ca](mailto:manderso@nrcan-mecan.gc.ca).

Sincerely yours,

  
Andrée Morissette  
A/Director  
Access to Information and Privacy

Enclosures: pages 1-13.





TAB

10

**SECRET**

---

**File No.: 2800-154  
(TD R503)**

**REVIEW OF CSIS'S PRIVATE SECTOR  
RELATIONSHIPS  
(SIRC STUDY 2010-02)**

**Security Intelligence Review Committee  
February 14, 2011**

February 14, 2011

1

Tab/Onglet 10

Page 712

2 of 19

AGC1064

## Table of Contents

TABLE OF CONTENTS .....	Error! Bookmark not defined.
1 INTRODUCTION .....	3
2 METHODOLOGY AND SCOPE .....	4
3 CSIS LIAISON AND AWARENESS EFFORTS .....	5
3.1 Goals and Outputs of CSIS Liaison and Awareness Efforts .....	6
3.2 Challenges Associated with CSIS Public Liaison and Awareness Efforts.....	10
4 WORKING WITH THE PRIVATE SECTOR AS "PARTNERS" .....	11
4.1 Sharing Information .....	12
4.2 Partial Solutions to the Limitation on Information Sharing.....	14
5 CONCLUSION .....	17
SUMMARY OF FINDINGS.....	18
SUMMARY OF RECOMMENDATION .....	18

February 14, 2011

2

Tab/Onglet 10

Page 713

## 1 INTRODUCTION

One of the most visible trends currently affecting security intelligence is the emphasis on achieving better intelligence by increasing integration and collaboration. This emphasis, in turn, places a new importance on the Service's relationships with partners, both foreign and domestic, including with law enforcement. This same emphasis also creates an incentive for the Service to develop relationships with non-traditional partners, such as the private sector.

The role of the private sector was acknowledged in the comments of former CSIS Director Jim Judd, who spoke of the addition of "new players" in security intelligence, asserting that the private sector has moved "into the field," bringing "new voices, new expertise and new opinions."<sup>1</sup> It is further reflected in the Government of Canada's National Security Policy (NSP), released in 2004, which identifies the need for "a co-ordinated approach with other key partners - provinces, territories, communities, the private sector and allies."<sup>2</sup> Nowhere is the new imperative to work closely with the private sector more visible than in the area of "critical infrastructure", where the need to protect that infrastructure requires the active participation of its private sector owners and operators.<sup>3</sup>

In past reviews, SIRC examined and commented on this movement towards greater cooperation and collaboration through CSIS's partnerships and outreach activities.<sup>4</sup> The present study focuses on the Service's relationship with the private sector and addresses issues connected to the evolving, and growing, role of the private sector in the context of national security. This is the first time that the Committee has examined this topic; as such, it is a baseline review that may inform subsequent reviews.

The review looks at the relationship between CSIS and the private sector in two ways. First, the discussion focuses on the Service's general liaison efforts vis-à-vis the private sector, the general goals of which are to raise awareness in the private sector, and in the public more broadly, about the Service and its mandate, as well as to advise certain vulnerable sectors of

---

<sup>1</sup> Remarks by Jim Judd, Director of CSIS, at the Global Futures Forum Conference, Vancouver, April 15, 2008.

<sup>2</sup> Privy Council Office, "Securing An Open Society: Canada's National Security Policy", April 2004, p. 5.

<sup>3</sup> This is further reinforced in the 2009 Public Safety Canada "National Strategy for Critical Infrastructure" that explicitly states that responsibility for critical infrastructure is shared by all levels of government - federal, provincial/territorial, and municipal - and the critical infrastructure "owners and operators". Public Safety Canada, "National Strategy for Critical Infrastructure", 2009, p. 3.

<sup>4</sup> See, as examples, "CSIS's Activities Involving Fundamental Societal Institutions" (SIRC Study 2009-03) and "CSIS's Relationships with Select Domestic Front Line Partners" (SIRC Study 2009-04).

specific threats<sup>5</sup>. This section goes on to discuss how these liaison efforts also serve the Service's own information needs by allowing the Service to tap into information held by the private sector. This section concludes with a recommendation that the Service expand on the efforts of the Regions to be more strategic in engaging the private sector, by articulating a Service-wide strategy to manage its relations with the private sector.

The second section moves from the more general liaison relationships to a discussion of the possibilities and constraints of CSIS working operationally in closer partnerships with the private sector, something that would, *inter alia*, require that the Service share information much more freely than is currently the case. This discussion refers principally to critical infrastructure, an area with much potential for cooperation given the substantial convergence of national and private interests. Although CSIS is not the lead within the federal government for critical infrastructure<sup>6</sup>, [REDACTED] as the principal collector of security intelligence, CSIS is one of the agencies implicated in this area.

The review concludes by finding that there are significant limitations on the extent to which CSIS is able to participate in close collaboration with the private sector on a legal and practical level. First and most significantly, the *CSIS Act*, developed in a different era with a different threat environment, expressly does not permit the sharing of intelligence with the private sector. Although operational policies have been developed to govern the sharing of information with the private sector, the policies are appropriately restrictive and provide strict parameters in which information can be disclosed. The Service also faces operational considerations - in particular the need to protect the integrity of an investigation - that deter it from sharing information with the private sector. On the other side of the equation, there is some reluctance on the part of the private sector to share proprietary information with law enforcement and government agencies, including CSIS.

That said, as will be discussed, there are a number of ways in which the Service does support the information needs of the private sector, albeit often indirectly by supporting the initiatives of other departments and agencies.

## 2 METHODOLOGY AND SCOPE

The review process focussed on CSIS interaction with representatives of specific industries from the viewpoint of two CSIS Regions - [REDACTED] - each with a different private sector focus. [REDACTED]

<sup>5</sup> As an example, CSIS's counter-intelligence activities would include an awareness component directed at sectors of the economy which are vulnerable to economic espionage.

<sup>6</sup> Public Safety Canada has the lead responsibility for coordinating Government of Canada efforts vis-à-vis critical infrastructure.

The intent was to have a sample that would permit a broad-based assessment of Service-private sector interaction. It is important to note that these cases do not represent all CSIS relationships with the private sector. CSIS has many relationships that serve a diverse range of requirements. [REDACTED]

SIRC received briefings at CSIS HQ and in the two Regions. Hard copy and electronic documentation were also examined. The review period extended from March 1, 2006 to January 1, 2010.

### 3 CSIS LIAISON AND AWARENESS EFFORTS

CSIS's relationships with the private sector range from the informal, with infrequent, ad hoc contacts to more formalized relationships [REDACTED]. This first section will describe what types of general liaison relationships exist and how they are managed.

CSIS's liaison and outreach activities are conducted primarily at the regional level, by regional officers who either respond to requests for information or who initiate contact with firms or organizations in the private sector to identify opportunities for briefings. [REDACTED]

CSIS has two main programs through which the bulk of these interactions take place: the Public Liaison and Outreach Program and the Liaison /Awareness Program.

The Public Liaison and Outreach Program is a means of informing the private sector, and the public more generally, about the mandate of CSIS. These briefings, referred to [REDACTED] are given to a range of public and private sector organizations, including schools and private security firms, security personnel at shopping malls, and operators of public transportation systems. These briefings are intended both to sensitize the recipients to CSIS's mandate and, more importantly, to establish CSIS as a possible point of contact for the private sector, and for members of the public in the event that they have information of possible relevance to national security.

[REDACTED]

February 14, 2011

5

Through its Liaison/Awareness Program, CSIS delivers more targeted, albeit still general information to the private sector and other public organizations (e.g. universities) on specific threats, including cyber threats and threats posed to Canadian interests by foreign governments known to engage in espionage. This type of outreach is often used in connection with specific investigations

[REDACTED]

[REDACTED]

the Regions are expected to foster communication and build awareness through partnerships with key public and private entities by educating and enabling our partners to identify what is a counterintelligence risk. [REDACTED]

[REDACTED]

### 3.1 Goals and Outputs of CSIS Liaison and Awareness Efforts

The following section discusses the ways in which these liaison and outreach efforts are useful to the Service and concludes with a discussion of the need to be more strategic and focussed in managing these outreach efforts. The issue of the Service's outreach efforts to non-traditional partners examined here is closely linked to SIRC's recent review of CSIS's activities involving fundamental institutions, specifically religious institutions. This earlier study looked at the outreach program that was designed by the Service to serve as a link [REDACTED] and concluded that if CSIS wishes to sustain its community outreach program, it must be more strategic, and clearly establish benchmarks against which the program's success can be measured.<sup>10</sup>

Service interactions with the private sector are important, in part because the private sector is ideally suited to provide the Service with unsolicited, but potentially valuable street-level information. Although beyond the scope of this review to examine in detail, it is worth noting that the ground rules for how private sector organizations may collect,

---

<sup>10</sup> SIRC Study, "CSIS's Activities Involving Fundamental Institutions", 2009. This study also found that community engagement requires the relationship to be mutually beneficial.

use or disclose personal information are set out in the *Personal Information Protection and Electronic Documents Act* (PIPEDA). The Act stipulates that businesses must obtain the individual's consent when they collect, use or disclose personal information.

However, section 7.3 permits disclosure of personal information without "knowledge or consent" for reasons of law enforcement, national security, defence of Canada, conduct of international affairs, and where otherwise required by law.<sup>11</sup>

The potential benefit to the Service of establishing contact with the private sector is that contacts who observe something that is a cause for concern from a national security perspective, may alert CSIS.<sup>12</sup> Likewise, CSIS liaison contacts can generate new investigative leads and be a source of information important in the context of specific investigations.

[REDACTED]

Contact with the private sector can [REDACTED] also assist the private sector in protecting itself against threats.<sup>14</sup> One such key area is cyber security, [REDACTED]

<sup>11</sup> The *Privacy Act* is the federal legislation that sets out rules for how institutions of the federal government, including CSIS, must deal with the personal information of individuals and limits the collection, use and disclosure of personal information. Sections 4 and 5 of the Act govern the collection of personal information. Section 4 indicates only that any personal information collected by a federal government department or agency must relate directly to the programs or activities of the institution. With certain exceptions, section 5 requires institutions to collect personal information directly from the person concerned and that the person be informed of the purpose of the collection. However, this is not necessary under the Act in instances when informing the individual would "defeat the purpose, or prejudice the use for which the information was collected" as per 5(3)(b) of the Act. Notwithstanding CSIS's obligations under the *Privacy Act*, as will be discussed in the next section, CSIS does not as a rule share information with the private sector given extant legal, policy and operational restrictions.

<sup>12</sup> In the U.S., there are at least two well known examples of the private sector supplying vital information to security officials. In 2001, a flight school reported a suspicious student who later turned out to be a 9/11 co-conspirator. The student was not present for the attacks because he was already in custody, thanks in part to the actions of the flight school. In another instance, a New Jersey store employee was described as "instrumental" in preventing a terrorist attack in Fort Dix in 2006 when he alerted authorities to a customer who had requested that terrorist training footage be transferred from VHS to DVD. See Stacy Reiter Neal, "Business as Usual? Leveraging the Private Sector to Combat Terrorism" in *Perspectives of Terrorism*, Volume II, Issue 3, February 2008.

<sup>13</sup> [REDACTED]

<sup>14</sup> This finding is consistent with SIRC's previous study that looked at the Liaison/Awareness Program in the context of CSIS's efforts to provide counter proliferation briefings to individuals working or studying in the private sector. In this case, the Service used



[REDACTED] the findings of an April 2009 University of Toronto report that concluded that "a vast electronic spying operation has infiltrated computers and stolen documents from hundreds of government and private offices around the world..."<sup>15</sup> [REDACTED]

CSIS liaison work and relationship building are also essential with respect to securing and maintaining access to more specific information. [REDACTED]

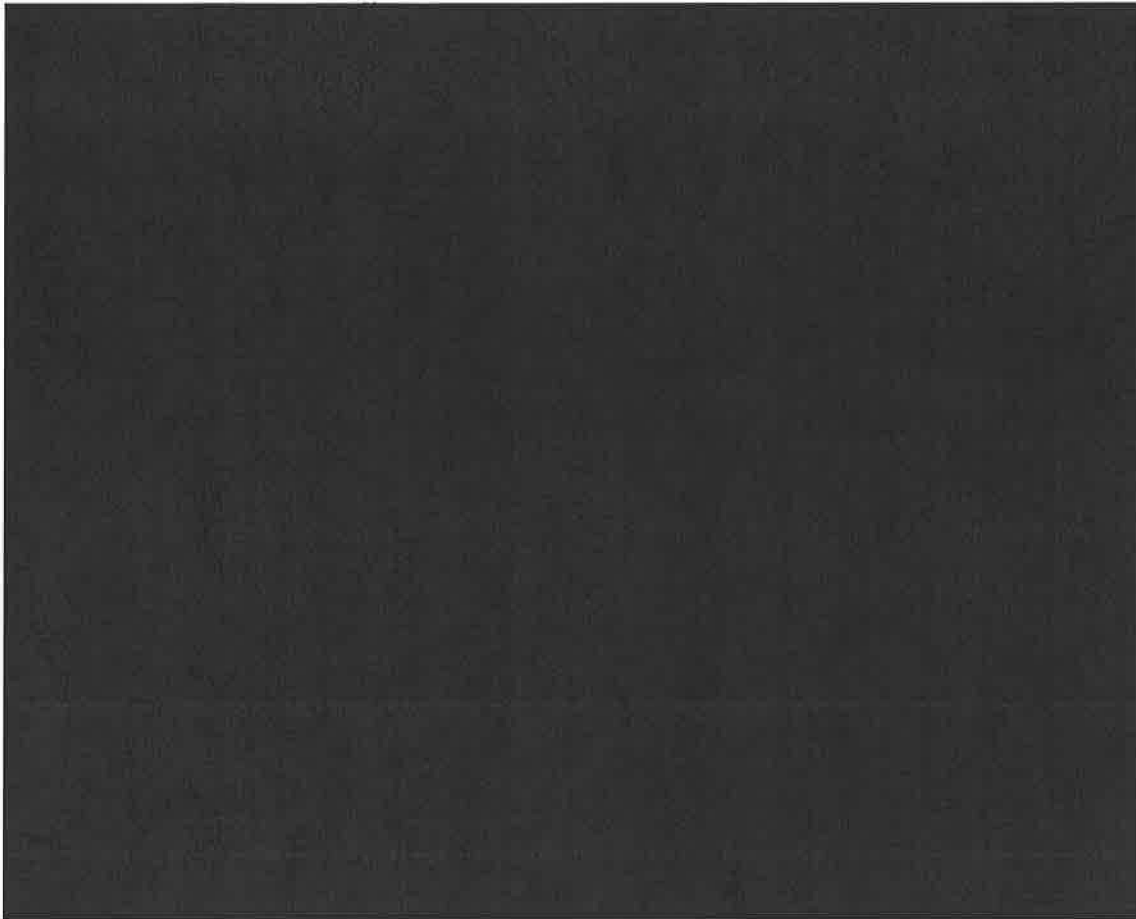
Finally, liaison relationships can be instrumental in securing Service access to private sector firms in specific instances when the Service is looking for more targeted information or assistance. [REDACTED]

the liaison program to develop contacts in relevant sectors and to sensitize individuals to the threat posed by proliferation. SIRC noted that the program succeeded in developing an ongoing dialogue with the Canadian business community about the threat posed by the proliferation of WMD (weapons of mass destruction), and intensified cooperation among industry representatives in this area. See SIRC's 2005 "Review of a Counter Proliferation Investigation" [REDACTED]

<sup>15</sup> "Vast Spy System Loots Computers in 103 Countries", *The New York Times*, March 28, 2009.

February 14, 2011

8



SIRC found that developing a rapport with specific individuals is key to CSIS tapping into private sector information. In particular, the Committee recognizes the efforts of the liaison officers in this regard and the skill that they employ in developing and maintaining these relationships to the advantage of the Service. This is noteworthy in light of the fact that there is very little CSIS can "give" the private sector in return, a theme that will be explored in more detail in following section.



February 14, 2011

19

### 3.2 Challenges Associated with CSIS Public Liaison and Awareness Efforts

Both [REDACTED] Region identified a general goal to liaise and establish a relationship, or at least make contact, with as many companies and organizations as possible. However, SIRC believes that there may be a need to devise ways of maximizing the return to the Service of these liaison efforts given the almost limitless number of private sector firms and organizations. Being focused is especially critical in light of the limited resources available to the Service to devote to this effort.

SIRC was told that the current, somewhat ad hoc nature of the Service's liaison efforts vis-à-vis the private sector represents a change, and that there were more coordinated efforts in the past to be targeted and strategic with respect to the private sector. [REDACTED]

The absence of a current strategy for managing relations with the private sector was explicitly acknowledged by the Service. Despite the efforts of the Regions to fill this gap, there appears to be no or little HQ involvement in the process. As noted, [REDACTED] Region has a dedicated Liaison Unit, but not all Regions have that same capacity. In the interests of leveraging the limited resources available for these activities, and of capitalizing on the experience already gained, SIRC would encourage an enhanced Service-wide discussion on the management of private sector relationships. To this end, **SIRC recommends that the Service expand on the efforts of the Regions by articulating a Service-wide strategy on managing its relations with the private sector.**

A more strategic approach that addresses issues of priority- and goal-setting could assist the Service in dealing with a potential problem identified by both [REDACTED] Region: that current liaison efforts run the risk of [REDACTED]

From SIRC's perspective, an effective strategy would involve identifying those sectors with the greatest potential to be of strategic value to the Service. [REDACTED]

February 14, 2011

10

#### 4 WORKING WITH THE PRIVATE SECTOR AS "PARTNERS"

This section takes a more detailed look at the limitations and possibilities of the Service working more closely with the private sector as full operational "partners", which would require substantial information-sharing and the development of an agreed set of objectives to serve the divergent goals of all partners.

The question of how the Service can, or cannot, work more closely with the private sector will be examined in the context of the protection of critical infrastructure, which has been identified as a principal security concern by the Government of Canada.<sup>26</sup> The government has articulated a "partnership" approach in Public Safety's "National Strategy for Critical Infrastructure". Specifically, the Strategy envisages cooperation and collaboration at different levels, with the goal of protecting critical infrastructure. Different responsibilities are assigned to various federal departments and agencies; between and among the three levels of government; and to partners outside of government. Critical infrastructure protection thus requires not just substantial interdepartmental cooperation, but also public-private collaboration. Although it is not the lead for critical infrastructure protection, CSIS is implicated in this discussion as the main collector of security intelligence.

**SIRC concluded that there are real limitations for CSIS in developing true partnerships with the private sector in the context of critical infrastructure protection, and in general.** In particular, the *CSIS Act* and the strict regime governing information-sharing limits the ability of the Service to work closely with the private sector. This challenge is not unique to Canada and, indeed, is something that western intelligence services in general are grappling with.<sup>27</sup>

<sup>26</sup>

It should be pointed out that the discussion will not focus on one sector of critical infrastructure as there are many, each sector exhibiting unique issues and different configurations of partners involving federal, provincial, and local government bodies, as well as different private sector entities. On CSIS's website, "critical infrastructure" is defined as "physical and information technology facilities, networks and assets (e.g. energy distribution networks, communications grids, health services, essential utilities, transportation and government services) which, if disrupted or destroyed could have a serious impact on the health, safety, security and economic well-being of Canadians". Public Safety's "National Strategy for Critical Infrastructure" classifies ten sectors under the rubric of "critical infrastructure": energy and utilities; communications and information technology; finance; health care; food; water; transportation; safety; government; and manufacturing.

<sup>27</sup>

For example, the March 2009, United Kingdom's Strategy for Countering International Terrorism, *Pursue Prevent Protect Prepare*, identifies as a challenge that "our understanding of those risks [for terrorism] will need to be shared with those responsible for [public] sites and public safety. Government will need to strike a balance between the familiar 'need to know' and the ever more important 'requirement to share'." There are many such statements coming as well from the United States.

However, there are several ways in which the Service does support the private sector, often by participating in the initiatives of other departments and agencies. This is consistent with the integrated approach to counterterrorism, an approach that emphasizes bringing together the range of governmental and non-governmental organizations to address national security.

#### 4.1 Sharing Information

The main challenge with respect to cooperation with the private sector has been accommodating the need, acknowledged by the Service as legitimate, of the owners and operators of critical infrastructure to have access to security intelligence while working within a system based on secrecy and the need to know principle.<sup>28</sup>

Indeed, [REDACTED] Regions reported that there is significant demand in the private sector for CSIS intelligence.<sup>29</sup> However, existing legal and operational guidelines governing information-sharing, developed before 9/11 created an impetus towards greater cooperation with a broader range of partners, limit the depth and scope of private-public collaboration. [REDACTED] the most substantial impediment is the fact that the *CSIS Act* does not contemplate disclosure of information collected by CSIS, to non-traditional/non-governmental partners such as the private sector.

#### Section 12: "Duties and Functions of Service"

Section 12 of the *CSIS Act* is the source of CSIS's authority to collect, analyse and retain information and intelligence on activities that are considered "threats to the security of Canada." It is also the basis on which the Service reports and advises the Government of Canada on its findings. Section 12 is important in this context because it limits the Service's "duties and functions" to reporting to and advising the Government of Canada, thereby restricting the Service's authority to report and advise individuals or organizations outside the Government of Canada, including the private sector.

#### Section 19: Disclosure of Intelligence to Government Actors

Section 19 of the *CSIS Act* prohibits disclosure of information obtained by the Service in the course of its investigations except for the purposes of the performance of its duties and functions

<sup>28</sup> SIRC was told that some, though not all, individuals in private sector firms understand the limits imposed on intelligence agencies in terms of sharing information. [REDACTED]

<sup>29</sup> One of the key critical infrastructure sectors in Canada - energy - has been the target of terrorist attacks here in Canada (Encana), and Canadian owned and managed energy assets have been identified as targets by terrorists overseas. In light of this, it is not surprising that there is a demand in the Canadian energy sector in particular for information the Service can provide on these or related threats.

under the Act, or the administration or enforcement of the *CSIS Act* or other laws. Section 19 specifies those situations where sharing information is permissible that depart from the Service's authority under Section 12. In particular, disclosures to law enforcement and to officers of the court in furtherance of an investigation or prosecution are permissible, as are disclosures to the Ministers of National Defence and International Affairs, or departmental officials, when the information is relevant to defence or international affairs. Section 19 also allows the Minister of Public Safety to authorize the Service to make disclosures to other Ministers or persons in the public service in the "public interest". The Act explicitly does not provide for the disclosure of information to the private sector.

### **"Special" Disclosures of Intelligence to Non-Government Officials**

CSIS has developed operational policies<sup>30</sup> to address the different circumstances under which information or intelligence may be disclosed to the private sector and other non-traditional partners. In particular, the Service may make "special" disclosures outside the Government of Canada in instances when the disclosure is deemed essential to the "national interest". This would involve disclosing specific and detailed information to Members of Parliament and Senators who are not Ministers of the Crown; governments, elected officials and institutions of the provinces and municipalities; and individuals in the private sector.

Ministerial approval is required to disclose security information to non-traditional partners, and this reflects the seriousness with which the Service protects its information.<sup>31</sup> Of note, in all instances of special disclosures, the CSIS Director is required to submit a report to SIRC. [REDACTED]

### **"Selective" Disclosures of Information to Non-Government Actors**

The Service may also make "selective" disclosures of information to members of the public, including those in the private sector, in order to carry out mandated investigations and programs and on a strict need to know basis. Policy stipulates that when making such disclosures, CSIS must ensure that its sources and methodologies are protected to the fullest extent possible, and that the rights, privacy and employment of an individual are not unnecessarily placed at risk. Disclosing that you are a CSIS employee to a member of the public [REDACTED] would be an example of such a disclosure.<sup>32</sup> Most information the Service shares with the private sector falls into the category of selective disclosures.

Despite the limitations on information-sharing, SIRC has found that the Service is committed to finding ways to share information with the private sector or other non-traditional partners in the event of an imminent threat to life. One option is to declassify the information so that it can be disseminated. [REDACTED]

<sup>30</sup>

Of particular relevance here is OPS-602 "Disclosure of Security Information or Intelligence". There are a number of other operational policies that deal with disclosures to specific partners, including law enforcement, that are not discussed here.

[REDACTED]

However, there are situations that are less clear

[REDACTED]

An additional challenge to cooperation with the private sector is

[REDACTED]

Risk assessments combine an analysis of a given entity's ability and intent to carry out an attack (in general or against a specific location, system, or installation) with an assessment of the specific target's vulnerabilities. This focus on the *target* or location of a potential attack that distinguishes a risk assessment from a more conventional *threat* assessment, which focuses on the potential *sources* of a threat.<sup>34</sup> It is also this focus on the potential location or target that makes risk assessments attractive to the private sector.

[REDACTED]

#### 4.2 Partial Solutions to the Limitation on Information Sharing

February 14, 2011

14

There are other, partial solutions to the limitation on sharing classified information that focus on sharing more unclassified information and expanding the number of private sector individuals with security clearances.

SIRC was advised that some of the Service's sharing of unclassified security information with the private sector takes place through ITAC (the Integrated Threat Assessment Centre), the integrated model for sharing and analyzing multi-source intelligence related to terrorism.

ITAC produces all-source, classified and unclassified threat assessments that are distributed to the private sector, first responders, and other federal and provincial/territorial departments and agencies. Provincial and federal institutions, including CSIS, support ITAC through their secondees. Secondees bring diverse skills and experiences to the Centre and facilitate access to information controlled by their respective organizations. This is one way, albeit indirectly, for CSIS to reach a broader public audience.<sup>36</sup>

CSIS also distributes ITAC unclassified products directly to industry. ITAC products are thus an important tool for liaison staff in that they are often the only item that the Service can share with the private sector (and other non-traditional partners).<sup>37</sup> An unclassified ITAC threat assessment was produced for the energy sector in October 2010: "Threat to Canadian Oil Company in Iraq". The report, which contained a general assessment of the threat against a particular company, provides the following rationale: "ITAC is providing this report for the situational awareness of the Canadian company, as well as its broader private sector readership".<sup>38</sup>

The Regions and ITAC did identify the challenge of convincing private sector recipients of the value of unclassified information. Industry clients are reportedly gradually coming to understand that unclassified assessments from ITAC, having gone through an extensive vetting process, are more reliable than information from open sources.

Efforts are also underway to increase the number of private sector individuals with security clearances.<sup>39</sup> A prominent example is the classified energy briefing led by Natural Resources Canada (NRCan), cited as one of the main mechanisms through which the Service shares classified information with the energy sector. These briefings, which typically take place at CSIS HQ and with CSIS support, are led by NRCan's Energy Infrastructure Protection Division,

<sup>36</sup> ITAC is consciously trying to build its own relationships with the private sector and has developed a large distribution network for its unclassified products, [REDACTED]

<sup>37</sup> The goal for ITAC is to have 50% of its products be unclassified. Of the [REDACTED] ITAC assessments prepared to date, approximately 45% have been unclassified. Part of the strategy has been using unclassified, open source material.

<sup>38</sup> ITAC unclassified Threat Assessment, "Threat to Canadian Oil Company in Iraq", 2010 10 01.

<sup>39</sup> There are now more firms with individuals with security clearances. [REDACTED] Region reported that private companies have been known to ask the Service for clearances; however, obtaining a security clearance requires that a government department or agency act as a sponsor [REDACTED]



established in 2001 with a mandate to, *inter alia*, liaise with the energy industry in Canada and provide leadership and support to the energy sector to strengthen the protection of Canada's critical energy infrastructure.<sup>40</sup>

[REDACTED]

The NRCan bi-annual classified briefings are a good example of how the Service can participate in a public-private relationship between its federal government partner (NRCan) and the private sector on a security issue.

[REDACTED]

The Service is also able to support the information needs of the private sector by conducting security clearances for the private sector. Through the Sensitive Site Screening program, for example, the Service provides security clearances for individuals with access to sensitive locations, including, for example, international airports, and events such as the Olympics.<sup>43</sup> This program also covers Canada's nuclear sites.

[REDACTED]

The Canadian Nuclear Safety Commission (CNSC) is the federal regulator of the nuclear sector and is responsible for regulating the entire life cycle of nuclear power plants and every aspect of their operation. In 2001, the CNSC imposed regulations under the *Critical Infrastructure*

---

<sup>40</sup>

NRCan's leadership in this area stems from its legislative responsibility for national energy issues, for international relations related to energy, and for civil emergency planning and response to energy-related emergencies.

[REDACTED]

February 14, 2011

16

*Protection Act* that require employees having access to nuclear sites to have at least Site Access Clearances (SAC).

To put the size of the Service's contribution to the nuclear sector into perspective, for 2006/2007 and 2007/2008 combined, the Service performed approximately 27,100 clearance checks for the sector. SIRC views the Service's activities in this area as a positive development that contributes to the security of critical infrastructure in a very concrete way.

## 5 CONCLUSION

This was a baseline review, SIRC's first examination of the Service's relationships with the private sector. It examined generally how private sector relationships are managed by the Service and identified some of the challenges and opportunities presented by these relationships. Of particular interest are issues connected to the sharing and receiving of information to and from the private sector, since information sharing is closely connected with the core mandate of the Service - to collect intelligence on threats to Canada, some of which implicate the private sector very directly.

SIRC observed that there is a new emphasis on increasing integration and collaboration in security intelligence, and that there is a private sector component of this trend. The consensus appears to be that collaboration is both good and necessary.<sup>44</sup> This is consistent with SIRC's own observations with respect to the utility of developing relationships with the private sector. SIRC applauds the efforts of the Regions to be more strategic and focused with respect to engagement of the private sector and encourages the Service to go further in this regard.

SIRC will continue to examine CSIS's relationships with the private sector in upcoming reviews as, returning to the remarks of former Director Judd, the private sector has "moved into the field". As part of these reviews, SIRC will pursue, as appropriate, the issues raised in this study to enhance its understanding of the benefits and challenges of the Service's relationships with the private sector as they continue to evolve.

<sup>44</sup>

See, for example, "Public-Private Partnerships (PPPs) for the Protection of Vulnerable Targets against Terrorist Attacks: Review of Activities and Findings", UNICRI (United Nations Interregional Crime and Justice Research Institute), (January 2009); Matthew J. Simeone, Jr., "Integrating Virtual Public-Private Partnerships into Local Law Enforcement for Enhanced Intelligence-led Policing" in *Homeland Security Affairs*, Supplement No.2 (2008); Jon D. Michaels, "All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror", in *California Law Review*, Vol. 96 (2008); and, Office of the Director of National Intelligence, "United States Intelligence Community (IC) 100 Day Plan for Integration and Collaboration" (2004).

February 14, 2011

17

## SUMMARY OF FINDINGS

- SIRC found that developing a rapport with specific individuals is key to CSIS tapping into private sector information. In particular, the Committee recognizes the efforts of the liaison officers in this regard and the skill that they employ in developing and maintaining these relationships to the advantage of the Service.
- SIRC observed that there are elements of the intelligence system that impede the development of true partnerships with the private sector in the context of critical infrastructure and in general.

## SUMMARY OF RECOMMENDATION

- SIRC recommends that the Service expand on the efforts of the Regions to be more strategic and focused with respect to engagement of the private sector by articulating a Service-wide strategy on managing its relations with the private sector.

February 14, 2011

18

Tab/Onglet 10

Page 72

## CLASSIFIED BRIEFING FOR ENERGY & UTILITIES SECTOR STAKEHOLDERS

Hosted by Natural Resources Canada (NRCan) — in collaboration with CSIS and RCMP  
LOCATION: Canadian Security Intelligence Service, 1941 Ogilvie Road, Ottawa, Ontario  
PURPOSE: To Discuss National Security and Criminal Risks to Critical Energy Infrastructure  
CHAIR: Jeff Labonté, Director General, Petroleum Resources Branch, NRCan

### DRAFT AGENDA

AGENDA THEME: *SECURITY OF ENERGY RESOURCES DEVELOPMENT*

**Wednesday, May 22, 2013**

6:30 PM – 9:00 PM : NETWORKING RECEPTION FOR ALL PARTICIPANTS  
DRAWING ROOM, FAIRMONT CHÂTEAU LAURIER, 1 RIDEAU STREET, OTTAWA  
RECEPTION CO-HOSTS:

**Thursday, May 23, 2013**

**Breakfast, Lunch and Coffee**

<b>7:00 – 8:00</b>	<b>REGISTRATION</b>	
8:00 – 8:05	CSIS Welcome and Protocols	
8:05 – 8:10	Reminder – Security Clearance Obligations	Raynald Lampron, NRCan
8:10 – 8:20	Introductory Remarks and Roundtable Introductions	Jeff Labonté, NRCan
8:20 – 8:50		Al Jones, CSIS
8:50 – 10:20	Cyber Security Briefing	Windy Anderson, CCIRC
<b>10:20 – 10:30</b>	<b>BREAK</b>	
10:30 – 11:15	Active Cyber Campaigns Against the U.S. Energy Sector	TBC
11:15 – 12:00		
<b>12:00 – 13:30</b>	<b>LUNCH and Networking Break</b>	
13:30 – 14:30	Inside Threat at the Royal Canadian Navy Case	Larry Tremblay, Chief Superintendent, RCMP
	<b>CASE STUDIES</b>	
14:30 – 15:15		
15:15 – 16:00	BC Resource Development JWG	RCMP INSET/ Sgt. Bill Kalkat / Laurie MacDonell
16:00 – 16:30	Round Table and Wrap-Up	Jeff Labonté, NRCan (Facilitator)

Note: The next Classified Briefing for Energy Sector Stakeholders is scheduled for: November 21, 2013  
(Preceded by the Networking Reception on WEDNESDAY, NOV. 20, 2013 - details to follow)



Natural Resources  
Canada

Ressources naturelles  
Canada

## CLASSIFIED BRIEFING FOR ENERGY & UTILITIES SECTOR STAKEHOLDERS

Hosted by Natural Resources Canada (NRCan) -- in collaboration with CSIS and RCMP  
 LOCATION: Canadian Security Intelligence Service, 1941 Ogilvie Road, Ottawa, Ontario  
 PURPOSE: To Discuss National Security and Criminal Risks to Critical Energy Infrastructure  
 CHAIR: Jeff Labonte, Director General, Population Resources Branch, NRCan

### AGENDA

AGENDA THEME: SECURITY OF ENERGY RESOURCES DEVELOPMENT

**Wednesday, November 28, 2012**

6:30 PM - 9:00 PM, NETWORKING RECEPTION FOR ALL PARTICIPANTS  
 ROOM: BALL ROOM MONT-CHATEAU LAUREN, 1 HEDRAL STREET, OTTAWA  
 RECEPTION CO-HOSTS:

**Thursday, November 29, 2012**

**Breakfast, Lunch and Coffee Breaks**

7:00 - 8:00	REGISTRATION	
8:00 - 8:05	CSIS Welcome and Protocols	
8:05 - 8:20	Introductory Remarks and Roundtable Introductions	Jeff Labonte, NRCan
8:20 - 8:50		Al Jones CSIS
8:50 - 9:50	National Security Criminal Investigations Update	James Mazila, Assistant Commissioner, National Criminal Investigation, RCMP
9:50 - 10:20		
10:20 - 10:40	BREAK	
10:40 - 11:00	Strategic Overview of Cyber Threats	Dr. Tiago Da Jesus, RCMP
11:00 - 11:45	Active Cyber Campaigns Against the U.S. Energy Sector	
11:45 - 12:15	Cyber Threats	Wendy Anderson, CCIRC
13:15 - 15:15	Industry Case Studies:	
15:15 - 16:15	Ubiquitous Convergence of Physical and Cyber Security: Threats and Opportunity	Professor José Fernando Tróia, Polytechnique de Montréal
16:45 - 16:30	Round Table & Wrap Up	Jeff Labonte, NRCan (facilitator)

Note: This document is classified as Secret and is to be controlled under the Access to Information Act. / Ce document est classé comme secret et est à contrôler en vertu de la Loi sur l'accès à l'information.



Natural Resources  
Canada

Securities and  
Investments Canada

# CLASSIFIED BRIEFING FOR ENERGY & UTILITIES SECTOR STAKEHOLDERS

Hosted by Natural Resources Canada (NRCan) — in collaboration with CSIS and RCMP  
 LOCATION: Canadian Security Intelligence Service, 1541 Ogilvie Road, Ottawa, Ontario  
 PURPOSE: To discuss National Security and Critical Infrastructure  
 CHAIR: Jeff Labonte, Director General, Portfolio Resources Branch, NRCan

## DRAFT A G E N D A

AGENDA THEME: SECURITY OF ENERGY RESOURCES DEVELOPMENT

Wednesday, May 23, 2012

6:30 PM - 7:00 PM: RECEPTION & REGISTRATION BY ALL PARTICIPANTS  
 ADAM BOWEN, FREEMONT CHATEAU LAURENT, 1 RUELLE D'ESTRÉE, OTTAWA  
 RECEPTION CO-HOSTS:  
 TBC

Thursday, May 24, 2012

MODERATOR: Mr. Tim O'Neil, RCMP

7:00 - 8:00	REGISTRATION	
8:00 - 8:05	CSIS Welcome and Protocols	
8:05 - 8:20	Introductory Remarks and Roundtable Introduction	Jeff Labonté, NRCan
8:20 - 9:20		Al Jones, CSIS
9:20 - 10:00		
10:00 - 10:15	BREAK	
10:15 - 11:15		
11:15 - 11:45	Strategic Overview of Cyber Threats	Dr. Yago De Jesus, RCMP
11:45 - 12:15	Economic and Corporate Espionage	Adam Mohamed / Mario Deschênes, NRCan
12:15 - 12:15	LUNCH	
13:15 - 13:45		
13:45 - 16:15	PANEL DISCUSSION: Panelists: Northern Gateway Project and other projects associated with Oil Sands "E" Division RCMP "E" Division RCMP Wes Elliot National Energy Board	
16:15 - 16:30	Round Table	Jeff Labonté, NRCan (Facilitator)

Note: The exact timing of the briefing is subject to change. The briefing will be held on May 24, 2012.  
 Organized by the Portfolio Resources Branch, NRCan, in collaboration with CSIS and RCMP.

Natural Resources Canada / Ressources naturelles Canada

## CLASSIFIED BRIEFING FOR ENERGY & UTILITIES SECTOR STAKEHOLDERS

Hosted by Natural Resources Canada (NRCan) -- in collaboration with CSIS and RCMP  
 LOCATION: Canadian Security Intelligence Service, 1941 Ogilvie Road, Ottawa, Ontario  
 PURPOSE: To Discuss National Security and Criminal Risks to Critical Energy Infrastructure  
 CHAIR: Jeff Labonté, Director General, Petroleum Resources Branch, NRCan

### AGENDA

AGENDA THEME: *NORTH AMERICAN ENERGY RESOURCES DEVELOPMENT AT RISK*

#### WEDNESDAY, NOVEMBER 16, 2011

6:30 PM - 9:00 PM: NETWORKING RECEPTION FOR ALL PARTICIPANTS  
 DRAWING ROOM, FAIRMONT CHATEAU LEONOR, 1100 AUSTIN STREET, OTTAWA  
 RECEPTION CO-HOSTS:

#### THURSDAY, NOVEMBER 17, 2011

MODERATOR -- Mr. Tim O'Neil, RCMP

7:00 - 8:00	REGISTRATION	
8:00 - 8:05	CSIS Welcome and Protocols	
8:05 - 8:10	Introductory Remarks	Jeff Labonté, NRCan
8:10 - 8:20	Roundtable Introductions	Jeff Labonté, NRCan
8:20 - 12:00	Challenges to Energy Projects from Environmental Groups	
8:20 - 9:20		
9:20 - 10:00	MSOC East Coast Operations -- Lessons Learned	RCMP MSOC
10:00 - 10:30	BREAK	
10:30 - 11:15		
11:15 - 12:00	Security Challenges Presented by Radicalized Individuals / Groups to Canada's Energy Sector -- The Great lakes Examples	Rose Stricker, RCMP, Great Lakes Maritime Security Operations Centre
12:00 - 13:00	LUNCH	
13:00 - 14:00	National Security Criminal Investigations Update	Gilles Michaud, Assistant Commissioner, National Criminal Investigations, RCMP
14:00 - 14:20	Suspicious Incident Reporting Update	Wendy Nicol, RCMP
14:20 - 14:30	BREAK	
14:30 - 16:30	PANEL DISCUSSION -- THE LEGAL CHALLENGES OF INFRASTRUCTURE PROTECTION: COLLECTING EVIDENCE FOR PROSECUTIONS IN THE CANADIAN	

	<b>EXPERIENCE</b> <ul style="list-style-type: none"> <li>• Moderator – Dr. Martin Rudner, Distinguished Research Professor Emeritus, Carleton University</li> </ul> <b>Panelists:</b> <ul style="list-style-type: none"> <li>• Mark Freiman, Attorney, Lerner LLP</li> <li>• Mylene Bouzigon, Senior Legal Counsel, CSIS Legal Services</li> <li>• Gerard Normand, General Counsel, Office of the Legal Advisor, Department of National Defence Canadian Forces</li> <li>• Luc Cadieux, Legal Counsel, Department of Justice</li> </ul>	
16 : 30 – 16 : 50	Round Table	Jeff Labonté, NRCan (Facilitator)

Note: The 2012 Coast Guard Briefing for Energy Sector Stakeholders will be on the following dates: THURSDAY, MAY 24, 2012 - FRIDAY, MAY 25, 2012  
Preceded by the Networking Reception on the following dates: WEDNESDAY, MAY 23, 2012 & THURSDAY, MAY 24, 2012, details to follow



Natural Resources  
Canada

Ressources naturelles  
Canada



## CLASSIFIED BRIEFING FOR ENERGY & UTILITIES SECTOR STAKEHOLDERS

Hosted by Natural Resources Canada (NRCan) — in collaboration with CSIS, ITAC and RCMP

LOCATION: Canadian Security Intelligence Service, 1941 Ogilvie Road, Ottawa, Ontario

PURPOSE: To Discuss National Security and Criminal Risks to Critical Energy Infrastructure

CHAIR: Jeff Labonté, Director General, Petroleum Resources Branch, NRCan

### AGENDA

AGENDA THEMES: (1) CYBER SECURITY AND INTERDEPENDENCIES

(2) TORONTO-18 INVESTIGATIONS DEBRIEF/LESSONS LEARNED

### TUESDAY, MAY 17, 2011

11:20 PM – 1:00 PM: NETWORKING RECEPTION FOR ALL PARTICIPANTS  
DRAWING ROOM, FOURMONT (1941), LAURIER: 1800 LAURIER STREET, OTTAWA

RECEPTION CO-HOSTS:

### WEDNESDAY, MAY 18, 2011

MODERATOR – Mr. Tim O'Neil, RCMP

7:00 – 8:00	REGISTRATION	
8:00 – 8:05	CSIS Welcome and Protocols	
8:05 – 8:15	Introductory Remarks	Jeff Labonté, NRCan
8:15 – 8:20	Roundtable Introductions	Jeff Labonté, NRCan
8:20 – 9:10		Al Jones, CSIS
9:10 – 10:40		
10:40 – 11:10	BREAK	
11:10 – 12:00		
12:00 – 13:00	LUNCH	
13:00 – 13:30		
13:30 – 14:00	The Next Generation of Stuxnet Threats	Tiago Alves de Jesus, RCMP
14:00 – 14:15	Analysis of RCMP Suspicious Incident Reporting	Scott Foster, RCMP
14:15 – 14:30	BREAK	
14:30 – 16:30	Toronto-18 Investigations Debrief/Lessons Learned	Marwan Zogherb, OINSEI, RCMP
16:30 – 16:50	Town Hall Discussion	Jeff Labonté, NRCan (Facilitator)
16:50 – 17:00	Themes for the Nov 17, 2011, Classified Briefing	

This document is classified by the Security Intelligence Review Board (SIRB) on May 17, 2011.  
Ce document est classifié par le Service de renseignement de la GRC (SRG) le 17 mai 2011.



Natural Resources  
Canada

Ressources naturelles  
Canada

## CLASSIFIED BRIEFING FOR ENERGY SECTOR STAKEHOLDERS

Hosted by Natural Resources Canada (NRCan) — in collaboration with CSIS, ITAC and RCMP

LOCATION: Canadian Security Intelligence Service, 1941 Ogilvie Road, Ottawa, Ontario

PURPOSE: To Discuss National Security and Criminal Risks to Critical Energy Infrastructure

CHAIR: Jeff Labonté, Director General, Petroleum Resources Branch, NRCan

### DRAFT AGENDA

AGENDA THEME: *The Geopolitics of the Arctic in a Globalized Energy Economy*

#### WEDNESDAY NOVEMBER 24, 2010

6:30 PM – 9:00 PM : NETWORKING RECEPTION FOR ALL PARTICIPANTS

LAURIER ROOM, FAIRMONT CHÂTEAU LAURIER, 1 RIDEAU STREET, OTTAWA

HOSTED BY:

#### THURSDAY NOVEMBER 25, 2010

MODERATOR – Mr. Tim O'Neil, RCMP

7:00 – 8:00	REGISTRATION	
8:00 – 8:10	CSIS Welcome and Protocols	
8:10 – 8:20	Introductory Remarks	Jeff Labonté, NRCan
8:20 – 9:20	Security Briefing on Canada's North	Lt. Col. Brian Watson, DND
9:20 – 10:00		
10:00 – 10:30	Criminal Intelligence Activities in Northern Canada	Luc MacAulay, RCMP
10:30 – 11:00	BREAK	
11:00 – 11:50	Intellectual Property Rights & Supply Chain Threats	Shawn Soubourin, RCMP
11:50 – 12:10	National Cyber Security Policy	Robert Dick, Public Safety Canada
12:10 – 13:00	LUNCH BREAK	
13:00 – 14:00	National Criminal Investigations	Gilles Michaud, Assistant Commissioner, National Criminal Investigations
14:00 – 14:30	Suspicious Incidents Reporting	Wendy Nicols, RCMP
14:30 – 15:00	G8 / G20 Debriefs	RCMP
15:00 – 15:15	BREAK	
15:15 – 16:00		
16:00 – 16:45		
16:45 – 17:15	Open Discussion	Jeff Labonté, NRCan (Facilitator)
17:15 – 17:30	WRAP UP	Jeff Labonté, NRCan
17:30 – 18:30	Review of Selected Classified Reports (optional for those who are interested)	Felix Kwamena / Tim O'Neil

Note: The next Classified Briefing for Energy Sector Stakeholders will be on Weds, May 18, 2011,  
(Preceded by the Networking Reception on Tuesday, May 17, 2011 - details to follow)



Natural Resources  
Canada

Ressources naturelles  
Canada

## CLASSIFIED BRIEFING FOR ENERGY SECTOR STAKEHOLDERS

Hosted by Natural Resources Canada (NRCan)

In Collaboration with CSIS, ITAC and RCMP

**LOCATION:** Canadian Security Intelligence Service, 1941 Ogilvie Road, Ottawa, Ontario

**PURPOSE:** To Discuss National Security and Criminal Risks to Critical Energy Infrastructure

**CHAIR:** Eric Landry, A/Director General, Petroleum Resources Branch, NRCan

### DRAFT AGENDA

AGENDA THEME: 2010 CANADA'S YEAR ON THE INTERNATIONAL STAGE

#### TUESDAY MAY 11 2010

6:30 PM - 9:00 PM : NETWORKING RECEPTION FOR ALL PARTICIPANTS  
RENAISSANCE ROOM, FAIRMONT CHÂTEAU LAURIER, 1 RIDEAU STREET, OTTAWA

HOSTED BY: [REDACTED]

#### WEDNESDAY MAY 12 2010

MODERATOR - Mr. Tim O'Neil, RCMP

7 h - 8 h	REGISTRATION	
8 h - 8 h 10	CSIS Welcome and Protocols	[REDACTED]
8 h 10 - 9 h 10	[REDACTED]	[REDACTED]
9 h 10 - 10 h	ITAC - The Terrorist Threat to Canada	[REDACTED]
10 h - 10 h 30	RCMP Suspicious Incident Reporting Update	Wendy Nicol, RCMP
10 h 30 - 10 h 45	BREAK	
10 h 45 - 11 h 30	Cyber Threats to Critical Infrastructure	Greg O'Hayon, RCMP Tiago Alves de Jesus, RCMP
11 h 30 - 12 h 15	[REDACTED]	[REDACTED]
12 h 15 - 13 h	LUNCH	
13 h - 13 h 45	Vancouver 2010 Olympic Games JIG Debrief	Adriana Poloz, RCMP
13 h 45 - 14 h 30	[REDACTED]	[REDACTED]
14 h 30 - 15 h 15	G8 / G20 Updates	[REDACTED]
15 h 15 - 16 h	[REDACTED]	[REDACTED]
16 h - 16 h 15	BREAK	
16 h 15 - 17 h	[REDACTED]	[REDACTED]
17 h - 17 h 20	Open Discussion	Eric Landry, NRCan (Facilitator)
17 h 20 - 17 h 30	WRAP UP	Eric Landry, A/DG, NRCan



Natural Resources  
Canada

Ressources naturelles  
Canada

CONFIRMED ATTENDANCE

MAY 12, 2010 – CLASSIFIED BRIEFING – 7:00 AM TO 5:00 PM

NRCan On-Site Staff: Marilyn Clarke & Sonia Chhabra

**A**

- [REDACTED]
- [REDACTED]
- Athanasiades, John RCMP
- Alder, Roberta RCMP

**B**

- [REDACTED]
- [REDACTED]
- [REDACTED]

**C**

- Corcoran, Steve RCMP
- [REDACTED]
- [REDACTED]

**D**

- [REDACTED]
- [REDACTED]
- Darling, David Natural Resources Canada
- Desforges, Benoit Natural Resources Canada
- [REDACTED]
- Duperre, Jean-François Natural Resources Canada
- Deschambault, Danielle Finance Canada
- De Jesus, Tiago RCMP

**E**

- Elliott, Wes National Energy Board
- Easton, Andrew New Brunswick Public Safety

**F**

- [REDACTED]

- 4 -

## N

o Nicol, Wendy RCMP

o [REDACTED]

## O

o O'Neil, Tim RCMP

o O'Hayon, Greg RCMP

o [REDACTED]

## P

o [REDACTED]

o Poloz, Adriana RCMP

o [REDACTED]

## R

o [REDACTED]

o Rudner, Martin Carleton University

o [REDACTED]

## S

o Schimmens, Brian Canadian Nuclear Safety Commission

o [REDACTED]

o Scratch, Dave Canada-Nova Scotia Offshore Petroleum Board

o Sturgeon, Jacques Public Safety Canada

o Schramm, Laurier Saskatchewan Research Council

## T

o [REDACTED]

o [REDACTED]



May 20, 2008

File No: EN9007-10

## TO ENERGY SECTOR STAKEHOLDERS

### Re: Classified Briefing for Energy Sector Stakeholders

On April 7, 2008, you received a letter, indicating that the Classified Briefings hosted twice a year (May and November) by Natural Resources Canada (NRCan) were being discontinued.

A number of stakeholders have indicated to me, and to others, that they would like to see if it is possible to continue to have some form of security clearances and security briefings. We are currently looking at ways we may be able to continue to provide a forum for this service. In the meantime, I am writing to invite you to attend a classified briefing scheduled for June 5, 2008, at the Canadian Security Intelligence Service (CSIS) Conference Centre, 1941 Ogilvie Road, Ottawa, Ontario, from 07:30 to 14:30 hours. A copy of the agenda is attached for your information. We will also use the opportunity of the meeting to discuss your views with respect to the importance of these sessions and the potential design of any future sessions along this line.

The purpose of this briefing is to share energy-related classified information regarding threat risk assessment and potential threats to the energy sector; as well as discuss national security and criminal intelligence relevant to critical energy infrastructure. I would also like to have a general discussion to seek your perspective on the usefulness of continuing these briefings.

For those of you who are not familiar with CSIS' security protocol, the following is provided for your information and guidance.

Access to CSIS facilities is strictly regulated and enforced at all times. NRCan will provide your names to CSIS in advance of the briefing and you will be required to provide photo identification upon entering the facilities. Your movement within CSIS' facilities will be restricted to the Conference Centre area, unless accompanied by a CSIS employee.

.../2

Canada

The following items are not permitted in the CSIS facilities: firearms, radio frequency transmitting equipment (i.e. cell phones, two-way pagers, two-way radios, "Blackberrys", etc.), image reproduction equipment (i.e. cameras, portable copiers, video cameras, recorders, etc.), digital storage equipment (i.e. personal digital assistants (PDAs), palm pilots and electronic organizers), laptops and memory sticks.

Visitors will be asked to check these items at the front desk for safe storage. To avoid delays and security concerns, we strongly encourage that you do not bring these items with you to the classified briefing.

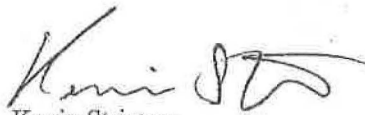
There are a limited number of visitor vehicle parking spaces available on CSIS property. CSIS has cautioned that its parking lots are patrolled on a regular basis and tickets will be issued to vehicles parked in unauthorized areas. CSIS recommends that visitors use taxi services. If you must bring your vehicle, there is a limited daily paid parking available. The cost is \$5.00 per day (coins only) on a first-come, first-serve basis. The parking lot is accessible from Ogilvie Road and is located along the fence facing Ogilvie and the shopping centre.

Please note that the briefing is restricted to only those who have been invited by NRCan and who possess a Level II Secret Clearance. Therefore, no alternates will be admitted. Also, be advised that note-taking will not be allowed.

To enable us to finalize arrangements for the briefings, we would ask that you confirm your attendance as soon as possible with Ms. Brenda Booth. She can be reached at [bbooth@nrcan.gc.ca](mailto:bbooth@nrcan.gc.ca) or by telephone at (613) 996-0501.

I look forward to seeing you on June 5th.

Yours sincerely,



Kevin Stringer  
Director General  
Petroleum Resources Branch  
Energy Sector

Attachment: (1)



# CLASSIFIED DEBRIEF FOR ENERGY SECTOR STAKEHOLDERS / SÉANCE DE DÉBREFFAGE CLASSIFIÉE POUR LES PARTIES INTÉRESSÉES À L'ÉNERGIE

In Collaboration with CSIS, ITAC, PSC and RCMP

**LOCATION:** Canadian Security Intelligence Service, 1941 Ogilvie Road, Ottawa, Ontario

**PURPOSE:** TO DISCUSS NATIONAL SECURITY AND CRIMINAL INTELLIGENCE, THREAT RISK ASSESSMENT AND TO SHARE ENERGY RELATED CLASSIFIED INTELLIGENCE

**CHAIR:** Kevin Stringer, Director General  
Petroleum Resources Branch, Energy Sector, Natural Resources Canada

## DRAFT AGENDA

Thursday, June 5, 2008		
07:30 - 08:00	REGISTRATION	
08:00 - 08:15	Welcome / Facility Orientation Canadian Security Intelligence Service (CSIS)	[REDACTED] Deputy Director General, Intelligence Assessments Branch
08:15 - 08:45	Opening Remarks Natural Resources Canada (NRCan)	Kevin Stringer, Director General Petroleum Resources Branch
08:45 - 09:15	Update on International Terrorism Canadian Security Intelligence Service (CSIS)	[REDACTED] Director General [REDACTED]
09:15 - 09:45	Integrated Threat Assessment Centre (ITAC) Initiatives	Daniel Giasson, Director, ITAC
09:45 - 10:15	Update Criminal Intelligence Royal Canadian Mounted Police (RCMP)	John MacLaughlan, Assistant Commissioner / Pierre Perron, C/Superintendent
10:15 - 10:45	B R E A K	
10:45 - 12:00	Regional Updates:  ▪ New Brunswick Department of Public Safety [REDACTED]  ▪ Alberta Solicitor General and Public Safety	<ul style="list-style-type: none"> <li>▶ Andrew Easton, Director, Public Safety, Security and Emergencies Directorate [REDACTED]</li> <li>▶ Denis Huot, Manager, Alberta Security and Strategic Intelligence Support Team</li> </ul>
12:00 - 13:00	L U N C H	
13:00 - 13:30	Explosive Modeling of Transformers Canadian Explosives Research Laboratory (CERL)	Dr. Phil Lightfoot, Manager, CERL / Bert Von Rosen, Explosives Applications Specialist
13:30 - 14:10	Usefulness/Continuation of the Classified Briefings for Energy Sector Stakeholders - the Way Forward	Kevin Stringer, Director General Petroleum Resources Branch, NRCan
14:10 - 14:15	Wrap-Up	Kevin Stringer, Director General Petroleum Resources Branch, NRCan



Natural Resources  
Canada

Ressources naturelles  
Canada

Canada



# CLASSIFIED DEBRIEF FOR ENERGY SECTOR STAKEHOLDERS / SÉANCE DE DÉBREFFAGE CLASSIFIÉE POUR LES PARTIES INTÉRESSÉES À L'ÉNERGIE

In Collaboration with CSIS

LOCATION: Canadian Security Intelligence Service, 1941 Ogilvie Road, Ottawa, Ontario

PURPOSE: TO DISCUSS NATIONAL SECURITY AND CRIMINAL INTELLIGENCE, THREAT RISK ASSESSMENT AND TO SHARE ENERGY RELATED CLASSIFIED INTELLIGENCE.

CO-CHAIRS: FELIX KWAMENA, DIRECTOR  
ENERGY INFRASTRUCTURE PROTECTION DIVISION

GUY MORIN, ACTING DIRECTOR  
SAFETY, SECURITY & EMERGENCY MANAGEMENT DIVISION

## DRAFT Conference Agenda Classified Briefing November 14, 2007

Tuesday, November 13, 2007		
7:00 pm - 9:30 pm	Networking Reception - Conference Center	
Wednesday, November 14, 2007		
7:30 am - 8:30 am	Registration and Continental Breakfast	
8:30 am - 9:00 am	CSIS Welcome	[REDACTED] Ted Flanigan, ADI
9:00 am - 9:15 am	Co-Chairs Remarks	Felix Kwamena & Guy Morin
9:15 am - 10:00 am	Integrated Threat Assessment Centre (ITAC) - General Terrorist Threat Assessment	[REDACTED]
10:00 am - 10:15 am	Break	
10:15 am - 11:00 am	Ontario Provincial Police (OPP) Presentation	Greg Moore
11:00 am - 11:30 am	Security and Emergencies Directorate, Department of Public Safety, New Brunswick	Andrew Easton
11:30 am - 12:00 pm	Alberta Security & Strategic Intelligence Support Team (ASSIST) - Alberta Threat Overview	Denis Huot
12:00 pm - 1:00 pm	Lunch	
1:00 pm - 2:00 pm	Criminal Intelligence Service Canada (CISC) - Organized Crime in Canada	Josée Therrien
2:00 pm - 2:45 pm	Canadian Cyber Incident Response Centre - Cyber Threat Assessment	Bruce Moore

2:45 pm - 3:15 pm	Break	
3:15 pm - 4:30 pm	<p>Case Study: [REDACTED]</p> <p>[REDACTED]</p> <p>Panel: [REDACTED] Ontario Provincial Police, Royal Canadian Mounted Police</p>	<p>Ms. Wendy Nicol - RCMP (Moderator)</p> <p>[REDACTED]</p> <p>Dennis Decker - RCMP TBD - OPP</p>
4:30 pm - 5:00 pm	Final Comments and Co-Chairs' Wrap-Up	Felix Kwamena & Guy Morin



Natural Resources  
Canada

Ressources naturelles  
Canada

Canada

2007 06 26

**NRCan - Energy Infrastructure Protection Division**  
**Classified Briefing for Energy Stakeholders**  
**CSIS HQ - 2008 06 05**

On 2008 06 05, the Energy Infrastructure Protection Division (EIPD) of Natural Resources Canada hosted the 6<sup>th</sup> in the series of Classified Briefings for Energy Stakeholders at CSIS HQ. The June 6 meeting had a preponderance of federal government employees (see the attached list of attendees) due in part to the abrupt cancellation of the Briefing originally scheduled for 14 May, and its re-scheduling at the direction of the Minister for PSCan.

The DDG IAB welcomed the energy stakeholders on behalf of CSIS, affirming the principle of enhanced information and intelligence sharing with critical infrastructure stakeholders, a principle acknowledged by our executive. What this means in practice is a work in progress. He noted multiple points of CSIS' contact with the private sector, committed to the sharing of specific information when we have it, and pointed out that the intelligence community's outreach to the private sector is not altruistic - it is based on recognition of mutual need.

Mr. Kevin Stringer, DG Petroleum Resources Branch, NRCan, indicated he was looking forward to a productive day of discussion on critical energy infrastructure protection, including the afternoon session on continuation of the Classified Briefings.

The DG [REDACTED] reviewed the positive developments of the past two years, the build-up and now central role of ITAC, and the initiatives of EIPD and PSCan, all of which represent contributions to the system we all know we need, while recognizing we're not there yet.

The international terrorism threat is not just Al Qaeda. The events of 9/11 put a chill into mass anti-globalization protests, [REDACTED]. Energy infrastructure may be vulnerable to denial of service or disruption attacks by elements within this milieu - stakeholders were advised [REDACTED]

The DG noted statements by senior US officials to the effect the US is near victory in Iraq and Afghanistan. [REDACTED] There is no doubt AQ has been seriously disrupted, particularly in its financing, and some branches are resorting to criminality to restore their resource base. [REDACTED]

[REDACTED] Internationally, energy assets are at risk, [REDACTED]

2007 06 26

[REDACTED]

RCMP C/Supt, Pierre Perron, (DG Criminal Intelligence) talked about how organized crime could affect energy infrastructure, through the theft of fuel trucks, and electricity for grow-ops. Russ Weisman, RCMP senior analyst, gave an overview of the [REDACTED]

Tim O'Neil, Energy Infrastructure analyst, RCMP, outlined the RCMP's experience in working with the rail and urban transit sector to develop a Suspicious Incident Reporting System (SIRS). The pilot project with Toronto and Vancouver transit authorities was deemed a success, and even as that is being made operational (which means solving all the legal and technical issues surrounding access to, and ownership of, information shared through Web portals) the RCMP is commencing work on a SIRS in the energy sector, beginning with the electricity stakeholders. [REDACTED] will have access when these reporting systems come on-line; the end-point is to have a fully functional SIRS system across all ten critical infrastructure sectors.

Mr. Denis Huot, Manager of Alberta's Security and Strategic Intelligence Support Team (ASSIST) provided an overview of changes to the province's counter-terrorism plan crisis management plan (ACTCMP), ASSIST's role, and security developments in the province. The key objectives of the plan are to identify a threat early enough for the government to warn first responders, security forces, communities and critical infrastructure owners of the threat, and to allow these entities to take immediate action to prevent a terrorist act from taking place, or lessen its effects. The corresponding objective is the ability to deliver essential services.

The key functions of the ACTCMP are to establish the threat level for the province; identify and rank critical infrastructure; activate the emergency notification system to allow CI partners to implement pre-determined protective security measures according to threat level and facility criticality; and activate the operations centre to coordinate implementation of additional federal/provincial protective measures.

The changes to the ACTCMP (2008 vs 2003 versions) are identified as being less task oriented, less command and control, more fluid, flexible and linked to the government's priority of 'providing safe and secure communities.' The 2003 ACTCMP is also identified as implying the GOA resources 'would be used to mitigate a terrorist threat, therefore exceeding their original intent and capability.' *Note: this is an interesting excision or clarification, which appears driven by recognition of legal risk and lead responsibility of the federal government for counter-terrorism operations.* (See accompanying power point of ASSIST presentation ).

2007 06 26

Andrew Easton, Director, Security and Emergencies Directorate, Ministry of Public safety, New Brunswick, provided an overview of the province's energy potential and the role of his office in providing public security, critical infrastructure protection, CBRNE response, executive security and all-hazards intelligence support. The province is on track to become a North American energy hub. This vision and the national security environment are increasing the demands on his office for critical infrastructure protection, information sharing, emergency response, and security exercises, and all-hazards risk management. [REDACTED]

[REDACTED] and this year experienced near-record floods in parts of the province. (See accompanying power point of NB presentation).

Bert von Rosen, research scientist, Canadian Explosives Research laboratory (CERL) presented the findings of the research on tests of [REDACTED]

[REDACTED] The Manager of CERL, Dr. Phil Lightfoot, noted that CERL's research, some of which has been funded by EIPD, includes pipeline, electricity and dam vulnerability, and other areas. Is there any interest in continuing this research? There was on the part of some of those present.

**National Strategy and Action Plan (NSAPCIP)  
for Critical Infrastructure Protection: Energy and Utilities Sector Consultations**

The second part of the day was an unclassified forum which included representatives from PSCan and energy utilities who had not been present for the Classified Briefing. This session was chaired by Kevin Stinger, DG Petroleum Resources Branch, NRCan, and the purpose was to get initial comments on PSCan's National Strategy for CIP. Mr. Stinger reviewed the NSAPCIP which includes building trusted partnerships, implementing an all-hazards risk assessment across the 10 sectors (health care; finance; communications and information technology; energy and utilities; government; food; water; safety; manufacturing; and transportation) sharing and protecting information. This consultative draft is open for comment until 30 June 2008, will be revised over the summer based on comments received, is subject to federal-provincial territorial consultations through the fall and is scheduled to be announced by Ministers in January 2009.

The issue of the NSAPCIP was entangled with the future of the Classified Briefings. There was consensus the Briefings should continue (the next scheduled - 13 November), recognizing existing funding limitations. There is no more money. [REDACTED] indicated it is part of his corporate responsibilities to belong to professional associations, and host or sponsor association functions. He has a budget for this purpose, and could accordingly cover part of the Classified Briefing's costs. Mr. Stinger indicated that he wanted an Advisory Group

Confidential

2007 06 26

to work with him, including private sector representatives and academics, mapping the way ahead in energy infrastructure. This will commence deliberations in September. What we do has to be consistent with other sectors.

In terms of industry expectations, the common theme was the continuing need for improving the quality and relevance of the intelligence community's threat information and advice to the energy stakeholders. Asset owners are not going to become intelligence professionals by coming to these meetings every six months, and you aren't going to understand the energy industry by meeting with us occasionally. One suggestion was to develop specific risk indicators for each sector, and even if the intelligence reports were to include for each indicator 'nothing to report', then the consumer knows that his issues have been looked at and assessed.

There was discussion of the Australian approach to CIP and its merits; some of what they are doing may be ahead of us, we'll have to look into that. Some of what they are doing may be replicated in the RCMP's planned Suspicious Incident reporting System. The DG [redacted] also suggested that if companies [redacted]

**Issues for Consideration:** subsequent to the Classified Briefing, in discussion with the Chief Calgary District, he noted that industry was ahead of government in understanding vulnerability, risk and interdependence. He could follow up with NESP members for their reactions, but re [redacted]

**Future Briefings:** the future of AQ; stability of Nigeria; AQ operations in Yemen. [redacted]

**Confidential**

2007 06 26

Tab/Onglet 7

Page 485

5 of 5

AGC1068

**SECRET**

16 February 2007

**Natural Resources Canada (NRCan)  
Classified Briefing Forum for Energy Sector Stakeholders  
in collaboration with CSIS, ITAC and the RCMP  
CSIS HQ, November 15-16, 2006**

**DG Intelligence Assessments Branch (IAB)**

1. The DG IAB welcomed the participants on behalf of CSIS, acknowledging the diversity of the audience, the transformation of energy security in light of transnational threats to critical infrastructure, and the corresponding need to build trusted relationships at the national and local levels between government (the national security community) and the private sector. (Complete text of the DG's remarks are in section 3.)

**The Report on Information Sharing with Energy Stakeholders**

2. [REDACTED] has been contracted by Dr. Felix Kwamena, Director, Energy Infrastructure Protection Division (EIPD NRCan) to review and comment on the Government of Canada's response to the energy sector's security requirements. Mr. [REDACTED] completed his review in early 2006 with the cooperation of public and private energy stakeholders and government agencies.

**Highlights:**

- Energy stakeholders consider themselves capable of responding to threats to their industry without government assistance.
- They are willing to work with the government if they are provided with realistic threat and risk assessments.
- The energy sector opined that no single federal agency could be relied upon to provide timely intelligence, and the federal government was suspected of withholding vital information. The belief is that government can do more to address sectoral concerns.
- Specifically, the EIPD should be designated as the lead federal agency to represent sectoral interests and requirements; and to provide energy-specific threat assessments.
- Concluded that progress has been made in the public/private partnership, but more needs to be done.

**NRCan's Response - Dr. Felix Kwamena, Director, Energy Infrastructure Protection Division (EIPD),**

3. Dr. Kwamena responded on behalf of EIPD.

**Highlights:**

- On the energy sector's request for a single point of contact with government, his office is



[REDACTED]  
**SECRET**

16 February 2007

working with the energy sector and the intelligence community to ensure that EIPD is recognized as the primary point of contact within the federal government to address sectoral concerns.

- EIPD is building partnerships with the intelligence community, sharing knowledge and contacts, and making available the scientific expertise of the Canadian Explosive Research Laboratory (CERL).
- [REDACTED]
- EIPD recently signed a letter of agreement with the RCMP to assist in funding an intelligence analyst who will work in the Critical Infrastructure Intelligence Section (CIIS) to analyse and report on threats to the energy sector; review suspicious incidents reported to the National Security Information Network and report regularly to critical infrastructure clients its analysis and related threat information.
- [REDACTED]
- Numbers and venues for information-sharing between government and energy stakeholders are increasing significantly. As befits a continentally integrated industry, many are international.
- EIPD co-hosts with the [REDACTED] the annual Pipeline Security Forum, sponsors Canadian representation at US classified briefings, participates at meetings of the [REDACTED] and in accordance with the Security and Prosperity Partnership (SPP) conducts joint vulnerability assessments [REDACTED] for select energy facilities that cross the Canada-US border.
- EIPD has access to sensitive law enforcement information that it assesses and reports regularly to select members of the energy sector.

**Comment:**

- Consensus that increased communication between intelligence analysts and private sector decision-makers is essential.
- Different views on intelligence needs: some want trends analysis to anticipate future security requirements, others want only focussed studies and equally focussed distribution.
- Suggestion of seconding industry representatives to ITAC.
- NRCan will continue to increase the number of individuals cleared to receive SECRET briefings.
- Reference to recent Australian legislation allowing a better dialogue between intelligence and industry.

[REDACTED] DG [REDACTED]

[REDACTED]  
**SECRET**

16 February 2007

4. The DG [REDACTED] initially addressed the 2<sup>nd</sup> Energy Stakeholders Classified Briefing in May 2006. He opened his remarks at this Forum by asking how many had been in contact with CSIS HQ or regional offices in the ensuing six months - a few hands went up. IAB was requested to follow up [REDACTED]

[REDACTED]  
to ensure that each attendee is provided with contact information for CSIS HQ, and the regional office in their location.

**Highlights:**

- The world is getting more complicated: those who direct the Islamist transnational terrorist threat, and those inspired by it, are clever and adaptive.
- CSIS has completed its radicalization study and domain mapping of threat agents in Canada; the Internet has become a graduate school for terrorists.
- How can the energy sector help us on the local threats - there is a need for mutual connectivity.
- [REDACTED]
- Integration of new citizens into Canadian culture is huge. Recently, the government launched a cross-cultural roundtable - PSEPC and Justice are coordinating a cross-country consultation on integration.

[REDACTED] **DG Prairie Region (PR)**

5. The DG PR indicated that CSIS and the RCMP work with NRCan and the Security Information Management (SIM) Unit of the Department of the Solicitor General and Public Security in Alberta to declassify information of relevance to the private sector and disseminate it to 500 stakeholders in the province. Alberta is well ahead of the curve in building trusted networks that cross the government-private sector divide.

**Highlights:**

- [REDACTED]
- [REDACTED]

**SECRET**

16 February 2007

- [REDACTED]

**Dr. Michael Rannie, Director of Human Resources Research and Intelligence, RCMP:  
Preventing Counterproductive Behaviours**

6. [REDACTED]

He presented the RCMP's findings on the use of various psychological testing tools to prevent counterproductive behaviours.

**Highlights:**

- [REDACTED]

- [REDACTED]

**[REDACTED] Partnership Between the Intelligence Community  
and the Private Sector**

7. [REDACTED] provided  
the first of the private sector briefings.

**Highlights:**

- HQ is doing trends analysis on this data which they regard as unique, but shareable with police and CSIS; have ranked five risks according to probability and impact:

[REDACTED]  
SECRET

16 February 2007

[REDACTED]

However, as the Toronto extremists included nuclear facilities in their broad target list, in response, the Canadian Nuclear Safety Commission (CNSC) heightened its awareness to defend nuclear facilities across the country, including Gentilly, Quebec. [REDACTED]

[REDACTED]

[REDACTED] - Response to Aboriginal Extremism

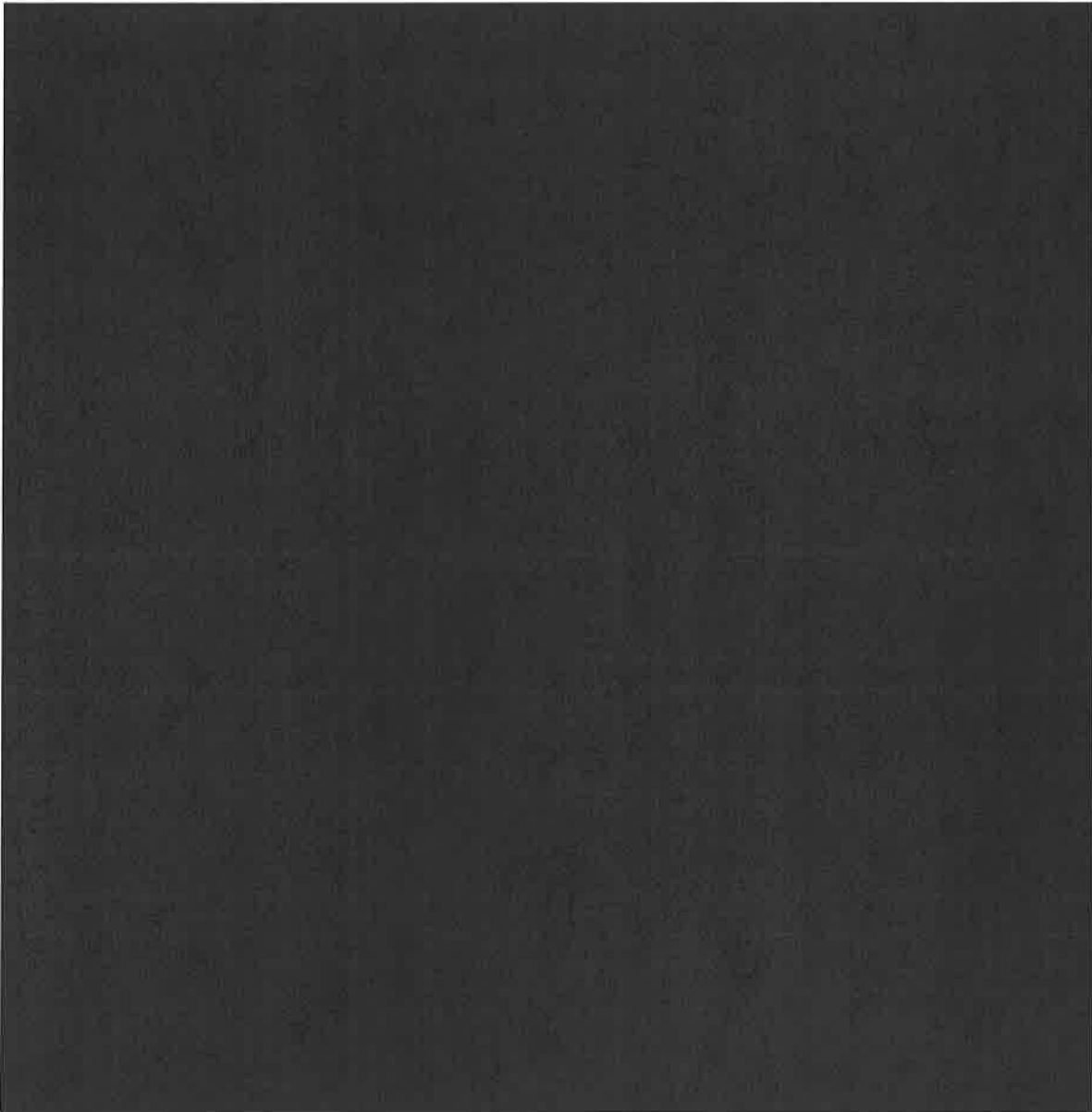
8. [REDACTED] gave a presentation to the energy stakeholders in May 2006 which focussed on [REDACTED]
- [REDACTED]

Highlights:

[REDACTED]

**SECRET**

16 February 2007



**Dr. Abass Braimah, Canadian Explosives Research Laboratory (NRCan), Historical  
Explosion-Induced Energy Failures**

9. Dr. Abass Braimah of the Canadian Explosives Research Laboratory (CERL - a branch of NRCan) reviewed explosion-induced energy infrastructure failures in broad streams -

**SECRET**

16 February 2007

electrical, and oil and gas. Electrical infrastructure consists of generation, transmission and distribution [REDACTED]

**Highlights:**

- Data presented on explosive amounts used to attack dams in Germany, Korea, Russia, Spain and Croatia and resulting damage. The attack on Quebec Hydro transmission towers was reviewed [REDACTED]
- Attacks on oil and gas pipelines in Iraq, Sudan, Russia, Pakistan, Algeria, Turkey, Colombia and India were presented to demonstrate the ease of transfer of attack modes between terrorist groups and extremist networks globally. The October 18, 1998 attack on the Orensa pipeline in Colombia was examined. The Ghislenghien pipeline in Belgium, and the Texas City BP Amoco refinery explosions were accidents, [REDACTED]

**Panel - Macro Impacts of Energy Infrastructure Security**

**10. Dr. Jim Young, Special Advisor to the Deputy Minister of PSEPC:**

- Advises PSEPC on preparations to cope with arrival of the next pandemic. 20<sup>th</sup> century pandemics occurred in 1918, 1957 and 1968. SARS was a poor spreader in the community; it could have posed a very severe problem. Avian flu is a candidate, but has not yet made the jump to human-to-human infection.

**11. Phil Murray, Commissioner RCMP (Rtd):**

- Security has to evolve constantly; the intelligence challenge is to detect the signal in the noise; the traditional system was built for the Cold War; the instinct is to keep using it.
- There is intelligence in the private sector, and while there are genuine problems for the federal government in dealing with the critical infrastructure owners and operators, we have to get past the silos and work constantly at improving communication across the public/private sector divide.

**12. Dr. Martin Rudner, Director, Canadian Centre for Intelligence and Security Studies, Carleton University:**

- Global energy markets are being transformed by politics and technology in ways that are creating new vulnerabilities and risks, not all of which are a function of the terrorist threat.
- There is shift in market supply and distribution: declining producers, North Sea and the Gulf; new producers, Canada, Russia, Caspian Sea and Central Asia; new consumers, China, India, Southeast Asia.
- Natural gas has traditionally been a segmented market, oil a global one. Technology is overcoming this: the Russians are selling LNG to eastern Canada where it will be gasified

SECRET

16 February 2007

- and sold to eastern American markets creating the beginnings of a market in natural gas.
- Since 2000, resource nationalism is on the ascendancy - government to government negotiations in energy security. This is the new mercantilism where trade and wealth creation are determined not by market principles, but political controls over energy resources deemed too valuable to be left to the market. The new players (Russia, Bolivia and Venezuela) are joining traditional suppliers, and consuming countries prefer bilateral deals to secure access. Indonesia and China recently signed a \$25 billion deal on LNG.
- The motivations for attacks on energy supply, and the risks vary enormously: in Baku and Nigeria, pressure tactics by those who feel they are left out of the wealth being generated; Russia-Ukraine is energy denial. The Russians, if anyone can believe it, told BP it didn't meet environmental standards for the Salken2 pipeline - the message is Russia controls the product. Al Qaeda's (AQ) global footprint is beginning to look like the map of the British empire, and it has a strategy for attacking the West's energy supply. There are also NIMBY alliances - aboriginals, environmentalists and anarchists.
- In terms of protection of this critical infrastructure, there are various approaches to the assessment of threats and risks. Some risks can be measured by actuarial (insurance) standards, other ones involve "wicked" probabilities, catastrophic vulnerabilities, and public externalities that don't lend themselves to mere actuarial calculations. It may be relevant to revert to the early post-World War Two discourse on "Welfare Economics", which conceptualized a public-private sector partnership for pursuing a full-employment strategy for economic growth; the same underlying welfare-economic principles could be applicable to a shared public/private formula for allocating the costs and benefits of protecting critical national infrastructure.

#### **Panel - Terrorist and Criminal Attacks Against the Energy Sector**

##### **13. Scott Foster, Critical Infrastructure Intelligence Section, National Security Investigations, RCMP:**

- While there is no specific threat to Canada's energy infrastructure, a number of groups have expressed an interest in targeting Canadian interests. The threat actors which display the highest propensity to target Canada's electricity sector are left-wing extremists, such as political radicals and eco-terrorists, and Aboriginal extremists.
- There is evidence the intentions of domestic left-wing extremists have changed over the years. Eco-terrorists are growing more accustomed to the idea of actions that result in casualties. This is particularly true if those harmed are considered to be direct adversaries. If destroying a piece of infrastructure that environmental extremists oppose can only be accomplished by inflicting casualties, there is increasing acceptance among some that this is justified.
- Recent extremist literature suggests the eco-terrorists' target of choice is not well-secured power plants, but the utility's critical transmission towers and isolated substations.
- In the case of Aboriginal extremists, incidents where critical electrical infrastructure is

SECRET

16 February 2007

sabotaged on (or near) reserve land are of the utmost significance. The arson attack on the Caledonia transformer station serves as a good case study for what could occur in other parts of the country. As long as the Caledonia dispute continues, the threat of copycat crimes remains. Initial reports indicate Aboriginal militants already regard the sabotage of Caledonia's transformer station as a tactic that easily can be used in other land-claims disputes in other parts of the province.

14.

- Provided an overview of key threats to the Canadian oil industry, domestically and internationally. [REDACTED]
- Among the eco-terrorists, the most recent example occurred on August 3, 2006 when individuals associated with the *Initiative de Résistance Internationalistes (IRI)* firebombed a car belonging to the Canadian Petroleum Products Institute spokesperson. This was the group's second known attack. In November 2004, the IRI bombed a Hydro Quebec power pylon. The August 2006 incident is their first attack against an individual: this group is becoming more violent.
- In December 2005, Michael Curtis Reynolds was arrested in Idaho after offering to blow up pipelines and oil facilities in the US on behalf of AQ the sum of \$40,000. Reynolds had faced previous explosives and criminal charges, and while there is no apparent ideological affiliation (his claimed motivation was opposition to the Iraq war), he made genuine attempts to solicit a response from AQ operators. In December 2006, a judge ordered a psychiatric examination.
- The Toronto 18 is an example of a homegrown network inspired, but not directed or funded by, the AQ senior leadership. Some were converts to radical Islam, others received training or indoctrination abroad, in countries such as Afghanistan or Yemen. These extremists are linked to the AQ ideology and propaganda by Internet forums.
- Their brainstorming target list included nuclear power plants near Toronto, and Hydro facilities in Niagara. The vehicle-borne improvised explosive device (VBIED) part of the network selected more readily accessible targets in Toronto, such as the CSIS regional office and the Toronto Stock Exchange. [REDACTED]
- AQ has named Canada as a target for attack a number of times in the past three or four years. In July 2006, Hossam Abdul Raouf of the Committee of Information and Strategy for AQ warned Canada to withdraw troops from Afghanistan or face attacks similar to 9/11, Madrid and London. In December 2005, restricted AQ Web forum included a call



[REDACTED]  
**SECRET**

16 February 2007

- for terrorists to attack oil facilities in Canada and the US, especially the Alaska pipeline. In light of the terrorist network's objective of disrupting US energy supplies and driving up the price of oil, AQ has the incentive to plan or inspire attacks on oil and gas infrastructure in Canada as a means of harming the US. The fact that Canada is a supplier of oil to the US is not lost on AQ's leadership.
  - While there is a risk to the industry, there are mitigating factors. A small cell would likely have difficulty carrying out an effective attack, much less a strategic one, against a major facility. A larger and more capable network would find it more difficult to elude intelligence scrutiny. In either case, the planning and logistical requirements for effective terrorist attacks on the energy infrastructure are not insignificant. [REDACTED]
  - [REDACTED] The former are ongoing, and vary by region - in the Niger delta, repeated kidnapping of oil workers, including Canadians. In Colombia, FARC and other insurgents attack pipelines and kidnap foreign workers. The Sudanese civil war has also generated the danger of attacks on facilities.
  - The 2006 09 15 attack on the Nexen-owned facility in Ash Shihir, Yemen was carried out by a suspected AQ cell. [REDACTED]  
[REDACTED] On 2005 02 24, terrorists attacked the Abqaiq Aramco oil facility in Saudi Arabia. Both attacks used a similar method of operations: two suicide VBIEDs, the first for breach, the second to inflict damage. The attackers wore clothing that resembled uniforms worn by employees and local security forces, and the vehicles were made to look official.
  - Both attacks failed. [REDACTED] Media reports indicate repositioning of UK and Italian naval vessels, and increased Saudi alert. AQ has carried out waterborne attacks in the past. [REDACTED]
15. [REDACTED]
- Analysed the September 2006 attacks against oil facilities in Yemen for the energy stakeholders. [REDACTED]
  - On 15 September 2006, two oil facilities were attacked by near-simultaneous suicide car bombs. One of these facilities was the Ash Shihir terminal on the Arabian sea, owned by the Canadian company Nexen; the other was the government-run Safir gas-oil separation

SECRET

16 February 2007

plant in Marib.

These operations are very similar to the failed attack on 2006 02 24 against the Abqaiq Aramco oil facility in Saudi Arabia, an attack claimed by AQ. The Yemen attacks were claimed a month later by a group calling itself Al Qaeda in Yemen, and appear to have been carried out by members of the AQ cell involved in the 2002 attack against the French supertanker *MV Limburg*.

16.

- Summarized themes that have surfaced in this and other recent energy forums - most common are transformation and integration. The reasons are clear: the Air India bombings, horrific as they were, did not transform either the national security community or its relations with the private sector - civil aviation had long been a terrorist target of choice, and in this attack, Canada was a venue, not a target.
- The terrorist attacks of 9/11, subsequent attacks on transportation infrastructure, and AQ's strategic vision constitute a fundamental shift in the threat of international terrorism. We have moved beyond the spillover of violence from conflicts abroad to a direct threat against Canada, its allies and global interests. This does transform the national security community and its relations with the private sector. Since critical infrastructure is at risk, there is a need to build trusted networks across this divide, whether in transportation, energy or any other sector.
- That is the essence of integration: government has been told repeatedly by the private sector that facility operators know how to manage risk - any competent business knows how to deal with accidents and malicious incidents. What they feel they don't yet know is how to protect themselves against national security threats, or to be more precise - what those threats are.
- noted the energy industry's expressed need for realistic threat and risk assessments. We have also heard repeated references to what is generally regarded as Alberta's advanced system for the dissemination of information to critical infrastructure stakeholders, and of alert levels integrated with security and emergency response measures right down to the municipal level. Perhaps a future stakeholders briefing would benefit from a presentation on Alberta's approach.
- An unspoken concept was one first encountered in the White supremacist area - the concept of leaderless resistance. The concept was derived from weakness, designed to

SECRET

16 February 2007

overcome the flaws of hierarchical or cellular organizations and its essence was: 'you know what needs to be done - go and do it.' It seems that this concept has metastasized across the political spectrum, and could just as easily be cited by bin Laden as by an environmental extremist group. It is globalization that has made this possible and invests even the most feeble of transnational terrorist or criminal networks with a strategic potential previously unavailable.

the recently disrupted plot in the UK to destroy multiple civil aircraft by persons carrying on of ingeniously designed liquid explosive devices. Our British colleagues are not easily horrified, but the official spokesperson clearly was when he described a catastrophic terrorist plot designed to kill thousands. What so pleased the 9/11 plotters was not simply the outcome, but the demonstration before the whole world of military competence and precision, even if for them, such competence was contingent on a suicide attack against defenceless civilians. Those who feel validated in their military competence, now seek equal validation of their scientific and technical expertise.

**Panel Discussion:**

17. asked

**Closing Remarks - DG PR**

18. The DG PR noted that in meeting the requests for support from those in the private sector who own critical infrastructure, we are pressing on the limitations of our mandate. Nevertheless, the fact that CSIS is supporting NRCAN in hosting these classified briefings,

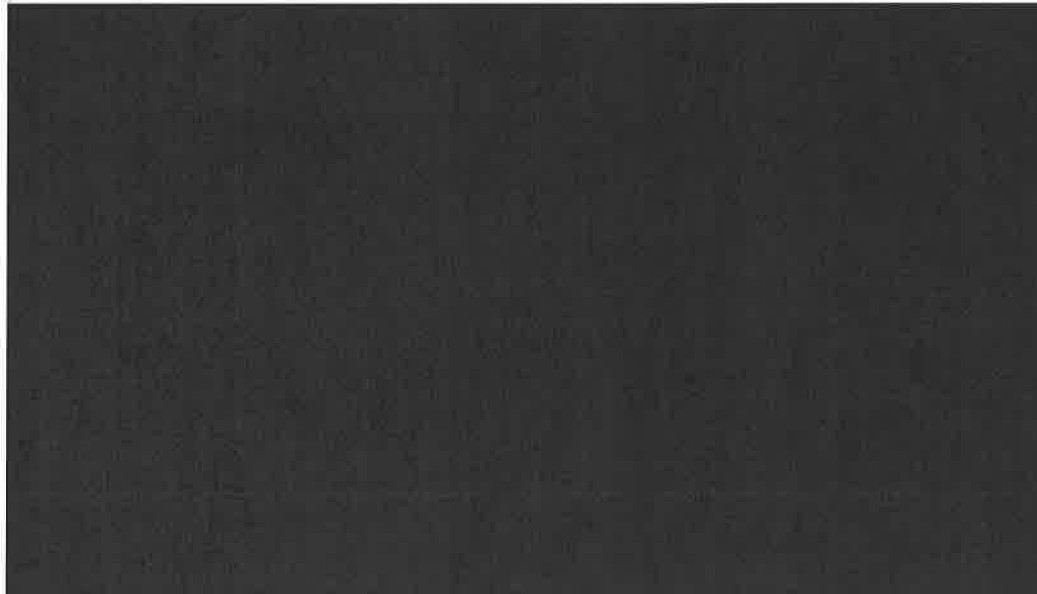
[REDACTED]

**SECRET**

**16 February 2007**

and is engaged on many fronts with the private energy sector, addresses the Service's recognition and willingness to press this envelope.

19.



20.

21.



TAB

7

# CLASSIFIED DEBRIEF FOR ENERGY SECTOR STAKEHOLDERS / SÉANCE DE DÉBREFFAGE CLASSIFIÉE POUR LES PARTIES INTÉRESSÉES À L'ÉNERGIE

In Collaboration with PSEPC, CSIS, RCMP & ITAC

LOCATION: Canadian Security Intelligence Service, 1941 Ogilvie Road, Ottawa, Ontario

PURPOSE : TO DISCUSS NATIONAL SECURITY AND CRIMINAL INTELLIGENCE, THREAT RISK ASSESSMENT  
AND TO SHARE ENERGY RELATED CLASSIFIED INFORMATION.

CO-CHAIRS: FELIX KWAMENA, DIRECTOR  
ENERGY INFRASTRUCTURE PROTECTION DIVISION

SHARON SAVOIE, DIRECTOR  
SAFETY, SECURITY & EMERGENCY MANAGEMENT DIVISION

## Conference Agenda

Tuesday, May 16, 2006		
6:30 pm - 9:00 pm	Networking Reception at The Delta Hotel, 361 Queen Street	Champlain Room
Wednesday, May 17, 2006		
7:30 - 8:30 am	Registration and Continental Breakfast	
8:30 - 8:40 am	Co-Chairs Remarks	Felix Kwamena & Sharon Savoie
8:40 - 9:30 am	Study Highlights: [REDACTED]	[REDACTED]
9:30 - 10:30 am	Guest Speaker: Assistant Commissioner [REDACTED] [REDACTED] Director, ITAC	
10:30 - 10:45 am	Break	
10:45 am - 12:30 pm	Canadian Security Intelligence Service (CSIS)	[REDACTED] DG, Counter Terrorism
12:30 - 1:30 pm	Lunch	
1:30 - 2:30 pm	Royal Canadian Mounted Police (RCMP)	Supt. Rick Reynolds
2:30 - 2:45 pm	Break	
2:45 - 4:20 pm	[REDACTED]	[REDACTED]

4:20 - 5:00 pm	Co-Chairs' Wrap-Up	Felix Kwamena & Sharon Savoie
----------------	--------------------	----------------------------------





Natural Resources  
Canada

Resources naturelles  
Canada

Canada