

Swift, Andrew

From: Swift, Andrew
Sent: Friday, October 05, 2012 9:55 AM s.19(1)
To: Durand, Stéphanie
Cc: Filipps, Lisa
Subject: FW: Urgent: Media Enquiry - [REDACTED] TorSun

Categories: ATI PRINT

FYI

From: Carmichael, Julie
Sent: Friday, October 05, 2012 9:53 AM
To: Giolti, Patrizia
Cc: Mackillop, Ken; Stokes, Mark; McGrath, Andrew; Swift, Andrew
Subject: RE: Urgent: Media Enquiry - [REDACTED] TorSun

Thanks for the chrono Pat,

I would say that 7 hours is a pretty considerable amount of time to develop a response.

A basic function of media relations is to respond in a timely manner – I don't know how 4 hours past a deadline happens.

This was a missed opportunity unfortunately.

From: Giolti, Patrizia [mailto:Patrizia.Giolti@cbsa-asfc.gc.ca]
Sent: October-05-12 9:49 AM
To: Carmichael, Julie
Cc: Mackillop, Ken; Stokes, Mark; McGrath, Andrew
Subject: Urgent: Media Enquiry - [REDACTED] TorSun

Hi Julie – as requested, here is the chrono – we received the call/email around 1000 and a proposed approach submitted from the region at roughly 1400. We did a number of checks here at the CBSA and then sent your way round 1700. [REDACTED] had already informed us that his story was already done (we called to negotiate a new deadline early afternoon).

Any questions, please advise.

Tks

From: DiGirolamo, Antonella
Sent: October-04-12 01:51:52 PM (UTC-05:00) Eastern Time (US & Canada)
To: Carnadin, Amitha
Cc: CBSA-ASFC-Media Relations; Sergong, Tsering; Barrasa, Vanessa; Vragovic, Goran
Subject: FW: Urgent: Media Enquiry - [REDACTED] TorSun

Urgent: For review and M.O.approval.

Approved by: [REDACTED]

RDG-GTA Goran Vragovic

Consulted with [redacted]

[redacted]

MEDIA CALL / APPEL DE JOURNALISTE

s.15(1) - Int'l
s.19(1)

Date: Oct. 4, 2012

Time: 10:17 am

Journalist: [redacted]

Media: Toronto Sun

Contact: [redacted]@sunmedia.ca, [redacted]

Deadline: Oct. 4, 2012 @ 1:00 pm

Issue: Alleged complaint to the Integrity Commissioner

Question: Seeking information on alleged complaint.

Background (for internal use only):

[redacted] email, copied below:

Good morning. I am seeking information in relation to a complaint that was filed to the Integrity Commissioner in which it is alleged that several CBSA officials acted in an unprofessional manner by getting drunk etc. during an Aug. 3 2012 dinner with officials of the Chinese embassy at a restaurant in Mississauga. The deadline for this is 1 p.m. today. Thank you. [redacted]

Background from [redacted]

A dinner on August 3, 2012, at traditional Chinese restaurant in Mississauga, did occur. The dinner was resultant of meetings/presentations held that day at GTEC with a delegation of Chinese [redacted] (management only) from the [redacted] in China. The meetings began at 8:00 am and lasted all day. The purpose of the meetings was for the Chinese officials to present to [redacted] and staff a listing of Chinese nationals who are "individuals of interest" to the Chinese authorities, and who are now believed to be in Canada (GTA).

The meetings were attended by various [redacted]

Those who attended at the dinner in the evening with the Chinese delegation, were the following:

[redacted]

At the dinner: [REDACTED] had been made aware of the cultural protocol involved ahead of time and had been advised by his HQ programs that a refusal to attend the dinner could be seen as offensive to the delegation.

The group of individuals listed above attended at the dinner with approximately eleven (11) of the Chinese officials. As per accepted protocol and with regard to the cultural differences regarding etiquette and manners [REDACTED] made a toast to his Chinese counterparts. The toast was made with a traditional Chinese alcohol and there was a resultant reciprocal toast.

The three officers who attended were paid overtime for the dinner.

Media Lines/Response:

The Canada Border Services Agency has no knowledge of a complaint made to the Public Service Integrity Commissioner.

I can advise however that a dinner on August 3, 2012, at traditional Chinese restaurant in Mississauga, did occur. The dinner was resultant of meetings/presentations held that day at the CBSA Greater Toronto Enforcement Centre (GTEC) between CBSA officials and a delegation of Chinese [REDACTED] Management Officials from the Ministry of Public Security and Safety in China. The meetings began at 8:00 am and lasted all day. The purpose of the meetings was to discuss the presence of potential Chinese fugitives in Canada.

The CBSA officials were invited to dinner following the meetings, by the Chinese delegation. A group of CBSA officials attended at the dinner with approximately eleven (11) of the Chinese delegation. As per accepted protocol and with regard to the cultural differences regarding etiquette and manners, a CBSA official made a toast to his Chinese counterparts. The toast was made with a traditional Chinese alcohol and there was a resultant reciprocal toast.

The CBSA and all our officers are committed to keeping Canada safe and secure while serving the public in strict adherence to the Agency's core values of professionalism, integrity and respect.

CBSA employees are held to a very high standard. They are expected to conduct themselves professionally and in accordance with: the Values and Ethics Code for the Public Service; the CBSA Code of Conduct; CBSA policies and the Agency's core values. Any behaviour that falls short of this expectation is addressed immediately.

s.15(1) - Int'l

s.19(1)

Swift, Andrew

From: Giolti, Patrizia <Patrizia.Giolti@cbsa-asfc.gc.ca>
Sent: Friday, October 05, 2012 9:51 AM s.19(1)
To: Swift, Andrew
Cc: Stokes, Mark; Filipps, Lisa
Subject: RE: Sun: Border brass booze-up

Categories: ATI PRINT

Sorry - Andrew - responded already directly to Julie Call in roughly 10ish yesterday Repsonse from region round 2ish
Internal CBSA approvals Sent to MO at roughly 1700

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

From: Swift, Andrew [mailto:Andrew.Swift@ps-sp.gc.ca]
Sent: October 5, 2012 9:39 AM
To: Giolti, Patrizia
Cc: Stokes, Mark; Filipps, Lisa
Subject: RE: Sun: Border brass booze-up

Pat,
MO is asking again about when the call came in to CBSA?
Andrew

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

From: Swift, Andrew
Sent: Friday, October 05, 2012 7:43 AM
To: 'Patrizia.Giolti@cbsa-asfc.gc.ca'
Cc: 'Mark.Stokes@cbsa-asfc.gc.ca'; Filipps, Lisa
Subject: Re: Sun: Border brass booze-up

Thanks Pat. MO has asked when the call came in?

Andrew Swift
Director, Public Affairs
Communications
Public Safety Canada
Tel: 613-991-3549
Andrew.Swift@ps-sp.gc.ca

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

From: Giolti, Patrizia [mailto:Patrizia.Giolti@cbsa-asfc.gc.ca]
Sent: Friday, October 05, 2012 07:27 AM
To: Swift, Andrew
Cc: Stokes, Mark; Filipps, Lisa
Subject: Re: Sun: Border brass booze-up

Here it is Andrew. We did respond however when we called to say we would not meet the 1300 deadline, [REDACTED] indicated he had already written his article. [REDACTED] We responded round 1630

s.15(1) - Int'l

s.19(1)

Reporter: [REDACTED]

Media: Toronto Sun

Issue: Email from Reporter -- Good morning. I am seeking information in relation to a complaint that was filed to the Integrity Commissioner in which it is alleged that several CBSA officials acted in an unprofessional manner by getting drunk etc. during an Aug. 3 2012 dinner with officials of the Chinese embassy at a restaurant in Mississauga. The deadline for this is 1 p.m. today.

Background (for internal use only): A dinner on August 3, 2012, at traditional Chinese restaurant in Mississauga, did occur. The dinner was resultant of meetings/presentations held that day at GTEC with a delegation of Chinese [REDACTED] Officers (management only) from the [REDACTED] in China. The meetings began at 8:00 am and lasted all day. The purpose of the meetings was for the Chinese officials to present to [REDACTED] management and staff a listing of Chinese nationals who are "individuals of interest" to the Chinese authorities, and who are now believed to be in Canada (GTA). The meetings were attended by various [REDACTED]

At the dinner: The [REDACTED] had been made aware of the cultural protocol involved ahead of time and had been advised by his HQ programs that a refusal to attend the dinner could be seen as offensive to the delegation.

A group of CBSA staff attended at the dinner with approximately eleven (11) of the Chinese officials. As per accepted protocol and with regard to the cultural differences regarding etiquette and manners, [REDACTED] made a toast to his Chinese counterparts. The toast was made with a traditional Chinese alcohol and there was a resultant reciprocal toast.

Questions: Can you confirm? Have you received the complaint? What is CBSA doing about it?

RESPONSE:

I can advise that on August 3, 2012, CBSA officials from the CBSA Greater Toronto Enforcement Centre (GTEC) attended a dinner with a Chinese delegation. The dinner followed meetings held that day.

The CBSA is committed to keeping Canada safe and secure while serving the public in strict adherence to the Agency's core values of professionalism, integrity and respect. CBSA employees are held to a very high standard. They are expected to conduct themselves professionally and in accordance with: the Values and Ethics Code for the Public Service; the CBSA Code of Conduct; CBSA policies and the Agency's core values. Any behaviour that falls short of this expectation is addressed immediately.

The CBSA has no knowledge of a complaint made to the Public Service Integrity (PSI) Commissioner with respect to this event. Should you have questions, it is recommended you contact the PSI Commissioner directly Canada at 613-946-2138.

Sent from my BlackBerry handheld.

Envoyé à partir de mon BlackBerry.

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

From: Swift, Andrew [mailto:Andrew.Swift@ps-sp.gc.ca]

Sent: Friday, October 05, 2012 07:24 AM

To: Giolti, Patrizia

Cc: Stokes, Mark; Filippis, Lisa <Lisa.Filippis@ps-sp.gc.ca>

Subject: Sun: Border brass booze-up

Pat,
Did I miss this enquiry yesterday? Can you share your lines? Julie has said this a.m. that she approved a response from CBSA late yesterday, and is asking why no response was provided.
Andrew

Border brass booze-up
Feds probe possible security leaks in 'frat party' with Chinese

THE OTTAWA SUN (FINAL)

Section: NEWS, Page: 3

TOM GODFREY, QMI AGENCY

TORONTO -- Federal investigators are probing whether national security rules were breached during a boozy dinner in which Canadian border services brass were allegedly wined and dined by members of the Chinese embassy and their public-security agents.

A complaint was filed to the Public Sector Integrity Commissioner following an Aug. 3 party at a Mississauga restaurant that was attended by five officials of the Canada Border Services Agency and a delegation from the Chinese embassy in Ottawa and visiting Ministry of Public Security agents.

Edith Lachapelle, of the commissioner's office, could not confirm what complaints were received.

CBSA officials did not provide comment.

"Reports from this 'meeting' suggest that it was nothing more than a drunk fest," read the complaint, which was obtained by QMI Agency. "The drinking was so extreme that some (officials) were totally incoherent and unable to operate their vehicle while others were puking in Canadian-government vehicles."

The complaint alleged one senior CBSA official had to be driven home.

The name of the complainant has been withheld due to fears of reprisals by CBSA management officials.

The document claimed CBSA staff are concerned about possible leaks of classified information on Chinese immigrants, fugitives or deportees.

"It is well known that Chinese officials are

generous hosts and push alcohol and other incentives as a means of co-opting and influencing Canadian government officials," the

commissioner was told. "Such 'tactics' on the part of Chinese officials have been widely reported."

"It is shocking that CBSA officials would not have been more aware and sensitive to the situation," the complaint said. "How do we know that information sensitive to Canadian national interests were not divulged to the Peoples' Republic of China or other sensitive information compromised?"

The complainant called the dinner a "frat party."

"This sort of behaviour is unbecoming of public servants representing Canada and certainly not what you would expect from our more senior officials," the complaint said.

CSIS director Richard Fadden told a Commons committee in 2010 that foreign influence "is more common here and elsewhere than many think."

Fadden said CSIS has ongoing investigations into politicians at the provincial and municipal level who are agents of influence for foreign governments in Canada.

Just last year, Tory MP Bob Dechert, then parliamentary secretary to the minister of justice, had to undergo fresh cabinet security checks after it was revealed he sent flirtatious e-mails to a journalist working for the state-run agency linked to China's intelligence services.

Dechert is now a parliamentary secretary to the minister of foreign affairs.

* Media contents in NewsDesk are copyright protected.

Andrew Swift
Director, Public Affairs
Communications
Public Safety Canada
Tel: 613-991-3549
Andrew.Swift@ps-sp.gc.ca

Durand, Stéphanie

From: Pacha, Tomasz
Sent: Tuesday, October 02, 2012 12:57 PM
To: Coady, Therese; Danaitis, Algis; Duguay, Marcel; Boily, Mario; Ku, Shawn; Guitor, Denis; McLeod, Tim; Currie, Chris; Duschner, Gabrielle; Mattioli, Mary-Ann; GOC-COG; Durand, Stéphanie; Champoux, Martin; Filippis, Lisa; Swift, Andrew; MacDonald, Michael; Wong, Suki; DeJong, Michael; Hashmi, Sabah
s.16(2)(c)
s.20(1)(c)
Cc: Anderson, Windy; Bendelier, Kenneth; Klassen, Nathan; Proulx, Véronique
Subject: CYBER NOTIFICATION 011- 1- MEDIUM IMPACT SEVERITY – INFORMATION DISCLOSURE – NOT FOR ESCALATION – Canadian Manufacturing Company Targeted by Cyber Intrusion (UPDATE One)

CYBER NOTIFICATION – INCIDENT

Note: Updates/Changes in BOLD text

Incident Number: CNT-12-011 – MEDIUM IMPACT SEVERITY – INFORMATION DISCLOSURE – NOT FOR ESCALATION

Description of Incident: It has been reported that [REDACTED] was recently targeted by a cyber intrusion. [REDACTED] is currently investigating the intrusion, and, as a precautionary measure, has disconnected portions of its networks. [REDACTED] who owns [REDACTED] has stated that its affected customers have been informed. CCIRC has confirmed that Canadian clients did receive this notification.

Sources of reporting: Open source media and trusted partners.

Current actions: CCIRC has reached out to the affected company to obtain additional information, and also offered to provide mitigation assistance, if required. CCIRC will continue to monitor this situation to accurately assess its impact severity. **(2 Oct 2012) CCIRC established initial contact with [REDACTED] representatives 28 Sep 2012. To date, no further information has been received directly from [REDACTED]**

CCIRC has obtained technical information related to this compromise. Indicators and mitigation advice will be provided to partners in Cyberflash CF12-003 (Update 5) scheduled for release 2 Oct 2012.

CCIRC will be hosting a meeting of the Cyber Triage Unit in order to synchronize federal government efforts. This meeting will be held on 2 Oct 2012.

CCIRC is in liaison with international partners, including ICS-CERT, to collaborate in the development of additional mitigation advice, share technical analysis and coordinate incident response efforts.

Updated analysis / assessment:

- **(2 Oct 2012) According to the company's website,** [REDACTED]
- This story has already been picked up by a number of media outlets, and has the potential to garner increasing media interest. These media reports have attributed this cyber intrusion to a Chinese hacking group called the "Comment Group", which has been previously linked to other cyber espionage campaigns.

- (2 Oct 2012) Subsequent reporting by [REDACTED] customers indicates potential second order effects as a consequence of this compromise. A non-essential data link between [REDACTED] and the [REDACTED] data network was temporarily disconnected. [REDACTED] information, there was no operational impact [REDACTED]

s.20(1)(c)

Disclaimer:

This notification is only for distribution within Public Safety and is for information purposes. No action or decision is required by recipients at this time. For the purposes of Access to Information Act requests, the originator will maintain and provide an official copy of this notification.

Prepared by: Ken Bendelier (993-5042)

Approved by: Ken Bendelier (993-5042)

Sent on behalf of Ken Bendelier by Tom Pacha.

Durand, Stéphanie

From: Dick, Robert
Sent: Thursday, September 27, 2012 1:15 PM
To: Gordon, Robert; Clairmont, Lynda; Durand, Stéphanie; MacDonald, Michael; Oldham, Craig
Subject: Fw: CYBER NOTIFICATION 011 – MEDIUM IMPACT SEVERITY – INFORMATION DISCLOSURE – Canadian Manufacturing Company Targeted by Cyber Intrusion

Info only. s.16(2)(c)
s.20(1)(c)

From: Proulx, Véronique
Sent: Thursday, September 27, 2012 12:01 PM
To: Dick, Robert; Matz, Mark; Hatfield, Adam; Labelle, Sébastien; Anderson, Windy
Cc: Bendelier, Kenneth; Klassen, Nathan; Pacha, Tomasz; Beaudoin, Luc; Clow, Patrick; Fortunato, Stephanie
Subject: CYBER NOTIFICATION 011 – MEDIUM IMPACT SEVERITY – INFORMATION DISCLOSURE – Canadian Manufacturing Company Targeted by Cyber Intrusion

CYBER NOTIFICATION – INCIDENT

Incident Number: CNT-12-011 – MEDIUM IMPACT SEVERITY – INFORMATION DISCLOSURE

Description of Incident: It has been reported that [REDACTED] was recently targeted by a cyber intrusion. This intrusion has reportedly affected the company's [REDACTED] is currently investigating the intrusion, and, as a precautionary measure, has disconnected portions of its networks. [REDACTED] who owns [REDACTED] has stated that its affected customers have been informed. CCIRC has confirmed that Canadian clients did receive this notification.

Sources of reporting: Open source media and trusted partners.

Current actions: CCIRC has reached out to the affected company to obtain additional information, and also offered to provide mitigation assistance, if required. CCIRC will continue to monitor this situation to accurately assess its impact severity.

Initial analysis / assessment:

- [REDACTED]
- [REDACTED]
- This story has already been picked up by a number of media outlets, and has the potential to garner increasing media interest. These media reports have attributed this cyber intrusion to a Chinese hacking group called the "Common Group", which has been previously linked to other cyber espionage campaigns.

Disclaimer:

This notification is only for distribution within Public Safety and is for information purposes. No action or decision is required by recipients at this time. For the purposes of Access to Information Act requests, the originator will maintain and provide an official copy of this notification.

Prepared by: Véronique Proulx (990-7102)
Approved by: Ken Bendelier (993-5042)

Véronique Proulx

Analyst | Analyste

Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques

Public Safety Canada | Sécurité publique Canada

257 Slater St. | 257 rue Slater

Ottawa, Ontario, Canada K1A 0P8

Tel : (613) 990-7102

veronique.proulx@ps-sp.gc.ca

Durand, Stéphanie

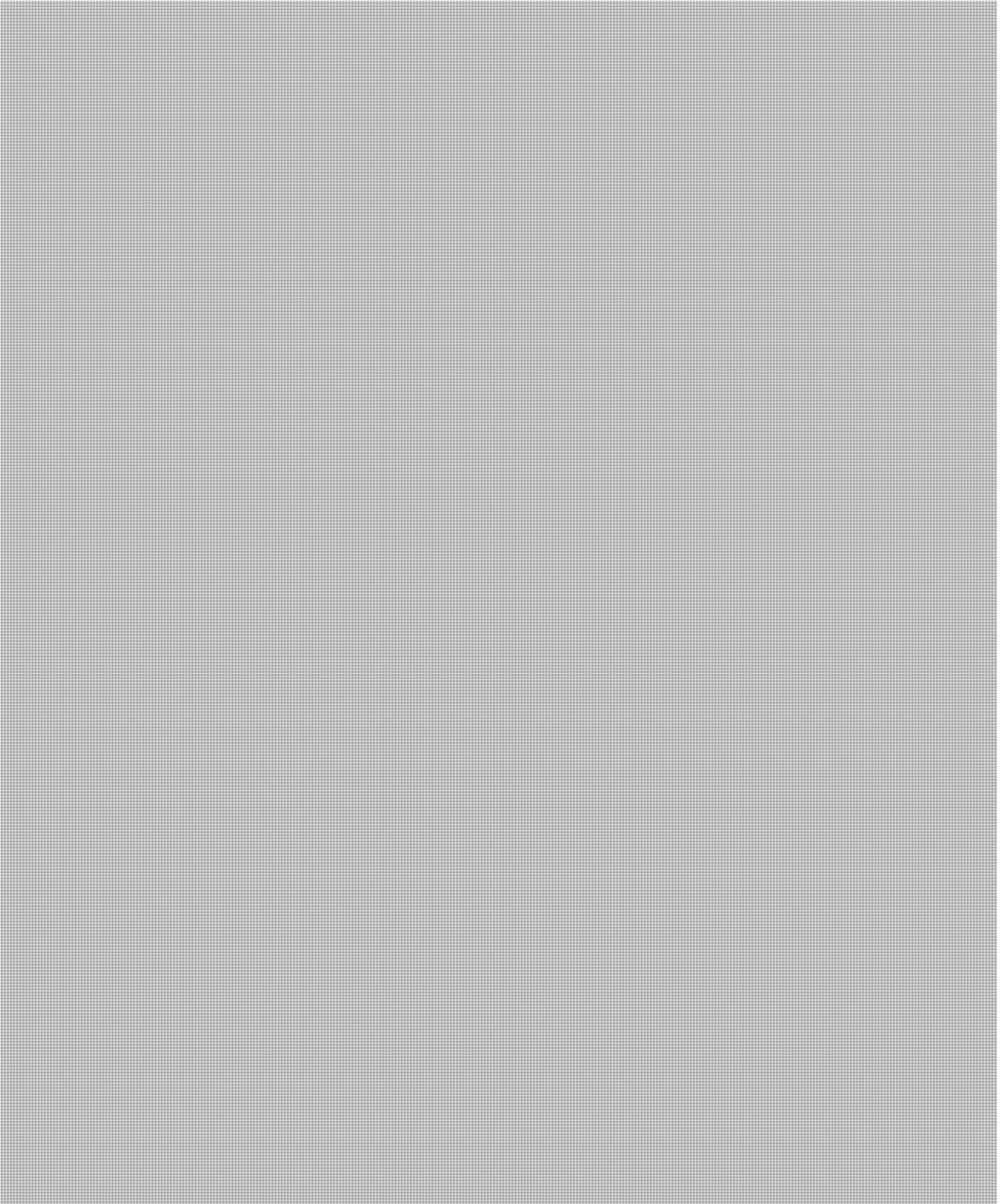
From: Mike.Theilmann@international.gc.ca
Sent: Thursday, September 13, 2012 12:27 PM
To: Hugh.Adsett@international.gc.ca; Anderson, Windy; Lucie.Angers@justice.gc.ca; DArnaud@pco-bcp.gc.ca; kaudcent@justice.gc.ca; annie.bollaert@international.gc.ca; Claude.Boucher@international.gc.ca; Ryan.Boudreau@international.gc.ca; Yves.Brodeur@international.gc.ca; Wendy.Bullion-Winters@international.gc.ca; Anne.Burgess@international.gc.ca; Cameron, Bud; Paul.Charlton@international.gc.ca; Cloutier, Joey; Chantal Couture; Oldham, Craig; De Santis, Heather; Greg.Dempsey@international.gc.ca; * GOC-SARA; Dick, Robert; brigitte.diogo@pco-bcp.gc.ca; Robin.Dubeau@international.gc.ca; Durand, Stéphanie; Duschner, Gabrielle; Dvorkin, Corey; gub@international.gc.ca; extott-ict@international.gc.ca; Mark.Glauser@international.gc.ca; Elissa.Golberg@international.gc.ca; Grigsby, Alexandre; Gulak, James; Hatfield, Adam; [REDACTED]@cse-cst.gc.ca; Khouri, Lisa; Tachelle.Kirkpatrick@international.gc.ca; Heidi.Kutz@international.gc.ca; Labelle, Sébastien; ldn-gr@international.gc.ca; Angelica.Liao-Moroz@international.gc.ca; Linder, Glen; [REDACTED] Clairmont, Lynda; MacKinnon, Paul; Maillé, Marie Anick; Marv.Makulowich@forces.gc.ca; Tamara.Mawhinney@international.gc.ca; Matthew.Mayer@international.gc.ca; McAllister, Andrew; Helen.McDonald@ic.gc.ca; Frederic.Miville-Deschenes@international.gc.ca; [REDACTED]@cse-cst.gc.ca; Motzney, Barbara; Sabine.Nolke@international.gc.ca; Tim.Oneil@rcmp-grc.gc.ca; Parenteau, Marie-Pierre; Dawn.Parks@international.gc.ca; Douglas.Proudfoot@international.gc.ca; CRAM@justice.gc.ca; Lesser, Robert; Gordon, Robert; Mike.Ryan@international.gc.ca; Schwartz, Jo-Ann; Beaudoin, Serge C; [REDACTED] Robert.Sinclair@international.gc.ca; Lesley.Soper@pco-bcp.gc.ca; Spallin, Julie; Debra.Spencer@international.gc.ca; Wong, Suki; Colin.Townson@international.gc.ca; Christa.Unfried@international.gc.ca; Brigitte.Walenius@international.gc.ca; Michael.Walma@international.gc.ca; Eric.Walsh@international.gc.ca; Waters, Michael; wendy.nicol@rcmp-grc.gc.ca; Artur.Wilczynski@international.gc.ca; Wilson, Gina; Brighton, Brian; Buchanan, Cameron; Grewal, Surinder; Mitchell, Kellie; Parnham, Diane; Robichaud, Claude; Scharf, Jo-Anne; Sigouin, Michel
Cc: ldn-gr@international.gc.ca; Colleen.Calvert@international.gc.ca; Theilmann, Michael; IMRepositoryRepertoireGI.CATS@international.gc.ca
Subject: XNGR 3163: Expert Offers Insights to China's Ambitions and Strategy in Cyber Space

s.15(1) - Int'l
s.15(1) - Subv

Summary: [REDACTED]

2. Report: On September 7, 2012, LDN attended a one-day workshop sponsored by the UK Information Systems Security Association and featuring Bill Hagestad, an internationally recognized expert on China's cyber ambitions and former Lieutenant-Colonel in the US Marines. He is also the author of *21st Century Chinese Cyber Warfare* published in March 2012 and has lived in China and

speaks Mandarin.



**Pages 158 to / à 159
are withheld pursuant to section
sont retenues en vertu de l'article**

15(1) - Int'l

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

Drafted/Released: LDN/Theilmann

Mike Theilmann
Counsellor (Public Safety)/ Conseiller (Sécurité publique)
Canadian High Commission/Haut-commissariat du Canada
Macdonald House, 1 Grosvenor Square
London W1K 4AB/Londres W1K 4AB
United Kingdom/Royaume-Uni
Mike.Theilmann@international.gc.ca
Telephone/Téléphone 020-7258-6640
Facsimile/Télécopieur 020-7258-6645
MITNET 445-3640
Government of Canada/Gouvernement du Canada

Flack, Graham

From: Clairmont, Lynda
Sent: Thursday, October 11, 2012 12:35 PM
To: Flack, Graham; Jarmyn, Tom; House, Andrew
Subject: Re: U.K. to probe Huawei, while Huawei announces (£1.3B UK expansion)

I flipped to all my colleagues - incl pco

From: Flack, Graham
Sent: Thursday, October 11, 2012 12:32 PM
To: Clairmont, Lynda; Jarmyn, Tom; House, Andrew
Subject: Re: U.K. to probe Huawei, while Huawei announces (£1.3B UK expansion)

From: Clairmont, Lynda
Sent: Thursday, October 11, 2012 12:18 PM
To: Jarmyn, Tom; House, Andrew; Flack, Graham
Subject: FW: U.K. to probe Huawei, while Huawei announces (£1.3B UK expansion)

s.15(1) - Subv
s.19(1)

fyi

From: Helen.McDonald@ic.gc.ca [mailto:Helen.McDonald@ic.gc.ca]
Sent: October-11-12 12:08 PM
To: Clairmont, Lynda; [REDACTED]@cse-cst.gc.ca
Subject: FW: U.K. to probe Huawei, while Huawei announces (£1.3B UK expansion)

U.K. to probe Huawei, BT relationship over security concerns

A U.K. parliamentary committee will examine the relationship between Huawei, which was accused of posing a national security threat by the U.S., and British Telecom, the U.K.'s largest telecoms provider.

By Zack Whittaker for Between the Lines | October 11, 2012

The relationship between embattled Chinese telecoms equipment maker Huawei, and the U.K.'s largest telecoms company British Telecom (BT) will be investigated by the U.K. Parliament's intelligence and security committee.

Sir Malcolm Rifkind, the parliamentary committee's chairman, confirmed that the companies' relationships will be examined by the panel, The Guardian confirmed earlier today, following earlier reports that the U.K. Parliament could investigate the firm in a similar style to a U.S. House probe.

According to the London newspaper, the committee is "reviewing the whole presence of Huawei in regard to our critical national infrastructure and whether that should give rise for concern," which could slow-down or even halt some ongoing broadband and mobile infrastructure projects should valid security fears regarding Huawei's equipment or company prove accurate.

Rifkind said there were allegations that the Chinese company was linked to the People's Liberation Army, the military faction of the Chinese government, and that "any Chinese company is ultimately subject to the Chinese government."

He added that the committee will look at the historical background to the contract between Huawei and BT and if there were security concerns at the time, and whether there are any further "causes for concern" since the Chinese telecoms maker became involved in the U.K.'s telecoms infrastructure.

But as Huawei is a major supplier of equipment to BT -- notably the rollout of the national fiber broadband, along with the new 4G LTE network offered by new cell network EE, among other clients -- the implications for the British market could be crucial.

Huawei, which has operated in the U.K. since the turn of the millennium, has not yet been asked to give evidence, but said it "welcome[s] all discussions and questions."

For now, the U.K. is one of the only countries still keen to saddle up to the Chinese firm. Most consumers may not even realize that the bulk of the technology used to power the British Internet is supplied from Huawei.

The Chinese firm's chief executive Ren Zhengfei recently met British Prime Minister David Cameron after pledging to invest \$2 billion (£1.3bn) in the U.K. economy. Any negative response from the parliamentary committee could be embarrassing for Downing Street and the coalition government.

Cameron said at the time: "The British Government values the important relationship with China, both countries have much to offer each other and the business environment we are creating in the U.K. allows us to maximize this potential."

However, Huawei continues to face extreme criticism in the U.S. following a probe by the U.S. House Intelligence Committee that concluded earlier this week. Lawmakers said in a 52-page report that Huawei, along with ZTE -- which also makes telecoms equipment for Western countries -- that the technology giants may pose a threat to U.S. national security, and discouraged American firms from buying their equipment.

Canada recently hinted that it may also soon pull the plug on any contracts that exist with Huawei over fears that the technology may contain security risks for the country's infrastructure.

Huawei was also barred from bidding on contracts for the Australian National Broadband Network over fears that the telecoms maker's devices could include backdoors that could open the door to foreign espionage.

Huawei dismissed the claims, saying:

...we have never damaged any nation or had the intent to steal any national intelligence, enterprise secrets, or breach personal privacy and we will never support or tolerate such activities, nor will we support any entity from any country who may wish us to undertake an activity that would be deemed illegal in any country

The U.K. government, taking an entirely different approach, said that such fears could be addressed by working closely with Huawei and examining its equipment.

The Chinese firm set up a base in Banbury, Oxfordshire, in 2010 where Huawei's products can be tested and examined for threats and security vulnerabilities in conjunction with the U.K.'s security services. The so-called Cyber Security Evaluation Centre allows for the vetting of telecoms equipment to ensure that only secure products can be used in the country's critical national infrastructure.

However, there have been no public reports that there is yet anything to worry about, or equipment has failed strict vetting procedures set out by the security services and private industry telecoms groups, such as BT.

Representatives for Huawei were unavailable for comment at the time of writing. Questions have been put in to Downing Street, but we did not hear back at the time of publication. We'll update the piece if we hear back.

Bernas, Angie

From: Clairmont, Lynda
Sent: Sunday, October 07, 2012 9:26 AM
To: Flack, Graham
Cc: Bernas, Angie
Subject: Fw: Fyi

See below - have already tasked out to Robert Dick - L

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

From: Jarmyn, Tom
Sent: Sunday, October 07, 2012 09:11 AM
To: Clairmont, Lynda
Subject: Re: Fyi

I have been following

Will someone be doing a quick analysis of the House Report tomorrow so that we can have a preliminary response. I suspect that we are going to be pushed substantively very quickly and no later than sometime Tuesday.

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

From: Clairmont, Lynda
Sent: Sunday, October 07, 2012 09:09 AM
To: Jarmyn, Tom
Subject: Fyi

Huawei is security threat, say US lawmakers Bloomberg / Washington Oct 07, 2012, 00:52 IST

US companies should avoid business with Huawei Technologies, China's largest phone-equipment maker, to guard against intellectual-property theft and spying, the US House Intelligence Committee chairman said.

US companies considering purchases from Huawei should "find another vendor if you care about your intellectual property, if you care about your consumers' privacy, and you care about the national security of the United States of America," Representative Mike Rogers told CBS News's "60 Minutes," according to a CBS release about an interview set to air tomorrow.

Rogers, a Michigan Republican, and the committee's top Democrat, Maryland Representative CA "Dutch" Ruppberger, are preparing to issue a report October 8 on their year-long investigation of Huawei and ZTE Corp, another Chinese phone-equipment maker. The lawmakers have been looking at whether the companies' expansion in the US market enables Chinese government espionage and imperils the US telecommunications infrastructure. "Huawei is a globally trusted and respected company doing business in almost 150 markets with over 500 operator customers, including nationwide carriers across every continent save Antarctica," William Plummer, a Washington-based spokesman for Huawei, said in an e-mail. "The security and integrity of our products are world proven. Those are the facts today. Those will still be the facts next week, political agendas aside."

Susan Phalen, a spokeswoman for the committee, didn't immediately respond to a request for comment.

Committee investigation

Executives for Huawei and ZTE, both based in Shenzhen, China, denied links to espionage during an intelligence committee hearing last month, telling lawmakers they aren't controlled by the Chinese government.

The companies said they favor independent audits of technology vendors' hardware and software as a way to ensure that devices and networks are secure.

The panel's probe coincides with increased US warnings about digital spying by China. US counterintelligence officials called China the world's biggest perpetrator of economic espionage in a report last November, saying the theft of sensitive data in cyberspace is accelerating and jeopardising an estimated \$398 billion in us research spending

Richer, Jean-Marc

From: McAteer, Julie
Sent: Friday, October 05, 2012 12:43 PM
To: * EXCOM/COMEX; * Parliamentary Affairs Division / Division des affaires parlementaires; Fisher, Adam; Allison, Catherine; Amy JOHNSON; Archambault-Chapleau, Nadine; Beaudoin, Serge C; Bedor, Tia Leigh; Blackie, Ian; Boucher, Patrick; Bourdeau, Anne; Brock, Darlene; Burton, Meredith; Caroline Douglas; Charles-Eric.Lepine@rcmp-grc.gc.ca; Christine Larose; Desnoyers, Christine; Clavel, Julien; Cogan, Tim; COMDO; Cyr, Lynne; Dagenais, Louise; de Jager, Gabriela; Dupuis, Chantal; [REDACTED] Fournier, Muriel; Issues / Enjeux; Johnson, Mark; karyn.curtis@rcmp-grc.gc.ca; Koops, Randall; Lambert, Louise; Larose, Nathalie; Leclair, Natalie; Leclerc, Carole; LeSage, Lynn; Roylt; [REDACTED] McAteer, Julie; McLaren, Victoria; Mueller, Mike; Nabil Temimin; nicole.greenough@cbsa-asfc.gc.ca; Paulson, Erika; Perry, Gates; prierma@npb-cnrc.gc.ca; Executive Services; Robin.Stong@cbsa-asfc.gc.ca; Ruth.Marier@cbsa-asfc.gc.ca; Sarah Estabrooks; Scheewe, Nathan; Sellers, Philip; Shannon Muldoon; Suzanne Schmidt; Veilleux, Martine
Subject: QP Transcript for October 5, 2012 / Transcription de la Période des questions pour le 5 octobre 2012
Attachments: QPN Transcript October 5, 2012.pdf

s.15(1) - Subv

Good afternoon,

Focus of Question Period today: Food safety

Questions answered by the Parliamentary Secretary:

Raymond Côté (Beauport—Limoilou) asked a question regarding the hiring of chaplains in correctional institutions (Transcription in yellow)

The offenders who are trying to redeem themselves through their religion are being told, sorry, we only accept christians. Rabbi, I ma'ams are being let go. We could even see elders from aboriginal communities shown the door, and yet this is not an expensive program. Will the Minister reconsider his decision to eliminate religious revs service force jewish, Muslim and sikh offenders? The speaker: The parliamentary secretary for the Minister of public safety and national security.

Candice Bergen (CPC): Thank you very much, Mr. Speaker. I want to begin by rejecting the premise of that question. Our government strongly supports the freed om of religion for all Canadians and convicted criminals continue to have reasonable access to any religious counsel counseling or services of their chris on a voluntary basis. The government does fund full-time chaplains in addition to serving members of their own faith, these chaplains also make themselves available on a by-request base toys provide spiritual advice to the general population. Mr. Speaker, the Canadian forces have used this type of chaplaincy program for years f it's good enough, Mr. Speaker, for our armed force's it's good enough for inmates in our federal penitentiaries.

Paul Dewar (Ottawa Centre) asked a question regarding the hiring of chaplains in correctional institutions (Transcription in orange)

Picking and choosing on the subject just don't -- won't wash, Mr. Speaker. This is not a costly program. The Minister has no justification for cutting it. You know, actually, she should listen to her colleague who said the following: Religious freedom is a fundamental freedom. One we are very, very pourive and feels very strongly about." Who do you know who said is that? T her klegg, yes, the Minister of foreign affairs, so the question for the Conservatives is how can they be so hypocritical in being strong apparently on religious firemen abroad when they won't support it at home?

The speaker: The honourable member -- the honourable parliamentary secretary to the Minister of public

safety and national security.

Candice Bergen (CPC): Mr. Speaker, the member is completely inaccurate. It's very sad to hear him display and say these kinds of mistruths. The government funds full-time chaplains that are determined based on the number of inmates requesting services from each faith determined by region. And as I said, in addition to serving members of their own faith, these chaplains also make themselves available on a by-request basis to provide spiritual advice to the general population. Mr. Speaker, this is a common practice. The Canadian forces has used. This similar chaplain say scam it's been successful forever many years, Mr. Speaker.

Alexandrine Latendresse (Louis-Saint-Laurent) asked a question regarding actions of CBSA officers (Transcription in green)

Americas we learned that money morning that the Chinese party organized a party where the drink was so extreme that some for senior officials went home dead drunk. This raises concerns about fact that state secrets could have been leaked during this drunk fest. We've already seen a former Minister leave top-secret documents at his girlfriend's house. Why don't Conservatives take espionage risks seriously?

The speaker: The honourable parliamentary secretary tore public safety.

Candice Bergen (CPC): Mr. Speaker, Canadians expect law enforcement officers to act with integrity at all times. CBSA is lack looking into the facts of this situation. Anyone found to have been behaved inappropriately or acting inappropriately will face sanctions and discipline, Mr. Speaker.

The speaker: (Voice of translator): The honourable member for you Louis-Saint-Laurent.

Alexandrine Latendresse (NDP) (Voice of translator): The Conservatives' everyone difference is appalling and it contrasts sharply with the seriousness of the situation and the potential for risk. When our customs officers are paid -- are applied with liquor to the point that they are throwing newspaper their government vehicles, the Conservatives should wonder. When CSIS is concerned about foreign state-owned enterprises having a stake in our natural resource, the Conservatives should ask themselves questions. When will they start taking threats to national security seriously.

The speaker: The honourable parliamentary secretary tore the public safety.

Candice Bergen (CPC): Well, Mr. Speaker, I will repeat, and I think that we are absolutely not indifferent. We as all Canadians do expect our law enforcement officers to act with integrity at all times. CBSA, and I'll repeat this, it looking into the facts of this situation. I would think the honourable member would appreciate that and would approve with that. There's due process for this kind of scenario, and if found to have been --

The speaker: The honourable parliamentary secretary tore the public safety.

Candice Bergen (CPC): Well, Mr. Speaker, I will repeat, and I think that we are absolutely not indifferent. We as all Canadians do expect our law enforcement officers to act with integrity at all times. CBSA, and I'll repeat this, it looking into the facts of this situation. I would think the honourable member would appreciate that and would approve with that. There's due process for this kind of scenario, and if found to have been -- acted inappropriately will face sanctions, will face discipline. Thank you, Mr. Speaker.

Irwin Cotler (Mount Royal) asked a question regarding the hiring of chaplains in correctional institutions (Transcript in blue)

Mr. Speaker, the government is cancelling the contracts of non-Christian chaplains in federal prisons, thereby requiring inmates of other faiths to turn to Christian chaplains for religious guidance. Minister says "he is no the business of picking and choosing which religions will be given preferential status" by

but he's doing precisely that. Will the Minister recognize his contradiction, reinstate funding for chaplains of all faiths and uphold the values of freedom of conscience and religion and equality before the law as enshrined in the charter of rights and freedoms? Thank you, Mr. Speaker.

The speaker: The honourable parliamentary secretary to the Minister of public safety.

Candice Bergen (CPC): Thank you, Mr. Speaker. Mr. Speaker, the government of Canada strongly supports the freedom of religion for all Canadians. Last month, the Minister of public safety asked for an immediate review of the chaplaincy program to ensure that taxpayers' dollars are being used wisely and

The speaker: The honourable parliamentary secretary to the Minister of public safety.

Candice Bergen (CPC): Thank you, Mr. Speaker. Mr. Speaker, the government of Canada strongly supports the freedom of religion for all Canadians. Last month, the Minister of public safety asked for an immediate review of the chaplaincy program to ensure that taxpayers' dollars are being used wisely and appropriately. Upon reviewing the program, it was determined that changes were necessary so that this program supports the freedom of religion of inmates while respecting taxpayers' dollars. Convicted criminals, Mr. Speaker, will continue to have access to religious services of their choice on a voluntary basis. Thanks Mr. Speaker.

The English unofficial transcript is attached.

The official transcript will be available in both official languages tomorrow morning on the Parliamentary website www.parl.gc.ca.

Thank you.

Bon après-midi,

Focus de la Période des questions aujourd'hui : La salubrité des aliments

La secrétaire parlementaire a répondu aux questions qui suivent :

Raymond Côté (Beauport—Limoilou) a posé une question concernant l'embauche d'aumôniers dans les institutions correctionnelles. (Transcription en rose)

Paul Dewar (Ottawa-Centre) a posé une question concernant l'embauche d'aumôniers dans les institutions correctionnelles. (Transcription en orange)

Alexandrine Latendresse (Louis-Saint-Laurent) a posé une question concernant le comportement de certains employés de l'ASFC. (Transcription en vert)

Irwin Cotler (Mont Royal) a posé une question concernant l'embauche d'aumôniers dans les institutions correctionnelles. (Transcription en bleu)

Veillez prendre note que la transcription n'est disponible qu'en anglais seulement.

La transcription sera offerte dans les deux langues officielles demain matin sur le site www.parl.gc.ca.

Merci de votre compréhension.

Natalie Leclair

Advisor / Conseillère
Parliamentary Affairs / Affaires parlementaires
Public Safety Canada / Sécurité publique Canada
Tel/Tél: (613) 990-2718
Fax: (613) 954-8774
Email/Courriel: natalie.leclair@ps-sp.gc.ca

QP Closed Captioning Transcript

Question Period

Today

Updated Mon. - Thurs. at 4:30 p.m. and Fri. at 12:45 p.m.

*For an official transcript, please consult the Hansard located on the Parliamentary website.
Pour obtenir une transcription officielle, veuillez consulter le hansard sur le site web
parlementaire.*

2012-10-05

*Transcript provided courtesy of the Privy Council Office. Please note that this transcript is produced via the closed captioning provided by CPAC and is available in English only. Disclaimer

The speaker: Oral questions. The honourable member for Vancouver east.

Libby Davies (NDP): Thank you, Mr. Speaker. Mr. Speaker, on September the 13th, the Canadian food inspection agency yanked xl's exporter license at the request of US Officials. The Minister of agriculture and his department determined this meat wasn't safe enough to be sold to American consumers. Yet the Minister didn't pull xl's Canadian license for another 14 days. So, for 14 days, the Minister of agriculture allowed the same tainted meat that wasn't safe enough for Americans to be sold to Canadian families. Why?

The speaker: The honourable Minister of agriculture.

Gerry Ritz : Well, Mr. Speaker, I welcome the question from the Minister -- from the member opposite. It gives me another chance to say that food safety is a prior to forthis government. Cfia began acting on October the 4 is this has continued to act -- on September the 4th, I'm sorry, and has continued to act based on science and information as it became available.

The speaker: The honourable member for Vancouver east.

Libby Davies (NDP): The Minister's pons is, again,very short on the facts, so let's review. The Minister said he was aware from day one of all the activities, which means he knew about the broken safety equipment. It means he knew on September the 6th that xl foods waswithholding critical data from government officials. It means he knew on September 13th that meat from xl wasn't safe enough for American consumers, so why, then, did he withhold vital public health information from Canadians?

The speaker: The honourable Minister of agriculture.

Gerry Ritz: Well, like I said, Mr. Speaker, cfia, saved based on science and timely access to information, began on operating on the September the 4th in the best interests of Canadian consumers. They continued to

do that. There's a time line that's been well published up on the cfia website that answers alot of the questions that the member opposite chooses to ignore.

The speaker: The honourable member for Vancouver east.

Libby Davies (NDP): Mr. Speaker, yesterday was a watershed taking at a for taking responsibility. First, cfia took responsibility for their part in this recall. Then xl took responsibility for the faulty operations at the plant. The only person with the infallibility complex who refuses to take responsibility is the Minister of agriculture himself. When will he apologize for his failure to keep Canadians informed and when will he tender his resignation?

The speaker: The honourable member -- the honourable Minister of agriculture.

Gerry Ritz: Ofcourse all of these decisions and actions are undertaken by the officials at cfia, Mr. Speaker. They continue to work on science-based reasoning and time lines as information becomes available. My job as Minister is to ensure that they have the capacity both from a budgetary process and human resources to get that important job done.

The speaker: (Voice of translator): The honourable member for gaspesie - iles-de-la-madeleine.

Philip Toone (NDP) (Voice of translator): Thank you, Mr. Speaker. People simply no longer have confidence in this government, that refuses to accept its responsibilities. The tainted meat crisis has spread from coast-to-coast. The number of infected people is growing daily. In total, officials from public health in Alberta and Saskatchewan and other provinces are currently investigate many e-coli cases. Can the Minister tell us how many cases are currently under investigation and how many were reported after September 13th?

The speaker: The honourable Minister of agriculture.

Gerry Ritz: Well, Mr. Speaker, that's -- those numbers are available on the public health Canada website. I'm certain the member will check that number out. We certainly began acting -- the cfia began acting on September the 4th. They continue to work on a science-based system that they have in place, and we'll continue to do that job on recalls as they become necessary.

The speaker: (Voice of translator): The honourable member for gaspesie - iles-de-la-madeleine.

Philip Toone (NDP) (Voice of translator): Honestly, this is a total fiasco, this crisis, and there are multiple problems. There are broken nozzles, inadequate cleaning, weak surveillance system and all of this allowed for the contamination of millions of pounds of beef. This continued for weeks, without competent authorities, the Minister included, reacting. As a result, the tainted meat has ended up on the plates of thousands of Canadians. The current Minister does not want to assume his responsibilities. Why not replace him with someone who will?

The speaker: The honourable Minister of agriculture.

Gerry Ritz: Well, of course, Mr. Speaker, the cfia continues to act on science-based reasoning. One illness is too much. Everybody agrees with that, Mr. Speaker. We continue to build a robust food safety system. We also have bill s-11, the safe food for Canadians act, coming outside before the Senate, Mr. Speaker, and I'd invite the members opposite to help us expedite that to give the cfia more powers of recall.

The speaker: The honourable member for Toronto centre.

Bob Rae: Mr. Speaker, the decision that was made by cfia to delist xl products from companies that are permitted to export to the United States, can the Minister tell the hour whether that decision was one that was requested by the American authorities was it one that was made independently by the food saying and was the Minister aware of that decision at the time that it was made?

The speaker: The honourable Minister of agriculture.

Gerry Ritz: We have a robust food safety system, Mr. Speaker, recognized by the Americans as well. We work in consort due to the integrated nature of our beef industry in North America. Having said that, Mr. Speaker, the cfia work with hair counterparts on the American side to put forward the best interests of Canadian and American consumers and will continue to do that.

The speaker: The honourable member on the Toronto.

Bob Rae: .However robust that system is, the Minister isn't very robust at answering simple questions. I'd like it ask the Minister again this time the only conclusion one with can come to is that the American authorities appear to have been more concerned about the safety of all American consumers than the Minister was concerned about the safety of Canadian consumers. Because if that was not the case, why is it that cfia decided to close the border to Canadian products going to the United States, to all American consumers, but did not at the same time close access to the Canadian market? It took a further two weeks for the government to protect the Canadian consumer. Why the delay? And why were the Americans doing a better job on behalf of their consumers than our government's goin' doing on behalf of our consumers?

The speaker: The honourable Minister of agriculture.

Gerry Ritz: Well as I said previously, Mr. Speaker, we have a robust food safety s there are differences between what the Americans do and what the Canadian cfia does. Havingsaid that, Mr. Speaker, we're both focused on the priority. Job number one is food safety for our consumers. Cfia continued to act. Starting on September the 4th and right up to today, Mr. Speaker.

The speaker: The honourable member for Toronto centre.

Bob Rae (Voice of translator): Mr. Speaker, they're the same facts. It's the same science in the United States. There isn't an American science and a Canadian science when dealing with the protection and safety of consumers. This is incomprehensible that a Minister of agriculture would close the bored sore that products not go to the Americans but that he'd leave those same products being sold to Canadians for two weeks. It makes no sense at all, Mr. Speaker. This is total negligence on the part of the Minister. How can he explain this problem, Mr. Speaker?

The speaker: The honourable Minister of agriculture.

Gerry Ritz: Well, actually, Mr. Speaker, cfia has explained those inadequacy, he tries to call. They they're certainly not that. Mr. Speaker, there are differences in our systems. What we have is secondary testing at Cfia level here in Canada. The Americans don't do that particular step. At the same time, Mr. Speaker, recall noticing were put out for the most at-risk products, the ground beef and trim on September the 16th. Americans did it the exact same date as we continued to build our recall system later in September, Mr. Speaker, the Americans did it on exactly the same day.

The speaker: The honourable member for dartmouth-cole harbour.

Robert Chisholm (NDP): Thank you, Mr. Speaker. In 2011, xl received \$1.6 Million in growing forward grants to install "state-of-the-art technology that will double its per-day capacity for ground beef." The downside of this high-speed processing is that there is no room for error. In other words, the Conservatives helped build this ultramodern facility. My question to the Minister, Mr. Speaker, is will he admit that he failed to provide the needed food safety resources to operate such an intense high-volume facility?

The speaker: The honourable Minister of agriculture.

Gerry Ritz: Well, Mr. Speaker, what we've done as a government is make sure that cfia has the inspection capabilities, the capacity to manage a plant such as this. We have 46 inspectors on-site on a daily basis. That's a 20% increase over the last few years, Mr. Speaker.

The speaker: The honourable member for dartmouth-cole harbour.

Robert Chisholm (NDP): So, imagine, Mr. Speaker, the brooks plant can now process 4,000 to 5,000 cows per day. Yet, since 2006, not a single new inspector position has been hired at the brooks plant except to fill vacancies. The Minister says otherwise. So, will he now provide this house with the names, locations and job descriptions of all cfia inspectors across this country and let's end the confusion once and for all?

The speaker: The honourable Minister of agriculture.

Gerry Ritz: Well, Mr. Speaker, there are things like privacy laws in Canada. What I can tell you is that the officials at cfia continue to work diligently on up food safety in this country, and they will continue doing that job.

The speaker: (Voice of translator): The honourable member for argenteuil-papineau-mirabel.

Mylène Freeman (NDP) (Voice of translator): It's no longer just xl foods that is targeted by the American authorities. There are now concerns on the other side of the border regarding our food inspection standards, which are simply not stringent enough for the American market. The Conservative incompetence in matters of food safety is potentially going to be very costly for our producers. Will the Conservatives begin to understand the scope the consequences of their cutbacks in food safety?

The speaker: The honourable Minister of agriculture.

Gerry Ritz: Of course, Mr. Speaker, there have been absolutely no cutbacks to food safety capacity in this great country. Quite the opposite, as a matter of fact. Over the last number of budgets and papers that we've produced, you can see a growing amount of dollars, some 20% increase in the budgetary capacity of cfia. Plus 20% increase in the inspections in this particular plant alone, Mr. Speaker.

The speaker: (Voice of translator): The honourable member for alfred-pellan.

Rosane Doré Lefebvre (NDP) (Voice of translator): Mr. Speaker, this 2011, xl pocketed no less than \$1.6 Million from the government in order to increase its production. The business doubled its ground beef production, but this number of inspectors remained the same. Canadian families deserve that xl meat be properly inspected. They also deserve that there be enough front-line inspectors so they can eat their duty here without any risk. Mr. Speaker, why are the Conservatives a ban dodge consumers had.

The speaker: The honourable Minister of agriculture.

Gerry Ritz: We continue to do just the opposite, Mr. Speaker. We bring in legislation that gives public health and cfia more powers. We're doing that now with bill s 1 is and I hope that the member opposite will rise in her seat and support that bill at every stage as it moves through.

The speaker: (Voice of translator): The honourable member for alfred-pellan.

Rosane Doré Lefebvre (NDP) (Voice of translator): Every day, the Minister tells that you say with bill s-11, which delays the review of cfia activities until 2017, things will be fine. The current crisis needs an imperative review now of the cfia. The NDP is asking for this. Consumers are and Canadian families are as well. But the Minister continues to put this bill on the backburner. To respond to Canadian families' concerns, can the Minister promise to hold a review of the cfia you now and not in five years' time?

The speaker: The honourable Minister of agriculture.

Gerry Ritz: Well, I can assure the member opposite that we've actually gone beyond that, Mr. Speaker. Countries around the world come to review what cfia is doing plant by plant. We have to do that in order to maintain our requirements to export to certain countries around the world and we continue to be buoyed by their results. And we'll continue to work with cfia to build a robust food safety system, Mr. Speaker. I'm hopeful that the NDP will support start to support budgetary actions that do that.

The speaker: (Voice of translator): The honourable member for rimouski-neigette - temiscouata - les basques.

Guy Caron (NDP) (Voice of translator): Compense expenses for the risk management system tied to safety and bio safety for food was \$160 million in 2011, but this will be cut by almost 32 million and there will only be 85 million in 2012-'13. The food safety program is cut by 5%. This information is found in the government's financial documents that the Conservatives themselves tabled in the House of Commons. Why are they stubbornly saying the contrary? We wonder if we could really could you want on their own financial documents. "Yes" or no?

The speaker: The honourable Minister of agriculture.

Gerry Ritz: I know the member is new here, but he should know that the budgetary process of the government stops on March 31st. Every year and then renews itself again on April the 1st. There are supplementary expenses. Therefore other things that are done during the year to add to the capacity of situations like cfia. We continue to do that, Mr. Speaker. They continue to vote against those.

The speaker: (Voice of translator): The honourable member for rimouski-neigette - temiscouata - les basques.

Guy Caron (NDP) (Voice of translator): Mr. Speaker, what the NDP did was to vote against their cuts, and we're proud of that. What I'm trying to understand and what they're telling us is that the documents they tabled in the house seem to be incorrect. (End of translation) show that food safety is down by 5% performance food safety and biosecurity risk management systems are being cut by 27%. And that's a fact, Mr. Speaker. How can they expect families to believe that their cuts will have no effect?

The speaker: The honourable Minister of agriculture.

Gerry Ritz: Well, Mr. Speaker, the member opposite is quoting from an incomplete report. What that report

states does not show the ongoing ability of the government to continue sun setting programs. He should probably be aware of that and help us move that through in the next budgetary cycle, Mr. Speaker.

The speaker: (Voice of translator): The honourable member for beauharnois-salaberry. -- The honourable member for beauport-limoilou.

Raymond Côté (NDP) (Voice of translator): The offenders who are trying to redeem themselves through their religion are being told, sorry, we only accept christians. Rabbi, I ma'ams are being let go. We could even see elders from aboriginal communities shown the door, and yet this is not an expensive program. Will the Minister reconsider his decision to eliminate religious revs service force jewish. Muslim and sikh offenders?

The speaker: The parliamentary secretary for the Minister of public safety and national security.

Candice Bergen (CPC): Thank you very much, Mr. Speaker. I want to begin by rejecting the premise of that question. Our government strongly supports the freed om of religion for all Canadians and convicted criminals continue to have reasonable access to any religious counsel counseling or services of their chris on a voluntary basis. The government does fund full-time chaplains in addition to serving members of their own faith, these chaplains also make themselves available on a by-request base toys provide spiritual advice to the general population. Mr. Speaker, the Canadian forces have used this type of chaplaincy program for years f it's good enough, Mr. Speaker, for our armed force's it's good enough for inmates in our federal penitentiaries.

The speaker: The honourable member for Ottawa centre.

Paul Dewar (NDP): Picking and choosing on the subject just don't -- won't wash, Mr. Speaker. This is not a costly program. The Minister has no justification for cutting it. You know, actually, she should listen to her colleague who said the following: Religious freedom is a fundamental freedom. One we are very, very pourive and feels very strongly about." Who do you know who said is that? T her klegg, yes, the Minister of foreign affairs, so the question for the Conservatives is how can they be so hypocritical in being strong apparently on religious firemen abroad when they won't support it at home?

The speaker: The honourable member -- the honourable parliamentary secretary to the Minister of public safety and national security.

Candice Bergen (CPC): Mr. Speaker, the member is completely inaccurate. It's very sad to hear him display and say these kinds of mistruths. The government funds full-time chap lips that are determined based on the number of inmates requesting services from each faith determined by region. And as I said, in addition to serving members of their own faith, these chaplains also make themselves available on a by-request basis to provide spiritual advice to the general population. Mr. Speaker, this is a common practice. The Canadian forces has used. This similar capelin say scam it's been successful forever many years, Mr. Speaker.

The speaker: The honourable member for york west.

Judy Sgro (LPC): Mr. Speaker, in a rare appearance yesterday, the Minister for agriculture begged Canadians to look at the tainted meat time line. Well, many Canadians did exactly that. And they're quite shocked by what they saw. What they saw, that it was the United States that discovered e-coli, not Canada. They also saw this government's clear foot-dragging and the Minister's continually-changing stories. When is this government -- when are the Conservatives going to start paying attention to the health and safety of Canadians, or are you waiting for another walkerton tragedy?

The speaker: I'll remind all members to address their comments to the chair. The honourable Minister of

agriculture.

Gerry Ritz: Thank you, Mr. Speaker. Of course, this government -- food safety is a priority. We continue to build a robust system and the capacity to move forward. As I've often said in this house and the time line on the website is nothing like the member opposite talks about the CFIA in the same timeframe as the Americans discovered a contaminated product on September the 4 and this they've continued working through every since. Mr. Speaker, the time line is there for all Canadians to see, and I'm certainly happy to answer real questions on it.

The speaker: (Voice of translator): The honourable member for Bourassa.

Denis Coderre (LPC) (Voice of translator): Mr. Speaker, this Minister has been reckless and incompetent and there's a certain innocence he keeps referring to. It was as if we'd prefer to protect the Americans by stopping that export rather than protecting Canadians. So, this is a public health issue. So, my question is for the Minister of health. Rather than playing with her iPad, she might answer questions and do her job. Why is public health not saying a single word about all of this? Get up for once.

The speaker : The honourable -- the honourable Minister of agriculture.

Gerry Ritz: Well, what a diatribe, Mr. Speaker. We immediately to raise the quality of debate in this house not lower it. Certainly the Minister of health is doing an admirable job. We work in partnership with our provincial colleagues in public health as much as the federal department of public health, Mr. Speaker. Everyone is anxious to get to the bottom of this and move on.

The speaker: The honourable member for Malpeque.

Wayne Easter (LPC): Mr. Speaker, it is day 31 since the Americans notified Canada on e-coli, and the Prime Minister still fails to hold his Ministers to account for the biggest recall ever. This is the list of products, Mr. Speaker, for Canada alone. Some 240 pages long. Remember the Minister claimed no product reached store shelves? The incompetence of the two Ministers of health and agriculture knows no downtown east side. Truck drivers knew there was a problem. Meat cutters knew there was a problem. But the Minister failed to act, and the health Minister was lost in silence. When will the Prime Minister take charge of this issue?

The speaker: The honourable Minister of agriculture.

Gerry Ritz: Of course, Mr. Speaker, we'll never apologize for the size of the recall. This is based on science. This is based on protocols that are developed well in advance of these types of situations. We take this very seriously, Mr. Speaker. That's why we continue to build a robust food safety system. Got Bill S-11 coming to us from the Senate. I'm hoping that the Liberals will support it when it gets here, Mr. Speaker.

The speaker: (Voice of translator): The honourable member for Laurier - Sainte-Marie.

Hélène Laverdière (NDP) (Voice of translator): Mr. Speaker, thanks to the clownish behaviour of the parliamentary secretary to the Minister of transport, the Robert Abdara affair is sparking more and more interest, and the Conservatives will eventually have to answer questions. So I'm going to keep it simple: Why were the PMO, Dimitri Soundgas -- Das and Leo Husak as so determined to get Abdara disappointed. What were they expecting in return?

The speaker: (Voice of translator): The honourable parliamentary secretary to the Minister of transport.

Pierre Poilievre (CPC) (Voice of translator): Mr. Speaker, I think that the honourable member is referring to an appointment that was not made and that we have no power to make. But the question that is before the house now is why did the NDP accept \$340,000 in union money that was illegal, and why, Mr. Speaker, do the NDP refuse to support a bill before the House of Commons to make union funding transparent? What do they have to hide?

The speaker: (Voice of translator): The honourable member for Laurier - Sainte-Marie.

Hélène Laverdière (NDP) (Voice of translator): Thank you, Mr. Speaker. Well, at least the RCMP doesn't have to raid our offices. Mr. Speaker, we're not talking about the Jewish partisan -- about the usual partisan attempts by the Conservative that we saw in the port of Toronto or the port of Quebec -- we're talking about someone who is facing serious allegations as part of the commission that is currently investigating corruption. So why was the candidacy of Mr. Abdula supported by the Prime Minister's press secretary, by Senator Human being as as and by Frank Zambito.

The speaker: The honourable parliamentary secretary.

Pierre Poilievre (CPC): Well, Mr. Speaker, she didn't answer the question. Why is it that her party would pose questions in the House of Commons about an appointment that was never made and we don't want to have the power to make when, in fact, her party was caught red-handed accepting \$340,000 in illegal union money? That was money that was taken out of the pockets of hard-working blue collar Canadians who gave no scent for that money to be funneled into the coffers of the NDP. They didn't care. They had no shame. The NDP was happy to just scoop up that illegal money and...

The speaker: (Voice of translator): The honourable member for Louis-Hébert.

Alexandrine Latendresse (NDP) (Voice of translator): Americas we learned that money morning that the Chinese party organized a party where the drink was so extreme that some for senior officials went home dead drunk. This raises concerns about fact that state secrets could have been leaked during this drunk fest. We've already seen a former Minister leave top-secret documents at his girlfriend's house. Why don't Conservatives take espionage risks seriously?

The speaker: The honourable parliamentary secretary tore public safety.

Candice Bergen (CPC): Mr. Speaker, Canadians expect law enforcement officers to act with integrity at all times. CBS is lacking looking into the facts of this situation. Anyone found to have been behaved inappropriately or acting inappropriately will face sanctions and discipline, Mr. Speaker.

The speaker: (Voice of translator): The honourable member for you Louis-Saint-Laurent.

Alexandrine Latendresse (NDP) (Voice of translator): The Conservatives' everyone difference is appalling and it contrasts sharply with the seriousness of the situation and the potential for risk. When our customs officers are paid -- are applied with liquor to the point that they are throwing newspaper their government vehicles, the Conservatives should wonder. When CSIS is concerned about foreign state-owned enterprises having a stake in our natural resource, the Conservatives should ask themselves questions. When will they start taking threats to national security seriously?

The speaker: The honourable parliamentary secretary tore the public safety.

Candice Bergen (CPC): Well, Mr. Speaker, I will repeat, and I think that we are absolutely not indifferent. We as all Canadians do expect our law enforcement officers to act with integrity at all times. Cbsa, and I'll repeat this, it looking into the facts of this situation. I would think the honourable member would appreciate that and would approve with that. There's due process for this kind of scenario, and nip found to have been -- acted inappropriately will face sanctions, will face discipline. Thank you, Mr. Speaker.

The speaker: The honourable member for sault ste. Marie.

David Wilks (CPC): Mr. Speaker, anyone MPs Day after day recite their tried old socialist talking points. Low tax, bad trade, bad business. Bad economic growth bad. In the NDP world, the solution to everything is their high-tax, big-government schemes like their job-killing carbon tax. Would the Minister of foreign affairs please share with the NDP parliament and all Canadians the result of our low-tax pro trade and pro-growth plan?

The speaker: The honourable Minister of foreign affairs.

John Baird: The NDP keep talking down the Canadian economy. They keep complaining that Canadians are not paying enough taxes. That's why they want to impose a \$21.5 Billion carbon tax on Canadians. The NDP can continue to do this, Mr. Speaker, but Canadians know that our job creation plan is working. Today, we saw the announcement of the creation of more than 50,000 net new jobs. -- 800,000 Jobs created, 9 Pots of them full-time, 80% Of them in the private sector. That's good news for Canadians.

The speaker: (Voice of translator): The honourable member for charlesbourg - haute-saint-charles.

Anne-Marie Day (NDP) (Voice of translator): Thank you, Mr. Speaker. It is very cute to hear you talking about a carbon tax. It is not own workers who are paying the price of ei reforms of it is the workers as well. Workers are leaving because working part-time simply isn't worth it. Pose are paying premiums, just like workers dorks so if should they be punished if they need part-time workers? The Conservatives' approach is not working. When will they help employers and working by correcting the problems in the working while on claim program?

The speaker: The honourable Minister for human resources and skills development.

Diane Finley (Voice of translator): Thank you, Mr. Speaker. Mr. Speaker, unlike the NDP, we are encouraged that there are many more people who are working now than before. That is good news for Canada. For example, now, over 820,000 jobs have been created since the recession. That is good news, Mr. Speaker. And she should support and help our workers. That's what they need.

The speaker: The honourable member for St. John's south-mount pearl.

Ryan Cleary (NDP): Mr. Speaker, I'd like to relate a tim hortons moment gone bad involving a man who helped keep minor hockey alive in my riding. Robert is 63 and he's work at a hockey rink for over 35 years. He's collected Canada pension since he turned 60 and collects ei for the months the ice is off the rink. Come January, robert's Canada pension will be clawed back 50 cents on the dollar from his ei cheque. Mr. Speaker, the question is this: Why is this government so set on punishing seniors?

The speaker: The honourable Minister of human resources.

Diane Finley: Well, Mr. Speaker, the fact is that we've done more to support seniors and make them financially better-off than any other government of Canada. Mr. Speaker, let's take a look at things that we

brought in that the NDP opposed: Pension income-splitting for seniors. The NDP opposed that. Increasing the -- increasing the age tax credit for seniors. Not once but twice. They opposed it. Mr. Speaker we also brought in the largest increase in the guaranteed income supplement. The largest increase in 25 years to help the poorest seniors. As usual, the NDP opposed that, too.

The speaker: The honourable member for churchill.

Niki Ashton (NDP) (Voice of translator): Mr. Speaker, like any other Canadian children, aboriginal children deserve a quality education. We can not deny this to yet another generation, and yet, this government is making unilateral decisions on education instead of working in collaboration and with respect for First Nations. In Manitoba, for example, provincial funding per student in some communities is almost double that of what is offered to aboriginal children. By -- by this federal government. When will the Minister pledge to invest in and support education on reserves for First Nations people?

The speaker: The honourable Minister of aboriginal affairs and northern development.

John Duncan (CPC): Mr. Speaker, we are taking concrete steps. We're working together with First Nations and, Mr. Speaker, we are starting to see improved student outcomes. We have comprehensive first nation education agreements in Nova Scotia and British Columbia, demonstrating improved student outcomes. Mr. Speaker, the NDP should stop spreading misinformation and start standing with us as we support First Nations students to resp their goals.

The speaker: The honourable member for churchill.

Niki Ashton (NDP): Mr. Speaker, the facts are clear. On First Nations across Canada, there are schools that don't have enough paper. They don't have enough materials. The classes are overcrowded. The rooms are full of mould. When will this Minister realize that to fix the crisis, he and his government have to sit down with aboriginal leaders and work with them, with respect. When will this Minister and this government negotiate -- negotiate in a meaningful way with First Nations? Because at the end of the day, the question is how many more generations of aboriginal children have to be deprived of a proper education in Canada?

The speaker: The honourable Minister of aboriginal affairs.

John Duncan (CPC): Mr. Speaker, we are proud of the investments that we've made in First Nations education. We are leading an initiative that's long overdue, and we expect outcomes. This is what First Nations students, their parents and their educators want. It's what we want to work with. And we will not be distracted by misinformation and polarization coming from the opposition. Mr. Speaker, we are investing in individual students. We're also committed to introducing a first nation education act which will improve governance and accountability for First Nations. Thank you.

The speaker: The honourable member for mount royal.

Irwin Cotler (LPC): Mr. Speaker, the government is cancelling the contracts of non-christian chaplains in federal prisons, thereby requiring inmates other faiths to turn to christian chaplains for religious guidance. Minister says "he is no the business of picking and choosing which religions will be given preferential status" by but he's doing precisely that. Will the Minister recognize his contradiction, reinstate funding for chaplains of all faiths and uphold the values of freedom of conscience and religion and equality before the law as enshrined in the charter of rights and freedoms? Thank you, mr. Speaker.

The speaker: The honourable parliamentary secretary to the Minister of public safety.

Candice Bergen (CPC): Thank you, Mr. Speaker. Mr. Speaker, the government of Canada strongly supports the freedom of religion for all Canadians. Last month, the Minister of public safety asked for an immediate review of the chaplaincy program to ensure that taxpayers' dollars are being used wisely and appropriately. Upon reviewing the program, it was determined that changes were necessary so that this program supports the freedom of religion of inmates while respecting taxpayers' dollars. Convicted criminals, Mr. Speaker, will continue to have access to religious services of their choice on a voluntary basis. Thanks, Mr. Speaker.

The speaker: The honourable member for winnipeg north.

Kevin Lamoureux (LPC) : Mr. Speaker. Canadians thought bey oda wasted money on limos. The Minister of citizenship and immigration makes bey oda look like a frugal campaigner against government waste. Minister for citizenship and immigration racked up 32,000 in limo fees while yet refugees can't get life-saving medications and basic health care. Who is abusing the Canadian taxpayer dollar now? How can the Minister justify the cuts to refugee health care when he himself is spending thousands on luxury transportation?

The speaker: The honourable parliamentary secretary for the Treasury board

Andrew Saxton (CPC): Thank you, Mr. Speaker. Our government treats taxpayers' money with the utmost respect, and we require that government business be done at a reasonable cost to taxpayers. Ministers' office budgets are, in fact, down over 16% compared to the last year the Liberals were in power, and the PMO budget is down a further 13.7% since 2010. We've reduced hospitality spending by over a third. Travel costs are down by over 15% compared to the former Liberal government. Mr. Speaker, we're taking action to reduce the cost of government.

The speaker: (Voice of translator): The honourable member for chateauguay - saint-constant.

Sylvain Chicoine (NDP) (Voice of translator): Mr. Speaker, the long list any of the Conservatives' errors regarding privacy protection of veterans was confirmed yesterday by the privacy commissioner. We learned in the report that veterans' affairs Canada uses subcontractors to dispose of the files of veterans. The report reveals a lack of oversight with regard to the safe destruction of files containing personal information about our veterans. When will the Conservative government take privacy protection matters seriously?

The speaker: The honourable parliamentary secretary to the Minister of veterans' affairs.

Eve Adams (CPC): Whether he can the recommendations brought forward by the independent privacy commissioner. (Voice of translator): We are taking measures to ensure that our processes meet the highest possible standards. (End of translation) -- all 13 of her recommendations. Mr. Speaker, our Conservative government treats the privacy of our nation's heroes as paramount and we will always act to ensure that their privacy is respected.

The speaker: (Voice of translator): The honourable member for saint-bruno - saint-hubert.

Djaouida Sellah (NDP) (Voice of translator): Mr. Speaker, the Conservatives are once again on the defensive with regard to their treatment of veterans. They are the ones who ignored the advice of the surgeon general by making reckless cuts to the services offered to soldiers suffering from post traumatic stress disorder. And yet the ombudsman was clear, 0.2% of the department's total budget is devoted today mental health issues. Why didn't the Conservatives listen to the NDP and spare veterans their ill-advised cuts?

The speaker: The honourable Minister of national defence.

Peter MacKay: Mr. Speaker, the reality is that over our time and budget, we have -- our time in office, we have seen the budget for health, including the mental health needs of the Canadian force, go up significantly. Some hundred million dollars of additional money has now been made available for the Canadian forces health concerns. We will continue to make investments for those ill and injured. Those in need in particular of mental health counselor, Mr. Speaker. We've just recently announced an \$11.4 Million increase to that overall budget. Specifically to hire more mental health professionals, to allow that support to flow to them and to their families and to our veterans.

The speaker: Hopefully we'll get it right this time. The honourable member for sault ste. Marie.

Bryan Hayes (CPC): Mr. Speaker, yesterday the NDP member for beaches-east york used a member's statement to attack Conservative members for speaking the truth about the NDP's economic policies. It's understandable why that member and the NDP want to stop us from talking about their policy. The NDP's plan for the economy is to impose a new \$21 billion job-killing carbon tax that would raise the price of everything. Can the parliamentary secretary to the Minister of natural resources tell this house what our Conservative government is doing to help grow the economy and create jobs?

The speaker: The parliamentary secretary.

David Anderson (CPC): Mr. Speaker, I want to thank the member from sault ste. Marie for his question, because he knows and Canadians are discovering the 2011 NDP campaign promise when they made a commitment to a carbon tax imposed through a cap and trade process that would force Canadians to turn over \$21 billion of their money. Mr. Speaker, our policies have helped create 800,000 jobs across this country. Just last month alone, there were another 50,000 new jobs. The NDP would cancel those 50,000 jobs and hundreds of thousands of others if they get their way. Mr. Speaker, that's why they can not be allowed to implement their dangerous policies.

The speaker: The honourable member for cape breton-canso.

Rodger Cuzner (LPC): Mr. Speaker, the acclaimed American actor samuel L Jackson has posted a powerful youtube video encouraging people to wake up and realize that some of their fellow citizens are experiencing hardship and pain. I encourage all members to go check out the video. Low-income earners who are receiving I benefits are experiencing such pain but some things the Minister is sleepwalking passed their hardship. So my plea is really to the Prime Minister: Will he take charge of this file and wake the front bench up?

The speaker: The honourable Minister of natural -- of human resources.

Diane Finley: Well, Mr. Speaker, our -- with the working while on claim pilot projects gst's aim is to encourage claimants to accept all available work while they're on claim. But in doing, that we want to make sure that the work does pay so that they're better-off working than not. Mr. Speaker, we always continue to work to ensure that our goals are met.

The speaker: (Voice of translator): The honourable member for shefford.

RéJean Genest (NDP) (Voice of translator): Mr. Speaker, after having tried to reopen the debate on abortion, a Conservative member is at it again. He will be in my riding this weekend to participate in an event organized by the Quebec pro-life campaign with an organization which promotes therapy for those who are

trying to cope with unwanted attraction to people of the same sex. In addition to being against women's right to choose, does the member believe that homosexuality is a disease that must be cured?

The speaker: The honourable parliamentary secretary to the Minister of justice.

Kerry-Lynne D. Findlay (CPC): Thank you, Mr. Speaker. I believe the member opposite is referring to some recent comments on the private member's bill c-27969 out of government is proved the fact that Canada's recognize recognized international lays a country that is deeply commit today the principles of with respect to for diversity and equality. The private member's bill that is currently before the justice committee we should allow that committee to do its work, Mr. Speaker. And we look forward to the report from that committee. Thank you.

The speaker: The honourable member for northumberland-quinte west.

Rick Norlock (CPC) (Voice of translator): Mr. Speaker, we're all used to the NDP's irresponsibility and its insistence on imposing a radical antitrade, antidevelopment agenda on all of Canada. Whereas the opposition is hell bent on playing petty politics, our government remains focused and is working hard to create jobs for Canadians. Can the Minister inform the house about the progress made in jobs?

The speaker: (Voice of translator): The honourable Minister of industry.

Christian Paradis (Voice of translator): Mr. Speaker, I'd like to thank my colleague for his question, that is very relevant, because, indeed, Mr. Speaker, we know that the NDP is pushing its radical agenda of a carbon tax of \$21 billion that would kill the economy and kill jobs. Whereas on our side, we have a very responsible government, and I'd like to point out that statistics Canada has over 52,000 net new jobs were created in September, so that's 820,000 jobs since the recession. We're doing the best of all g7 countries. So we're supporting the economy, Mr. Speaker. We're supporting families and we don't want a carbon tax.

The speaker: (Voice of translator): The honourable member for pontiac.

Mathieu Ravnat (NDP) (Voice of translator): Mr. Speaker, yesterday, the environment Minister announced a new phase of the site decontamination project in this country. In 2011, Quebec had a hundred high-priority sites that presented risks for public health and the environment. And yet only 67 of those sites were chosen in Quebec for cleanup. Mr. Speaker, they're turning their back on the val cartier military base, the canal and pcb contaminated sites in the kahnawake reserve. Will the federal government present a more exhaustive cleanup plan or will it pass the buck to Quebec?

The speaker: The honourable parliamentary secretary to the Minister of the environment.

Michelle Rempel (CPC): Well, Mr. Speaker, as we've said earlier in the house this, we're on this particular issue and the announcement that we've made this week to ensure the continuation of t he federal contaminated sites action planning our government is, in fact, making excellent project in this regard. We've invested over \$1 billion over three years to 2014 to manage this program. We've earmarked additional funding this week. For sites across the country. We also have a review process which, threw a scientific process, make sure that we're cleaning up those that are most affected first. We're halfway through that plan, and we're making good progress.

The speaker: (Voice of translator): The honourable member for richmond-arthabaska.

André Bellavance (BQ) (Voice of translator): Mr. Speaker, the Minister of the environment has nothing to be

proud about , about his announcement yesterday concerning the 2300 contaminated sites in Quebec. That and that is less money to Quebec than elsewhere for decontamination. How can the Minister announce such a weak plan for Quebec? This has been going on for too long. There are too many contaminated excites it's taking too long to solve this problem.

The speaker: The honourable parliamentary secretary to the Minister of the environment.

Michelle Rempel (CPC): Well, Mr. Speaker, as I just stated, our government is, in fact, making excellent progress in cleaning up contaminated sites across the country. The announcement that we made this week shows our government's commitment to this plan by earmarking additional funds for sites across the country. Mr. Speaker, we have a very strong plan, a very strong review process to assess these sites and then to clean them up afterwards, Mr. Speaker. We're making good progress.

The speaker: The honourable member thunder bay

Bruce Hyer (IND): severe motor adjournment Mr. Speaker, this government wants to bulldoze a reckless lookout through b.C. To ship raw bitumen to eastern China as fast as possible. Easterners pay a lot for gasoline and home heating oil. We must build a new pipeline to bring western petroleum to eastern Canada. Will the resources Minister support a new pipeline to the east that ensures our energy security and shares energy and value-added jobs with eastern Canadians?

The speaker: The honourable parliamentary secretary to the Minister of natural resources.

David Anderson (CPC): Across this country, we have a strong review process. We have a strong national energy board that looks at those applications, and I'm sure if the application is made, they will be taking a look at that application. But the pipelines are being reviewed. He mentioned the northern gateway pipeline and that's being reviewed by an independent panel and we're paying trying to make sure that that is a political process but one that's bad on science, as with any other decision.

The speaker: That brings to answered the oral questions. (End of oral questions)

(End of Question Period)

The Privy Council Office's Media Centre /
Le Centre des médias du Bureau du Conseil privé

Disclaimer

The unofficial Question Period transcript is based on closed captioning (rough)

**Transcript provided courtesy of the Privy Council Office. Please note that this transcript is produced via the closed captioning provided by CPAC and is available in English only. For an official transcript please consult the Hansard located on the Parliamentary Internet site.*

Media Centre / Centre des médias
Requests / Demandes : 613.952.6922 or
mediacentre@bnet.pco-bcp.gc.ca

Centre des médias / Media Centre
Demandes / Requests : 613.952.6922 ou
mediacentre@bnet.pco-bcp.gc.ca

Richer, Jean-Marc

From: Leclair, Natalie
Sent: Friday, September 28, 2012 12:48 PM
To: * EXCOM/COMEX; * GOC-OPS Support; * Parliamentary Affairs Division / Division des affaires parlementaires; Fisher, Adam; Thibouthot, AkimIsabelle; Allison, Catherine; Amy JOHNSON; Archambault-Chapleau, Nadine; Beaudoin, Serge C; Bedor, Tia Leigh; 'Blackie, Ian'; Boucher, Patrick; Bourdeau, Anne; Brock, Darlene; Burton, Meredith; 'Caroline Douglas'; 'Charles-Eric.Lepine@rcmp-grc.gc.ca'; 'Christine Larose'; Desnoyers, Christine; Williams, Christopher; Clavel, Julien; Cogan, Tim; COMDO; Cyr, Lynne; Dagenais, Louise; de Jager, Gabriela; Dupuis, Chantal; [REDACTED] Fournier, Muriel; s.15(1) - Subv Issues / Enjeux; Johnson, Mark; 'karyn.curtis@rcmp-grc.gc.ca'; Koops, Randall; Lambert, Louise; Larose, Nathalie; Leclair, Natalie; Leclerc, Carole; LeSage, Lynn; Roylt; [REDACTED] [REDACTED] McAteer, Julie; McLaren, Victoria; Mueller, Mike; 'Nabil Temimin'; 'nicole.greenough@cbsa-asfc.gc.ca'; Paulson, Erika; Perry, Gates; 'prieurma@npb-cnlc.gc.ca'; Executive Services; 'Robin.Stong@cbsa-asfc.gc.ca'; 'Ruth.Marier@cbsa-asfc.gc.ca'; 'Sarah Estabrooks'; Scheewe, Nathan; Sellers, Philip; 'Shannon Muldoon'; Suzanne Schmidt; Veilleux, Martine
Subject: QP Transcript for September 28, 2012 / Transcription de la Période des questions pour le 28 septembre 2012
Attachments: QP transcript.pdf

Good afternoon,

Focus of Question Period today: Employment Insurance, food safety.

Question answered by the Parliamentary Secretary:

Kennedy Stewart (Burnaby—Douglas) asked a question regarding cyber security. (Transcript in pink)

The speaker: The honourable member for burnaby-douglas.

Kennedy Stewart (NDP): Mr. Speaker, it'd be nice if they stopped making things up about the opposition and tried answering some questions, so let's see if we can get an answer here. Mr. Speaker, Reuters reports a new computer security breach by a Chinese group. Calgary-based Tellus was the target if it wasn't for the company warning their customers, the public would have never even known, so can the government confirm foreign government involvement in this attack and in light of this, can Conservatives tell us if national security is

part of the criteria for the Nexen takeover review?

The speaker: The honourable parliamentary secretary to the Minister of public safety.

Candice Bergen (CPC): Mr. Speaker, our government takes cyber-security seriously and operates on the advice of security experts. Our government recently made significant investments of \$90 million in a cybersecurity

strategy designed to defend against electronic threats, hacking and sign cyber-espionage.

Telecommunications carriers operating in Canada are certainly subject to Canadian law. We'll continue to work to protect the interests of Canadians and protect them from cyber-security threats. Thank you, Mr.

Note:

Mathieu Ravnat (Pontiac) asked a question regarding organized crime. The Parliamentary Secretary (Justice) responded. (Transcript in blue)

Scott Brison (Kings—Hants) asked a question regarding foreign investment. The Minister of Industry responded. (Transcript in orange)

The English unofficial transcript is attached.

The official transcript will be available in both official languages tomorrow morning on the Parliamentary website www.parl.gc.ca.

Thank you.

Bon après-midi,

Focus de la Période des questions aujourd'hui : L'assurance-emploi, la salubrité des aliments.

La secrétaire parlementaire a répondu à une question :

Kennedy Stewart (Burnaby—Douglas) a posé une question concernant la Cybersécurité. (Transcription en rose)

Notez :

Mathieu Ravignat (Pontiac) a posé une question concernant le crime organisé. Le secrétaire parlementaire (Justice) a répondu. (Transcription en bleu)

Scott Brison (Kings—Hants) a posé une question concernant l'investissement étranger. Le ministre de l'Industrie a répondu. (Transcription en orange)

Veillez prendre note que la transcription n'est disponible qu'en anglais seulement.

La transcription sera offerte dans les deux langues officielles demain matin sur le site www.parl.gc.ca.

Merci de votre compréhension.

Natalie Leclair

Advisor / Conseillère

Parliamentary Affairs / Affaires parlementaires

Public Safety Canada / Sécurité publique Canada

Tel/Tél: (613) 990-2718

Fax: (613) 954-8774

Email/Courriel: natalie.leclair@ps-sp.gc.ca

QP Closed Captioning Transcript

Question Period

Today

Updated Mon. - Thurs. at 4:30 p.m. and Fri. at 12:45 p.m.

*For an official transcript, please consult the Hansard located on the Parliamentary website.
Pour obtenir une transcription officielle, veuillez consulter le hansard sur le site web
parlementaire.*

2012-09-28

*Transcript provided courtesy of the Privy Council Office. Please note that this transcript is produced via the closed captioning provided by CPAC and is available in English only. Disclaimer

The speaker: Oral questions. The honourable member for Vancouver east.

Libby Davies (NDP): Mr. Speaker. Canadians are rightly concerned about the future of their health care system. Conservatives unilaterally cut \$36 billion in health transfers without any consultation whatsoever. And in yesterday's report, the pbo stated federal government has transferred the problem of future health costs to the provinces. This defunding will only hurt health services across Canada. Why is this government lagging in its funding of health care and why are very damaging the fiscal capacity of the provinces?

The speaker: The honourable Minister of industry.

Christian Paradis: Mr. Speaker, this statement is completely false. There's no cut there. They are still dealing with increasing of health care transfer. We are responsib government. We want to make sure it the transfer will be able to -- that we will be able to do it on a sustainable way, but what we -- what we understand from the NDP given the action that is they are taking, they don't have any idea about the health care plan. They have no idea about what they're doing on this.

The speaker: The honourable member for Vancouver east.

Libby Davies (NDP): We've had a major national campaign yesterday on health characters so we definitely do have a vision and want to talk to Canadians. A ship of beef trimmed from xl foods tested positive for e-coli. September 13th, xl's US Permit was pulled. Late yesterday, September 26th, the xl plant there brooks, Alberta had its license suspend. This is almost a full month's delay if the discovery of the contamination to closure of thesource. Why did it take so long for officials to act, and why isn't the government putting the health and safety of Canadians first?

The speaker: The honourable Minister of agriculture.

Gerry Ritz: Mr. Speaker, that's exactly what we do. Canadian consumers are always our first priority when it comes to food safety. Our government will continue to ensure food safety officials have the resources they need and respond efficiently based on sound science to ensure that safe food. We've hired an additional 700 new inspectors since 2006, including 170 dedicated to meat lines, and of course, the NDP constantly votes against those initiatives.

The speaker: The honourable member for Vancouver east.

Libby Davies (NDP): Mr. Speaker, it's a failed policy. Yesterday's press release from CFIA states "to date the company has not adequately implemented agreed-upon corrective actions and has not presented acceptable plans to address longer-term issues." It's a clear indication that the Conservative policy of a self-policing industry has failed. It's put a lot of work out of work. It has failed public safety. And it's hurt the industry overall. Pulling front-line CFIA inspectors was wrong. Mr. Speaker, when will they reverse this policy?

The speaker: The honourable Minister of Agriculture.

Gerry Ritz: Of course, Mr. Speaker, we've added inspectors to the line and given CFIA the capacity from a monetary perspective to do their job in a more professional way. Canadians can count on the fact that the government is focused on food safety so that, in the end, this industry had the help of 46 inspection staff on a daily basis in that plant, Mr. Speaker. We'll continue to work on scientific protocols that are internationally recognized to make sure that our food is safe for Canadian consumers.

The speaker: (Voice of translator): The honourable member for Hull-Annville.

Nycole Turmel (NDP): (Voice of translator): Mr. Speaker, the E. coli contamination began almost a year ago, but the Conservatives have just shut down the source of E. coli. The self-regulatory policies that the Conservatives love so dearly are a failure. The contamination could have been worse. When will this government explain the unacceptable delay and put an end to this politically dangerous experiment?

The speaker: The honourable Minister of Agriculture.

Gerry Ritz: Well, Mr. Speaker, the time line actually backs up the fact that our system does work. There is no endemic situation out there from E. coli. E. coli exist across the country on a daily basis. Having said this, the government is focused on food safety. We want to go beyond what consumers expect. We've done that, Mr. Speaker, which constantly reinforces what CFIA needs in the form of more inspection staff and more dollars to get the job done. We will continue to focus on food safety, Mr. Speaker. I wish they would vote to help us do that on our initiatives.

The speaker: (Voice of translator): The honourable member for Hull-Annville.

Nycole Turmel (NDP) (Voice of translator): Mr. Speaker, if the system were so effective, then what explains the fact that the American inspectors are the ones that identified the contamination? The CFIA has revealed that it has no plan to put in place to prevent contamination of this nature. Canadians are concerned and they're losing faith in this government's ability to protect our food. What will the -- when will the Conservatives make public health a priority and put an end to cuts to food safety?

The speaker: (Voice of translator): The honourable Minister of Agriculture.

Gerry Ritz: Well, of course, Mr. Speaker, there are no such cuts. The last budget, we put another \$100 million into CFIA at that to give this many the capacity to make sure that Canadian consumers can enjoy safe

food on a daily basis. Of course the NDP voted against that initiative, Mr. Speaker. We continue to build the capacity of cfia to get the job done on behalf of Canadian consumers.

The speaker: The honourable member for wascana.

Ralph Goodale (LPC): Mr. Speaker, the xl food contamination problem continues. The whole plant is now shut down. The company fell short of proper standards way back in August. And this government's inspection system failed to be on top of it then. Partly, that's because government inspectors don't actually inspect much anymore. They just monitor company inspections. Even worse, 12 days went by before Canadians were told. Why did the science take that long? Is it because this government fired 90 biologists, the scientists whose job it was to do that science?

The speaker: The honourable Minister of agriculture.

Gerry Ritz: Another ill-informed opposition member, Mr. Speaker. And if he would care to remember, the system that cf immaterial a is using now, called cvs, was brought in in 2005 under his government. If he didn't like it now, why did he not say so then? I don't understand what he's caterwauling go. What we've done as a government is consistently construct a stronger cfia to make sure they have the capacity to make sure our consumers are safely served.

The speaker: The honourable member for wascana.

Ralph Goodale (LPC): Mr. Speaker, that complacency brought you walkerton. (Voice of translator): The Americans are the first ones to have discovered the contamination at xl foods. Not Canada. That's embarrassing. Why did it take 12 days for Canadians to be made aware of these risks? Will the government admit that this delay is due to the fact that it eliminated 90 positions of biologists?

The speaker: (Voice of translator): The honourable Minister of agriculture.

Gerry Ritz: Well, absolutely not true, Mr. Speaker. And we'll continue to ensure food safety officials respond efficiently based on sound science and internationally-accepted protocols to ensure the safety of the food for our Canadian consumers. Now, we are introducing important legislation to hep-c fia respond to food safety situations more swiftly, me. If the opposition is as serious will "p" about food safety as they claim, I hope the Liberals will support cs-11.

The speaker: The honourable member for wascana.

Ralph Goodale (LPC): Mr. Speaker, former Conservative Minister Jim print tysse took this government to the woodshed yesterday offer its mismanagement of pile lines. Canadian resources need access to markets but the process for getting there is badly blank mangled bill this government's failure to cult aboriginal peoples. "There will be no way forward to west coast access without the central participation of First Nations" Mr. Prentice said. The crown obligation to engage First Nations in a meaningful way has yet to be taken up, he said. Why is that, Mr. Speaker?

The speaker: The honourable parliamentary secretary to the Minister of natural resources.

David Anderson (CPC): Mr. Speaker, as usual the member opposite has it wrong. When the Canadian council for aboriginal business estimates that oilsand companies do \$1.3 Billion worth of business each year with aboriginal honed companies, I think we can suggest that that shows a consultation and energy development is working for those -- those -- those aboriginal communities. Mr. Speaker, an independent

comprehensive deveaux, science-based 'valves the proposed northern gateway project is currently underway. First Nations are being consulted extensively as province that review.

The speaker: The honourable member for Halifax.

Megan Leslie (NDP) (Voice of translator): Mr. Speaker, more and more Conservatives are criticizing the Conservatives. There's dissension in the ranks. The form he Minister of fisheries, tim siddon, has already stated that the Conservative plan for fish has been the is disaster and now the former Minister of environment, Jim prentice is denouncing his former colleagues be who are refusing to consult with first nation on oil pipelines. The Conservatives aren't listening to citizens. The first nation, nor will nor or Conservatives. Whether or not are they listening to? Lobbyists?

The speaker: The honourable Minister parliamentary secretary to the Minister of natural resources.

David Anderson (CPC): Mr. Speaker, I can tell youwho we're listening to. We're listening to the 41 first nation that is we're providing funding for that they can come and participate in the northern gateway pipeline review. Those are the communities we are "a" worry listening. To as I mentioned, we've got an independent comprehensive science-based evolves the northern gateway pipeline taking place, and the only ones who seem to want to interfere with that process, that science-based process, is the opposition and their house leader.

The speaker: The honourable member for Halifax.

Megan Leslie (NDP): Mr. Speaker, they are not consulting, and I can understand why the Minister is reluctant to engage in mingful consultation with First Nations. It's because he'll probably hear an answer that he doesn't want to hear. But as Mr. Prentice warned his party yesterday, complacency is dangerous. Northern gateway carries enormous "h"moysé risk and if Conservatives succeed in ramming it through, it's Canadians who will pay the price. Will the Minister take the advice of an old friend? Will he do his homework and will he actually consult with First Nations?

The speaker: The honourable parliamentary secretary.

David Anderson (CPC): Well, Mr. Speaker, the only ones who've made their mind build-up this project are the opposition and they oppose every development project that's everbeen proposed in Canada. They oppose our trade deals. Everything that thistalk about, including their 21 billion-dollar carbon tax, works against Canadians. It's times they set aside their ideology, joining with us and start to create jobs for Canadians across this country.

The speaker: The honourable member for burnaby-douglas.

Kennedy Stewart (NDP): Mr. Speaker, it'd be nice if they stopped making things up about the opposition and tried answering some questions, so let's see if we can get an answer here. Mr. Speaker, reuters reports a new computer security breach by a Chinese group. Calgary-based tell vent was the target f it wasn't for the company warning their customers, the public would have never even flown, so can the governmentconfirm foreign government involvement in this attack and in light of this, can Conservatives tell us if national security is part of the criteriafor the nexen takeover review?

The speaker: The honourable parliamentary secretary to the Minister of public safety.

Candice Bergen (CPC): Mr. Speaker, our government takes cyber-security seriously and operates on the

advice of security experts. Our government recently made significant investments of \$90 million in a cyber-security strategy designed to defend against electronic threats, hacking and sign cyber-espionage. Telecommunications carriers operating in Canada are certainly subject to Canadian law. We'll continue to work to protect the interests of Canadians and protect them from cyber-security threats. Thank you, Mr. Speaker.

The speaker: The honourable member burn been.

Kennedy Stewart (NDP): From that side is more broken promises and here's another one. Canadians may be surprised to learn that Conservatives tabled new great trade agreement with Klein this week. Paul Wells of Mclean's reports the agreement allows arbitration allowing Canadian companies to be dealt with behind closed doors. So, why did Conservatives agree to have arbitration done in secret with no transparency? And when will they bring the deal before the house for debate and a vote?

The speaker: The honourable parliamentary secretary to the Minister of international trade.

Gerald Keddy (CPC): Mr. Speaker, improving access to high-growth markets in the Arab shpacific region is a key part of our government's protrade plan. And our priority, Mr. Speaker, is to remove Chinese trade barriers and increase exports such as lumber, grains, beef and value-added Canadian products. Now, part of this plan, Mr. Speaker, and, of course, in our government's long-standing commitment to provide public access to investor disputesettlement mechanisms, Canada's fepa with China is no different. As we do with other investor state disputes, this provides for Canada to make alldocument submitted through the arbitration tribunal available to the public.

The speaker: (Voice of translator): The honourable member for rimouski-neigette - temiscouata - les basques.

Guy Caron (NDP) (Voice of translator): Mr. Speaker, contrary to the Conservatives, the NDP believe that we need clearite cite ear why to avaluate trade deisms Conservatives shade they would table any new draft agreement in the chamber, in effect, for debate and comment over a 21-day period bucks they haven't said whether they wouldput them a vote rearview mirror they afraid of the results? Based on thedraft agreement with China, a secret arbitrage system would be put in place instead of the sports according to experts, this project is based on achinese model ask that's more advantageous it the Chinese. Will the Conservatives allow the house to vote without limiting debate on these issues?

The speaker: The honourable government house leader.

Peter Van Loan: Well, Mr. Speaker, our objective with this agreement is, of course, to ensure that, for the first time, Canadians can have real protection for the investments they make in China. We think that's important to protect Canadian business people and investors. Now, you in terms, Treaty, we, of course, under our government have introduced an unprecedented process for putting Canadian treaties, international treaties, to the scrutiny of the House of Commons. That's why it was tabled in this house. That's why there is a period of time and a process set out, and the opposition can, if they television see a vote an that treaty in the house, they can have it. In fact, they have an opportunity on Monday to have it debated and voted. If don't like t they could do it and Tuesday are and have it reillustrate debatedand voted. It's up to them whether they want to do that.

The speaker: (Voice of translator): The honourable member for rimouski-neigette - temiscouata - les basques.

Guy Caron (NDP) (Voice of translator): Yesterday in a speech in New York, the Prime Minister didn't announce cuts to programs to seniors. No, instead he launched into die at that three at that diatribe against the international con kept suggestion. Consensus on banning asbestos. Consensus on fighting climate change and a consensus on banning cluster bombs and on weapons trade. The Prime Minister seems to agree more with rogue states then with our allies. Do they have anything to boast about in that?

The speaker: The honourable parliamentary secretary to the Minister of northern foreign afares.

Bob Dechert (CPC): Mr. Speaker, the suggestion that Canada is not interested in arms trades treaties and cluster munitions treaties is ridiculous. Canada has set some of the highest global standards in export control of munition and Canada looks forward it new negotiations of an arms trade treaty. Thank you.

The speaker: The honourable member for Ottawa centre.

Paul Dewar (NDP): Yesterday, Mr. Speaker, the Prime Minister refused to walk even a few blocks, a few blocks to address the UN And promote Canada. And today, he's refusing to meet with Canadian mediato answer questions. While our allies are doing the hard work of diplomacy, Mr. Speaker, Conservatives have put Canada on the sidelines. Does the Prime Minister think that a policy of self-imposed isolation is the bestway of advancing Canada's interests?

The speaker: The honourable parliamentary secretary to the Minister of foreign affairs.

Bob Dechert (CPC): Well, Mr. Speaker, as the honourable member will know, the Prime Minister will be meeting with two world leaders later today in New York, and -- but under our government, Canada's policy is no longer to please every dictator with a vote at the United Nations. We've taken strong principled positions to promote freedom, human rights and the rule of law. In fact, the Prime Minister has delivered the UN General assembly speech twice as many times as in two previous Prime Ministers of Canada.

The speaker: (Voice of translator): The honourable member for pontiac.

Mathieu Ravignat (NDP): Mr. Speaker, not was the purchase to purchase f-35s a complete fees could he, but the actual decision to purchase them was made without key information. In a report presented to government, the airforce clearly mentioned that more information was needed on meeting competing character "a" Arable available to Canada. Mr. Speaker, if the Conservatives knew that important information was missing on other option, why did they buyingly go-ahead and pick thef-35s?

The speaker: The honourable parliamentary secretary to the Minister of public works.

Jacques Gourde (CPC) (Voice of translator): The secretariat has been put in place to ensure transparency and regionality -- reasonable timeframes in the replacement of the f-35. No funding has been spent to purchase Friday any lighter aircraft. Nor will it be spent until the secretariat takes an independent look at all costs associated with replacing thef-18s.

The speaker: (Voice of translator): The honourable member for pontiac.

Mathieu Ravignat (NDP) (Voice of translator): On another topic, Mr. Speaker, yesterday's doubling revelation were made by man linked to organized crime and to the Conservatives. The entrepreneur, anyone know zambito, lifted the veil on collusion, payouts to the immediate "in" in federal budget, political financing, but I don't need to explain that that to them. A lot, a Conservative candidate, beneficiary of the generosity of amazon.com bito. Thousands of dollars from him and his partners are now in the hands of the voters. Since

again. Let's take lock the fishermen's ei for just a moment. Sources throughout Atlantic Canada are now telling that you say they are advised not to find a second claim in the new year. So, naturally, they're scared, because they've they feel in the spring of 2013, their benefits will be dramatically reduced or eliminated altogether. So, let's clear the air. To the Minister: Will they preserve the sanctity of fishermen's ei?

The speaker: The honourable parliamentary secretary. .

Kellie Leitch (CPC): Well, thank you very much, Mr. Speaker. And unlike the opposition who seem to just be against things, we're actually for Canadians and making sure they have an opportunity to be employed. We've created 770,000 net new jobs over the last years and we're going to continue to do that. Helmets to hard hats or whether that be an improvement in the opportunities found "a" opportunity for small business - - small business criticism immaterial to make sure, a do all my colleagues be that Canadians have opportunity for employment. Unlike the NDP and the Liberals that vote against all these initiatives.

The speaker: (Voice of translator): The honourable member for Hochelaga.

Marjolaine Boutin-Sweet (NDP) (Voice of translator): Mr. Speaker, the Minister said that no one would be negatively impacted by the Conservatives' changes to EI. In my riding, people were hard-hit by business closures, with lost -- with 700,000 jobs lost. Hochelaga this a job creation plan for its workers being but the Minister of human resources -- will the Minister finally admit a she was wrong and will she stop her crusade against Canadians who were following the rules? Will she backtrack on the reform?

The speaker: (Voice of translator): Tass the honourable parliamentary secretary.

Kellie Leitch (CPC): Thank you very much, Mr. Speaker. And as I've said already, our government wants sunshine that those who work more keep more of their evening earnings and that's why economic action plan 2012 is focused on making sure unemployed Canadians have opportunities to get whether that be the \$50,000,000 Over two years in the youth employment strategy or new apprenticeship v.I.P. Ship grants opportunities, items that both the Liberals and the NDP have continually voted against, our maybe the NDP carbon tax of \$21 billion that would kill jobs across this country. These are things we're focused on making sure Canadians have opportunities and are employed. Thank you.

The speaker: Trance trap the honourable member for Drummond.

François Choquette (NDP) (Voice of translator): Mr. Speaker, the Minister spent the week saying that her changes to EI would not have any negative impacts on workers. And yet, that is yet, that is not what is being reported by the rights advocacy group for the unemployed in Drummondville. People reporting all kinds of penalties that they're experiencing because of her changes. These new rules penalize Canadians, especially the most disadvantaged. The Conservatives know this is true and will they finally admit it and reverse on the changes to the program?

The speaker: The honourable parliamentary secretary to the Minister for human resources and skills development.

Kellie Leitch (CPC): This government has created 770,000 net new jobs since the downturn of the recession. In fact 90% of those are full-time jobs. That's because of a very effective economic action plan that includes a number of initiatives that provide opportunities for employment of young people, older individuals, aboriginal and Métis Canadians and new immigrants. We're working to make sure every Canadian has opportunity to have a job and be attached to the workforce. I'm not sure why the NDP and the Liberals continually vote against these opportunities.

The speaker: (Voice of translator): The honourable member for vercheres-les patriotes.

Sana Hassainia (NDP) (Voice of translator): Mr. Speaker, the Minister of human resources spent the entire week trying to make us believe her absurd stories. She can stick her head in the sand and reto whoever will listen that no one will lose money you had her reform, but that's wrong. We know people who are unfortunate enough to clues their jobs but are not c.E.O. New Zealand the oil patch will receive no assistance in this government, and yet, the Conservatives continue to deny the facts. So, for how long will the Conservatives keep their heads in the sand? .

The speaker: (Voice of translator): The honourable member honourable parliamentary secretary to the m inister of human resources.

Kellie Leitch (CPC): This government has provided unprecedented opportunities for Canadians to find employment. We're doing everything that we can to better-connect Canadians with jobs that are available. It 's the Liberals and the NDP, their opposition to these great initiatives that really have stifled that opportunity. So, whether that's voting against the youth employment strategy or against afriend present ship funding. These are things that will help Canadians find jobs and be attached to the workforce. The opposition continue to vote against them.

The speaker: (Voice of translator): The honourable member for lac-saint-louis.

Alexandrine Latendresse (NDP): Trance tass the Conservatives have been making up stories. Their ei tales are so farfetched that they're about to tell us about hobb irregularities its, but we in the NDP have talked to people across the country. People are worried. Will the Conservatives emerge interest never, neverland and recognize the harmful consequences of their ill-considered reform?

The speaker: The (voice of translator): The honourable parliamentary secretary. .

Kellie Leitch (CPC): It's allowing those people that are unemployed to find jobs. It's better-connecting them a an opportunity to have a job so theycan improve the quality of life their families. Unlike the Liberals and NDP that vote against all these initiatives that are providing Canadians with opportunities for jobs, we're there for Canadians. We're focused on finding jobs so they can improve the quality of life of their families.

The speaker: The honourable member for don valley west.

John Carmichael (CPC): Mr. Speaker, statistics Canada announced today that Canada's economy grew again in July. The surprise economic growth in the nearly 770,000 net new jobs created since July 2009 are positive signs. Now while we're focus on growing the economy and creating jobs, the NDP is pushing radical economic schemes. Like massive barre tax. Can the

the speaker: The honourable parliamentary secretary to the Minister of finance.

Shelly Glover (CPC): Well, our government is focused on what matters to Canadians: Creating jobs and promoting economic growth. We're working to keep can a's economy growing with measures like the job creating hiring credit for small business, and as reported, July's economic growth shows that we are right on track. But the NDP is pushing radical economic schemes, like a massive carbon tax that will kill Canadian jobs and economic growth. Even worse, their carbon tax would increase the price of everything that Canadian families buy. Like grass and goeseries and electricity. While Canadians and our economy can't afford their radcle economic schemes.

The speaker: (Voice of translator):The honourable member for honore-mercier.

Paulina Ayala (NDP) (Voice of translator): Mr. Speaker, big banks are increasing banking fees for their customers. On November 5th, the national bank will increase its fees on bank transactions from 65 cents to \$1. That is a hike of over 50%. They are not con at the time with their record profits of his 7.8 Billion that they racked enough the last quarter. This is much more than inflation. Why won't the Conservatives protect families against the Greed of banks? Why are they allowing them to raid their customers' wallets?

The speaker: The honourable parliamentary secretary to the Minister of finance.

Shelly Glover (CPC) (Voice of translator): Thank you, Mr. Speaker. And I would like it thank my colleague for her question, because it gives me the opportunity to say that banks are paying taxes to support our social programs and to support all of our health care system as well. In addition, if we look the NDP's plan, their carbon tax program, that would affect everything that Canadian families purchase, whether it be groceries, electricity, everything families buy would be affected, and Canadians don't want to go down that path.

The speaker: (Voice of translator): The honourable member for Quebec.

Annick Papillon (NDP) (Voice of translator): We know what the Conservatives do in these situations. They propose voluntary codes of conduct. Yes, that's right, Mr. Speaker. Voluntary. That's what they did with credit cards, and we saw the results of that. Cardholders continue to pay astronomical interest rates and household debt continues to climb to historical highs. Mr. Speaker, the fees charged by banks are already unreasonable, so when will the Conservatives act to protect consumers?

The speaker: (Voice of translator): The honourable parliamentary secretary.

Shelly Glover (CPC) (Voice of translator): Thank you very much, Mr. Speaker. And once again, I would like to thank my colleague for the question. But the NDP doesn't want to listen to us. Despite all the measures that we have put in place to create jobs. But let's listen to the Canadian federation of independent business that said on this topic "the code served merchants well. It put in place fair rules and that means that we are protecting Canadian consumers, but, unfortunately, the NDP always votes against this.

The speaker: (Voice of translator): The honourable member for Quebec.

Annick Papillon (NDP) (Voice of translator): You know that's not true, complexion it's not just about banking fees that -- where consumers are being gouged. While the Conservatives stand idly by, waiting for something to happen. Mr. Speaker, gas price have exploded. 36% In the past little while. In yes, the average price is often above \$1.40 Per litre. The policies of the Conservatives are too expensive. How long are they going to wait before they do something to protect consumers? When are they going to act?

The speaker: (Voice of translator):The honourable Minister of industry.

Christian Paradis (Voice of translator): Mr. Speaker, I would ask the member for Quebec to come back to planet earth, because we've dropped the gst by 2%. We've put in an oversight measure at the gas pump for fairness. We also strengthened the powers of the competition bureau, and what is "w" what does the NDP offer us instead? A carbontax that would cost Canadian taxpayers \$21 billion. \$12 Billion, Mr. Speaker. That's not just on the price on gas. That would be a tax on everything, so please come back to reality, dear colleagues.

The speaker: (Voice of translator): The home.

Alain Giguere (ndp) (Voice of translator): Mr. Speaker, the Conservatives are so business making up stories about the NDP, that they've completely forget an about motorists. 36 Cents in an increase, that's \$15 billion. Now, that's a tax. That's putting taxes and it's your fault, because, clearly, we're coming up to another long weekend and everyone knows that gas prices are going to be employed against but you're still doing nothing. What we want to know is when are you going to look after Canadian consumers and motorists?

The speaker: (Voice of translator): The honourable Minister of industry.

Christian Paradis (Voice of translator): Mr. Speaker, my colleague was not here in the last parliament and maybe that's why he didn't notice that we dropped the GST by 2%. He didn't notice that we put in fairness oversight measures at the gas pumps. He did not notice that we strengthened the powers of the competition bureau. But when I look at their platform, I can see a carbon tax that would cost Canadian taxpayers, \$12 billion. Mr. Speaker, can you imagine gas applies "m" prices? Can you imagine collateral prices? Groceries, Energy. Everything would go up, so once again, would you come back to relate, please, my dear colleagues.

The speaker: Order. The honourable member for Kings-Hants.

Scott Brison (LPC): Regarding the proposed Nexen sale to CNOC to ensure long-term net benefit to Canada, is the government requiring that Canadians make up the majority of the Nexen board? And that there would be Canadian representation on the CNOC board? Further, Canadian banks continue to face significant barriers to growth when doing business in China. Is the government leveraging on the Nexen discussion to attain greater access to Chinese markets for the Canadian financial services sector?

The speaker: (Voice of translator): The honourable Minister of industry.

Christian Paradis: Maybe this approach was the one adopted from the previous government, but on our side, Mr. Speaker, each single deal that is proposed here will have to provide net benefit for Canada. We will consider the highest interests for Canadians, Mr. Speaker. So, speaking about this transactioner I report, that will be scrutinized very closely, and, Mr. Speaker, whatever happens will be for the best interests of Canada.

The speaker: The honourable member for Markham-Unionville.

John McCallum (LPC): Jim Prentice, this government's former aboriginal affairs Minister, has slammed the government for failing to perform their constitutional duty to consult with aboriginal people on the northern gateway pipeline. Does this government understand that the Prime Minister doesn't make all the rules and will they commit to consult and accommodate aboriginal peoples on issues like resource development, which impact on their rights? Or are they simply saying that Jim Prentice is a liar?

The speaker: The honourable parliamentary secretary to the Minister of natural resources.

David Anderson (CPC): Well, Mr. Speaker, as I said before, we're conducting an independent comprehensive science-based evaluation of proposed northern gateway pipeline. First nations are being consulted extensively during that and I've got a list here of 14 first nations that is we're helping with funding so that they can present before the northern gateway pipeline. So, Mr. Speaker, when we hear that aboriginal companies do \$1.3 billion worth of business with oilsands companies, we think that the aboriginal -- the consultation and the energy development is working for aboriginal communities.

The speaker: (Voice of translator): The honourable member for Beauharnois-Salaberry.

Anne Minh-Thu Quash (NDP) (Voice of translator): Mr. Speaker, Canadians who visit federal parks today will be met with signs, note guides. Why? Once again, Conservative cuts. \$30 Million less for services to customers. That is 600 guide researcher and archaeological positions that have been cut: In addition to job loss, the reduction of the number of visitors and tourists will have a major impact on the economic spinoffs for the regions. In my riding, the battle of the chateaugay national historic site had its business hours reduced, whereas we're celebrating -- they are "a" they're celebrating the anniversary war of 1812. Why are the Conservatives attack our heritage?

The honourable parliamentary secretary to the of the environment.

Michelle Rempel (CPC): It's been our government that's been committed to protecting our country's natural heritage through our parks system we will absolutely continue to do so. Mr. Speaker, our parks service is well -- is well-funded and will continue to deliver the service that all Canadians expect through and visitors to Canada to see our natural heritage.

The speaker: (Voice of translator): The honourable member for Terrebonne-Blainville. .

Charmaine Borg (NDP) (Voice of translator): Mr. Speaker, the people in my riding are extremely concerned by the closure of the Terrebonne post office on October 26th. This closure is part of a worrisome trend towards the privatization of post services. Numerous citizens and businesses will be affected by this reckless closure. Once again for the Conservatives, profits more important than people. Why do the Conservatives insist on jeopardizing the economy in my riding by privatizing essential services such as those offered by Canada Post this.

The speaker: The (voice of translator): Honourable Minister of State for Transport of.

Steven Fletcher (CPC): Mr. Speaker, Canada Post is an arm's length crown corporation that makes decisions -- the day a day decisions, operating decisions, based on market demand. Now, I know -- I know that -- that that's difficult for members of the NDP to understand. But if we want to make Canada Post viable in the long-term, they will have to make adjustments from time to time. And that is what Canada Post has done.

The speaker: The honourable member for Cariboo-Prince George.

Richard Harris (CPC): Mr. Speaker, our natural resource industry is a powerhouse in the Canadian economy and employs hundreds of thousands of Canadians. It's because, Mr. Speaker, this Conservative government has taken action to strengthen this important sector by streamlining reviews while ensuring -- ensuring that Canada's environment remains safe. Could the parliamentary secretary explain what the NDP's plan to add even more red tape burden and a carbon tax would do to Canada's resource sector.

The speaker: The parliamentary secretary.

David Anderson (CPC): Mr. Speaker, I have to thank the member from Cariboo-Prince George for his insightful question and his excellent work on this file. The industry Minister pointed out clearly he can't have the NDP's dangerous carbon tax would increase prices for all Canadians. It would kill Canadian jobs in the resource sector. It wouldn't just damage the west as the leader of the NDP would claim, but all of Canada. And let's listen to what Ontario Finance Minister Dwight Duncan has to say. Alberta's oil sands are a valuable resource both in Alberta and the entire country. A resource that helps fuel the Canadian economy. When will the NDP bail on their wrecking ideology, change their policies and join us as we create jobs for Canadians? .

The speaker: The honourable member for scarborough-guildwood.

John McKay (LPC): Mr. Speaker welcomes the Prime Minister was hanging without his buddies in New York, the leaders of the free world were actually battling it out on the floor of the United Nations. Ironically, one of the mine Prime Minister's guests in this love-in was none other than the king of n.H.L. Lockouts, gary bettman. Could the Minister tell the house whether they exchanged views on the benefits of lockouts and prorogation or did the commission just merely advise the Prime Minister toe stay off the ice while the big boys battle itout?

The speaker: The honourable parliamentary secretary to the Minister of foreign afurs.

Bob Dechert (CPC): As mentioned earlier, prance the member wasn't paying attention, the Prime Minister is meeting with two world leaders in New York today, and he should probably also know that the Prime Ministerreceived the states machine the year award last night... Great mark of distinction for Canada. And one that he will also know was --

the speaker: (Voice of translator): The honourable member for notre-dame-de-grace - lachine.

Isabelle Morin (NDP): Trance continue Mr.Speaker, there's another group that is suffering around underthe Conservatives. Stats can revealed recent delay young people must still live at home with theron their parents foreven longer because of their more vulnerable economic situation. Insteadof helping them, the Conservatives are cutting programs that they count on, such as Canada services for young people. Will the government act for our young people? When are they going to put forward plan to stimulate job creation for young people?

The speaker: (Voice of translator): The honourable parliamentary secretary to the Minister of human resources.

Kellie Leitch (CPC): Mr. Speaker, what we actually did put forward plan the budget in march. It's \$50 million, called the youth employment the extra just a minute it'sactually an augmentation of an existing \$300 million program but the NDPvoted against it. So I guess my question really is is that we read the budge. We know what's in it. We know that we're supporting students, whether is it be through youth employment strategy or changing the Canada student loans programs to allow them a get the education they want to enter the workforce. Why did the NDP vote against all these initiatives?

Thespeaker: The honourable member for miramichi.

Tilly O'Neill-Gordon (CPC): Mr. Speaker, while the opposition panders to extremists ngo and preten showers hollywood stars being they outright disappointing for Canada's fishermen and sealers. Our government will continue to defend the rights of our sealers. To providea live I hood for their families through our humane, responsible and sustainable harvest. Canada has a long history of hunting and gathering. It 's part of who we are, Mr. Speaker. Can the parliamentary secretary update us on our government's continued fight against the European Union seal ban?

The speaker: The honourable parliamentary secretary to the Minister of fisheries and oceans.

Randy Kamp (CPC): Thank you, Mr. Speaker. And I thank myhard-working colleague from miramichi for her very good question. And I want to assure her that our government is committed to protecting hard-working Canadian sealers. While members of both the NDP and the Liberal party have spoken out against the seal hunt, our government continues to fight for it. We're addressing the European Union ban by initiating a dispute settlement proceeding at the world trade organization. The ban on sealproducts adopted in the

European Union was a decision that has no scientific basis and is inconsistent with free trade practices. So we'll continue to support the jobs, growth and economic prosperity of Atlantic Canadians and aboriginal peoples.

The speaker: (Voice of translator): The honourable the honourable member for laurentides-labelle .

Marc-André Morin (NDP): Trance it happens thank you, Mr. Speaker. The Conservatives have been cutting eism and the Minister says this no one is being affected. Component that there are 300,000 more unemployed people than there were before the recession. The Conservatives' only plan is to force people to take a job 300 kilometres away from their home. Now, with gas prices the way they are, the Minister better than said that there are no consequences. Why do the unemployed have to pay for the tax breaks tots oil patch this.

The speaker:(Voice of translator): The honourable parliamentary secretary to the him Minister ever human resources.

Kellie Leitch (CPC):Thank you very much, Mr. Speaker, there will be 770,000 net new jobs created since July 2009. 90% Of those are full-time jobs. There are a number of initiatives that have been put forward in the last number of budgets. So whether that be the youth employment strategy, the targeted initial to have older work he is, apprenticeship programs, the working income tax bothment the apprenticeship incentive grant, the ei hiring tax credit, all of those are opportunities for helping Canadians become employed. I ask the NDP members opposite, why do they just wants to raise taxes and kill jobs?

The speaker: Order! (Voice of translator): The honourable member for richmond-arthabaska.

André Bellavance (BQ) (Voice of translator): Mr. Speaker, the Minister for the status of women's support for a motion seeking to reopen the abortion debate caused massive disapproval among women's groups in Quebec. After the women -- Quebec women's federation and the birth planning federation, who are calling for her regular anyways, many others have spoken out against her vote. The Quebec Minister for the status of women. More than see new people have signed petitions that have been started up in the past 24 hours. The Minister voted for her values, you about will she admit that she is enable or incapable of occupying a position where she's suppose today defend the rights of women?

Susan Truppe (CPC): Thank you, Mr. Speaker. MPs Have voted. The House of Commons voted. And we now have to get on with other issues. This government -- I'm very proud of what this government has done for women and girls . This government has supported over 550 projects for women and girls from coast-to-coast-to-coast, and we've increased funding for women and girls to its highest level ever, over any other government. Thank you, Mr.Speaker.

The speaker: (Voice of translator): The honourable member for richmond-arthabaska.

André Bellavance (BQ) (Voice of translator): Within the Conservative caucus itself, some people want to close the debate, such as the member for mississauga-brampton south, who says this this debate brings us back to the age the dine saw, about other people want to reopen it. Will the Prime Minister, whose leadership was challenged by the majority vote of his caucus that breaks his campaign promise, put an end to the ambiguity that surrounds this question, as has been called for by the Quebec national assembly in a innocent -- unanimous motion?

The speaker: (Voice of translator): The honourable parliamentary secretary to --

Susan Truppe (CPC): thank you, Mr. Speaker. As I said, MPs Werening their constituents. The house

House of Commons voted. It's time to move on. We are they proud prude of what our government has done for women and girls as I said, over 50550 projects were supported for women and girls from coast to coast to coast ask we have approved the most amount of money for women and girls over any other government. Thank you, Mr. Speaker.

The speaker: That will bring question period to an end for today.

(End of Question Period)

The Privy Council Office's Media Centre /
Le Centre des médias du Bureau du Conseil privé

Disclaimer

The unofficial Question Period transcript is based on closed captioning (rough)

**Transcript provided courtesy of the Privy Council Office. Please note that this transcript is produced via the closed captioning provided by CPAC and is available in English only. For an official transcript please consult the Hansard located on the Parliamentary Internet site.*

Media Centre / Centre des médias
Requests / Demandes : 613.952.6922 or
mediacentre@bnet.pco-bcp.gc.ca

Centre des médias / Media Centre
Demandes / Requests : 613.952.6922 ou
mediacentre@bnet.pco-bcp.gc.ca

**Pages 288 to / à 289
are withheld pursuant to sections
sont retenues en vertu des articles**

15(1) - Subv, 16(1)(a)(iii), 16(1)(c)

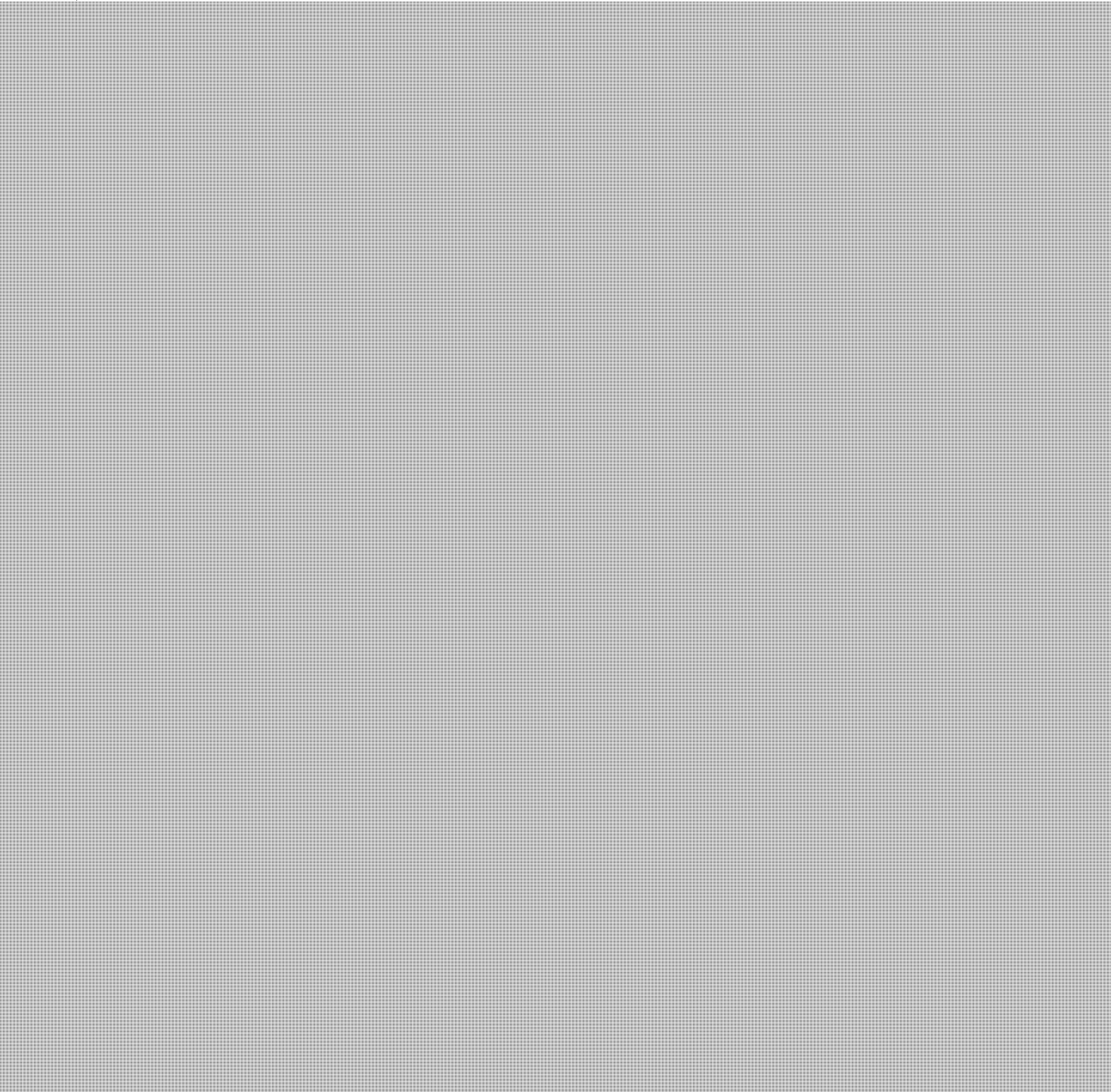
**of the Access to Information
de la Loi sur l'accès à l'information**

Maillé, Marie Anick

From: Brown, Émilie
Sent: May-15-12 9:55 AM
To: Plunkett, Shawn
Cc: Trudel, Pierre; Kingsley, Michèle; Maillé, Marie Anick
Subject: RE: Urgent - Line request

s.21(1)(b)

See my changes highlighted in yellow below:





Émilie Brown

Senior Policy Analyst / Analyste de politiques principale Emergency Management Planning Division (EMPD)/Division Planification de la gestion des mesures d'urgences (DPGMU) Public Safety Canada / Sécurité publique Canada Tel : 613-949-3995

cell: 613-790-6841

Email/Courriel : emilie.brown@ps-sp.gc.ca

s.21(1)(b)

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

From: Plunkett, Shawn

Sent: Tuesday, May 15, 2012 9:46 AM

To: Brown, Émilie

Cc: Trudel, Pierre; Kingsley, Michèle; Maillé, Marie Anick

Subject: RE: Urgent - Line request

Importance: High

Thanks Em,

One last thing. Can you take a look at what we have produced (attached) in the next couple of minutes and let me know if anything is incorrect.

Much appreciated.

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

From: Brown, Émilie


Sent: May-15-12 9:30 AM


To: Plunkett, Shawn

Cc: Trudel, Pierre; Kingsley, Michèle; Maillé, Marie Anick

Subject: RE: Urgent - Line request

Hi Shawn,

It's accurate but I would change it to: 



Emilie

Émilie Brown

Senior Policy Analyst / Analyste de politiques principale Emergency Management Planning Division (EMPD)/Division Planification de la gestion des mesures d'urgences (DPGMU) Public Safety Canada / Sécurité publique Canada Tel : 613-949-3995

cell: 613-790-6841

Email/Courriel : emilie.brown@ps-sp.gc.ca

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

From: Plunkett, Shawn

Sent: Tuesday, May 15, 2012 8:33 AM

To: Brown, Émilie

Cc: Trudel, Pierre; Kingsley, Michèle; Maillé, Marie Anick

Subject: Urgent - Line request

Importance: High

Hi Em,

We are working on an urgent briefing request for Min's office, related to Huawei.

Is the following line accurate?



Would need input by 10am.

Thanks.

Shawn Plunkett

613.614.4362

PS/SP Canada

s.21(1)(b)



UNCLASSIFIED

**Minister Toews' Meeting with Nicola Roxon,
Australian Attorney General,
June 14, 2012**

s.13(1)(a)
s.15(1) - Int'l
s.21(1)(a)

ISSUE

Canada and Australia's approaches to securing telecommunications infrastructures.

STRATEGIC OBJECTIVES



BACKGROUND

Concerns about untrusted foreign telecommunications and technology firms, in particular but not exclusively from China, are frequently raised by our close allies' government authorities, politicians and media.

The Australian government has recently decided to block Huawei Shenzhen Technology (Huawei) from tendering for contracts in the country's National Broadband Network (NBN), a new infrastructure being built by the government through an arrangement similar to a crown corporation. This decision is not without consequences as the development of this network, an investment of \$38 billion dollars, is the most significant telecommunications reform in Australia's history: it aims to connect 93% of homes, schools and businesses to high speed broadband internet access.

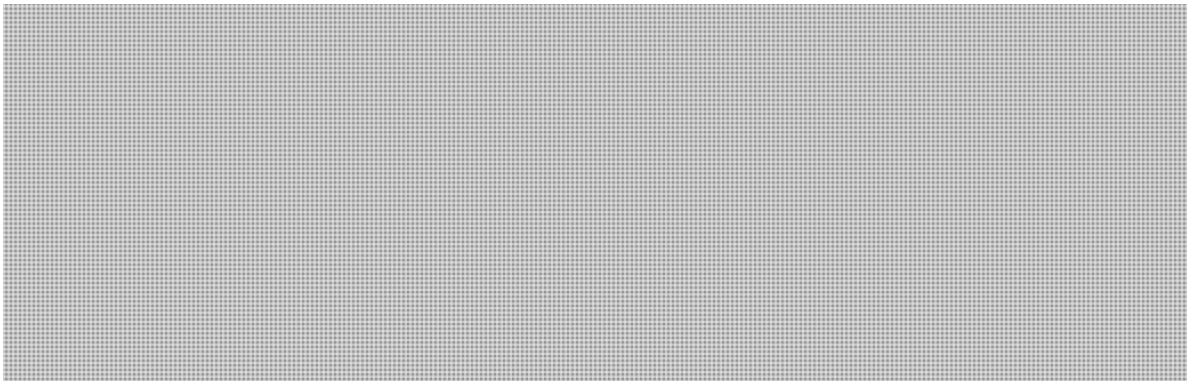
The United States (U.S.) has taken similar action. In the fall of 2011, an official at the Department of Commerce stated that Huawei would not be participating in building the U.S. interoperable wireless network for emergency responders, due to national security concerns.



s.13(1)(a)
s.15(1) - Int'l
s.21(1)(a)
s.21(1)(b)

UNCLASSIFIED

STRATEGIC CONSIDERATIONS



Potential associated risks are mitigated through a series of tools, mechanisms and partnerships developed over the years by the security and intelligence community. Efforts notably include the Canadian Cyber Incident Response Centre, which works hand in hand with national and international counterparts to collect, analyze and disseminate data on cyber threats, provides intelligence and technical support to the industry, and coordinates the national response to any cyber security incident. Also included are strong partnerships built with the telecommunications industry (within the *Canada's Cyber Security Strategy* and the *National Strategy and Action Plan for Critical Infrastructure*), both at the operational and decision making levels, to address security issues within the sector. Further measures will be brought forward as the threat environment dictates.

TALKING POINTS

RESPONSIVE

- **We take national security very seriously, and a thriving telecommunications industry must fundamentally be a safe and secure one. This is particularly important as these networks are the backbone of our economy. We have in place tools and mechanisms to identify, mitigate and address any risk to Canada's telecommunications sector, and we work with our partners and allies, such as Australia, to best leverage knowledge, intelligence and expertise. We will remain vigilant and pursue further strategies as needed to best secure our telecommunications sector.**



UNCLASSIFIED

- **I congratulate you on the National Broadband Network undertaking. This is quite significant. How do you see the procurement process unrolling? Do you expect to continue down the path of excluding specific players? What do you see as the key next steps and challenges as the telecommunications sector evolves, in the longer term?**

s.15(1) - Int'l

s.15(1) - Subv

Zygoumis, Terri

From: Louis-Martin.Aumais@international.gc.ca
Sent: Thursday, September 20, 2012 9:53 PM
To: Dick, Robert; Gordon, Robert; linda.clairmont@ps-sp.gc.ca; [REDACTED]@cse-cst.gc.ca; Christopher.Blain@pco-bcp.gc.ca; Mark.Glauser@international.gc.ca
Cc: Banerjee, Ritu; [REDACTED]
[REDACTED] James.Galt@international.gc.ca; paul.grimshaw@defence.gov.au; Claudie.Senay@international.gc.ca; Artur.Wilczynski@international.gc.ca; David.Nelson@international.gc.ca; Colin.Shonk@international.gc.ca; Tricia.Geddes@pco-bcp.gc.ca; Michael.Small@international.gc.ca; David.McKinnon@international.gc.ca; Stephen.Burridge@international.gc.ca; Mark.Berman@international.gc.ca; Kent.Vachon@international.gc.ca; Roland.Legault@international.gc.ca; Linder, Glen
Subject: CNBRA-ILO-010: CYBER: Aus Parliamentary Hearing on National Security Legislation -- Public Submissions to the Committee (20120921)
Attachments: PJCIS -- NatSec Leg Rev - Huawei Submission.pdf; PJCIS -- NatSec Leg Rev - Telstra Submission.pdf; PJCIS -- NatSec Leg Rev - ASIO Public Submission.pdf; PJCIS -- NatSec Leg Rev - Inspector-General I&S Submission.pdf

UNCLASSIFIED

Colleagues,

As you know by now, at the request of the Attorney General, the Australian Parliament has started hearings concerning the review of National Security legislation, in particular concerning the modernization of the interception regime and telco sector security. Inquiry's own webpage: http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsi2012/index.htm

Sign of the public interest so far, the Committee has received 208 submissions. I attach a sampler of submissions, which I trust you will find of interests:

1. **Huawei**, which echos the recent public criticism it has directed to the Australian government of late;
2. **Telstra**, Australia's largest telecommunications company, and key partner in the National Broadband Network. On the issue of telco sector security reform, Telstra in its submission interestingly states: "*Telstra supports measures to ensure that C/CSPs [carriers and carrier service providers] have appropriate incentives to focus resources on network security and believes this can be achieved through the modification of some of the [Aus Govt's] proposed measures to avoid adverse impacts on our ability to undertake **efficient procurement and network design and operations.***"
3. **ASIO**, whose public submission has been picked up by the Australian press this morning <http://www.abc.net.au/news/2012-09-21/asio-wants-phone-and-email-data-stored-for-two-years/4272982>;
4. **The Inspector-General of Intelligence and Security** -- the Australian Intelligence Community's oversight body, who seeks additional resources from the Government is she is to be called in future legislation to oversee the new interception regime <http://www.abc.net.au/news/2012-09-20/data-retention-changes-to-cost-more/4271898>

I will continue to monitor and report on the subject, as developments warrant.

Louis-Martin Aumais
Counsellor | Conseiller
Louis-Martin.Aumais@international.gc.ca
Telephone | Téléphone : +61 (02) 6270 4029

Facsimile | Télécopieur : +61 (02) 6273 3285
Commonwealth Avenue, Canberra ACT 2600
Canadian High Commission | Haut-commissariat du Canada
Government of Canada | Gouvernement du Canada

Zygoumis, Terri

From: [redacted]@csis.org> s.19(1)
Sent: Monday, October 08, 2012 1:20 PM
To: Banerjee, Ritu
Subject: 60 Minutes Report on China Telecom Giant Huawei Features CSIS Experts

To ensure receipt of our email, please add us to your safe senders list



October 08, 2012

Dear Colleague,

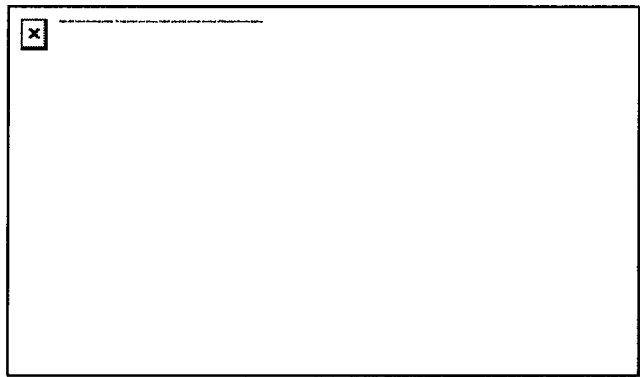
Last night 60 Minutes correspondent Steve Kroft reported on Huawei, the Chinese telecom giant being probed for national security and espionage concerns by the House Intelligence Committee. CSIS Technology and Public Policy program director Jim Lewis and CSIS China studies chair Chris Johnson are both featured in Kroft's report. If you missed the segment, you can watch it [here](#).

60 Minutes also posted a "web extra" interview between Kroft and Lewis which runs about 2 minutes which can be viewed [here](#).

I hope you find the Kroft report featuring our experts interesting.

As always, I welcome your feedback.

Watch "Huawei Probed for Security, Espionage Risk"



Sincerely,



Center for Strategic and International Studies (CSIS)

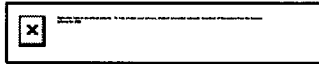
www.csis.org



s.19(1)



To unsubscribe from all CSIS emails, please [click here](#).



Zygoumis, Terri

From: COMDO on behalf of PSMediaCentre/CentredesmediasdeSP
Sent: Saturday, October 27, 2012 4:02 PM
To: Today's News / Actualités
Subject: Radio-Canada : Partenariat Canada-États-Unis pour la cybersécurité (Ministre mentionné)

Partenariat Canada-États-Unis pour la cybersécurité

Radio-Canada
26 octobre 2012, 22h23 HE

Le Canada et les États-Unis vont travailler de concert pour protéger leurs infrastructures technologiques contre des cyberattaques. Les deux pays ont annoncé vendredi le lancement d'un plan commun, qui sera placé sous la supervision du ministère de la Sécurité publique au Canada et du Département de la Sécurité publique aux États-Unis.

Le Plan d'action vise à améliorer la collaboration entre les deux pays sur la gestion des cyberincidents. Il s'agit de protéger les infrastructures numériques communes en permettant des interventions conjointes lorsque les événements le dictent.

« Le Canada et les États-Unis ont intérêt à travailler en partenariat à la protection des infrastructures communes. Nous tenons à travailler ensemble afin d'assurer la protection des systèmes cybernétiques essentiels, de rétablir les services en cas de perturbation et d'améliorer la sécurité du cyberspace pour tous les citoyens. » — Vic Toews, ministre canadien de la Sécurité publique

Le Plan d'action comprend également un volet pour stimuler la participation du secteur privé et l'échange d'informations. En septembre, le **ministre Toews avait déjà présenté un nouveau partenariat entre son gouvernement et une coalition d'entreprises privées, d'organismes gouvernementaux et d'organisations à but non lucratif afin de faciliter l'information du public quant aux mesures de sécurité pertinentes lors de la navigation sur Internet.**

Cette annonce intervient peu après l'avertissement lancé au début du mois par les États-Unis à l'effet que des équipements de télécommunications fournis par les groupes chinois Huawei (OUA OUE) et ZTE pourraient être utilisés à des fins d'espionnage.

Plusieurs mesures déjà annoncées

Cette collaboration s'inscrit également dans le cadre du Plan d'action Par-delà la frontière pour la sécurité du périmètre et la compétitivité économique, annoncé par les deux gouvernements en décembre 2011. Des initiatives visant notamment la protection des renseignements personnels, la sécurité du fret maritime et la circulation des personnes entre le Canada et les États-Unis ont déjà été présentées.

Le gouvernement canadien a récemment annoncé un investissement de 155 millions \$ pour la sécurité des réseaux informatiques, afin de permettre une meilleure coordination de la réponse des autorités fédérales et provinciales en cas de cyberattaque. Le Canada a également lancé depuis peu une campagne de sensibilisation sur le sujet, intitulée Pensez cybersécurité, destinée aux citoyens.

[Lien](#)

Zygoumis, Terri

From: Clairmont, Lynda
Sent: Sunday, October 28, 2012 11:47 PM
To: Banerjee, Ritu
Subject: Fw: AFP: US, Canada launch joint cybersecurity plan (Minister quoted)

From: PSMediaCentre/CentredesmediasdeSP
Sent: Saturday, October 27, 2012 11:39 AM
To: Today's News / Actualités
Subject: AFP: US, Canada launch joint cybersecurity plan (Minister quoted)

US, Canada launch joint cybersecurity plan
AFP
2012-10-26

OTTAWA — Canada and the United States announced they were launching a joint cybersecurity plan to protect their digital infrastructure from online threats.

The action plan, under the auspices of the US Department of Homeland Security and **Public Safety Canada**, aims to better protect critical digital infrastructure and improve the response to cyber incidents.

"Canada and the US have a mutual interest in partnering to protect our shared infrastructure," said the **Public Safety Minister Vic Toews**.

"We are committed to working together to protect vital cyber systems, to respond to and recover from any cyber disruptions and to make cyberspace safer for all our citizens."

Homeland Security Secretary Janet Napolitano said the plan "reinforces the robust relationship" between their two agencies.

Through the plan, Washington and Ottawa hope to improve collaboration on managing cyber incidents between their respective cyber security operation centers, enhance information sharing and engagement with the private sector and pursue US-Canadian collaboration to promote cyber security awareness to the public.

The announcement came after the US House Intelligence Committee warned earlier this month that equipment supplied by Chinese telecoms groups Huawei and ZTE could be used for spying and called for their exclusion from government contracts and acquisitions.

Canada later invoked a "national security exception" that could exclude China's Huawei Technologies from a role in helping build its new super secure government network.

[Link](#)

Zygoumis, Terri

From: Banerjee, Ritu
Sent: Sunday, October 28, 2012 11:52 PM s.19(1)
To: [REDACTED]
Subject: Fw: AFP: US, Canada launch joint cybersecurity plan (Minister quoted)

From: Clairmont, Lynda
Sent: Sunday, October 28, 2012 11:47 PM
To: Banerjee, Ritu
Subject: Fw: AFP: US, Canada launch joint cybersecurity plan (Minister quoted)

From: PSMediaCentre/CentredesmediasdeSP
Sent: Saturday, October 27, 2012 11:39 AM
To: Today's News / Actualités
Subject: AFP: US, Canada launch joint cybersecurity plan (Minister quoted)

US, Canada launch joint cybersecurity plan
AFP
2012-10-26

OTTAWA — Canada and the United States announced they were launching a joint cybersecurity plan to protect their digital infrastructure from online threats.

The action plan, under the auspices of the US Department of Homeland Security and **Public Safety Canada**, aims to better protect critical digital infrastructure and improve the response to cyber incidents.

"Canada and the US have a mutual interest in partnering to protect our shared infrastructure," said the **Public Safety Minister Vic Toews**.

"We are committed to working together to protect vital cyber systems, to respond to and recover from any cyber disruptions and to make cyberspace safer for all our citizens."

Homeland Security Secretary Janet Napolitano said the plan "reinforces the robust relationship" between their two agencies.

Through the plan, Washington and Ottawa hope to improve collaboration on managing cyber incidents between their respective cyber security operation centers, enhance information sharing and engagement with the private sector and pursue US-Canadian collaboration to promote cyber security awareness to the public.

The announcement came after the US House Intelligence Committee warned earlier this month that equipment supplied by Chinese telecoms groups Huawei and ZTE could be used for spying and called for their exclusion from government contracts and acquisitions.

Canada later invoked a "national security exception" that could exclude China's Huawei Technologies from a role in helping build its new super secure government network.

[Link](#)

UNCLASSIFIED

Highlights of Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE

Report by Chairman Mike Rogers and Ranking Member C.A. Dutch Ruppersberger of the Permanent Select Committee on Intelligence, U.S. House of Representatives, October 8, 2012

Context

- In February 2011, leading Chinese telecoms equipment manufacturer Huawei, published an open letter to the U.S. government denying security concerns with the company or its equipment, and requesting a full investigation into its corporate operations
- In November 2011, the House Permanent Select Committee on Intelligence initiated this investigation in order to inquire into the counterintelligence and security threat posed by Chinese telecoms companies doing business in the U.S.
- The investigation focused on Huawei and ZTE, the top two Chinese telecoms equipment manufacturers, as they seek to market their equipment to U.S. telecoms infrastructure and hope to expand in the U.S.
- Conclusion of the investigation: the risks associated with Huawei and ZTE's provision of equipment to U.S. critical infrastructure could undermine core U.S. national security interests

Summary of the Report's Recommendations

Communicating the threat / CFIUS / U.S. government systems and contractors

- The U.S. Intelligence Community should actively seek to keep cleared private sector actors as informed as possible of the threat posed by continued penetration of the US telecoms market by Chinese companies
- The Committee on Foreign Investment in the United States (CFIUS) must block acquisitions, takeovers, or mergers involving Huawei and ZTE given the threat to U.S. national security
- Congressional committees should consider legislative proposals seeking to expand CFIUS to include purchasing agreements
- U.S. government systems, particularly sensitive systems, should not include Huawei or ZTE equipment, including component parts

UNCLASSIFIED

- U.S. government contractors, particularly those working on contracts for sensitive U.S. programs, should exclude ZTE and Huawei equipment in their systems

U.S. private sector and network providers

- Private-sector entities in the U.S. are strongly encouraged to consider the long-term security risks associated with doing business with either ZTE or Huawei for equipment or services
- U.S. network providers and systems developers are strongly encouraged to seek other vendors for their projects

Unfair trade practices

- Unfair trade practices of the Chinese telecoms sector, in particular China's continued financial support for key companies, should be investigated by committees of jurisdiction within the U.S. Congress and enforcement agencies within the executive branch

Increased openness and transparency of Chinese companies

- List on western stock exchange with advanced transparency requirements
- Offer more consistent review by independent third-party evaluators of financial information and cyber security processes
- Comply with U.S. legal standards of information and evidentiary production
- Obey all intellectual property laws and standards
- Increase transparency and responsiveness to U.S. legal obligations

Legislative Options

- Potential legislation to better address the risk posed by telecoms companies with nation-state ties or otherwise not clearly trusted to build critical infrastructure should be considered by committees of jurisdiction in the U.S. Congress
- Legislation could include increased information sharing among private sector entities, and an expanded role for the CFIUS process to include purchasing agreements

Classified Annex

- The publicly available report references a classified annex, which provides both classified information relevant to the discussion, as well as information about the resources and priorities of the U.S. Intelligence Community

Lord, Yves

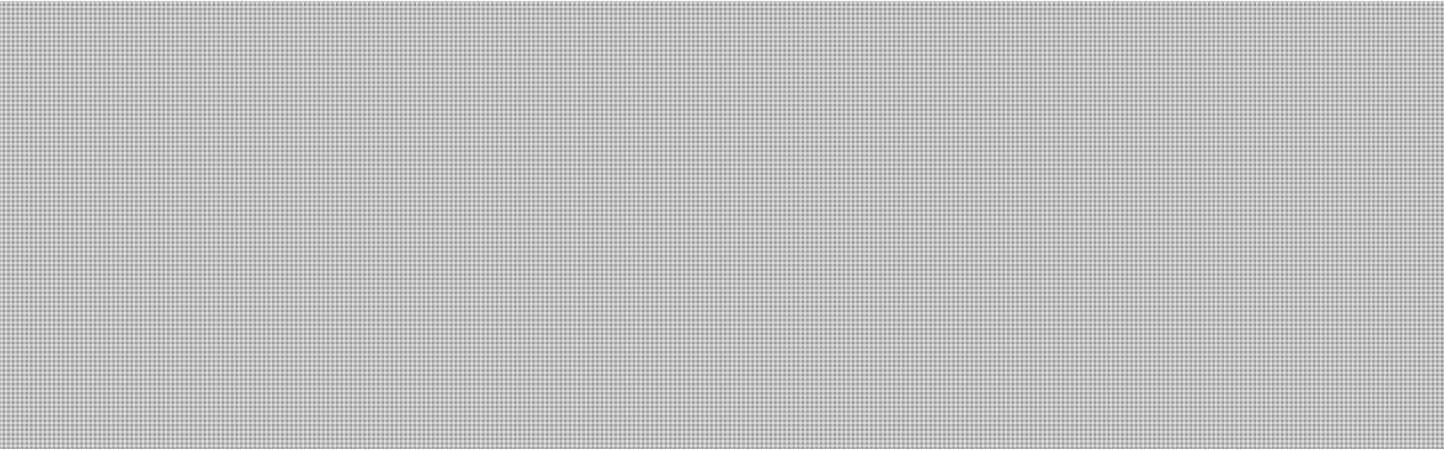
From: Grigsby, Alexandre
Sent: Monday, July 23, 2012 4:20 PM
To: Smith, Maggie M (CIC); **Davies, John**; MacDonald, Michael; Wilczynski, Artur (FAC-AEC); Senay, Claudie (FAC-AEC); Kirkpatrick, Tachelle (FAC-AEC); [REDACTED] (CSIS-SCRS); Soper, Lesley (PCOSANDI-BCPSETR); [REDACTED] (CSE-CST); [REDACTED] (CSE-CST); [REDACTED] (CSIS-SCRS); Hunt, Ryan; Sixsmith, Sara SL - Civ (DND-MDN)
Cc: Gordon, Robert; Dick, Robert; Dvorkin, Corey; Matz, Mark
Subject: Report: [REDACTED] meeting June 19-20.

Classification: SECRET// [REDACTED]

s.13(1)(a)
s.15(1) - Int'l
s.15(1) - Subv
s.21(1)(b)

Industry Canada: Please pass to Heather Dryden and Janis Doran
DFAIT: Please circulate to relevant personnel and appropriate missions

1. Summary: On June 19-20, 2012, Canada hosted a meeting of the [REDACTED]. Bob Gordon, Special Advisor, Cyber Security, Public Safety Canada, and Michael Walma, Director of International Crime and Terrorism at the Department of Foreign Affairs and International Trade (DFAIT) represented Canada.



Budapest Conference on Cyberspace

4. Background: [REDACTED]

5. [REDACTED]

Representatives from over 65 countries, the private sector, and civil society met to discuss the economic, social and security aspects of cyberspace. At the end of the London Conference, Hungary agreed to host a follow-up conference in October 2012 and South Korea will host one in 2013. [REDACTED]

6. **Format for Budapest:** The Conference format will be very similar to that of London, and will be focused on a series of plenary sessions, with keynote speakers. Likely speakers will include Foreign Ministers and senior private sector executives. Following these plenary sessions, there will be simultaneous panel discussions on the following topics:

s.13(1)(a)

s.15(1) - Int'l

- Economic growth and development in and through cyberspace (this panel is expected to focus particularly on information and communication technologies (ICT) for development issues)
- The social benefits of cyberspace (e.g. education, human rights benefits)
- Cyber security (e.g. cyber hygiene, due diligence, CERT collaboration)
- The international security dimensions of cyberspace
- Cybercrime (e.g. cross border cooperation, the *Convention on Cybercrime*)

7. The panel discussions are expected to continue in workshops, where working-level experts could establish concrete deliverables for the conference.

[Redacted]

[Redacted]

10. **Level of participation:**

[Redacted] so he may provide a keynote address via teleconference. [Redacted] Cabinet Office which is responsible for cyber coordination in the U.K., will likely lead the U.K. delegation. He will be accompanied by [Redacted]

[Redacted]

[Redacted] Canada indicated that the Minister of Public Safety's Office was aware of the event but was not in a position to commit to the Minister's attendance. Canada noted however that Acting Deputy Minister of Public Safety, Graham Flack, will attend.

11. [Redacted] reiterated that their prospective delegations were subject to change, [Redacted]

12. **Outcome document:** As was the case at the London Conference, Hungary is expected to release a Chairman's Summary, as opposed to a Communiqué, which would require a negotiated and agreed to text.

**Pages 307 to / à 310
are withheld pursuant to sections
sont retenues en vertu des articles**

13(1)(a), 15(1) - Int'l

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

Drafted: PS/Grigsby
Consulted: PS/Dvorkin
Approved: PS/Gordon

Lord, Yves

From: Banerjee, Ritu
Sent: Friday, August 24, 2012 4:33 PM s.13(1)(a)
To: Renaud, Josee-Anne; Foerster, Jennifer; Des Rochers, Patrick s.15(1) - Int'l
Cc: Davies, John s.15(1) - Subv
Subject: FW: Australia, new cyber security regime

Classification: CONFIDENTIAL

From: Aumais, Louis-Martin [mailto:aumaisl@fac-aec.gc.ca]
Sent: Friday, August 24, 2012 2:07 AM
To: (CSE-CST); Gordon, Robert
Cc: (CSE-CST); Dick, Robert; Banerjee, Ritu
Subject: RE: Australia, new cyber security regime

Classification: CONFIDENTIAL

Bob,

[REDACTED]

Best,

Louis-Martin AUMAIS

ILO Canberra

From: [REDACTED]@cse-cst.gc.ca]

Sent: Wednesday, August 22, 2012 7:45 AM

To: Gordon, Robert

Cc: [REDACTED]; Dick, Robert; Aumais, Louis-Martin

Subject: RE: Australia, new cyber security regime

Classification: CONFIDENTIAL

Bob,

[REDACTED]

Cheers

[REDACTED]

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

From: Gordon, Robert [mailto:GordonR@psepc-sppcc.gc.ca]

Sent: August 20, 2012 6:04 PM

To: [REDACTED]

Cc: [REDACTED] Dick, Robert (PSEPC-SPPCC)

Subject: Australia, new cyber security regime

Classification: CONFIDENTIAL

s.15(1) - Subv

s.21(1)(a)

[REDACTED]

The following is part of an article in the public press concerning efforts by the Australian Government to secure IT network equipment as it relates to cyber security threats from hostile interests or organized crime. [REDACTED]

[REDACTED]

Thank you in advance.

Bob

"Proposed security sweep of IT plans after Huawei decision

By Geoff Kitney

A new cyber-security regime to be considered following the decision to ban Chinese telecommunications giant Huawei from involvement in the NBN will compel businesses to inform security agencies about plans to buy and install new IT network equipment and network designs.

An outline of proposed changes to national security laws to reduce Australia's vulnerability to cyber security threats from hostile interests and organized crime, argues there is an overwhelming case for intervention in the market by security agencies to protect the national interest.

The proposals have provoked industry concern and are behind the decision by Huawei to go public - in an interview with The Australian Financial Review on Friday - with its concerns about the rising power of security agencies.

Huawei Australia's chairman, John Lord, told the Financial Review that its Australian clients and potential customers had indicated to Huawei they were concerned about the potential impact of a tough new cyber security regime on their ability to do business.

One possibility, according to Huawei, was that under new rules being requested by the security agencies, foreign companies operating in Australia's technology industries could be given a "security standard".

"That is an area of uncertainty which concerns us," he said. "We are addressing that very closely."

In draft proposals in a paper written by the Attorney-General's Department, and soon to be considered by a powerful parliamentary committee, it is proposed that the Telecommunications Act 1997 be amended to "institute obligations to provide government with information on significant business and procurement decisions and network designs".

It is also proposed that the Australian telecommunications industry be required by law to protect its networks from unauthorized interference.

The paper says there is a lack of awareness of the national security risks associated with communications and IT systems.

Because Australia was at a critical stage of telecommunications infrastructure development driven by the construction of the NBN, there was a compelling case for urgent action to require businesses to ensure that national security interests were protected.

Meanwhile, the chief author of the government's Asian century white paper, Ken Henry, has played down the impact of the decision on security grounds to exclude Huawei from involvement in the NBN.

Dr. Henry said the decision was not a surprise and had not caused much damage.

The Australian Financial Review"

Lord, Yves

From: Aumais, Louis-Martin [aumaisl@fac-aec.gc.ca]
Sent: Thursday, September 20, 2012 5:21 AM
To: Glauser, Mark (FAC-AEC); Gordon, Robert; Dick, Robert
Cc: Clairmont, Lynda; [REDACTED] (CSE-CST); [REDACTED] (CSE-CST); Banerjee, Ritu; Elliott, Michael (FAC-AEC); Blackmore, Michael (FAC-AEC); Sinclair, Robert (FAC-AEC); McKinnon, David (FAC-AEC); Burt, Stephen (PCOIAS-BCPBEI); Senay, Claudie (FAC-AEC); Kirkpatrick, Tachelle (FAC-AEC); Lister, Michael (FAC-AEC); Solomon, Jonathan (FAC-AEC); Liao-Moroz, Angelica (FAC-AEC); [REDACTED] (CSE-CST); [REDACTED] (CSIS-SCRS); Desmartis, Isabelle I - Civ (DND-MDN); Wilczynski, Artur (FAC-AEC); Lister, Michael (FAC-AEC); Armstrong, Roy RC - LCol (DND-MDN); Banerjee, Ritu; Barber, Carolyn (FAC-AEC); [REDACTED] (CSIS-SCRS); Blain, Christopher (PCOSANDI-BCPSETR); Buchan, Gavin (PCOSANDI-BCPSETR); Blouin, Amélie (FAC-AEC); [REDACTED] LCol (DND-MDN); [REDACTED] (CSE-CST); [REDACTED] - LCdr (DND-MDN); [REDACTED] (CSE-CST); Dalziel, Alexander (PCOIAS-BCPBEI); Davies, John; [REDACTED] (CSIS-SCRS); Diogo, Brigitte (PCOSANDI-BCPSETR); Dorgan, Erin (PCOSANDI-BCPSETR); [REDACTED] Col (DND-MDN); Geddes, Tricia (PCOSANDI-BCPSETR); [REDACTED] (CSIS-SCRS); Henry, Hugh (PCOIAS-BCPBEI); Henshaw, Peter (PCOIAS-BCPBEI); Irfani, Elyas (PCOIAS-BCPBEI); [REDACTED] - Civ (DND-MDN); [REDACTED] - Civ (DND-MDN); [REDACTED] (CSIS-SCRS); LeDuc, Genevieve (FAC-AEC); [REDACTED] (CSIS-SCRS); [REDACTED] (CSE-CST); Marcoux, Rennie (PCOSANDI-BCPSETR); Marland, Karin (FAC-AEC); McRae, Robert (PCOIAS-BCPBEI); [REDACTED] (CSE-CST); Olson, David (FAC-AEC); Parkinson, Ted TFW - Cdr (DND-MDN); [REDACTED] (CSE-CST); Rheault, Denis JGDG - Civ (DND-MDN); [REDACTED] (CSE-CST); [REDACTED] (CSE-CST); Seguin, Bill (FAC-AEC); Shaffer, Gordon (PCOSANDI-BCPSETR); [REDACTED] (CSE-CST); Marland, Karin (FAC-AEC); Galt, James (FAC-AEC); [REDACTED] - Cdr (DND-MDN); [REDACTED] (CSE-CST); Radujko, Victor (PCOIAS-BCPBEI); Testa, Anna (PCOIAS-BCPBEI)

s.15(1) - Int'l
s.15(1) - Subv
s.21(1)(a)

Subject: [REDACTED]

Attachments: [REDACTED]



Classification: SECRET / [REDACTED]

SUMMARY: [REDACTED]

**Pages 316 to / à 318
are withheld pursuant to sections
sont retenues en vertu des articles**

15(1) - Int'l, 21(1)(a)

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

Page 319
is a duplicate
est un duplicata

Page 320
is a duplicate
est un duplicata

Page 321
is a duplicate
est un duplicata

Page 322
is a duplicate
est un duplicata

**Pages 323 to / à 328
are withheld pursuant to sections
sont retenues en vertu des articles**

15(1) - Int'l, 21(1)(a)

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

Dick, Robert

From: Julianne.Prokopich@international.gc.ca
Sent: October-22-12 12:30 PM
To: Julianne Prokopich
Subject: WSHDC Look ahead: Cybersecurity (OCT 22 - 26, 2012)
Attachments: CQ- Cyber - Reid Seeks Lame-Duck Action.docx

THIS WEEK IN WSHDC:

OCT 18 – Iranian hackers renewed a campaign of cyberattacks against US banks this week, and openly defying US warnings to halt, U.S. officials and others involved in the investigation into the attacks said. The attacks, which disrupted the banks' websites, showed the ability of the Iranian group to sustain its cyberassault on the nation's largest banks for a fifth week, even as it announced its plans to attack in advance. US officials said the attacks were sponsored by the Iranian government and approved at high levels as part of a low-grade cyberwar that officials warned could lead to retaliation. Unclear is at what point attacks would call for a forceful response from the US. [Article](#)

WHITE HOUSE:

OCT 22 –[CBS News](#) reports that a new White House executive order would direct U.S. spy agencies to share the latest intelligence about cyberthreats with companies operating electric grids, water plants, railroads and other vital industries to help protect them from electronic attacks. The 7-page draft order is in the process of being finalized. Meanwhile, CQ later reported that Senate Majority Leader Harry Reid released a statement saying he plans to bring cyber legislation back to the floor when this year's lame-duck session gets underway. [See attached for CQ article]

OCT 18 –A White House-ordered review of security risks posed by suppliers to U.S. telecommunications companies found no clear evidence that Huawei Technologies Ltd had spied for China, two people familiar with the probe told Reuters. Instead, those leading the 18-month review concluded early this year that relying on Huawei, the world's second-largest maker of networking gear, was risky for other reasons, such as the presence of vulnerabilities that hackers could exploit. [Article](#)

DoD:

OCT 11 –In a speech at the Intrepid Sea, Air and Space Museum in New York, Defense Secretary Leon Panetta warned that the United States was facing the possibility of a “cyber-Pearl Harbor” and was increasingly vulnerable to foreign computer hackers who could dismantle the nation's power grid, transportation system, financial networks and government. [Article](#)

DHS:

OCT 16 – Michael W. Locatis III, the DHS’s assistant secretary for cybersecurity communications, during a forum in Arlington, Va. predicting that the Department will be able to fully deploy its automatic network intrusion detection system Einstein 3 across federal systems by 2015—three years ahead of initial projections. Thanks to a change in implementation strategy, the DHS is leveraging commercial entities, such as Internet service providers (ISPs) to build Einstein 3 capabilities into their infrastructure “using information that can only be provided by the federal government,” he said. DHS has Einstein 2 deployed at 17 of 19 of the federal agencies that were slated to receive it.

FALL 2012 –In order to attract the highly skilled and qualified cybersecurity workers at the DHS, a Homeland Security Advisory Council’s CyberSkills Task Force Report recommends reserving its coolest cybersecurity hobs for federal works, not contractors, to focus more on real-work experience and expertise. To do this, the DHS needs to build a system for actively measuring these skills, such as pilots that undergo situational testing. The report identifies the need to hire at least 600 new cybersecurity professionals.

THINK TANKS:

OCT 15 –The nonprofit National Cyber Security Alliance, along with Symantec, has published the findings of a survey of more than 1,000 small and midsize businesses that found that 83 percent of respondents said they don’t have a written plan for protecting their companies against cyberattacks, while 76 percent think they are safe from hackers, viruses, malware and cybersecurity breaches.

UPCOMING EVENTS:

OCT 25 from 8:30am to 12:00pm – CSIS will host an event titled, “building a Cyber Security Workforce Through Diversity. Secretary Napolitano will deliver remarks. Location: 1800 K St., N.W.

ARTICLES/ REPORTS OF INTEREST:

OCT 22 – Facebook Gains as Tool for Terrorists Seeking Friends, UN Says. Bloomberg. Article

OCT 18 – So What’s Mitt Romney’s Take on Cyber Security? Foreign Policy Magazine. Article

OCT 17 – Canada to Beef Up Its Cyber Defenses. The Wall Street Journal. Article

OCT 15 –Google Privacy Policy Rethink Demanded by EU. BBC. Article

Julianne Prokopich

Research Analyst, Public Safety and Border Security | Analyste en Recherche, Sécurité publique et de la sécurité des frontières

Embassy of Canada | Ambassade du Canada

501 Pennsylvania Avenue NW, Washington, DC 20001

Phone: (202) 682-7743 Ext 7743 | Fax (202) 682-7792

Julianne.Prokopich@international.gc.ca

Dick, Robert

From: Austria, Jamela
Sent: October-17-12 5:14 PM
To: Dick, Robert; Hatfield, Adam; Matz, Mark; Anderson, Windy; Labelle, Sébastien; Fortunato, Stephanie; Weir, Sarah
Cc: Carta, John; Willey, Chris
Subject: RE: Transcript: Public Safety Minister Vic Toews press conference - 2012-10-17, 10:00 ET
Attachments: RT - CBC News: Coverage of Minister Toews cyber security funding announcement - 2012-10-17 - 10h00 EDT; Today's News / Actualités - (08:00 - 14:00 ET) - 2012-10-17

Hello,

For your information, please find pasted below the official transcript of today's cyber security funding announcement.

We have not received any additional media enquiries following the announcement; however, we have received good media coverage. Please find attached various articles and transcripts.

Thanks again to Adam for supporting the Minister this morning – and thanks again to you all for helping us with the products.

s.19(1)

Jamela Austria

Senior Communications Advisor | Conseillère principale en communications
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone : 613-949-1675
Mobile | Cellulaire : [REDACTED]
Fax | Télécopieur : 613-954-0800
E-mail | Courriel: jamela.austria@ps-sp.gc.ca

From: COMDO On Behalf Of PSMediaCentre/CentredesmediasdeSP

Sent: Wednesday, October 17, 2012 4:28 PM

To: * COMMS ADG / Bureau du directeur général associé; * COMMS Communication Services Division / Division des services de communication; * COMMS DGO / Bureau de la directrice générale; * COMMS Program Communications Division / Secteur des communications de programmes; * COMMS Public Affairs Division / Secteur des affaires publiques; * Speeches / Discours; Thibouthot, AkimIsabelle; Astravas, Rutha; Banerjee, Ritu; Beaudoin, Serge C; Bolton, Stephen; Boucher, Patrick; Boucher-Lalonde, Murielle; Cameron, Bud; Carmichael, Julie; Champoux, Elizabeth; Clairmont, Lynda; Clifford, Kurtis; Coburn, Stacey; Crawford, Andrée; Csversko, Christine; Currie, St. Clair; Daoust, Normand; Davis, Jeremy; De Santis, Heather; Duschner, Gabrielle; Easson, Grant; Gareau-Lavoie, Genevieve; Gordon, Robert; Hitchcock, Christy; House, Andrew; Huggins, Rachel; Humeniuk, Elena; Hunt, Ryan; Jarmyn, Tom; Johnson, Mark; Kelland, Stephen; Khouri, Lisa; Kubicek, Brett; Lavoie, Micheline; Leclair, Natalie; Leclerc, Carole; Leonidis, Nelly; Lesser, Robert; MacDonald, Nicholas; MacKinnon, Paul; Marchand, Renee; McAteer, Julie; McGrath, Andrew; McLaren, Victoria; Morris, Marika; Mueller, Mike; Mundie, Robert; Murdock, Lyndon; Murray, Erin; Nicole, Jean-Thomas; Oldham, Craig; Panthaky, Jasmine; Porter, Neal; Pozhke, Nicholas; Rosario, Giselle; Roy, Isabelle; Saunders, Joanne; Schulz, Caroline; Shuttle, Paul; Slack, Jessica; Thibault, Stéphane; Tupper, Shawn; Van Crieking, Jane; Verret, Scott; Vinodrai, Arjun; Wex, Richard; Wilson, Gina

Subject: Transcript: Public Safety Minister Vic Toews press conference - 2012-10-17, 10:00 ET

TIME:

10:00 ET

LENGTH:

10:00 MINUTES

DATE:

OCTOBER 17, 2012

SUBJECT:

PRESS CONFERENCE WITH PUBLIC SAFETY MINISTER VIC TOEWS

MIKE SPARLING (Director of Information Technology and Business Intelligence, Algonquin College): Good morning, ladies and gentlemen. If I could ask everyone to take their seats, we'll begin. My name is Mike Sparling. I'm the Director of Information Technology and Business Intelligence here at Algonquin College.

It is my pleasure to be here with you today for this announcement.

To give you an idea of this event will unfold, we will have a series of remarks from Public Safety Minister Vic Toews and member of Parliament Shelley Glover. This will be followed by a question-and-answer session and a photo opportunity.

You will note the microphone installed in the room. It will be made available during the question-and-answer session.

For those of you interested, copies of the news release are available at the back of the room.

Without further ado it is my pleasure to introduce the Honourable Vic Toews, Minister of Public Safety. Minister Toews was first elected to the House of Commons in 2000 and re-elected in 2004, 2006, 2008 and 2011. In February 2006, Mr. Toews was appointed Minister of Justice and Attorney General of Canada and in January 2007, was named President of the Thunder Bay. He was appointed Minister of Public Safety in January 2010.

Please welcome Minister Toews.

VIC TOEWS (Public Safety Minister): Thank you, Mike. Good to see you here, Shelley. I'm going to have to put this over somebody's recording equipment here, but in any event, thank you very much and thank you very much to Algonquin College for hosting this event. Just put it right there.

All right, it'll work. But thank you very much for all Algonquin College hosting this event. I understand that there are full and part-time students here of over 50,000, quite remarkable. And I know that you're doing a very good job and there is a reason why we're making this announcement here today because some of the courses that your college offers in terms of cyber security and the people that you are training for what is indeed a very expanding field.

I'm delighted to be here with Shelley, who is the Parliamentary Secretary to the Minister of Finance, Member of Parliament for St. Boniface, my colleague from Manitoba, to make an important announcement that further demonstrates our government's commitment to cyber security.

As you know, October is cyber security awareness month. This month is recognized by Canada and some of our closest allies as a time to encourage individuals, families and the public and private sectors to learn more about cyber risk and to use the tools and resources online to help them stay safe online.

As part of the activities we are engaged in this month, raising awareness of the things Canadians can do to keep themselves and their families safe online, I want to come to this campus today, or I wanted to come to this campus today where so many young people are developing the skills to one day protect the systems that form the core of our society.

But first, let me note that keeping our cyber networks and infrastructure secure and resilient is one of the most challenging issues facing our government, our citizens and our allies. I can assure you that our government is fully engaged in meeting and overcoming this challenge. As part of this, we announced Canada's cyber security strategy in 2001. This security strategy rests on three pillars: securing government networks, strengthening partnerships across diverse sectors in governments, both at home and abroad, and educating Canadians on how to reduce the risks that come with living in an online society.

To achieve these goals, we provided a \$90 million investment over five years and \$18 million on ongoing funding towards the cyber security strategy. Over the last two years we made steady progress in meeting our goals. For example, we worked closely with our partners to identify common risks as well as common solutions to keeping critical infrastructure like banks, power grids and the transportation sector resilient against cyber attacks.

We have also moved forward in our efforts to engage Canadians and Canadian businesses on the risks associated with living in a digital age. Last year at this time we launched the Get Cyber Safe Public Awareness Campaign to help

Canadians better understand the cyber threats they face online and the simple straightforward steps they can take to minimize those risks.

Further to this, last month Canada became the first country to sign onto the U.S.-based Stop, Think, Connect Campaign.

Under this agreement, our two nations will benefit from increased cooperation and more streamlined public messaging on how to stay safe online. And I made that announcement a few weeks ago then in Toronto.

Our government has taken significant steps to strengthen our federal government networks against cyber attacks. Canadians and Canadian businesses want to know that the private information they entrust to government will stay private. They want to feel comfortable doing their taxes, paying their bills and conducting their business online.

At the same time businesses and governments want to ensure critical infrastructure and services to Canada and industry are not disrupted in that sensitive commercial information, information that often translates into jobs for Canadians is fully protected.

Key among our efforts to strengthen our own networks was the introduction of Shared Services Canada, an initiative to streamline the hundred different e-mail systems over 300 data centres and the hundreds of telecommunication networks that provide voice and service, data services to over 300,000 users within the federal public service.

This is a significant step in making our government networks more secure, cost effective and reliable and allows us to improve our services to Canadians.

We have achieved a great deal but we are far from finished and that's what brings me to why we are here this morning. Today I am pleased to announce that we are committing an additional \$155 million over five years to reinforce federal government information technology infrastructure and to improve the detection of and response to evolving cyber threats.

This funding will allow us to further implement Canada's cyber security strategy and to accelerate efforts to achieve a secure, stable and resilient digital infrastructure.

This includes increasing the capacity of the Canadian Cyber Incident Response Centre, our National Computer Security Incident Response Team that is responsible for monitoring and providing advice on cyber threats as well as coordinating national response against cyber attacks. By securing our government's cyber systems, we can better protect the private information of Canadians and Canadian businesses. Today's funding announcement is another step forward in our efforts to strengthen digital networks that allow Canadians to safely work online and to keep our critical infrastructure and government networks resilient to cyber attacks.

Through activities like cyber security awareness month and the Get Cyber Safe Campaign, we are making sure that all Canadians understand the role they play in keeping our cyber space secure. We will have... we all have a stake in strengthening cyber security. We all have a role to play. When I think of the 50,000 to 60,000 individuals here both full time and part time, and all of those who are also taking computer security programs like those offered here at Algonquin College, I'm confident that the future of our cyber infrastructure is in very good hands.

I would encourage all of you to visit getcybersafe.ca and learn more about the threats and the ways to protect yourselves, your families and your businesses online. Thank you.

And now my colleague Shelley Glover will say something in French.

MIKE SPARLING: Thank you, Minister Toews, for this important announcement.

I will now invite... Excuse me. I would now like to invite Member of Parliament Shelley Glover to speak.

Shelley Glover is a member of the Parliament for St. Boniface in Winnipeg, Manitoba where she was first elected in 2008 and re-elected in 2011. In 2008, she was named Parliamentary Secretary for Official Languages and in 2010, Mrs. Glover was named Parliamentary Secretary for Indian Affairs and Northern Affairs Canada. In January 2011, Mrs. Glover was named Parliamentary Secretary to the Minister of Finance.

Until her election, Mrs. Glover served as a member of the Winnipeg Police Service for almost 19 years.

Please welcome MP Glover.

SHELLEY GLOVER (Parliamentary Secretary to the Minister of Finance, Member of Parliament for St. Boniface):

Thank you, Michael. I appreciate that.

Alors, bonjour et merci de vous rejoindre ici avec nous. Moi aussi, je veux dire un merci spécial au Collège Algonquin et à M. Brûlé qui est ici avec nous aujourd'hui, votre support est vraiment apprécié.

Alors ce matin on parle du cyber sécurité. Nous sommes au milieu du mois de la sensibilisation à la cyber sécurité, mois où nous encourageons les particuliers, les familles, le public et le secteur privé à se renseigner au sujet des cybers risques et à utiliser les outils et les ressources à leur disposition pour continuer à assurer leur propre sécurité en ligne.

Assurer la sécurité et la résilience des réseaux informatiques est l'un des défis les plus importants qui se posent pour notre gouvernement, les citoyens et nos alliés. Je peux vous assurer que le gouvernement est pleinement résolu à faire face à ce défi et à le surmonter.

Dans cette optique nous avons lancé la stratégie de cyber sécurité du Canada en 2010. Cette stratégie repose sur trois piliers : protéger les systèmes gouvernementaux, renforcer les partenariats avec différents secteurs et gouvernements au pays et à l'étranger, et renseigner les Canadiens sur les moyens à prendre pour réduire les risques liés à la vie au sein d'une société branchée.

Pour atteindre ces objectifs nous avons octroyé à l'époque un financement de 90 millions de dollars sur cinq ans et un financement permanent de 18 millions par année par la suite pour mettre en œuvre la stratégie de cyber sécurité.

Au cours des deux dernières années nous avons réalisé des progrès soutenus en vue d'atteindre nos objectifs. Par exemple, nous avons collaboré étroitement avec nos partenaires pour recenser les risques collectifs et trouver des solutions communes en vue d'assurer la résilience d'infrastructure essentielles comme les banques, les réseaux de distribution d'électricité, et le secteur des transports en cas de cyber attaque.

Nous avons également réalisé des progrès dans le cadre des efforts que nous déployons afin de communiquer aux Canadiens et aux entreprises canadiennes les risques associés à l'ère numérique.

L'an dernier nous avons lancé la campagne de sensibilisation du public intitulée Pensez cyber sécurité pour aider les Canadiens à mieux comprendre les cybers menaces en ligne et à les renseigner sur les mesures simples mais efficaces que chacun peut prendre pour atténuer les risques.

Le mois dernier le Canada est devenu le premier pays à conclure une entente afin de participer à la campagne américaine Stop, Think, Connect. Grâce à cette entente, nos deux pays collaboreront encore plus étroitement et harmoniseront les messages au public sur les moyens d'assurer la sécurité en ligne.

Notre gouvernement a pris d'importantes mesures pour renforcer les réseaux gouvernementaux fédéraux contre les cybers attaques. Les Canadiens et les entreprises canadiennes veulent être assurés que les renseignements confidentiels qu'ils communiquent au gouvernement resteront confidentiels. Ils veulent pouvoir sans crainte préparer leurs déclarations de l'impôt, payer leurs factures et mener leurs activités en ligne.

Parallèlement, les entreprises et les gouvernements ne veulent pas que les infrastructures de même que les services essentiels offerts aux Canadiens et à l'industrie soient perturbés. Ils tiennent à ce que les renseignements sensibles de nature commerciale, lesquels se traduisent souvent par des emplois pour les Canadiens, soient pleinement protégés.

La création de Services partagés Canada est l'une des principales mesures mises en place par le gouvernement pour renforcer les réseaux. Cette mesure a permis de rationaliser une centaine de systèmes de courriels différents, plus de 300 centres de données, et des centaines de réseaux qui fournissent des services de télécommunications, voix et données à plus de 300 000 utilisateurs de la fonction publique fédérale.

Il s'agit là d'un pas important en vue d'accroître la sécurité, la rentabilité et la fiabilité des réseaux du gouvernement et d'améliorer les services à la population canadienne.

Aujourd'hui je suis très heureuse de vous annoncer que le gouvernement accordera un montant additionnel de 155 millions de dollars sur cinq ans pour renforcer l'infrastructure de technologie de l'information du gouvernement fédéral ainsi que pour améliorer la détection et l'intervention des cybers menaces. Ces fonds nous aideront à concrétiser la stratégie de cyber sécurité du Canada et à accélérer nos efforts visant à assurer une infrastructure numérique sûre, stable et résiliente. Ces fonds permettront de renforcer les capacités du Centre canadien de réponse aux incidents

cybernétiques, ce qui aidera l'équipe nationale d'intervention en cas d'incidents informatiques chargés de surveiller les cybers menaces, de donner des conseils à ce sujet et de coordonner l'intervention nationale en cas de cyber attaque.

Le financement annoncé aujourd'hui constitue un pas de plus en vue de la création de réseaux numériques solides, ce qui permettra aux Canadiens de travailler en ligne en toute sécurité et contribuera à assurer la résilience des infrastructures essentielles et des réseaux du gouvernement en cas de cyber attaque.

Alors nous gagnons tous à renforcer la cyber sécurité et nous avons tous un rôle à jouer. Je vous remercie encore une fois.

MIKE SPARLING: Thank you, MP Glover.

This brings us now to the question-and-answer session. As I mentioned earlier, there is a microphone for your use. It's appreciated if you could begin your question by identifying yourself and naming the media outlet that you represent.

If you could initially keep your questions focused on the announcement it would be appreciated.

QUESTION: Hello. Good morning, Minister Toews. Now in the last recent years we've had a number of high profile security breaches, be it at the federal government, be it at let's say energy industry giant Telvent most recently when it came to hacking cyber security. How can you ensure that Canada's cyber, Canada has good cyber security and that Canadian information and the information held by Canadian companies is safe from these threats?

VIC TOEWS: Well, I think what we have to first of all understand is that this is a shared responsibility between government and the private sector and other organizations. The responsibility doesn't fall simply on government to address these issues. It would simply be impossible to do it without the very close cooperation of the private sector and indeed, of individuals.

What the government has been doing on a very proactive basis is recognizing that we have to not only coordinate activities inside government to ensure that we have a strong cyber security network, but also that we continue to work with the private sector in order to ensure that we are on top of all of these threats. Furthermore, this is also extended to working with our allies.

We constantly share information and assess security threats on a general nature and a specific nature with our ... with our allies and this money here today is ... essentially goes towards strengthening the federal infrastructure in terms of cyber security and one more step that we are taking to make sure that we are doing our part, both domestically and internationally.

QUESTION: As a follow up, U.S. Secretary of Defence Leon Panetta recently warned that the U.S. was at risk of a cyber Pearl Harbour. Do you have the same concerns for Canada?

VIC TOEWS: Well, I don't know whether he has overstated it, but certainly there is a risk to cyber security. Cyber security is something that every developed nation has to be worried about, given the nature of the technology and the rapid change of technology.

I know that in speaking to the officials here at Algonquin College, they have at any one day 60,000 devices that are being used. Only 8,000 of which are actually college devices. So they have to worry about the security of their own devices, those 8,000 being utilized by 50,000 other devices. So even at a very local level, this is a... this is something that the organization here is mindful of. We are certainly mindful of it as a national level and in working very closely with our international partners.

VALERIE BOYER (CBC): Good morning, Minister Toews. Valerie Boyer, from CBC. I'm just wondering, you said that you're working with your allies regarding cyber security.

VIC TOEWS: Right.

VALERIE BOYER: Yes, our allies last week in the United States came out and warned Canada against working with Huawei. Yet your government refuses to say whether it will block Huawei from bidding on a secure government network, the new secure government network that you talked about with Shared Services. Why is your government reluctant or afraid to talk about the Chinese at this stage?

VIC TOEWS: Well, I don't think we're afraid to talk about anything. I think there's an appropriate time to talk about things. Decisions have to be made and those decisions will be made in due course. At this time there is nothing to announce in that respect.

VALERIE BOYER: Yet, they came out pretty strong and it would be the forum to talk about it, no?

VIC TOEWS: Well, the Americans make their own decisions. We make our decisions. We certainly look at what the Americans are doing and consider that. But we will make decisions in the best interests of Canada.

VALERIE BOYER: It's also the Australians, the U.K., they've all, you know, raised concerns about Huawei. Why is Canada not raising concerns about Huawei when they're working on systems such as Bell, SaskTel, Wind Mobile, Telus?

VIC TOEWS: I can assure you that we're quite aware of any potential threats in respect of compromising our security and we will take appropriate action.

VALERIE BOYER: Put it this way: is it... how can you reassure Canadians that while they're working on ...

VIC TOEWS: Well...

VALERIE BOYER: No, hold on. While they're working on, you know, systems with Bell, that it's okay for them but you're considering something different for a secure government network?

VIC TOEWS: I don't know where you got that information from that we're considering something different?

VALERIE BOYER: Well, you haven't said whether you would block Huawei.

VIC TOEWS: Well, that doesn't mean that we're considering something different.

UNIDENTIFIED MALE SPEAKER: That's five questions.

VALERIE BOYER: Okay.

UNIDENTIFIED MALE SPEAKER: Sorry.

PAUL VIEIRA (Wall Street Journal): Paul Vieira, from the Wall Street Journal. Can you please, can you please tell us whether the Prime Minister's spokesman let it express that ... express some doubt about Huawei, whether Huawei would be allowed to bid on the Shared Services contract? Will it be barred from bidding on that contract? Is China the biggest cyber threat and is this money and this announcement related to concerns raised by the U.S. Congress and by the naval ... the naval case in Halifax?

VIC TOEWS: Thank you very much. All I can say is I'm not going to speak about any specific corporation at this time. I can assure you that this is not only, this announcement is not only in response to concerns that have been raised but part of our ongoing strategy that we announced over two years ago to ensure that Canadian infrastructure both in terms of government and the private sector is as best as we can possibly make it.

We recognize that we have to work in international context and need to keep our part of this network secure. And I think that our relationship with our allies is very close, very strong and we recognize these threats that are identified from time to time.

I'm not going to get into discussing any specific corporations or any countries.

TONDA MCCHARLES (Toronto Star): Tonda McCharles, Toronto Star. Minister Toews, can you tell me your views on this? This morning at a panel, the former CSIS operative Ray Boisvert, who's speaking at a MacDonald Laurier Institute Forum, he's talking... he among others were talking about whether the Canadian Investment Act has strong enough national security provisions to protect and do what you were just talking about this morning, protect Canada's infrastructure. Do you, as the Minister responsible for National Security, feel that that act needs boosting on that... in that area to protect against potential cyber threats, be it from China or other companies?

VIC TOEWS: Well, we're constantly looking at ways to upgrade our security system. That sometimes requires the input of money, technology, and indeed legislation. I think quite frankly that we have a very robust system, but we would be living in a fool's world if we think that we can establish any type of legislative framework or technological framework and have

that last indefinitely. This is a constant struggle because of the nature of technology and how quickly technology is evolving. So we are certainly looking at all possibilities when we look to further buttress our secure mechanisms.

TONDA MCCHARLES: And just as a follow up, in terms of the technological ability of Canada to protect either front door or back door attacks into its cyber network, The Economist reports that Britain does it through, they have their own standalone agency and that Canada does it through a shared agency with the U.S. And it's based in the U.S.

Is it not in your view advisable for Canada to have that kind of work done by a standalone agency here in Canada to check the switches, the comms gear, all the hardware, the software that Canadian companies and public sector departments may be buying? Should that work be done in Canada by a separate agency?

VIC TOEWS: Well, I'm not especially concerned about whether it's done by a separate organization or one that works very closely with our allies in an integrated fashion. I think to deal with these matters in isolation is... brings its own risks. So all I'm saying at this point is that we will continue to look at both issues regarding software and hardware in a way that best protects Canadians.

TONDA MCCHARLES: Thank you.

TOM PERRY (CBC): Hi, Minister Toews. I'm Tom Perry, with CBC. Why are you reluctant I guess to call out certain countries? I mean, we've got the Russians who are, you know, paying a Canadian naval officer. There's clearly been threats from China. The U.S. talks about Iran. Why don't you want to sort of call it a... any particular country that's a particular threat?

VIC TOEWS: I don't think that's going to serve any particular purpose for me calling out any particular country at this time. I'm certainly aware of where threats come from and we are constantly being briefed by our allies on developments in that respect. If there is a national security interest that requires the disclosure of some of these names and companies, that will be done in due course.

At this time I don't... I don't see simply making general allegations without talking about why I would be saying that.

TOM PERRY: But surely you must see some countries as being more of a threat than others?

VIC TOEWS: I think there's no question that some countries are more a threat than others.

TOM PERRY: Could you name them?

VIC TOEWS: I think it's best that I... best that I not. Look, I can just go to the CBC websites and the Globe and Mail websites and they've talked about many of these things. I'm not going to add fuel to the fire on this kind of stuff. It doesn't serve any purpose.

What I can assure you is that the government of Canada is very concerned about ... about cyber security and what I think during this month in October, cyber security month, we don't want Canadians to become complacent.

I'm very encouraged when I talk to people here at Algonquin to the extent to which they are mindful of the secure threats to their own security, whether that comes from a nation, whether that comes from simple criminal activities, this is the kind of sophistication I think that more of our non-government organizations and educational institutions as well as the private sector should demonstrate. It's a very difficult task but I'm confident that the work that people are doing in colleges like this, including training young people to assist us in this is ... is all very good in terms of securing our technology.

MODERATOR: We'll take one more question.

FRANÇOIS CORMIER (Radio Canada): Bonjour. François Cormier, de Radio-Canada. Si vous voulez pas nous nommer les pays auxquels vous avez ... desquels vous avez peur, à quelle menace est-ce que vous vous attendez? De quoi, de quel genre de menace est-ce que vous avez peur?

SHELLEY GLOVER: Je vous remercie pour la question et moi, je dirais que toutes les menaces sont importantes. Et c'est pour ça que le gouvernement du Canada, sous la direction du ministre Toews, a créé la stratégie de cyber sécurité depuis 2010. Et aujourd'hui on annonce plus d'argent pour évidemment améliorer la stratégie qui existe. Mais toutes les menaces, tous les risques sont pris très sérieusement et sous la direction de ministre Toews, on continue avec des améliorations pour protéger les données personnelles de tous les Canadiens et on va renforcer le système gouvernemental du gouvernement du Canada comme annoncé aujourd'hui.

FRANÇOIS CORMIER : Vous dites que vous le faites pour protéger les données. On a vu avec l'affaire de l'espion russe la semaine passée que ça semble assez facile de sortir des données, même des services de renseignements. Est-ce que vous faites quelque chose aussi pour les menaces de l'interne qui peuvent sortir ces données-là?

SHELLEY GLOVER : On a aussi fait plusieurs choses, comme on avait dit dans nos discours. Les Services partagés, on a créé des services partagés à l'intérieur du gouvernement du Canada pour rassurer les Canadiens et pour s'assurer à l'interne qu'on peut réduire les risques de cyber sécurité. Alors nous continuons comme a dit ministre Toews, de renforcer nos systèmes, d'améliorer les systèmes qu'on a, et d'assurer les Canadiens et les Canadiennes que leurs faits, leurs données, leurs dossiers privés, etc., sont une priorité pour le gouvernement du Canada.

MODERATOR : We have one more question on the (inaudible) .

RICHARD MADDEN (CTV): Hi, Minister. Richard Madden, with CTV. I just wanted to switch gears for a moment and talk about that shooting last night at the Canada - U.S. border in British Columbia. If you can give us an update as to your understanding of what happened; and secondly, as you know, border guards are expected to be on by 2016. There's been some concerns that perhaps that timeline should be sped up, so two questions. First of all, just an update of what you know what happened.

And secondly, should border guards get their weapons sooner, in light of this?

VIC TOEWS: Thank you very much. Yes, I was advised about that very unfortunate shooting some time yesterday afternoon. In fact, very shortly after that shooting had occurred. I still don't have all of the details and all I know at this point is that the officer appears to be in stable condition. Our thoughts and prayers go out to the officer and her family.

We... I'll of course await any other updates on that and I think it's in our interest to release that as quickly as possible, given the family nature. Of course we have to hold back some of that information until the family is fully briefed.

The RCMP is of course doing an investigation in this and therefore at this time it wouldn't be appropriate for me to say anything more about that particular shooting.

What I can also say about the arming of the border guards, as you know, our government made that commitment in 2006 when we came into government and it has been a very important process of strengthening the CBSA. The ... just a few days ago on Monday in fact, I made the announcement of the 57.5 million dollars facility at Rigaud. It's quite a facility in terms of assisting officers in acquiring the skill of using fire arms. It... the new facility is where all of the officers will be trained. We're trying to train approximately 1,000 officers a year in that respect, and that should bring us to about 2016.

It's always important to move as quickly as possible, but I want to ensure that officers who do carry fire arms are appropriately trained not simply in terms of the fire arm itself but the steps before lethal force is in fact used. And that facility, which we just opened and invested the 57.5 million dollars goes to a large extent to doing exactly that.

I would invite the members of the media to take... make arrangements with CBSA to tour that facility. I think it's quite a remarkable modern facility that is geared toward exactly that issue.

RICHARD MADDEN: So bottom line then you're not going to speed up the timeline for border guards to get their...

VIC TOEWS: Well, I think 1,000 officers a year given the expansion of the front line officers that we've done is ... is remarkably good progress and I think it's prudent. I'd be very reluctant to tell the agency to speed that up if it meant compromising the security training.

RICHARD MADDEN: Thank you.

VIC TOEWS: Thank you very much.

RICHARD MADDEN: So we don't know whether the shooter knew the border guard?

VIC TOEWS: No, I don't know any ... any details of those. Thank you very much, Mike.

MIKE SPARLING: It's a pleasure.

SHELLEY GLOVER: Thank you, Michael.

MIKE SPARLING: That concludes today's event. News releases on the announcement will be made available today on the Public Safety Canada website. Thank you for your time.

This transcription has been prepared by an outside supplier exclusively for departmental employees. Copyright laws prevent redistribution outside of Public Safety. Cette transcription a été préparée par un fournisseur externe exclusivement pour les employés du Ministère. Les lois sur le droit d'auteur en empêchent la diffusion à l'extérieur de la Sécurité publique.

Questions? Please contact us at PSMediaCentre/CentredesmediasdeSP@ps-sp.gc.ca.

Questions? Veuillez communiquer avec nous au PSMediaCentre/CentredesmediasdeSP@ps-sp.gc.ca.

s.15(1) - Subv

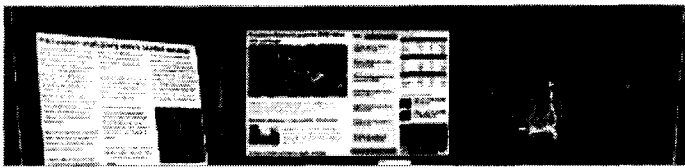
Dick, Robert

From: [redacted]@CSE-CST.GC.CA>
Sent: October-17-12 11:43 PM
To: [redacted] Dick, Robert; Matz, Mark; Martin.Proulx@ic.gc.ca; Maggie.Smith@ic.gc.ca
Subject: Fw: White House-ordered review found no evidence of Huawei spying: sources | Technology | Reuters

From: [redacted]
Sent: Wednesday, October 17, 2012 11:03 PM
To: [redacted]
Subject: White House-ordered review found no evidence of Huawei spying: sources | Technology | Reuters



BEGIN Content



NEWS PRO FOR IPAD

News and market data for business professionals

» [CLICK HERE TO DOWNLOAD](#)

Wed 17 Oct 2012 | 22:52 EDT

You are here: [Home](#) > [News](#) > [Technology](#) > [Article](#)

[HOME](#)

[NEWS](#)

[Top News](#)

[Business](#)

[Canada](#)

[Sports](#)

[Entertainment](#)

[Technology](#)

[WORLD INDICES](#)

[Products & Services](#)

[Support](#)

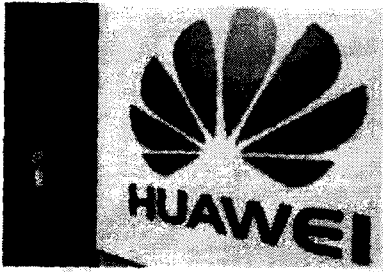
[About Thomson Reuters](#)

letrail

BEGIN: Section

White House-ordered review found no evidence of Huawei spying: sources

Wed Oct 17, 2012 10:43pm EDT



1 of 1 Full Size

By Joseph Menn

SAN FRANCISCO (Reuters) - A White House-ordered review of security risks posed by suppliers to U.S. telecommunications companies found no clear evidence that Huawei Technologies Ltd had spied for China, two people familiar with the probe told Reuters.

Instead, those leading the 18-month review concluded early this year that relying on Huawei, the world's second-largest maker of networking gear, was risky for other reasons, such as the presence of vulnerabilities that hackers could exploit.

These previously unreported findings support parts of a landmark U.S. congressional report last week that warned against allowing Chinese companies Huawei and ZTE Corp to supply critical telecom infrastructure.

But they may douse speculation that Huawei has been caught spying for China.

Some questions remain unanswered. For example, it is unclear if security vulnerabilities found in Huawei equipment were placed there deliberately. It is also not clear whether any critical new intelligence emerged after the inquiry ended.

"The White House has not conducted any classified inquiry that resulted in clearing any telecom equipment supplier," White House National Security Council spokeswoman Caitlin Hayden said. She also noted that Huawei had been barred from participating in an emergency network for first responders a year ago "due to U.S. government national security concerns."

At the White House's direction, according to people familiar with the matter, intelligence agencies and other departments conducted the largely classified inquiry, delving into reports of suspicious activity and asking detailed questions of nearly 1,000 telecom equipment buyers.

"We knew certain parts of government really wanted" evidence of active spying, said one of the people, who requested anonymity. "We would have found it if it were there." **Continued...**

[View article on single page](#)
[Previous Page](#) [1](#) | [2](#) | [3](#) | [4](#) [Next Page](#)

NEXT ARTICLE: Nokia to post loss ahead of make-or-break launches

MORE NEWS

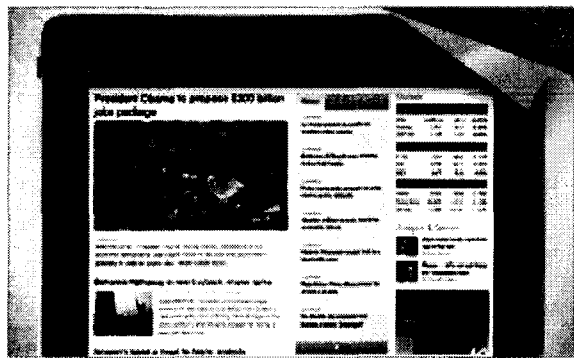
[Analysis: How long can Google's shares stay airborne?](#)
[Nokia to post loss ahead of make-or-break launches](#)

EBay posts strong results; cautious on holiday outlook
New app from Finland takes crime fighting to phone screen
More...

Ads by Google
What's This?

Scotiabank Corporate Card
Flexible, Scalable, Custom VisaCardPlatform for Your Corporation.
Scotiabank.com/ApplyToday
U.S. Market Will Collapse
The Dow is artificially inflated and this bubble is about to burst.
reports.money Morning.com/2013-crash
Market Crash on 10/31/12?
Analyst Dennis Slothower foresaw 2008 collapse; issues new warning
www.StealthStocksOnline.com
BYOD Guide from Forrester
View Free Forrester Report on BYOD corporate mobile device management
Absolute.com

START News Content Page Tags 'Text' | 'Picture' | 'Slideshow' | 'Video' ie. articleId ie. articleId ie. articleId ie. headline
for article ie. headline for article END News Content Page Tags



NEWS PRO FOR iPad

News and market data for business professionals

» CLICK HERE TO DOWNLOAD

END: Section

content

END Content BEGIN baseFooterHTML

ca.reuters.com: Help & Info | Contact Us

Thomson Reuters Corporate: Copyright | Disclaimer | Privacy Policy | Careers

International Editions :

Africa | Arabic | Argentina | Brazil | Canada | China | France | Germany | India | Italy | Japan | Latin America | Mexico | Russia
Spain | United Kingdom | United States

Thomson Reuters is the world's largest international multimedia news agency, providing investing news, world news, business news, technology news, headline news, small business news, news alerts, personal finance, stock market, and mutual funds information available on Reuters.com, video, mobile, and interactive television platforms. Thomson Reuters journalists are subject to an Editorial Handbook which requires fair presentation and disclosure of relevant interests.

END baseFooterHTML BEGIN baseFooter END baseFooter

Matz, Mark

From: Carta, John
Sent: October-11-12 5:29 PM
To: Matz, Mark; Binne, Christine; Bradley, Kees
Subject: FW: Media Scan - Foreign Acquisitions of Canadian Companies & Government Reviews - Updated October 11, 2012
Attachments: Media Scan - Foreign Acquisitions of Canadian Companies Government Reviews.doc

Just fyi, media scan of nexen and telecomm issues.

From: Brennan, Nicholas Adam
Sent: October-11-12 4:44 PM
To: MacDonald, Michael; Kagedan, Allan; Savoy, Jennifer; Kingsley, Michèle; Rathbone, Steven; Kwavnick, Andrea; Barrett, Andrew
Cc: Durand, Stéphanie; Swift, Andrew; Miller, Kevin; Carta, John; Paulson, Erika
Subject: Media Scan - Foreign Acquisitions of Canadian Companies & Government Reviews - Updated October 11, 2012

Media Scan
Foreign Acquisitions of Canadian Companies & Government Reviews
Updated: October 11, 2012

Print and Online Media

Ottawa strengthens investment rules

The federal government is strengthening its ability to ensure foreign corporations live up to undertakings about jobs and investment in Canada when they buy a Canadian business. The much-maligned Investment Canada Act is being changed to allow the federal government to hold security bonds from foreign companies asking permission to complete a corporate takeover in this country. The security would cover "payment of any penalties ordered by a court for a contravention" of undertakings promised as a condition of the foreign acquisition, according to an announcement by Industry Canada on Friday. [Toronto Star](#), A20 (2012-04-28)

Opaque rules scare away Chinese investment: think-tank

Canada is missing out on billions of investments from cash-rich China because of Ottawa's confusing foreign takeover rules, says a report from the Conference Board. The Ottawa-based think-tank makes clear it is a supporter of foreign investments, including from China, saying simply that economies that have access to global capital do better in terms of growth and job creation. But the Conference Board argues that once national security issues are resolved, China should be treated like any other foreign investor. As well, Canada should spell out its rules for investors so that they know the tests they need to pass. That's not the perception today, the report says. The Investment Act's "net benefit" rule, although seldom invoked to reject a takeover, is opaque, and as a result adds costs and political risk to what should be a business decision. The Conference Board says the Act should be amended along the Australian model with clearly defined rules about ownership and governance. It also calls for a national interest test and a national security test. [Vancouver Sun](#), C1 (2012-07-06)

Benefit rule tests China's patience

Chinese investors are being turned off from coming to Canada, the Conference Board of Canada said Thursday, blaming the federal government's protectionist policies on foreign direct investment. Canada's thriving resources sector has attracted accelerating levels of interest from the rising Asian superpower in recent years. If the country wants those funds to continue flowing, the Ottawa-based think-tank argues in a new report, the indefinable "net benefit" test must be rewritten. Most Chinese investors are state-owned by the Communist government in Beijing, Mr. Hodgson said, "so it is perfectly legitimate to ask whether they have been behaving as commercial players or as agents of Chinese foreign policy, and if it is the latter we have every reason to ask questions about our national security interest." [National Post](#), FP1 (2012-07-06)

Nexen officials talked "security" with CSIS Director Richard Fadden last April

An opinion piece states, "Just a few hours after news of the potential takeover of Alberta-based Nexen by the China National Offshore Oil Company went public, Industry Minister Christian Paradis issued a statement confirming that the proposal will undergo a full review under the Investment Canada Act, with approval to be granted only if he's "satisfied" that it would be "of net benefit to Canada... On what may or may not be a related note, reports filed with the lobbying commissioner, Nexen officials met with CSIS director Richard Fadden on April 12 to discuss unspecified "security" issues. Did the prospect of a deal with a state-owned Chinese energy company spur the sudden interest in foreign security? Given Fadden's controversial past comments on the risk of foreign influence and espionage, it would be fascinating -- if likely impossible -- to find out what he might have had to say on the matter if it came up during those discussions..." CBC News (2012-07-23)

China bets big on Canadian oil

China is taking a historic step toward its ambition to become a global resources powerhouse with a \$15.1-billion (U.S.) bid to buy Calgary-based oil producer Nexen Inc. The bid by state-backed CNOOC Ltd. is the largest by a Chinese firm for a foreign company, and confirms that Canada has become a proving ground for China's rise in the global economic order as it deploys some of its trillions of dollars in foreign reserves to secure strategic resource properties around the world. The deal builds on a string of previous acquisitions by Chinese firms in Canada's oil sands. It would be the second-largest deal ever in Canada's energy sector and, if approved, the sixth-largest takeover ever in Canada. Though it may test the Harper government's stance on foreign ownership, two years after it blocked a \$39-billion (Canadian) takeover offer for Potash Corp. of Saskatchewan Inc., there are strong indications that the deal will be approved. Globe and Mail, A1 (2012-07-24)

Lessons learned on takeovers

An editorial states, "Presumably, the Chinese government's pending purchase of Nexen, a major oil-and-gas producer based in Calgary, was in the works before **Premier Alison Redford** went to China mere weeks ago to drum up foreign investment... The deal requires a two-thirds majority vote of shareholders on Sept. 21 and with windfall profits in the offing, chances of acceptance seem high. That vote could become moot, however, if the deal doesn't pass muster during an Investment Canada Review conducted by Industry Minister Christian Paradis. CNOOC's president believes his company will prove a "net benefit" to Canada, which is at the crux of the review... Canadian government website lists factors influencing its review. They include the effect of the takeover on economic activity, productivity, technological development, competition and product innovation in Canada. Also, the government considers the degree of Canadian participation, compatibility with national industrial, economic and cultural policies and the contribution to Canada's ability to compete globally. Paradis will consult with industry and government officials, including Redford, as part of the review. Given that the premier and Prime Minister Stephen Harper have both travelled to China recently to embrace foreign investment, this deal should fit seamlessly into Alberta's vision of oilsands development... With those concessions in mind and governments in Alberta and Ottawa likely onside, the deal is likely to proceed." Edmonton Journal, A16 (2012-07-24)

Feds' probe into Chinese takeover could fall short

There are new fears the federal review process for foreign takeovers of Canadian companies falls apart on issues of national security. "There's no definition of what national security is," said Terry Glavin, a journalist and author who is a strong critic of China. While Paradis has said the deal has to comply with national security requirements, the Investment Canada Act doesn't specify what criteria must be met. Toronto Sun, 28 (2012-07-26)

CSIS said to be probing First Nations, China links

Canadian intelligence services appear to have probed financial links between First Nations groups and Chinese companies as scrutiny continues to mount on China's interest in this country's natural resources sector. This week, Chinese oil company CNOOC Ltd. announced a \$15-billion takeover bid for Calgary-based Nexen, a proposal that will have to pass scrutiny under the Canada Investment Act. The deal seems to be raising warning flags among politicians who fear the energy-hungry superpower's influence in Canada's oil patch. According to the CBC, Nexen's CEO also met with CSIS director Richard Fadden in April of this year to discuss security issues. National Post, A1 (2012-07-26)

Chinese have learned from mistakes made in Unocal bid

An opinion piece states, "Experts, pundits and netizens have all weighed in on the pros and cons of a \$15.1-billion US purchase of Nexen by Chinese National Offshore Oil Corp. There have been various analyses of China's intentions and the implications for Canada's future relations with China... Today's Canada, in contrast, has enthusiastically encouraged Chinese investment, making energy diversification to Asian market a strategic priority. With even the NDP not opposing the Nexen deal, the Canadian government approval process is unlikely to see the kind of hostility the CNOOC-Unocal deal encountered in the U.S. in 2005... The entire process will still require review by the federal government, and there are some uncertainties as to how the American and British governments will react..." National Post, FP11 (2012-07-26)

Foreign firms covet Canada's energy

This week's bid by a state-owned Chinese company for ownership of Calgary's Nexen Inc. underscores a growing Asian interest in companies involved in Canada's resource sector. The \$15-billion Nexen offer by the China National Offshore Oil Corporation (CNOOC) follows last month's proposed purchase of Progress Energy by Petronas, Malaysia's state-owned oil and gas company. Friday Petronas raised its bid from \$4.8 billion to \$5.16 billion to counter a competing offer. Both deals, which are subject to review under the Investment Canada Act, have implications for British Columbia because the targeted Canadian companies have large natural gas properties in B.C. Vancouver Sun, D3 (2012-07-28)

Slick road ahead

CNOOC's bid to buy Nexen should be the catalyst to a national debate on the direction of Canada-China relations, says the head of the Institute for Asian Research. The deal must still be approved by Industry Canada and CNOOC has said Nexen's head office will remain in Calgary. Calgary Sun, 24 (2012-07-29)

U.S. senator wants to halt Chinese takeover of Nexen

A U.S. senator wants his government to hold up a Chinese state-owned company's \$15.1-billion take-over of Calgary-based Nexen Inc. as a means to press China on its trade policy as the U.S. securities regulator also looks into allegations of insider trading surrounding the deal. Charles Schumer made his argument in a letter sent Friday to Treasury Secretary Timothy Geithner, who chairs the Committee on Foreign Investment in the United States, or CFIUS, a body that reviews foreign investments in U.S. companies. Calgary Herald, B3 (2012-07-30)

The 'petro-dictators' are among us

British Columbia Premier Christy Clark's belated but necessary assertion of B.C.'s bottom lines on the preposterously irresponsible \$5.6-billion Enbridge Inc. pipeline-and-tanker scheme has caused a great deal of windy indignation to erupt from Ottawa. Clark is hijacking the prospects for a national energy strategy, we're told. Even worse, what's at stake is the delicate balance of Confederation itself. Applying the Investment Canada Act's "national security" test to the CNOOC bid will set off a similar charade because that's what it's in-tended to be, too. When the Act was amended in 2009, the federal cabinet ruled out any definition of "national security" and explicitly rejected recommendations to conduct national security reviews according to "concrete," "objective" and "transparent" criteria. Just trust us, we know what's best. "This deal prompts great concern about the Chinese government's continued attempts to use its state-owned enterprises to acquire global energy resources." Who said that about CNOOC's Nexen bid? Was it Industry Minister Christian Paradis? NDP boss Tom Mulcair? Liberal helmsman Bob Rae? No. It was Drew Hamill, spokesman for U.S. Ottawa Citizen, A11 (2012-07-31)

The net losses test

The recent announcement that CNOOC, China's large multinational oil company, is bidding \$15.1-billion for Canadian energy producer Nexen brings into focus the Canadian government's vetting process. Under the Investment Canada Act, foreign takeovers of large Canadian companies must pass a "net benefit" test. That is, a foreign takeover of a Canadian company must convey additional economic benefits to the Canadian economy over and above those currently being realized under domestic ownership. National Post, FP13 (2012-08-01)

Lowe's offers to buy Canada's Rona for \$1.8B

Under the Investment Canada Act, Ottawa can review any foreign investment worth more than C\$330 million and can block a deal it thinks is not in Canada's best interests. It has exercised that prerogative only twice, most recently in 2010 when it said BHP Billiton's BHP.AX hostile bid for Canadian fertilizer maker Potash Corp POT.TO was not of net benefit. Telegraph-Journal, B2 (2012-08-03)

Canada will widen export markets

An opinion piece states, "...If approved, China National's acquisition of Calgary-based Nexen will be the largest foreign acquisition ever by a foreign company in Canada... The punditocracy in the U.S. and Canada worry that China's appetite for energy will interfere with our ability to utilize our own natural resources. Politicians on both sides of the 49th parallel will want to use the approval process to extract concessions on market access issues, never an easy proposition, especially with China... While we are the closest of allies, Canada and the United States have divergent energy interests. Canada is a net energy exporter. The United States is a net importer. Canada wants to diversify its markets, while the U.S. wants a reliable supply of imports. Canada will create incentives for its energy companies to diversify their customer base. The U.S. hadn't even considered the possibility of Chinese competition for Canadian oil..." The Record, A9 (2012-08-10)

Quebec parties vow to give local companies teeth of veto power over foreign takeovers

Quebec could become the first province to arm companies with a veto power over foreign takeovers, under a proposal with potential domino-effect implications for other parts of the country. Two political parties have now promised that if they win the Sept. 4 election they would allow a company's board of directors to repel a foreign acquisition if it's deemed to be against the interest of workers or the greater community. The latest such pledge from the Charest Liberals, whose

promise Monday resembles an earlier one from the Parti Quebecois, prompted one analyst to predict copycat moves elsewhere in Canada. The Guardian, A5 (2012-08-14)

CNOOC's bid for Nexen is a key move on China's global chess board

An opinion piece states, "...Moreover, might some of the people who come to Canada with CNOOC to run Nexen be operatives of Chinese security agencies with mandates to engage in political and economic espionage? At present, the RCMP, CSIS and CSEC do not have the resources to effectively counter any Chinese state challenge to Canada's security. If CNOOC moves in, Ottawa would have to rethink its priorities for domestic counter-intelligence, and make some hard budgetary decisions. In the end, if the Harper government decides that CNOOC's \$15.1-billion investment meets the "net benefit to Canada" test, we must be prepared for the implications of enhanced Chinese state presence in our economy." Toronto Star (2012-08-22)

CSIS warns of threats of foreign takeovers - Report comes as Tories review Chinese firm's bid for Nexen

As the federal government reviews a proposed takeover of a Calgary-based energy company by a state-owned Chinese oil giant, Canada's spy agency is warning such acquisitions can pose a threat to national security. The shareholders of petroleum producer Nexen overwhelmingly approved Thurs-day the \$15.1-billion US foreign takeover of the company by the China National Offshore Oil Corporation (CNOOC). The vote by Nexen share-holders came the same day the Canadian Security Intelligence Service warned in its latest annual report that some state-owned foreign companies are pursuing "opaque agendas" in Canada and that attempts to acquire control over strategic sectors of the Canadian economy pose a threat to national security. Ottawa Citizen

Ottawa awaits CNOOC proposal

Canada's industry minister says there is no deadline for his decision to approve or reject a Chinese state-owned company's multibillion-dollar bid for Calgary-based Nexen Inc. The deal faces a review by both Industry Minister Christian Paradis and the federal Competition Bureau. Paradis said his department is still waiting for a formal proposal from the Chinese company before a review can begin. "I was told that CNOOC was going to table a proposal soon so that is the state of the matter. After that this will be a reviewable transaction," Paradis told reporters in Calgary. Paradis said once the official proposal is received by his department, the offer will be scrutinized to make sure there is a "net benefit" for Canada. Edmonton Journal, B3 (2012-08-23)

A different kind of oil takeover

The proposed sale of Nexen Inc. to China National Offshore Oil Corporation (CNOOC) is being applauded by some as potentially opening the doors to Asian oil and gas markets and providing an assured source of capital for resource development. On the other hand, some regard it as yet another sale of Canadian petroleum resources to foreign interests that could have serious long-term implications for Canadian energy security. Vancouver Sun, A11 (2012-08-23)

Harper vows scrutiny of CNOOC-Nexen deal

Prime Minister Stephen Harper said Thursday that the federal government will closely evaluate a Chinese company's bid for the largest takeover of a Canadian energy company. In a sign that the government is acutely aware of public perception of China having a controlling stake in Canadian energy resources, Harper said not only will the deal be scrutinized for its net benefit to Canada under federal law, but also the long-term policy implications of allowing the deal to go through. The proposed takeover must still receive federal approval under the Investment Canada Act. According to the act, the foreign takeover of a Canadian company can only happen if the government considers it to be of net benefit to the Canadian economy. This new takeover bid has again run into political obstacles in the United States where Nexen has holdings, and in Canada where the deal must be reviewed by the Competition Bureau and under Investment Canada Act. Calgary Herald, A8 (2012-08-24)

Outcome of Nexen/CNOOC merger murky

The thick smoke signals sent by Prime Minister Stephen Harper in recent days on the proposed \$15.1-billion takeover of Nexen Inc. by CNOOC Ltd. are a warning to the market that a wide range of outcomes is possible. As the prime minister correctly noted, Canada's response to China's largest overseas takeover offer would have big implications for the economy. It would also mark a point-of-no-return for the Canadian oil and gas industry. The market has been betting on two outcomes: Most believe the deal will get federal approval because it fits known "net benefit" criteria under the **Investment Canada Act**. National Post, FP5 (2012-08-25)

CNOOC seeks Ottawa's approval for Nexen takeover

CNOOC Ltd. applied for Investment Canada approval for its proposed \$15.1-billion acquisition of Calgary-based Nexen Inc. on Wednesday, setting the clock ticking on a key decision for the federal government in its relations with China. The proposed deal has sparked concerns about growing investment by state-owned enterprises in the Canadian oil and gas sector, and Ottawa has pledged to take those concerns into account as it assesses the CNOOC-Nexen deal. Globe and Mail (2012-08-29)

CSIS warns against takeovers by state-owned firms

Opposition MPs believe when Canada's spy agency warns that foreign, state-owned companies taking over strategic sectors of the economy could pose a threat to national security, the government should listen. "When I read that CSIS is concerned about foreign companies and their investments in Canada raising security risks, I want to know more," said Liberal MP Geoff Regan. Calgary Sun (2012-09-22)

National security a priority in Nexen takeover, Fast says

The federal government sought to reassure Canadians Friday that national security will be a priority as it reviews a state-owned Chinese oil giant's proposed takeover of Calgary-based energy company Nexen. "The Investment Canada Act contains provisions to protect national security," Foreign Affairs Minister John Baird said in the House of Commons, "and the people of Canada can be sure that our government has done its job and makes good decisions in the interest of Canada." The comments come a day after Canada's spy agency warned that some state-owned foreign companies are pursuing "opaque agendas" in Canada as they attempt to acquire control over strategic sectors of the Canadian economy. The Ottawa Citizen (2012-09-22)

Nixing Nexen deal would be good for Canada's soul

David Kilgour was an Edmonton Member of Parliament for 27 years, and during that time served in both Conservative and Liberal governments, and finally became an independent MP on issues of principle. At present he is best known for investigative work with human rights lawyer David Matas, into China's appalling record of harvesting human organs from convicts and Falun Gong dissidents for sale to foreigners. Their book, *Bloody Harvest*, is a powerful indictment of the practice and is taken seriously in the UN and around the world. So, Kilgour is no fan of Beijing's policies or methods. Right now he's upset -justifiably so -at China's bid to buy Nexen, Inc., Canada's sixth largest oil company, for \$15 billion. The sale would reap a tidy profit for Nexen share holders, who overwhelmingly have voted to accept the offer. The prospective buyer is the China National Offshore Oil Corp (CNOOC), which means the Beijing government. Kilgour notes that it is now up to Prime Minister Stephen Harper to decide whether the sale represents a "net benefit" to Canada, and doesn't undermine or threaten "national security," as defined by the Investment Canada Act. Edmonton Sun (2012-09-23)

Ambassador promoting Nexen takeover

China's ambassador in Canada is on a charm offensive, appealing to the public to look favourably on Chinese investment in the oilpatch. Ambassador Zhang Junsai has given two recent media interviews coming just after Nexen shareholders overwhelmingly approved a generous takeover from Chinese state-owned CNOOC - a deal that still needs Ottawa's blessing to go ahead. In interviews with the *Globe and Mail* and CTV, Zhang said Chinese businesses are interested in Canada because the investment climate is stable and regulations are "mature." The Vancouver Sun (2012-09-24)

Nexen: la Chine en mode séduction

L'ambassadeur de la Chine au Canada tente présentement de séduire le public afin qu'il voie d'un oeil favorable les investissements chinois dans le secteur du pétrole canadien. Zhang Junsai a accordé deux entrevues dans la foulée de l'approbation par une majorité écrasante d'actionnaires de l'achat de Nexen, une entreprise de Calgary, par la société d'État chinoise China National Offshore Oil Corp. (CNOOC), une transaction à laquelle Ottawa doit toutefois donner son aval pour qu'elle devienne réalité. Le Devoir, A4 (2012-09-24)

Takeover of large resource companies by foreigners needs scrutiny

A senior Conservative cabinet minister says the federal government must apply a "rigorous lens" to takeovers of large Canadian resource companies by stateowned foreign enterprises, such as the CNOOC-Nexen deal. Immigration Minister Jason Kenney, one of Prime Minister Stephen Harper's top lieutenants and a longtime critic of China's human rights record, said Monday the \$15.1-billion takeover bid of Calgary-based energy producer Nexen by a Chinese state-owned oil giant will be reviewed by the government in an impartial and lawful way. The Conservative cabinet is currently examining whether to approve China National Offshore Oil Corporation's (CNOOC) takeover of Nexen under the Investment Canada Act, and whether the deal is of "net benefit" to Canada. The agreement was overwhelmingly approved last week by Nexen shareholders. Their blessing came the same day Canada's spy agency warned some state-owned foreign companies are pursuing "opaque agendas" in Canada as they attempt to acquire control over strategic sectors of the Canadian economy. Montreal Gazette, A17 (2012-09-25)

Huge potential in China deal

An opinion piece states, "Four in 10 Canadians see China as a threat, if opinion polls are to be believed. Seven in 10 oppose approval of the \$15.1-billion bid by China's CNOOC for Calgary oil company, Nexen... This was clearly the fear of China's ambassador in Ottawa, Zhang Junsai, who is urging that the deal be judged solely on business terms... But for the Harper government to bow to its baser political instincts would be to put short-term political self-interest ahead of the long-term prosperity of the country. There appear to be no reasons of any substance to blow up the transaction." National Post, A4 (2012-09-25)

Nexen debate should be all about security

An opinion piece states, "Ottawa's forthcoming decision whether to approve the take-over of Nexen by the Chinese National Offshore Oil Corporation (CNOOC) will set an important precedent in this country. The decision will also reverberate globally, not least because this is the largest Chinese SOE acquisition anywhere in the world. Almost all of the Canadian commentary to date has centred on the economics and business merits of the acquisition... These are important questions to be sure, but they fail to address the fundamental issue, namely, could CNOOC's acquisition of Nexen be inimical to Canada's foreign policy and national security?" Ottawa Citizen, A13 (2012-09-25)

Ottawa should quash Chinese bid for Nexen

A letter states, "The Chinese National Off-shore Oil Company's bid to take over Nexen, one of Canada's largest energy companies, is against our national interests and should be quashed... Even our national spy agency, CSIS, is raising concerns about such takeovers." Vancouver Sun, A10 (2012-09-25)

CSIS report raises a question to be asked about the CNOOC-Nexen deal

An editorial states, "Foreign espionage is surely not a net benefit to Canada. That phrase is the essential criterion for the approval of takeovers by foreign companies, under the Investment Canada Act. It is striking that the most recent annual report of the Canadian Security Intelligence Service, released last Thursday, implicitly draws a connection between foreign-investment policy and security and intelligence a point that decision-makers and policy-makers need to bear in mind. In particular, CSIS's report says that certain state-owned enterprises and private firms with close ties to their home governments have pursued opaque agendas or received clandestine intelligence support for their pursuits here." Globe and Mail (2012-09-25)

China eyes pipeline tech

Canada's spy agency, CSIS, has warned that foreign state-owned companies that buy up significant portions of Canada's oilpatch threaten the sovereignty and security of this country by gaining access to sensitive technology and strategic resources. Chinese oil companies have invested billions of dollars into the Alberta oilpatch, and one of them is seeking to purchase Calgary-based Nexen Inc. Edmonton Sun, 22 (2012-09-26)

Asking how close are the ties to the state

An editorial states, Foreign espionage is surely not a "net benefit to Canada." That phrase is the essential criterion for the approval of takeovers by foreign companies, under the Investment Canada Act. It is striking that the most recent annual report of the Canadian Security Intelligence Service, released last Thursday, implicitly draws a connection between foreign-investment policy and security and intelligence - a point that decision-makers and policy-makers need to bear in mind. In particular, CSIS's report says that "certain state-owned enterprises and private firms with close ties to their home governments have pursued opaque agendas or received clandestine intelligence support for their pursuits here." To be fair, it must be said that the International Energy Agency published a paper last year, which said that CNOOC Ltd. and two other state-owned Chinese oil companies are not "state-run" but "state-invested." CNOOC's application to Investment Canada for its purchase of the Canadian oil company Nexen Inc. is pending. Globe and Mail, A18 (2012-09-26)

Big questions over Chinese bid for Nexen

A opinion piece states, The Chinese state company CNOOC's \$15-billion bid for Nexen, a major Canadian oil and gas company, raises major issues about the future of Canada's economy. Red Deer Advocate, A4 (2012-09-26)

DBRS: Net benefits of Nexen takeover somewhat mixed'

The net benefit of a \$15.1-billion takeover of Nexen Inc. (TSX:NXY) by a Chinese company is "somewhat mixed" because the deal offers only limited direct financial benefits but may help trade relations, says the DBRS debt-rating agency. Alberta Tory MP Ted Menzies has said he's been getting a lot of negative feedback from constituents about the takeover by a state-owned Chinese firm. The Canadian Security Intelligence Service report for 2010-11 also warned last week that when companies with links to foreign intelligence agencies or hostile governments try to acquire control over strategic sectors of the Canadian economy, it can represent a threat. Canadian Press (link to CTV News) (2012-09-26)

Editorial: The Nexen test

An editorial states Generally speaking, foreign investment in Canada is a good thing. That holds true in the oilpatch just as in other sectors of the economy. If the China National Offshore Oil Corporation wants to pay a premium to take over Canadian-based oil and gas company Nexen Inc., that's good for the shareholders and could have all kinds of knock-on benefits in Canada. That said, critics of the deal are right to point out that CNOOC is not just a company like any other. It's owned by the Chinese state, which happens to be run by communists who do not respect human rights within China or outside it, and whose foreign policy on crucial security matters often runs directly counter to Canada's. If a deal poses a national security threat, the Canadian government should nix it. Ottawa Citizen (2012-09-26)

The Nexen test

An editorial states, "...If a deal poses a national security threat, the Canadian government should nix it. But the law that governs foreign take-overs has left the definition of national security so loose that no one really knows whether Chinese investment in the oil-patch qualifies Ottawa Citizen, A12 (2012-09-27)

Energy CNOOC may need to boost spending to secure Nexen

CNOOC Ltd. may need to boost investments in Canada to secure government approval for its \$15.1 billion takeover of Nexen Inc., according to two people familiar with the Beijing-based company's plans. Financial Post (2012-09-28)

Private Members' Biz Watch: Is the CNOOC/Nexen merger the next "human being" debate? A blog post states, Inspired, it seems, by his former caucus colleague's ill-fated attempt at special committee creation, Independent MP Peter Goldring has adopted the same procedural strategy -- and, indeed, much of the same wording -- in crafting a pitch, in the form of a private members' motion, for full parliamentary review of the controversial CNOOC/Nexen takeover bid... Inside Politics Blog CBC News (2012-09-28)

Foreign takeover map pledged

It's guiding a huge chunk of foreign investment in Canada and the government's broader economic goals, but critics assail it for being too vague and lacking necessary safeguards to protect the economy and national security. The Investment Canada Act is steering the federal government's decisions on major foreign takeovers that could have huge ramifications on the national economy - including China National Offshore Oil Corp.'s \$15.1-billion takeover bid of Calgary-based petroleum producer Nexen. The Gazette, C10 (2012-09-29)

Takeovers need clear rules

An editorial states, "If a deal poses a national security threat, the Canadian government should nix it. But the law that governs foreign takeovers has left the definition of national security so loose that no one really knows whether Chinese investment in the oilpatch qualifies. "While the vast majority of foreign investment in Canada is carried out in an open and transparent manner," the Canadian Security Intelligence Service warned in its 2010-2011 report, "certain state-owned enterprises (SOEs) and private firms with close ties to their home governments have pursued opaque agendas or received clan-destine intelligence support for their pursuits here." ..." Vancouver Sun, D3 (2012-09-29)

Canada can't be naive about China

An opinion piece states, "Canadians should be upset and insulted that China's biggest grab for control of a major resource company anywhere in the world is the \$15-billion Nexen Inc. deal. Clearly, China is testing whether this Boy Scout of a nation will roll over. This is just one of many reasons why Canada must reject this takeover. Another is a warning by CSIS against foreign buyouts of strategic assets, and another is that polls show public opposition to the deal. National Post, FP2 (2012-09-29)

Time to prove Canada open for business

An opinion piece states, "...Last week CSIS reported again that Chinese industrial espionage is a serious threat. This is nothing new; CSIS has been issuing this warning for a decade. Will rejecting a needed investment change this behaviour? Not in the slightest. The cure for illegal behaviour is law enforcement, not market restrictions. CNOOC is not proposing to buy a \$15-billion oil company to better spy on industrial rivals! ..." National Post, FP17 (2012-09-29)

CNOOC-Nexen deal not worth taking a foreign-investment stand on

An opinion piece states, "As national and international debate over the CNOOC-Nexen deal heats up it becomes more and more obvious that Ottawa should just wave a wand of approval over the \$15-billion takeover. China, which owns CNOOC Ltd., is a growing global threat, politically and economically, but that's no reason for Ottawa to rush into a new interventionist foreign-investment stance over what is essentially a marginal transaction for a company — Nexen Inc. — that is of no strategic importance.." Financial Post (2012-09-29)

China's big play

A crossroads in Canada's relations with China is fast approaching, with Prime Minister Stephen Harper's government on the verge of a foreign investment decision that will spell out the risks Ottawa is willing to take to tap into Asia's economic juggernaut. As political and commercial stakes mount by the day, federal officials are secretly laying the groundwork for a yes-or-no decision on the \$15.1-billion play by China's state-controlled oil giant for a precedent-setting role in Canada's oil sands development. Toronto Star, IN4 (2012-09-30)

Nexen deal reveals clash of cultures

An editorial piece states, "As the rhetoric intensifies over the purchase of Calgary oil and gas producer Nexen by a Chinese state oil company and issues from free trade to human rights are raised as bargaining chips to approve the deal it speaks to a clash of cultures in the changing geopolitical reality globally..." Calgary Herald (2012-09-30)

Nexen deal beneficial, Redford says

Premier Alison Redford says her government believes "there's a lot of benefit for Alberta and Canada" in the proposed sale of Nexen Inc. to a state-owned Chinese firm. In an interview with the Herald, Redford said her office has advised the Harper government in its review of China National Offshore Oil Corp.'s contentious \$15.1 billion US bid for the Calgary based petroleum producer. Calgary Herald, A4 (2012-10-01)

There's good reason to be wary of China

An opinion piece states, "...Clearly, Canada's CEOs never met a Chinese business opportunity they did not want to embrace. And yet these titans of our business world weren't listening to what was being said at their own conference...Is this the same China whose ambassador to Canada threatened us recently that if we didn't approve of a Chinese state-owned company's bid for Nexen, a Canadian energy company, that we "wouldn't be able to do business together?" The same China that ruthlessly and insouciantly throws peasants off land they have been farming for generations with little or no compensation because their presence has become inconvenient for Communist Party apparatchiks?...China respects strength and resolve. So should we." Calgary Herald, A11 (2012-10-01)

Alberta leader backs Nexen deal, executives less sure

The premier of the oil-rich province of Alberta said she sees benefits from the proposed \$15.1 billion sale of Canadian oil producer Nexen Inc to a Chinese state-owned company, but a survey published on Monday showed half the country's executives would oppose a no-strings deal. Reuters UK; Financial Post (2012-10-01)

Best to show strength in dealings with China

An editorial states, "East is east and west is west, wrote Rudyard Kipling, and never the twain shall meet. It's plain dear old Rudyard was never exposed to the Canadian business class hot on the scent of Chinese profits...Is this the same China whose ambassador to Canada threatened recently that if we didn't approve of a Chinese state-owned company's bid for Nexen, a Canadian energy company, that we "wouldn't be able to do business together?" The same China that ruthlessly and insouciantly throws peasants off land they have been farming for generations with little or no compensation because their presence has become inconvenient for Communist Party apparatchiks?..." The Province, A16 (2012-10-02)

Don't rubber-stamp CNOOC-Nexen deal, Canada opposition urges

Canada's main opposition party urged the Conservative government on Tuesday not to rubber-stamp a bid by China's CNOOC Ltd to buy oil company Nexen Inc without public consultations, saying opinion had hardened against the deal. Reuters; CTV News (2012-10-02)

No Need for Manners in Nexen Deal, Canada

An opinion piece states, "Canadians should be upset and insulted that China's biggest grab for control of a major resource company anywhere in the world is the \$15-billion Nexen deal. Clearly, China is testing whether this Boy Scout of a nation will roll over. This is just one of many reasons why Canada must reject this takeover. Another is a warning by CSIS against foreign buyouts of strategic assets, and yet another is that polls show public opposition to the deal..." Huffington Post (2012-10-02)

Takeover process entirely arbitrary

An opinion piece states, "As a general rule, there is no particular reason to treat a foreign takeover any differently than a domestic one. When Acme Ballbearings of Guelph, Ont., makes a bid for Ballbearings R Us of Brandon, Man., no government agency is assigned to ponder whether the transaction is of "net benefit" to Canada...Still, if that's where we're drawing the line now - no longer opposed to foreign takeovers as such, but only to those emanating from repressive regimes - that's progress in itself. The prime minister has promised a broader redrafting of foreign investment rules in the wake of the Nexen decision. If rejecting or modifying CNOOC's bid provided cover for a general opening of our borders, that would be a pretty good trade." Ottawa Citizen (2012-10-02)

Approving Nexen deal would be treason, Canada MP says

Canada's Conservative government will commit treason if it approves a \$15.1 billion bid by China's state-owned CNOOC Ltd to buy Canadian oil company Nexen Inc, opposition Member of Parliament Pat Martin said on Tuesday. Martin was speaking during debate in the House of Commons on a motion by his left-leaning New Democratic Party demanding that the government hold public consultations before deciding whether to approve the deal. Reuters; Canadian Press (2012-10-02)

Hearings on Nexen illegal, Tory says

The federal government would be breaking the law if it held public hearings on the CNOOC-Nexen deal as the opposition demands, Treasury Board President Tony Clement says. The federal NDP, which will announce this week whether it supports CNOOC's take-over of Nexen, wants public hearings into foreign ownership in the Canadian energy sector by state-owned enterprises such as Beijing-based CNOOC. Christian Paradis stressed that the government has made several changes to the Investment Canada Act over the past few years, including new guidelines for state-owned

enterprises, additional national security provisions and more ability to communicate decisions to the public. Ottawa Citizen, A4 (StarPhoenix; Edmonton Journal; Calgary Herald); Globe and Mail (2012-10-03)

There are bigger threats than China's purchase of Nexen

An editorial piece states, "If Canada's potential tensions with China are confined to matters such as the purchase of Nexen by the Chinese National Offshore Oil Company, CNOOC, we are the envy of the world. To begin with, the CNOOC purchase is as close to a no-brainer as you can get. CSIS, Canada's counterspy bureaucracy, trying to prove it is still useful, muttered imprecations about Chinese spies. But Nexen, like CNOOC, is an exploration company." Calgary Herald, A14 (2012-10-03)

Le NPD réclame des audiences publiques

Le Nouveau Parti démocratique (NPD) a une fois de plus pressé le gouvernement Harper de tenir des audiences publiques sur la vente de la société pétrolière Nexen à des intérêts chinois, hier, estimant que l'opinion publique canadienne se cristallise contre la transaction. Le gouvernement Harper doit bientôt décider s'il donne son aval à la transaction de 15 milliards de dollars qui permettrait à l'entreprise étatique China National Offshore Oil Company (CNOOC) d'acquérir la société de Calgary. La Presse, S6 (Le Quotidien) (2012-10-03)

Redford sets terms for Nexen bid approval

Premier Alison Redford has set out specific conditions for Alberta's approval of the sale of Calgary-based petroleum producer Nexen to a company controlled by China's state-owned national offshore oil corporation, but she remains supportive of the deal. The premier has asked the federal government to impose stricter employment and management conditions on CNOOC's \$15.1-billion takeover of Nexen, including a guarantee that half of the corporation's management and board is Canadian, according to a report from Bloomberg. Calgary Herald, A6 (2012-10-04)

Nexen deal difficult from policy angle: PM

Prime Minister Stephen Harper says CNOOC's takeover bid for Canadian energy company Nexen "raises a range of difficult policy questions" for his government as it decides whether to approve the \$15-billion transaction. The Conservative cabinet is currently reviewing, under the Investment Canada Act, whether China National Offshore Oil Corporation's (CNOOC) \$15.1-billion takeover of Calgary-based petroleum producer Nexen is of "net benefit" to Canada. Edmonton Journal, A8 (Calgary Herald, Times & Transcript); Toronto Sun (2012-10-05)

Nexen: Are we naive or visionary?

An opinion piece states, the NDP lost a vote in the Commons which would have forced the Conservatives to hold public hearings into the takeover bid. Julian acknowledged national security concerns, but conceded there are more questions than answers. He referred to a previous statement from the company in which it referred to itself as a "mobile national territory," hardly the definition of a Crown corporation that would be familiar to Canadians. In Canada, national security concerns posed by foreign takeovers are left to the industry minister and the cabinet to arbitrate. Hamilton Spectator, A19 (2012-10-05)

Chinese wall needed

An editorial states, China National Offshore Oil Corp.'s proposal to acquire Nexen for \$15-billion should be approved - with specific conditions attached that address the underlying concerns of citizens and business leaders. In addition, the minister should commit to modernizing the Investment Canada Act in the near future. By creating the right policy framework around the Nexen deal, Canada would finally clarify for investors at home and around the globe what they can expect when making a major capital investment in the Canadian economy. National Post, FP11 (2012-10-05)

Canada 'at risk' from Chinese firm, U.S. warns - Head of U.S. committee says ordinary Canadians should be worried about Huawei

The head of the powerful U.S. Intelligence Committee is urging Canadian companies not to do business with the Chinese telecommunications giant Huawei as a matter of national security. In a scathing report released Monday in Washington, the congressional committee branded Huawei a threat to U.S. national security, and urged American telecommunications companies using the Chinese firm to find other vendors. But in an exclusive interview with CBC News, committee chairman Mike Rogers warns that Canada is equally at risk. CBC News (2012-10-09)

China syndrome: is sinophobia driving dread of Nexen takeover?

An opinion piece states What's so scary about the CNOOC-Nexen deal? Is it the litany of human rights abuses by CNOOC's ultimate owner the Chinese government? Is it the suspicions of espionage and intellectual property theft that swirl around most big-ticket Chinese industries? Is it the fact CNOOC is a state-owned enterprise (SOE)? Pinpointing exactly what irks Canadians about CNOOC's takeover of Nexen can be baffling. As for espionage, most news reports offer a brief quote from CSIS director Richard Fadden in 2010 regarding his suspicions about Chinese spies and a couple of ultimately inconclusive examples. iPolitics.ca (2012-10-09)

Bell not worried despite U.S. concerns on Huawei

A U.S. Congressional committee report attacking two Chinese telecom network equipment makers raises questions of whether Canadian governments and enterprises should feel their data is secure here. The finding raises concern in this country because Huawei is a major equipment supplier to BCE Inc.'s Bell Canada, Telus Corp., Videotron and SaskTel. ZTE is a supplier to Public Mobile. This morning, a Bell spokesman issued a statement saying the telco has no worries. Bell networks are secure, the statement said. Indeed our high levels of security are a primary reason most Canadian governments and businesses choose to rely on Bell network services. IT World Canada (2012-10-09)

Huawei faces exclusion from planned Canada government network

Canada indicated strongly today it would exclude Chinese telecom equipment giant Huawei Technologies Co Ltd from helping to build a secure Canadian government communications network because of possible security risks. Reuters (2012-10-09)

McGuinty sticks up for Chinese firm Huawei accused of spying

Premier Dalton McGuinty has come to the defence of Huawei Canada, a unit of China's biggest telecom equipment maker that is facing U.S. accusations of espionage. Toronto Star (2012-10-09)

ON Tories call on McGuinty gov't to review Huawei grant amid security concerns

The Ontario Tories are calling on the Dalton McGuinty government to review a \$6.5-million provincial grant to a China-owned company deemed a national security threat by the US House of Representatives Intelligence Committee. Sun News Network (2012-10-09)

NDP says Huawei concerns in U.S. a wake up call to Canada on Nexen

A U.S. congressional panel's scathing criticism of China technology firms should give the Harper government cause to reject the proposed Chinese takeover of Alberta oil company Nexen, the opposition NDP said Tuesday. Canadian Press (2012-10-09)

Cisco Bashes Huawei, Cuts Ties With ZTE

Networking giant Cisco is making it clear that it wants no part of doing business with ZTE and Huawei, two Chinese technology companies that have come under fire in the United States in recent months for their dealings with Iran and alleged ties to elements within the Chinese government who pose a threat to U.S. cybersecurity. PC MAG (2012-10-09)

Telecom networks at risk, experts warn

If Chinese telecommunications firms are allowed to provide components for Canadian networks, the rising Communist super-power could compromise this country's security. The warning comes from the U.S. congressional intelligence committee that labelled Huawei Technologies Co. and ZTE Corp. as national security threats. National Post, FP1, Ottawa Sun (2012-10-10)

Ottawa mum on which firms getting contracts

The Harper government is invoking a "national security exemption" as it hires firms to help build a secure communications network for Canada. However, it is refusing to say if that exemption - which allows the government to discriminate against companies and nations considered security risks - will be used to block the Chinese company, Huawei Technologies Co. Ltd, from getting a contract. National Post, A8; Globe and Mail; Ottawa Citizen; Montreal Gazette (2012-10-10)

Sasktel defends relationship

SaskTel's president is downplaying security concerns about Chinese telecom equipment giant Huawei Technologies Co. Ltd. after the Canadian government hinted strongly it would exclude the company from helping to build a secure government communications network. Leader-Post, A1 (2012-10-10)

Tories ask for review of deal

The Ontario Tories are calling on the Dalton McGuinty government to review a \$6.5-million provincial grant to a China-owned company deemed a national security threat by the U.S. House of Representatives Intelligence Committee. The grant to Huawei, based in Markham, Ont., has meant an employment boost for the province, McGuinty said. London Free Press, B3; Toronto Sun; Toronto Star (2012-10-10)

Huawei warning another reason to nix Nexen deal, says NDP

The opposition New Democrats say a U.S. congressional panel's scathing criticism of China technology firms should give the Harper government cause to reject the proposed Chinese takeover of Alberta oil company Nexen. Industry Canada could announce as early as this week the result of its review of the \$15.1-billion bid by the state-owned China National Offshore Oil Co. for Calgary-based Nexen Inc. Chronicle Herald, C2 (2012-10-10)

Oilsands stake for Canadians

An opinion piece states "Premier Alison Redford's pursuit of foreign investment, in particular from China, works against any Canadian Energy Strategy, which is rapidly becoming an oxymoron. Chasing after the seductive, easy money from China does not serve Canada's national security." Edmonton Journal, A20 (2012-10-10)

U.S. fears Huawei's equipment

Washington's real concern with Huawei--and the reason a U.S. Congress intelligence committee recommended it be banned from U.S. markets -- is a fear that the Chinese telecom giant could be churning out equipment riddled with security "back doors." The switches and routers Huawei produces, warns the intelligence committee's Monday report, might arrive in the United States with hidden code that would allow the Chinese military to control the devices from afar. National Post, A7 (2012-10-10)

The trouble with Huawei

Here at Maclean's, we appreciate the written word. And we appreciate you, the reader. We are always looking for ways to create a better user experience for you and wanted to try out a new functionality that provides you with a reading experience in which the words and fonts take centre stage. We believe you'll appreciate the clean, white layout as you read our feature articles. But we don't want to force it on you and it's completely optional. Click "View in Clean Reading Mode" on any article if you want to try it out. Once there, you can click "Go back to regular view" at the top or bottom of the article to return to the regular layout. After seeming not particularly concerned five months ago about Huawei's dealing with Canadian firms, the Prime Minister is now maybe concerned about the possibility of the Chinese telecommunications company dealing with the federal government. Maclean's (2012-10-10)

Canada won't say if security exemption shuts China's Huawei out of contract

The federal government is invoking a national security exemption as it hires firms to help build a secure communications network for Canada. However, it refuses to say if that exemption which allows the government to discriminate against companies and nations considered security risks will be used to block the Chinese company, Huawei Technologies Co Ltd, from getting a contract. StarPhoenix

Huawei faces exclusion from planned Canada government network

Canada indicated strongly on Tuesday it would exclude Chinese telecom equipment giant Huawei Technologies Co Ltd from helping to build a secure Canadian government communications network because of possible security risks. Meanwhile, the European Commission has delayed a trade case against Huawei and another Chinese telecom equipment maker, ZTE Corp, easing tensions between the European Union and China, its second-biggest trading partner. BDNews24

Huawei corruption allegations given to FBI

The U.S. intelligence committee has turned over to the FBI evidence of possible bribery and corruption by Chinese telecommunications firm Huawei, CBC News has learned. The U.S. intelligence committee released a scathing report Monday about the security risks of dealing with China's two leading telecommunications firms, Huawei and ZTE. CBC News (2012-10-10)

Fear not China

An opinion piece states, Over the past few months, a number of public figures have pronounced themselves on CNOOC's purchase of Nexen Inc. Many have sounded an alarm about China and the peculiar threat of state-owned firms. Even Canada had a flagship state-owned oil firm until quite recently - PetroCan. But now the hue and cry goes that Petro can but China can't. China is uniquely opaque, apparently. Have you been to Saudi Arabia lately? These state-owned companies are under the thumb of the Chinese Communist Party. Inconveniently, yes, they are. I happen to be an expert on the CCP, and these days the CCP actually wants those firms to be active market players run on commercial terms National Post, FP11 (2012-10-11)

A seat in front row for CNOOC

An opinion piece states, As the debate intensifies over whether Ottawa should open the floodgates to Chinese investment in the Canadian oil and gas sector, some argue that Nex-en Inc., the Calgary-based oil and gas producer targeted by CNOOC Ltd., isn't worth protecting because its assets are predominantly based overseas. CNOOC is paying big money to own it, but has it earned it and should it be for sale? National Post, FP1 (2012-10-11)

Complaints against Huawei, ZTE probed

A U.S. congressional report that urged American companies to stop doing business with Chinese telecom equipment makers Huawei and ZTE has triggered a fresh wave of complaints against the firms, opening a second phase to the panel's investigation. Adding to Huawei's problems, Canada indicated on Tuesday that it could exclude Huawei from firms

allowed to build a secure Canadian government communications network, citing possible security risks. Ottawa Citizen, A5 (2012-10-11)

The challenge with China

Yes, China should be treated differently. That's the consensus view of security experts examining the dealings of both Chinese telecommunications technology company Huawei, which has been vying for federal government communications work, and the bid by China National Offshore Oil Corporation (CNOOC) to take over an Alberta oil company. The lack of transparency in China's business methods means corporate espionage is always a concern for both Canadian firms and legislators, they say. Ottawa Citizen, A5 (2012-10-11)

Risk to national security

A letter to the editor states, Using any foreign company, except maybe one of our closest allies, to build Canada's secure communication network would be highly risky to our national security.

Using China's Huawei in this capacity would plain and simply be foolhardy. The takeover of Nexen poses very little national security concern, especially since most Nexen assets are outside Canada. Ottawa Citizen, A12 (2012-10-11)

Wall defends ties to Chinese company

Premier Brad Wall is defending SaskTel's relationship with controversial Chinese company Huawei Technologies Co. Ltd., about which security concerns continue to be raised in other parts of the world. A U.S. House Intelligence Committee report this week said Beijing could use equipment made by Huawei, the world's second-largest manufacturer of routers and other telecom gear, and ZTE Corp, the fifth largest, to engage in espionage and endanger vital systems. The panel urged network providers to seek other vendors. StarPhoenix, A3(2012-10-11)

Chinese firm says it's no threat

It's business as usual for Huawei in Canada despite allegations the telecom giant's technology is susceptible to being used by the Chinese government for cyber-espionage. "We remain committed to Canada," spokesman Scott Bradley said on Wednesday. "We've been operating (in Canada) since 2008 without issue." Huawei sells mobile technology to companies that include Bell Canada, Telus, Wind Mobile, Sasktel and Ice Wireless, but has come under intense scrutiny following a recent scathing report from a U.S. congressional committee outlining cyber-espionage concerns with Huawei and another global telecom company, ZTE. Ottawa Sun, 12 (2012-10-11)

Harper in pickle over China telecoms

An opinion piece states, The fuss over Chinese telecom firms and national security has put Prime Minister Stephen Harper in a quandary. On the one hand, his free-market instincts tell him that business knows no nationality, that cheapest is best and that, if Chinese companies can deliver high-quality telecommunications equipment at low prices, then Canadian firms would be fools not to buy it. And for the rest of us? Don't get too spooked. Most of our Internet and phone conversations are already susceptible to monitoring, either by Canada's Communications Security Establishment or the U.S. National Security Agency. Just don't put anything online that you don't want the CIA - or the Chinese Communist Party - to know. Toronto Star, A6 (2012-10-11)

Cyber fears go beyond trade with China

An opinion piece states, Yes, China should be treated differently. That's the consensus view of security experts examining the dealings of both Chinese telecommunications technology company Huawei, which has been vying for a federal government communications work, and the bid by China National Offshore Oil Corporation (CNOOC) to take over an Alberta oil company.

The lack of transparency in China's business methods means corporate espionage is always top of mind for both Canadian firms and legislators, they say Vancouver Sun, B1 (2012-10-11)

Spy scandal may help swing Nexen deal

An opinion piece states, In the peculiar world of global geopolitical frenemies, U.S. allegations that China's two largest phone-equipment makers facilitate spying by Beijing may prove to be a benefit for the Chinese company that is seeking to take over Calgary oil producer Nexen

While Canada should address national security, industrial protectionism and human rights with Beijing that shouldn't preclude pragmatic economic engagement with China. Calgary Herald, D1 (2012-10-11)

Federal government gives itself another 30 days to decide on Nexen takeover bid by Chinese company

The Conservative government has extended its review of the CNOOC-Nexen deal by 30 days, until mid-November, although even more time than that may be needed before a final decision is announced. The Cabinet has been examining whether to approve China National Offshore Oil Corporation's (CNOOC) \$15.1-billion takeover bid of Nexen under the Investment Canada Act, and whether the deal is of "net benefit" to Canada. The government's original 45-day review

period was set to expire Friday, so the announcement Thursday morning gives it another month to make a decision, although another extension beyond November is also possible. Montreal Gazette (2012-10-11)

Former Bank chief David Dodge says Canada should allow CNOOC's bid for Nexen

Canada should approve CNOOC Ltd.'s \$15.1 billion bid for Nexen Inc., the former head of the country's central bank said. Former Bank of Canada Governor David Dodge said the proposed acquisition by Beijing-based CNOOC is in the country's interest, and that opposition to the purchase of Calgary-based Nexen may be rooted in anti-Chinese sentiment Financial Post (2012-10-11).

Canada minister: CNOOC bid being reviewed for security

A Canadian government review of the \$15.1 billion Chinese bid for Nexen Inc will take security concerns into consideration in addition to a broader economic analysis of the transaction, Public Safety Minister Vic Toews said on Thursday. Toews' remarks came in response to questions about the effect that reports of Chinese espionage might have on the government's decision on whether to approve the proposed takeover of the Canadian oil producer by state-owned CNOOC Ltd. "I can tell you that every transaction that is referred to cabinet is considered from a security and safety point of view," Toews told reporters. Reuters (2012-10-11)

Broadcast Media

CBC News' The National reported on Nexen and a CSIS report regarding the potential threat of foreign takeovers in Canada. Rough Transcript (2012-09-20)

CTV News' Power Play interviewed Wehran Jang with the Asia Pacific Foundation on CSIS' annual report that raises concerns on foreign takeovers. Rough Transcript (2012-09-21)

CBC News' Power & Politics interviewed Conservative MP Pierre Poilievre, NDP MP Paul Dewar and Liberal MP Geoff Regan regarding the Nexen takeover bid from China and a tabled CSIS report examining the potential threat of foreign takeovers in Canada. Following this, *Power & Politics* speaks with CBC reporter Greg Weston regarding the subject. Rough Transcript (2012-09-21)

CBC News' Power & Politics interviewed Ray Boisvert, former assistant director of intelligence for CSIS regarding the issue of foreign takeovers in Canada. Rough Transcript (2012-09-21)

CBC News' Power & Politics spoke with CBC reporters Greg Weston, Kady O'Malley and Canadian Press reporter Rob Russo regarding the Nexen takeover bid and a CSIS report examining the risk posed by foreign takeovers in Canada. Rough Transcript (2012-09-21)

CTV's Power Play interviewed former CSIS assistant director Ray Boisvert on CSIS' annual report that raises concerns on foreign takeovers. Rough Transcript (2012-09-21)

Global News' The West Block interviewed Foreign Affairs Minister John Baird on Chinese investment in Canada and national security concerns. Rough Transcript (2012-09-23)

CTV's Question Period interviewed China's Ambassador to Canada, Zhang Junsai, on Chinese investment in Canada and national security concerns. Rough Transcript (2012-09-23)

CBC News reported on findings from the U.S. Congress House Intelligence Committee that Chinese communications companies Huawei and ZTE Corporation may pose a security threat to American interests. Rough Transcript (2012-10-08)

CNN reported on the potential security threat posed to the United States by Chinese communications companies Huawei and ZTE. Rough Transcript (2012-10-08)

CBC News reported on reactions from Ontario Premier Dalton McGuinty and others on reports from the U.S. of security concerns over Chinese company Huawei. Rough Transcript (2012-10-09)

CTV News' Power Play interviewed Wenran Jiang, Senior Fellow at the Asia Pacific Foundation, and Geoffrey O'Brian, former Director General of Counter-Intelligence at CSIS, regarding the threat posed by Chinese telecom firm Huawei. Rough Transcript (2012-10-09)

CBC News' Power & Politics reported on the national security threat posed by Chinese telecommunications firm Huawei. MPs Pierre Poilievre, Paul Dewar, and Wayne Easter were then interviewed for their insight on this topic. Rough Transcript (2012-10-09)

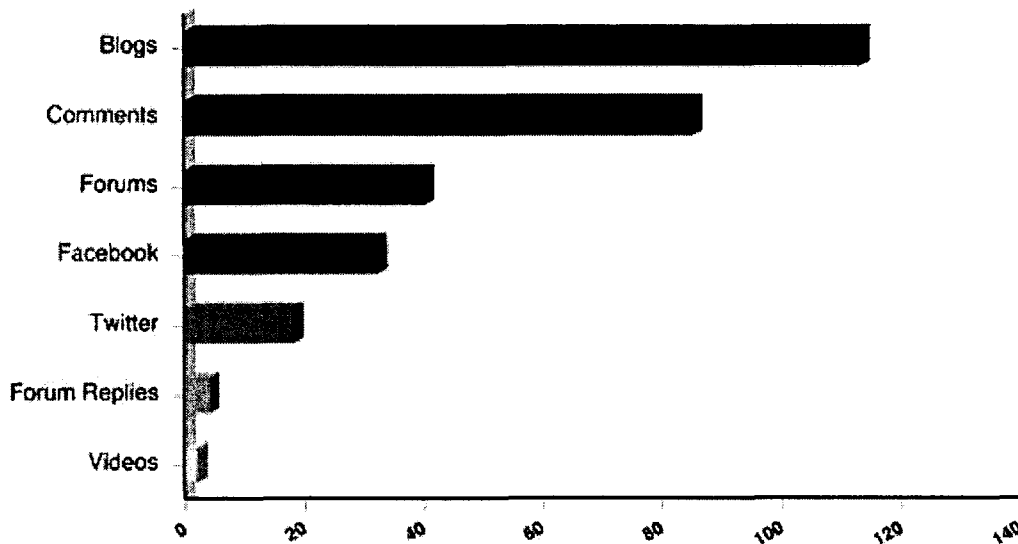
CTV News' Power Play interviewed MPs Paul Dewar, Pierre Poilievre, and Geoff Regan regarding the threat posed by Chinese telecom firm Huawei. Rough Transcript (2012-10-09)

CBC News' The National reported on the national security threat posed by Chinese telecom firm, Huawei. Rough Transcript (2012-10-09)

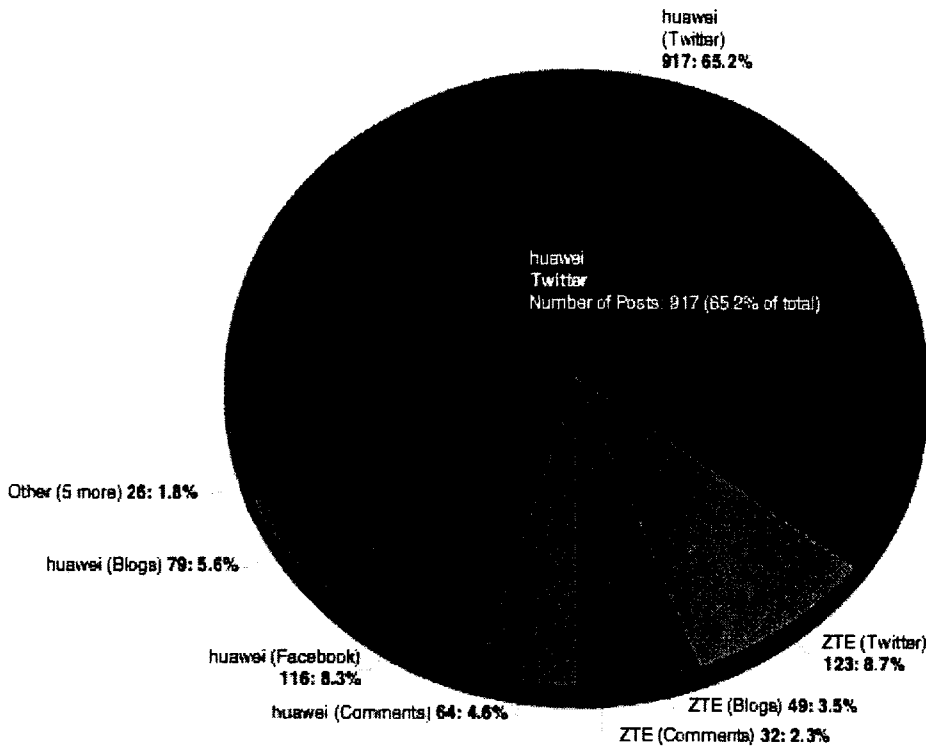
CBC News' Power & Politics interviewed Nik Nanos on whether Canadians are suspicious of doing business with China. Rough Transcript (2012-10-10)

Social Media

Coverage on foreign acquisitions of Canadian companies & government reviews, specifically CNOOC's proposed takeover of Nexen, was distributed over social media platforms as follows:



Coverage of Huawei and ZTE was distributed over social media platforms as follows (2012-10-01 – 2012-10-11):



A conversation cloud captures the most common terms on Twitter – re: Nexen and CNOOC:



A subsequent conversation cloud captures the most common terms on Twitter – re: Huawei, ZTE, Nexen and CNOOC (2012-10-01 to 2012-10-11):



Noteworthy Tweets:

metroottawa

Canada's spy agency warning that some foreign takeovers are a threat to national security <http://ow.ly/dSaol> (2012-09-20)

CTVNews

Spy agency warns foreign takeovers are risky for security <http://ow.ly/dT5VM> (2012-09-21)

PnP_CBC

Geoff Regan tells #pnp the CSIS report, released yesterday, shows Canadians should be concerned about the Nexen deal. #cdnpoli (2012-09-21)

ctvqp

Nexen is on the stockmarket and is ultimately responsible to its shareholders, says China's Ambassador to Canada #ctvqp #cdnpoli (2012-09-23)

CBCNews

Federal NDP opposes Nexen takeover bid <http://bit.ly/QvxC3o> (2012-10-04)

BloombergNews

U.S congressional report says Huawei, ZTE provide opportunities for China spying | <http://bloom.bg/UwCmvd> (2012-10-07)

Reuters

China rejects U.S. accusations against telcoms firms <http://reut.rs/QQG12Y>

CP24

NDP says Huawei concerns in U.S. a wake-up call to Canada on Nexen <http://www.cp24.com/news/ndp-says-huawei-concerns-in-u-s-a-wake-up-call-to-canada-on-nexen-1.989226> ... (2012-10-09)

Forbes

A Better Approach To Huawei, ZTE And Chinese Cyberspying? Distrust And Verify <http://bit.ly/RcaGIC> (2012-10-10)

YahooFinanceCA

Ex-central banker David Dodge says Canada should approve CNOOC bid for Nexen <http://yhoo.it/QYNSKk> (2012-10-11)

660News

The gov't is extending the review period for CNOOC's proposed takeover of Nexen by 30 days under the Investment Canada Act. (2012-10-11)

Reuters Canada

Canada minister: CNOOC bid being reviewed for security <http://reut.rs/RzX07J> (2012-10-11)

TechRadar UK

UK Government: Huawei and ZTE are safe: In light of reports from the US Intelligence Committee saying Huawei and...
<http://bit.ly/TC26Vp>

*Prepared by Public Safety Canada Media Monitoring /
Préparé par la Surveillance des médias de Sécurité publique Canada*

Question Period Note

SECURITY OF CANADA'S TELECOMMUNICATIONS NETWORKS

ISSUE:

On Sunday, October 7, 2012, 60 Minutes aired a 15 minute segment probing alleged security and espionage risks related to the telecommunications company, Huawei. The segment alluded to outcomes that were contained in a report that was released the following day, October 8, 2012, by the United States (U.S.) House Permanent Select Committee on Intelligence (HPSCI). On Monday, October 8, 2012, the Canadian Broadcasting Corporation did a follow up on the HPSCI report on "The National".

BACKGROUND:

Today, telecommunications equipment manufacturing is undertaken by a small number of global vendors. It is alleged that foreign intelligence organizations seek to exploit global supply chains for national advantages by embedding "backdoors" to allow remote access to systems and information during the manufacturing process or through maintenance arrangements or software upgrades. The two reports focus especially on a Chinese company, Huawei, given its perceived links to the Chinese government.

The HPSCI report is the result of an investigation that the House Committee initiated in November of 2011 regarding the security threat posed by Chinese telecommunications companies doing business in the U.S. The Committee has recommended that:

- the intelligence community provide threat briefings to cleared private sector entities;
- the U.S. Congress consider legislation to strengthen the Committee on Foreign Investment in the United States (CFIUS), and increase information sharing;
- the private sector consider the long term security risks of doing business with ZTE or Huawei;
- U.S. Government systems not include Huawei or ZTE components;
- the U.S. force more financial and management transparency through auditing, and compliance with U.S. laws and standards; and
- the U.S. Congress and law enforcement agencies investigate unfair trade practices especially companies financially supported by the Chinese Government.

When asked about doing business with Chinese telecommunications equipment manufacturers the HPSCI Chairman succinctly quoted, "If I were an American company today, and I'll tell you this as the Chairman of the House Permanent Select Committee on Intelligence, and you are looking at Huawei, I would find another vendor if you care about your intellectual property, if you care about your consumers' privacy, and you care about the national security of the United States of America."

The 60 Minutes segment and the recommendations contained in the HPSCI Report publicly highlight serious concerns and allegations held by the U.S. related to Huawei and ZTE, and are likely to have a lasting impact on their ability to conduct business in the U.S.

It is expected that Canadian companies that operate on both sides of the border will pay close attention to the Investigative Report by HPSCI, given the potential impacts on their business operations. As part of *Canada's Cyber Security Strategy*, Public Safety Canada leads coordinated federal threat briefings on cyber security risks and threats to Canada's private sector and critical infrastructure owners and operators. In particular, we have a strong and ongoing partnership with our telecommunications companies: they are well informed of national security issues and can develop sophisticated solutions to respond to them.

As service providers, it is in the business interests of Canada's telecommunications companies to take decisions to ensure that their customers have access to a reliable, secure network.

s.20(1)(c)

s.20(1)(d)

SECURITY OF CANADA'S TELECOMMUNICATIONS NETWORKS

PROPOSED RESPONSE:

- The Canadian telecommunications sector is the backbone of a strong and prosperous Canadian economy. The Government is committed to ensuring that Canada's telecommunications sector remains competitive and secure.
- The Government is working with private sector telecommunications carriers who are also committed to providing secure and reliable services to consumers. We will respond decisively to address any emerging threats to Canada's digital infrastructure.
- *Canada's Cyber Security Strategy* outlined how the Government would develop partnerships to bring together industry, provinces and territories and our international allies. An example of this is the Canadian Security Telecommunications Advisory Committee, which was formed with Canada's telecommunications companies providing a high level forum to share information and discuss sensitive security issues.
- I will not engage in speculation or rumours around the activities of specific companies. I can assure you that we are and will remain vigilant to potential national security concerns regarding the telecommunications sector and we are taking actions to address any issues as they develop.

CONTACTS:

Prepared by
Mark Matz
Director
National Cyber Security
Directorate

Tel. no.
613-993-9635

Approved by (ADM level only)
Lynda Clairmont
Senior ADM, National Security

Tel. no.
613-990-4976

Question Period Note

SECURITY OF CANADA'S TELECOMMUNICATIONS NETWORKS

ISSUE:

On Sunday, October 7, 2012, 60 Minutes aired a 15 minute segment probing alleged security and espionage risks related to the telecommunications company, Huawei. The segment alluded to outcomes that were contained in a report that was released the following day, October 8, 2012, by the United States (U.S.) House Permanent Select Committee on Intelligence (HPSCI).

BACKGROUND:

Today, telecommunications equipment manufacturing is undertaken by a small number of global vendors. Global manufacturing is susceptible to exploitation by foreign intelligence organizations seeking to exploit global supply chains for national advantages. It has been publicly reported that a number of states have concerns with a Chinese company, Huawei, given its perceived links to the Chinese government. The 60 Minutes story highlighted a number of concerns that have been previously reported and attempts to seek answers related to Huawei's activities. 60 Minutes interviews former intelligence officials, a mobile network operator, Bill Plummer, the Vice President of External Relations for Huawei Technologies Co., and both the Chair, Mike Rogers (R-MI) and the ranking Democrat, Dutch Ruppersburger (D-MD) of the House Permanent Select Committee on Intelligence (HPSCI) to discuss aspects of the report that HPSCI was to release the following day.

The HPSCI report is the result of an investigation that the Committee initiated in November of 2011 regarding the counterintelligence and security threat posed by Chinese telecommunications companies doing business in the U.S. The Committee's investigation involved two parts: a review of open source information on the companies' histories, operations, financial information, and potential ties to the Chinese government or Chinese Communist Party; and a review of classified information, including a review of programs and efforts of the U.S. intelligence community to assess whether the intelligence community is appropriately prioritizing and resourced for supply chain risk evaluation. The Committee found that the risks associated with Huawei's and ZTE's provision of equipment to U.S. critical infrastructure could undermine U.S. national security interests. The Committee has recommended that:

- The U.S. should view with suspicion the continued penetration of the U.S. telecommunications market by Chinese telecommunications companies.
 - The U.S. intelligence community must remain vigilant and focused on this threat. The intelligence community should actively seek to keep cleared private sector actors as informed of the threat as possible.
 - The Committee on Foreign Investment in the United States (CFIUS) must block acquisitions, takeovers, or mergers involving Huawei and ZTE given the threat to U.S. national security interests. Legislative proposals seeking to expand CFIUS to include purchasing agreements should receive thorough consideration by relevant Congressional committees.
 - U.S. government systems, particularly sensitive systems, should not include Huawei or ZTE equipment, including in component parts. Similarly, government contractors, particularly those working on contracts for sensitive U.S. programs, should exclude ZTE or Huawei equipment in their systems.
- Private-sector entities in the United States are strongly encouraged to consider the long-term security risks associated with doing business with either ZTE or Huawei for equipment or services. U.S. network providers and systems developers are strongly encouraged to seek other vendors for their projects. Based on available classified and unclassified information, Huawei and ZTE cannot be trusted to be free of foreign state influence and thus pose a security threat to the United States and to our systems.
- Committees of jurisdiction within the U.S. Congress and enforcement agencies within the Executive Branch should investigate the unfair trade practices of the Chinese telecommunications sector, paying particular attention to China's continued financial support for key companies.
- Chinese companies should quickly become more open and transparent, including listing on western stock exchange with advanced transparency requirements, offering more consistent review by independent third-party evaluators of their financial information and cyber security processes, complying with U.S. legal standards of information and evidentiary production, and obeying all intellectual-property laws and standards.
- Committees of jurisdiction in the U.S. Congress should consider potential legislation to better address the risk posed by telecommunications companies with nation-state ties or otherwise not clearly trusted to build critical infrastructure. Such legislation could include increasing information sharing among private sector entities, and an expanded role for the CFIUS process to include purchasing agreements.

The 60 Minutes segment and the recommendations contained in the HPSCI report publicly highlight serious concerns and allegations held by the U.S. related to Huawei Technologies Co., and are likely to have a lasting impact on their ability to conduct business in the U.S.

Public Safety Canada coordinates the efforts of federal departments and agencies to identify threats and develop comprehensive approaches to address risks within the Government and across Canada. Public

Safety Canada is strengthening partnerships with Canada's private sector and critical infrastructure sectors to achieve shared economic and national security objectives. We have a strong and ongoing partnership with our telecommunications companies: they are well informed of national security issues and can develop sophisticated solutions to respond to them. Naturally, as service providers, it is in the business interests of Canada's telecommunications companies to take decisions to ensure that their customers have access to a reliable, secure network.

SECURITY OF CANADA'S TELECOMMUNICATIONS NETWORKS

PROPOSED RESPONSE:

- The Canadian telecommunications sector is the backbone of a strong and prosperous Canadian economy. The Government is committed to ensuring that Canada's telecommunications sector remains competitive and secure.
- The Government is working with private sector telecommunications carriers who are also committed to providing secure and reliable services to consumers. We will respond decisively to address any emerging threats to Canada's digital infrastructure.
- *Canada's Cyber Security Strategy* outlined how the Government would develop partnerships to bring together industry, provinces and territories and our international allies. An example of this is the Canadian Security Telecommunications Advisory Committee, which was formed with Canada's telecommunications companies providing a high level forum to share information and discuss sensitive security issues.
- I will not engage in speculation or rumours around the activities of specific companies. I can assure you that we are and will remain vigilant to potential national security concerns regarding the telecommunications sector and we are taking actions to address any issues as they develop.

CONTACTS:

Prepared by
Mark Matz
Director
National Cyber Security
Directorate

Tel. no.
613-993-9635

Approved by (ADM level only)
Lynda Clairmont
Senior ADM, National Security

Tel. no.
613-990-4976

Matz, Mark

From: Dick, Robert
Sent: October-08-12 10:36 AM
To: 'Tony.Pickett@rcmp-grc.gc.ca'; '[REDACTED]@CSE-CST.GC.CA';
'ROBERT.MAZZOLIN@forces.gc.ca'; 'Gregory.Loos@Forces.gc.ca';
'Martin.Proulx@ic.gc.ca'; '[REDACTED]@cse-cst.gc.ca'
Cc: Labelle, Sébastien; Hatfield, Adam; Anderson, Windy; Matz, Mark
Subject: Fw: 60 Minutes transcript

Transcript of last night's coverage of Huawei.

From: Matz, Mark
Sent: Monday, October 08, 2012 10:25 AM
To: Dick, Robert
Subject: Fw: 60 Minutes transcript

Fyi

From: Carta, John
Sent: Sunday, October 07, 2012 08:20 PM
To: Matz, Mark; Binne, Christine; Bradley, Kees
Subject: Fw: 60 Minutes transcript

From: COMDO
Sent: Sunday, October 07, 2012 08:20 PM
To: Carta, John; Miller, Kevin; Willey, Chris
Cc: Swift, Andrew
Subject: 60 Minutes transcript

Aside from the RT that was just distributed, CBS has also put up a full transcript of the segment, located here:

http://www.cbsnews.com/8301-18560_162-57527441/huawei-probed-for-security-espionage-risk/

Sean Despard
Communications Duty Officer/ Agent de service des communications
Government Operations Centre/ Centre des opérations du gouvernement
Tel.: (613) 991-7010
Fax/Télécopieur: (613) 996-0995
Email/courriel: COMDO@ps-sp.gc.ca

Matz, Mark

From: Carta, John
Sent: October-07-12 8:20 PM
To: Matz, Mark; Binne, Christine; Bradley, Kees
Subject: Fw: RT: CBS News (60 Minutes) - Report on the telecommunications company Huawei - 2012-10-07, 19:30 ET

I can't see the full distribution list, so in case you didn't receive it:

s.15(1) - Subv

From: PSMediaCentre/CentredesmediasdeSP
Sent: Sunday, October 07, 2012 08:04 PM
To: * COMMS ADG / Bureau du directeur général associé; * COMMS Communication Services Division / Division des services de communication; * COMMS DGO / Bureau de la directrice générale; * COMMS Program Communications Division / Secteur des communications de programmes; * COMMS Public Affairs Division / Secteur des affaires publiques; * Speeches / Discours; Thibouthot, AkimIsabelle; Astravas, Rutha; Banerjee, Ritu; Beaudoin, Serge C; Bolton, Stephen; Boucher, Patrick; Boucher-Lalonde, Murielle; Cameron, Bud; Carmichael, Julie; Champoux, Elizabeth; Clairmont, Lynda; Clifford, Kurtis; Coburn, Stacey; Crawford, Andrée; Csversko, Christine; Currie, St. Clair; Daoust, Normand; Davis, Jeremy; De Santis, Heather; Duschner, Gabrielle; Easson, Grant; Gareau-Lavoie, Genevieve; Gordon, Robert; Hitchcock, Christy; House, Andrew; Huggins, Rachel; Humeniuk, Elena; Hunt, Ryan; Jarmyn, Tom; Johnson, Mark; Kelland, Stephen; Khouri, Lisa; Kubicek, Brett; Lavoie, Micheline; Leclair, Natalie; Leclerc, Carole; Leonidis, Nelly; Lesser, Robert; MacDonald, Nicholas; MacKinnon, Paul; Marchand, Renee; McAteer, Julie; McGrath, Andrew; McLaren, Victoria; Morris, Marika; Motzney, Barbara; Mueller, Mike; Mundie, Robert; Murdock, Lyndon; Murray, Erin; Nicole, Jean-Thomas; Oldham, Craig; Panthaky, Jasmine; Porter, Neal; Pozhke, Nicholas; Rosario, Giselle; Roy, Isabelle; Saunders, Joanne; Schulz, Caroline; Shuttle, Paul; Slack, Jessica; Thibault, Stéphane; Tupper, Shawn; Van Crieelingen, Jane; Verret, Scott; Vinodrai, Arjun; Wex, Richard; Wilson, Gina; Amitha.Carnadin@cbsa-asfc.gc.ca <Amitha.Carnadin@cbsa-asfc.gc.ca>; Bev.Arseneault@csc-scc.gc.ca <Bev.Arseneault@csc-scc.gc.ca>; Bindman, Stephen; Brunette, Lynn <lynn.brunette@csc-scc.gc.ca>; cbsa.media@cbsa-asfc.gc.ca <cbsa.media@cbsa-asfc.gc.ca>; Cgirouad@justice.gc.ca <Cgirouad@justice.gc.ca>; Williams, Christopher; Churney, Daryl; Cobbsu@csc-scc.gc.ca <Cobbsu@csc-scc.gc.ca>; Cocking, Marie <Marie.Cocking@PBC-CLCC.GC.CA>; Couture, Jocelyne <000160815.SC10.EDIV_LMD@rcmp-grc.gc.ca>; Derek Cefaloni <derek.cefaloni@rcmp-grc.gc.ca>; Douglas, Caroline; C. Girouard; Hart, Melissa <Melissa.Hart@CSC-SCC.GC.CA>; Desantis, Heather; Bradley, Jolene; Julianne Prokopich; Mackillop, Ken; Lamothe, Maureen; [REDACTED] Lavoie, Daniel; Mailhot, Esther; Stokes, Mark; Mary.Schlosser@rcmp-grc.gc.ca <Mary.Schlosser@rcmp-grc.gc.ca>; John McMeekin; Media.Monitoring@cbsa-asfc.gc.ca <Media.Monitoring@cbsa-asfc.gc.ca>; CBSA Media Monitoring; RCMP Media Monitoring; Martin, Nadie; Robinson, N.; Nichols, Megan; Noftle, Tracie <Tracie.Noftle@csc-scc.gc.ca>; Parkes, Sara; Giolti, Patrizia; Press Clippings Officer CSC <PressClippingsOfficer@csc-scc.gc.ca>; Prieur, Mark <mark.prieur@pbc-clcc.gc.ca>; Rioux, Veronique; Rondeau, Martine; Sbinman@justice.gc.ca <Sbinman@justice.gc.ca>; Dumoulin, Stéphanie
Subject: RT: CBS News (60 Minutes) - Report on the telecommunications company Huawei - 2012-10-07, 19:30 ET

Rough Transcript

Station: CBS – 60 Minutes
Time/Heure: 19:30 ET
Date: 2012-10-07

Summary: CBS' 60 Minutes reported on the telecommunications company Huawei.

>> Kroft: If you're concerned about the decline of American economic power and the rise of China, then there is no better case study than Huawei. Chances are you've never heard of this Chinese technology giant, but in the space of 25 years, it's become the largest manufacturer of telecommunications equipment in the world-- everything from smart phones to switchers and routers that form the backbone of the global communications network. It's an industry the U.S. invented and once dominated, but no more. Now, Huawei is aggressively pursuing a foothold in the United-States, hoping to build the next generation of digital networks here. It's prompted an outcry in Washington, and a year-long investigation by the

house intelligence committee that has raised concerns about national security, Chinese espionage, and Huawei's murky connections to the Chinese government. Huawei's world headquarters is located on this sprawling Google-esque campus in Shenzhen, not far from Hong Kong. China's first international conglomerate is a private company, ostensibly owned by its 140,000 employees, but exactly how that works and other details of corporate governance are closely held secrets. What we do know is that Huawei is now the world leader in designing and building fourth-generation communication networks, known as 4G, the latest technology for moving high volumes of phone calls, data, and high definition video. Its innovative low-cost systems have already captured markets in Africa, Latin America and Europe. Now, with Huawei eyeing potential customers in the U.S., congressional leaders and the national security establishment are doing everything they can to prevent it from happening. Do we trust the Chinese?

>> Mike Rogers: If I were an American company today-- and I'll tell you this as the chairman of the house permanent select committee on intelligence-- and you are looking at Huawei, I would find another vendor if you care about your intellectual property, if you care about your consumers' privacy, and you care about the national security of the United States of America.

>> Kroft: Republican congressman Mike Rogers and the ranking democrat on the house intelligence committee, Dutch Ruppersberger, believe that letting a Chinese company build and maintain critical communication infrastructure here would be a serious mistake.

>> Dutch Ruppersberger: One of the main reasons we are having this investigation is to educate the citizens in business in the United States of America. In the telecommunications world, once you get the camel's nose in the tent, you can go anywhere.

>> Kroft: Their overriding concern is this-- that the Chinese government could exploit Huawei's presence on U.S. networks to intercept high-level communications, gather intelligence, wage cyber war, and shut down or disrupt critical services in times of national emergency.

>> Jim Lewis: This is a strategic industry, and it's like aircraft or space launch or computers, I.T. It's a strategic industry in the sense that an opponent can gain serious advantage, can gain serious benefit from being able to exploit the telecommunications network.

>> Kroft: Jim Lewis has followed Huawei's explosive growth for years from the state department and the commerce department, where his job was to identify foreign technologies that might pose a threat to national security. How did they get so big and so cheap so quickly?

>> Lewis: Two answers. First, steady, extensive support from the Chinese government. If you're willing to funnel hundreds of millions, maybe even billions of dollars to a company, they're going to be able to grow. The second reason is industrial espionage. And Huawei was famous in their developing years for taking other people's technology.

>> Kroft: You mean stealing?

>> Lewis: I guess technically, yes, it would be theft.

>> Kroft: Cisco accused Huawei of copying one of its network routers, right down to the design flaws and typos in the manual. And Motorola alleged that Huawei recruited its employees to steal company secrets. Both cases were settled out of court. But the pentagon and the director of national intelligence have identified Chinese actors as the world's most active and persistent perpetrators of economic espionage.

>> Bill Plummer: Huawei is Huawei; Huawei is not China.

>> Kroft: Bill Plummer is the American face of Huawei, the company's U.S. vice president of external relations and the only executive the home office in Shenzhen would let us speak to. We met him at Huawei's North American headquarters in Plano, Texas.

>> Plummer: We have the responsibility to clean up ten years of misinformation and innuendo.

>> Kroft: What's the misinformation and innuendo?

>> Plummer: The suggestion that a company, by virtue of its heritage or flag of headquarters, is somehow more vulnerable than any other company to... to some sort of mischief.

>> Kroft: Plummer told us that Huawei is just another multinational corporation doing business in the United States, no different than Siemens, Samsung, or Hyundai.

>> Plummer: This room is a clean room.

>> Kroft: He says Huawei buys \$6 billion in components from American suppliers every year and indirectly employs 35,000 Americans. And he says that the latest telecom gear Huawei hopes to sell in the U.S. poses no threat. One national security expert said that, if you build a network like this in another country, you basically have the keys to intercepting their communications. Is that a true statement?

>> Plummer: Part of that might be a little bit fantastical, but you know, Huawei is a business in the business of doing business. \$32.4 billion in revenues last year across 150 different markets; 70% of our business outside of China. Huawei is not going to jeopardize its commercial success for any government, period.

>> Kroft: What's the relationship between Huawei and the Chinese government?

>> Plummer: We have a Beijing office. So, you know, we're a regulated industry the same as we are here. You need to be able to interface with government.

>> Kroft: So you're saying the Chinese government has no influence over Huawei.

>> Plummer: We're another business doing business in China.

>> Kroft: If you look at Huawei, it looks like just a big international company with an American face.

>> Chris Johnson: Yep. And that's the intent.

>> Kroft: Until last spring, Chris Johnson was the CIA's top analyst on China, and he's briefed the last three presidents on what's been happening behind the scenes in Beijing. He tells a different story than Huawei's Bill Plummer.

>> Johnson: The problem, I think, is really it boils down to an issue of will the company take some steps to make themselves, you know, more transparent about their operations and what their ultimate goal is, especially this relationship with the Chinese government, with the Chinese communist party, and with the people's liberation army.

>> Kroft: Johnson says the military has always played a role in Chinese telecommunications, and that Huawei's reclusive C.E.O. served as an army major in telecommunications research before he retired and founded Huawei, supposedly with a few thousand dollars in savings and no help from the Chinese government. What could you tell me about the guy that runs this company, Ren?

>> Johnson: Ren Zhengfei, yeah. He's a very mysterious figure. (Laughs) and, you know, there really isn't that much known about him.

>> Kroft: Has he ever given an interview?

>> Johnson: Not that I'm aware of. Of course, it does then generate these concerns about why he won't give an interview, and why he won't say something about his role in the company and his philosophy of how the company operates.

>> Kroft: Unlike western companies that are usually regulated and scrutinized, about the only entity privy to the inner workings of Huawei is a communist party committee, which has offices inside the company's headquarters.

>> Johnson: You know, at the end of the day, the communist party controls the entire economy. They ultimately decide who the winners and losers are. The ultimate leverage that they have over these type of companies is that they can, you know, launch a corruption investigation against the chairman, for example.

>> Kroft: If the Chinese government told Huawei that they wanted them to spy on the U.S. telecommunication system and extract information, could Huawei say no?

>> Johnson: It'd be very difficult for them, given the nature of their system.

>> Lewis: It's a different system than ours. Here, companies are used to, you know, throwing their weight around and telling the government what to do. In china, a company is a chia pet. The state tells them what to do and they do it.

>> Kroft: There is no hard evidence that's happened with Huawei, but the Obama administration has been unwilling to take the risk. Two years ago, when it appeared that Huawei might land its first big American deal-- a \$5 billion contract to build sprint's new 4G wireless network, the U.S. government stepped in.

>> Lewis: You had the secretary of commerce call the C.E.O. of Sprint and lay out the U.S. concerns, say that the U.S. was really worried about Huawei. And they would be a lot happier if Sprint didn't do the deal.

>> Kroft: And Sprint said, "okay."

>> Lewis: Sprint said, "okay."

>> Kroft: Since then, Huawei has blanketed U.S. airwaves with commercials, and hired an army of lobbyists and public relations firms to help it get a foothold into the world's largest telecom market.

>> Lewis: They're determined. They're in it for the long haul. The line that most people think about is, Mao had a strategy called "win the countryside, surround the cities, and then the cities will fall." And Huawei seems to be following that Maoist strategy.

>> Kroft: In the last couple of years, Huawei has managed to install and maintain a handful of networks in U.S. rural markets, including a vast quadrant of South-western Kansas. Craig Mock is the president and general manager of United Wireless, based in the historic cowboy town of Dodge City.

>> Craig Mock: We're trying to reach out as far as we can into rural areas.

>> Kroft: Mock told us the new Huawei network delivers some of the fastest internet speeds in the country. But last spring, after the deal had been signed with Huawei, Mock received an unwelcome visit from two federal agents. Who were they, intelligence people?

>> Mock: Not going to say.

>> Kroft: Why did they come out here?

>> Mock: I think they would've preferred that we bought equipment from somebody else.

>> Kroft: What was your reaction? Were you upset that they came out?

>> Mock: I was not pleased.

>> Kroft: Because?

>> Mock: Because I saw it as interference in our operations. If we're not able to buy the very best equipment and deploy it in a efficient manner, then everybody suffers.

>> Kroft: Were there any American companies that bid on this?

>> Mock: I don't know of any American companies that makes this equipment.

>> Kroft: About the only real American competitor Huawei has left is Cisco, which is still a worldwide player, but doesn't produce all the equipment necessary to construct a 4G network. The only companies that do are all foreign-- Huawei; Ericsson, which is Swedish; and the French company Alcatel-lucent.

>> Lewis: That's where we've ended up. We now depend entirely on foreign suppliers-- three European, two Chinese. No Americans.

>> Kroft: The United States used to dominate this field.

>> Lewis: Yeah, it's true. You know, I guess just we were asleep at the switch.

>> Kroft: What happened?

>> Lewis: Some of it was just bad planning at the company level. Some of it was a lack of attention by the government. I mean, we would not have let the space industry go out of business. We would not say, "Oh, we'll depend on foreign companies to launch our satellites." But we didn't do that for telecom.

>> Kroft: Concerned and suspicious of what it calls "continued Chinese penetration of U.S. telecommunications," the house intelligence committee called Huawei executive Charles Ding to answer questions about the company's corporate structure, ownership, finances, and management. The committee seemed to get nowhere.

>> Rogers: The committee has been disappointed that the company's provided little actual evidence to ameliorate the committee's concerns.

>> Kroft: Huawei's Bill Plummer says the company bears some of the responsibility for the lack of communication.

>> Plummer: You're right that, over the ten years of explosive growth, we were not as good at communicating about ourselves as we could or should have been. But over the last couple of years, we've really stepped that up. I mean, you want to know more about us? We're an open book.

>> Kroft: Really?

>> Plummer: Yeah.

>> Kroft: Has Mr. Ren ever given an interview?

>> Plummer: Mr. Ren is not terribly well-known for his... his getting out in front of the media.

>> Kroft: We requested interviews at various points along the way with company officials, both in China and here. And we got their most important spokesman and lobbyist here in the United States. But it's not like they swung open the doors and said, you know, "We're an open book."

>> Plummer: Well, I think that...

>> Kroft: You allowed our camera crews into your facilities in Shenzhen, and there was a big banner saying, "Welcome, '60 Minutes'." But we weren't allowed to talk to anybody, to speak to anybody.

>> Plummer: The goal of the visit to Shenzhen was to give a really rich and visual impression of the company. It is a company that has experienced a history of not fully balanced treatment by the media, and that's created a sense of wariness.

>> Kroft: Huawei is not going to like the treatment it receives from the house permanent select committee on intelligence any better. Its final report is due tomorrow.

Due to the nature of closed captioning, grammatical and editorial errors may be found within the attached transcript. Étant donné la nature du sous-titrage, il peut y avoir des erreurs grammaticales et de rédaction dans la transcription ci-attachée.

Questions? Please contact us at PSMediaCentre/CentredesmediasdeSP@ps-sp.gc.ca.

Questions? Veuillez communiquer avec nous au PSMediaCentre/CentredesmediasdeSP@ps-sp.gc.ca.

Matz, Mark

From: Carta, John
Sent: October-07-12 8:21 PM
To: Matz, Mark; Binne, Christine; Bradley, Kees
Subject: Fw: 60 Minutes transcript

From: COMDO
Sent: Sunday, October 07, 2012 08:20 PM
To: Carta, John; Miller, Kevin; Willey, Chris
Cc: Swift, Andrew
Subject: 60 Minutes transcript

Aside from the RT that was just distributed, CBS has also put up a full transcript of the segment, located here:

http://www.cbsnews.com/8301-18560_162-57527441/huawei-probed-for-security-espionage-risk/

Sean Despard
Communications Duty Officer/ Agent de service des communications
Government Operations Centre/ Centre des opérations du gouvernement
Tel.: (613) 991-7010
Fax/Télécopieur: (613) 996-0995
Email/courriel: COMDO@ps-sp.gc.ca

Matz, Mark

From: Carta, John
Sent: October-06-12 7:12 PM
To: Carmichael, Julie; Durand, Stéphanie; Swift, Andrew; Issues / Enjeux; Filippis, Lisa; Austria, Jamela; Willey, Chris; Matz, Mark; Binne, Christine; Bradley, Kees; Manji, Natasha
Subject: Report - huawei

Fyi in case anyone hasn't seen it --- report with comments from US House Intelligence Committee Chairman, reference to the 60 Minutes piece, and confirmation that the US report is coming out on the 8th.

Huawei is security threat, say US lawmakers Bloomberg / Washington Oct 07, 2012, 00:52 IST

US companies should avoid business with Huawei Technologies, China's largest phone-equipment maker, to guard against intellectual-property theft and spying, the US House Intelligence Committee chairman said.

US companies considering purchases from Huawei should "find another vendor if you care about your intellectual property, if you care about your consumers' privacy, and you care about the national security of the United States of America," Representative Mike Rogers told CBS News's "60 Minutes," according to a CBS release about an interview set to air tomorrow.

Rogers, a Michigan Republican, and the committee's top Democrat, Maryland Representative CA "Dutch" Ruppersberger, are preparing to issue a report October 8 on their year-long investigation of Huawei and ZTE Corp, another Chinese phone-equipment maker. The lawmakers have been looking at whether the companies' expansion in the US market enables Chinese government espionage and imperils the US telecommunications infrastructure. "Huawei is a globally trusted and respected company doing business in almost 150 markets with over 500 operator customers, including nationwide carriers across every continent save Antarctica," William Plummer, a Washington-based spokesman for Huawei, said in an e-mail. "The security and integrity of our products are world proven. Those are the facts today. Those will still be the facts next week, political agendas aside."

Susan Phalen, a spokeswoman for the committee, didn't immediately respond to a request for comment.

Committee investigation

Executives for Huawei and ZTE, both based in Shenzhen, China, denied links to espionage during an intelligence committee hearing last month, telling lawmakers they aren't controlled by the Chinese government.

The companies said they favor independent audits of technology vendors' hardware and software as a way to ensure that devices and networks are secure.

The panel's probe coincides with increased US warnings about digital spying by China. US counterintelligence officials called China the world's biggest perpetrator of economic espionage in a report last November, saying the theft of sensitive data in cyberspace is accelerating and jeopardising an estimated \$398 billion in US research spending

s.15(1) - Int'l

s.15(1) - Subv

Weir, Sarah

From: Louis-Martin.Aumais@international.gc.ca
Sent: September-20-12 11:02 PM
To: Dick, Robert; Gordon, Robert; Clairmont, Lynda; [REDACTED]@cse-cst.gc.ca; Christopher.Blain@pco-bcp.gc.ca; Mark.Glauser@international.gc.ca
Cc: Banerjee, Ritu; [REDACTED]; Gwen.Beauchemin@international.gc.ca; James.Galt@international.gc.ca; [REDACTED] Claudie.Senay@international.gc.ca; Artur.Wilczynski@international.gc.ca; David.Nelson@international.gc.ca; Colin.Shonk@international.gc.ca; Tricia.Geddes@pco-bcp.gc.ca; Michael.Small@international.gc.ca; David.McKinnon@international.gc.ca; Stephen.Burridge@international.gc.ca; Mark.Berman@international.gc.ca; Kent.Vachon@international.gc.ca; Roland.Legault@international.gc.ca; Linder, Glen
Subject: CNBRA-ILO-010: CYBER: Aus Parliamentary Hearing on National Security Legislation -- Public Submissions to the Committee (20120921)
Attachments: PJCIS -- NatSec Leg Rev - Huawei Submission.pdf; PJCIS -- NatSec Leg Rev - Telstra Submission.pdf; PJCIS -- NatSec Leg Rev - ASIO Public Submission.pdf; PJCIS -- NatSec Leg Rev - Inspector-General I&S Submission.pdf

RESENT -- to correct email addresses

UNCLASSIFIED

Colleagues,

As you know by now, at the request of the Attorney General, the Australian Parliament has started hearings concerning the review of National Security legislation, in particular concerning the modernization of the interception regime and telco sector security. Inquiry's own webpage: http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsi2012/index.htm

Sign of the public interest so far, the Committee has received 208 submissions. I attach a sampler of submissions, which I trust you will find of interests:

1. **Huawei**, which echos the recent public criticism it has directed to the Australian government of late;
2. **Telstra**, Australia's largest telecommunications company, and key partner in the National Broadband Network. On the issue of telco sector security reform, Telstra in its submission interestingly states: "*Telstra supports measures to ensure that C/CSPs [carriers and carrier service providers] have appropriate incentives to focus resources on network security and believes this can be achieved through the modification of some of the [Aus Govt's] proposed measures to avoid adverse impacts on our ability to undertake **efficient procurement and network design and operations.***"
3. **ASIO**, whose public submission has been picked up by the Australian press this morning <http://www.abc.net.au/news/2012-09-21/asio-wants-phone-and-email-data-stored-for-two-years/4272982>;
4. **The Inspector-General of Intelligence and Security** -- the Australian Intelligence Community's oversight body, who seeks additional resources from the Government is she is to be called in future legislation to oversee the new interception regime <http://www.abc.net.au/news/2012-09-20/data-retention-changes-to-cost-more/4271898>

I will continue to monitor and report on the subject, as developments warrant.

Louis-Martin Aumais
Counsellor | Conseiller

Louis-Martin.Aumais@international.gc.ca

Telephone | Téléphone : +61 (02) 6270 4029

Facsimile | Télécopieur : +61 (02) 6273 3285

Commonwealth Avenue, Canberra ACT 2600

Canadian High Commission | Haut-commissariat du Canada

Government of Canada | Gouvernement du Canada



Submission No 149

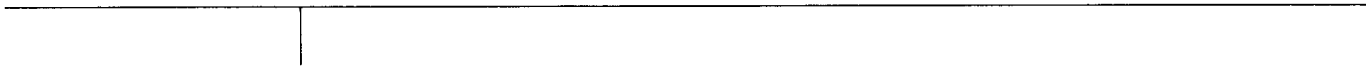
Inquiry into potential reforms of National Security Legislation

Organisation: Huawei Technologies (Australia) Pty Limited

Parliamentary Joint Committee on Intelligence and Security

**Submission from Huawei Technologies (Australia)
Pty Limited (Huawei Australia) to the Parliamentary
Joint Committee on Intelligence and Security on the
Potential Network Security Reforms**

20 August 2012



Equipping Australia against Emerging and Evolving Threats

About Huawei

Huawei is a privately owned global technology company that operates in over 140 countries. Our technology supports almost half the planet's population.

We employ 150,000 people. We are used by 45 of the world's top 50 telecommunications operators and, as at the end of 2011, our products and solutions had been deployed by more than 500 telecommunications operators in 140 countries.

We are essentially a science and engineering based company: we have 7,500 employees with PhDs and 62,000 employees engaged in research and development. As of 2011 we have 36,344 patent applications filed in China, 10,650 patents filed under the Patent Cooperation Treaty and 10,978 patent applications filed in other jurisdictions. We have been awarded 23,522 patent licenses, 90% of which are invention patents. We have 23 R&D centres around the world, 34 joint innovation centres with key customers and 45 training centres.

Overall, about 70% of our revenue is generated outside of China.

We source 70% of our materials from non-Chinese companies with the US being the largest provider of components with 32% of our materials sourced through 185 US suppliers. China provides 30% of our components (which are mainly low tech mechanical parts, cables and final assembly), Taiwan 22% and Europe 10%. We source products from Australian owned and/or Australian based suppliers.

Huawei Australia has approximately 900 staff, a local Board of Directors and is working with all of Australia's major operators.

50% of Australians already use at least one Huawei product for their telecommunications needs.

Executive summary

As a major equipment vendor with a reach in over 140 countries, we are primarily interested in providing a global perspective to the proposal to impose obligations on the Australian telecommunications industry to address security risks (item 16 of the Committee's Terms of Reference).

We appreciate the challenges that the network security reforms are intended to address. We are committed to playing a leading role in cyber-security globally and to ensuring our customers are confident in the integrity and security of our products. We believe our business will grow in a regulatory regime which puts a premium on security – provided that such regulation is applied in a non-discriminatory way.

We believe security outcomes are best delivered by a competitive, well-informed marketplace – so we strongly support the flexible and outcomes-based approach suggested by the Discussion Paper. We believe this model would reflect the importance of competitive and innovative vendors like Huawei in the market and the contributions they make to security outcomes.

Given the commentary surrounding the proposed reforms, we do have concerns that the security standards proposed in the Discussion Paper will be imposed in a way that discriminates against particular vendors, or vendors from a particular country of origin with little or no benefit for security outcomes.

We believe it is essential that any specific requirements imposed are objectively justified, vendor neutral and give affected industry players a genuine opportunity to understand and address specific concerns. We believe the principle of non-discrimination should be clearly set out in any legislative reforms.

Network security regulation which is consistent with non-discrimination and open

access to markets is important to achieving security outcomes – it would increase competition, innovation and investment, which are all essential to security. It would:

- increase Australia's access to the latest technologies, foster competition and innovation and result in lower end-user prices;
- improve Australia's competitiveness in the region and globally;
- be the only approach which can be rationally enforced, given the complexity of the global supply chain (for example, the fact that every major telecommunications equipment provider's supply chain structures are similar); and
- support Australia's trade commitments, obligations and relationships.

Finally, we believe that effective reforms should:

- **be flexible and outcomes-based** – noting that network security standards which mandate the use of particular technologies or standards can be quickly rendered inadequate or redundant;
- **address the role of all stakeholders in the security equation** – including Australian and offshore governments, equipment vendors, carriers/CSPs and end users. The complex and globally interconnected nature of today's telecommunications mean that there is a limit to the effectiveness of domestic regulation since much network traffic will be vulnerable to access outside Australia. Accordingly, a broader strategy to work towards "end-to-end" security outcomes is needed;

- **clearly emphasise the need for appropriate risk assessment** – network security threats are growing in number and threats are increasingly unpredictable. We believe that any obligation on carriers/CSPs should be based on what is reasonable and proportionate in the circumstances;
- **not require major business decisions or network designs to be provided to the Government** – this approach is not consistent with an “outcomes based” model and goes significantly further than the notification models adopted in comparable jurisdictions; and
- **have a graduated and proportionate enforcement regime** – as the Discussion Paper notes, there are already relevant enforcement mechanisms and national security provisions in the *Telecommunications Act 1997* (Cth) (**Telco Act**). In our view, only incremental changes to the enforcement mechanisms in the Telco Act are required.

Introduction

Huawei is pleased to have this opportunity to comment on the Attorney-General's Department's discussion paper, *Equipping Australia against Emerging and Evolving Threats (Discussion Paper)*.

As a major telecommunications equipment vendor in Australia (rather than a carrier/CSP) we are not in a position to comment on the interception or intelligence gathering issues canvassed in the Discussion Paper. Our submission addresses only the proposal to amend the Telco Act to impose new obligations on the Australian telecommunications industry to address security risks, as set out in Term of Reference 16 (**Network Security Reforms**).

We acknowledge the importance of ensuring telecommunications legislation is sufficient to address growing threats to network security and we welcome the opportunity to contribute to the Network Security Reforms.

We strongly support measures which will create real improvements in the security of Australia's telecommunications networks. We believe a holistic and end-to-end approach to security is required, which addresses the broad range of security threats faced by networks,¹ and does so at each of the infrastructure, services and applications layers. In our view, confidence in the security and integrity of telecommunications networks is in the interests of all players in the Australian telecommunications industry, including the government, noting that:

- vendors are increasingly required by their customers to meet stringent security requirements – particularly as competition in the market intensifies. As a supplier to 45 of the world's top 50 telecommunications operators we understand these competitive pressures well. We are investing significant resources to ensure our products are secure and to assure our customers of this security;

- carriers/CSPs need to demonstrate their networks are safe and secure to win business, particularly in the market for security-conscious government and enterprise customers. This drives carriers/CSPs to require higher security standards from vendors; and
- end users' confidence in the security of telecommunications services and the integrity of telecommunications networks is essential to drive uptake in services. This will be important to realise the Australian Government's strategy of leveraging the digital economy to improve Australia's "*productivity, global competitive standing and improved social wellbeing*".²

Simply put, good network security is good business.

However, it is important the Network Security Reforms do not simply amount to additional red tape. They need to be effective in achieving better network security. To be effective, the Network Security Reforms need to focus on actual security risks rather than irrelevant criteria such as the country of origin of a vendor. They must also be proportionate to the regulatory costs imposed on industry (and, indirectly, on end users).

¹ These include threats to availability, integrity and confidentiality: ITU-T, *Recommendation X.805 Security Architecture for Systems Providing End-to-End Communications* (10/03).

² Department of Broadband, Communications and the Digital Economy, *Australia's Digital Economy: Future Directions* (2009) available at http://www.dbcde.gov.au/_data/assets/pdf_file/0006/117681/DIGITAL_ECONOMY_FUTURE_DIRECTIONS_FINAL_REPORT.pdf.

Our submission is intended to explain how the Network Security Reforms could achieve this objective:

- **Section 1** outlines our view of what effective Network Security Reforms would look like;
- while we are supportive of the proposed Network Security Reforms, **Section 2** outlines some areas where the approach set out in the Discussion Paper could be adjusted to improve the effectiveness of the reforms; and
- **Section 3** outlines Huawei's Cyber Security Global Policy.

1 What would effective Network Security Reforms look like?

The security of telecommunications networks is a significant and growing issue both in Australia and worldwide. We support the Australian Government taking steps to address this issue and believe the Discussion Paper sets out a sensible way to proceed. In this section we outline how the Network Security Reforms would most effectively promote improvements in network security – with the ultimate goal of improving confidence in Australia's telecommunications networks to maximise the opportunities created by the digital economy.

1.1 Effective reforms should be consistent with thriving competition and open markets

Every carrier, CSP and equipment vendor has a commercial interest in improving the security of their networks and equipment. We believe that competition in the market improves security outcomes and we welcome the Discussion Paper's acknowledgement that the free market creates incentives to ensure networks are

secure.³

The Discussion Paper notes that competitive neutrality is an “important element” of an effective regulatory system.⁴ Indeed, the Discussion Paper recognises the role of a competitive marketplace in achieving security outcomes – but notes that market players may have “incomplete information about the national security environment”.⁵ This can be addressed by ensuring stronger engagement between the Government and the industry. It is not a matter which should compromise Australia’s commitment to open and competitive markets.

Similarly, we note that the security thresholds adopted in the Discussion Paper – “competent supervision” and “effective control”⁶ – appear on their face to be competitively neutral. We fully support these standards provided that they will not be used to discriminate against any vendor – including based on their country of origin. To achieve the goal of better network security the Network Security Reforms should be consistent with open competition – and recognise that the most effective and innovative security measures emerge from a competitive environment where carriers, CSPs and vendors are able to compete on a level playing field.

We believe a commitment to competition should be a central tenet of the Network Security Reforms, for the following reasons.

³ Discussion Paper, p 31.

⁴ Discussion Paper, p 34.

⁵ Discussion Paper, p 31.

⁶ Discussion Paper, p 35–36.

(a) **Security improvements emerge from competitive pressures**

As we note in section 1.2 below, effective end-to-end security outcomes require input from all stakeholders.

As competition among players in the telecommunications sector has grown there is increasing competitive pressure to demonstrate the security and integrity of equipment, software and other components of telecommunications networks. Equally, there is increasing pressure on all stakeholders to introduce additional safeguards to reduce security vulnerabilities.

In the short term, demonstrating the security of their equipment is fundamental for market players to win business. Competition creates pressure to develop innovative security solutions, to identify security weaknesses and to address them as quickly and effectively as possible.

In the long term, promoting confidence in the integrity of telecommunications networks is essential for the industry and to driving growth in the use of telecommunications services. Ultimately the goal of all market players will be to ensure end-to-end security outcomes.

Competition has driven Huawei to invest significant resources in promoting network security and addressing the supply chain through the adoption of standards globally across the industry. In terms of our contribution to industry standards globally, we:

- have joined 132 domestic and international industry standards bodies, including the 3GPP, IETF, IEEE, ITU, BBF, OMA, ETSI, CCSA, and ATIS;

- occupy 180 leadership positions in these forums, including chairpersons of the ETSI, ATIS, IEEE-SA, OMA, TMF, and CCSA, WFA, and W3C; and
- are actively involved in these forums. For example, in 2011, we submitted more than 5,000 standard proposals as part of our engagement with these industry forums.

We have been recognised as a market leader in contributing to global telecommunications network and equipment standards. For example, in 2011 we received the TM Forum's Industry Leadership Award and an Outstanding Contributor Award.⁷

We believe our commitment to security has been a key factor in our commercial success. Network security is critical to network operators. We work with 45 of the world's top 50 telecommunications operators. We have achieved this market position by establishing open and transparent telecommunications solutions that meet the high standards of the world's tier 1 operators.

We also supply equipment for next generation fibre networks in the United Kingdom, Singapore, Malaysia and New Zealand (among others) – and this has often involved significant engagement and investment to

⁷ The TM Forum is a global, non-profit industry association focused on enabling service provider agility and innovation. See <http://www.tmforum.org/>.

ensure our customers and regulators have absolute confidence in the security of our products.⁸

Our success demonstrates the significant efforts we have undertaken in this area – and that we make the necessary investments to satisfy our customers of the integrity of our products. We believe these investments set a new benchmark for security.

A competitive marketplace is essential to spurring market players like Huawei to continue to invest in market-leading security solutions. Preventing a vendor from competing in a market purely because of its country of origin will deprive that market of such security benefits.

It is important to recognise that, for a “technology taker” like Australia, which has only a small local equipment industry,⁹ a competitive marketplace requires that all foreign vendors can compete and innovate in the Australian marketplace.

(b) **There is no evidence that “closed” ecosystems or barriers to trade improve security**

In our view, there is no evidence that supposedly “closed” ecosystems which discriminate against vendors from particular countries deliver better security outcomes.

As an example, Huawei does not have a meaningful presence in or market share of US tier 1 carrier networks, yet there is no evidence that this has made any difference to the security of those networks nor is there any evidence that its networks are any more secure than those in the United Kingdom or New Zealand (despite the fact that we have worked closely with major network operators in those countries, including supplying equipment for their next generation fibre networks). On the

supplying equipment for their next generation fibre networks). On the contrary, threats to US telecommunications networks continue to grow.¹⁰ For example, the number of incidents reported by US federal agencies to the US Computer Emergency Readiness Team increased from 5,503 incidents in 2006 to 42,887 incidents in 2011.¹¹

In fact, recent developments in the US suggest that even ardent advocates of national security such as Senator John McCain are moving

⁸ Huawei, *Huawei Opens Cyber Security Evaluation Centre in the UK* (Press Release, 6 December 2010) available at http://huawei.com/au/about-huawei/newsroom/press-release/hw-u_151000.htm. The centre was developed to test end-to-end solutions (both hardware and software) for its ability to withstand growing cyber security threats and UK government security standards.

⁹ An April 2012 IBISWorld report notes that "The Telecommunication, Broadcasting and Transceiving Equipment Manufacturing industry in Australia is constrained by a small local market, a lack of locally sourced components and investment in research and development, and high costs. Industry operators tend to concentrate on small niche markets, which are often outside the radar of large foreign transnational companies": IBISWorld, *Telecommunication, Broadcasting and Transceiving Equipment Manufacturing in Australia: Market Research Report* (April 2012) available at <http://www.ibisworld.com.au/industry/default.aspx?indid=266>.

¹⁰ In February 2011, the Director of National Intelligence noted that there had been a dramatic increase in malicious cyber activity targeting U.S. computers and networks, including a more than tripling of the volume of malicious software since 2009: see United States Government Accountability Office, *Cybersecurity: Continued Attention Needed to Protect Our Nation's Critical Infrastructure* (Testimony Before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives, 26 July 2011) p 6, available at <http://www.gao.gov/assets/130/126702.pdf>.

¹¹ United States Government Accountability Office, *Cybersecurity: Threats Impacting the Nation* (Testimony Before the Subcommittee on Oversight, Investigations, and Management, Committee on Homeland Security, House of Representatives, 26 July 2011) p 9, available at <http://www.gao.gov/assets/130/126702.pdf>.

away from prescriptive regulation which limits competition, and are instead looking to promote information-sharing and to "*leverage the ingenuity and innovation of the private sector*".¹²

(c) **An open vendor ecosystem will maximise the availability of emerging technologies for Australians**

We believe that an open ecosystem is particularly important to ensure Australians have early access to emerging technologies (particularly given the very limited domestic manufacturing industry). Foreign vendors like Huawei are driving innovation – including in security technologies, techniques and solutions. In terms of our contribution to innovation:

- we invest approximately 10% of our revenue in research and development each year;
- our research and development spend for 2011 totalled US\$3.76 billion (about 10% of the Australian Government's annual budget) and over the past decade totalled more than US\$15 billion. This was achieved through 23 research and development centres worldwide; and
- as of 2011, Huawei had 36,344 patent applications filed in China, 10,650 filed under the Patent Cooperation Treaty and 10,978 filed in other jurisdictions. We have been awarded 23,522 patent licenses, 90% of which are invention patents.

The same applies to other vendors in China: indeed, China has now surpassed the US in terms of total patent filings.¹³

Discriminatory security reforms would limit investment, innovation and the availability of new technologies for Australian consumers, businesses and governments. As noted by the President of the Business Council of Australia:

Foreign investment is critical because it underpins our exporting industries, provides access to technology and know-how and makes a vital contribution to innovation.¹⁴

Discouraging investment and innovation will ultimately be to the detriment of network security outcomes.

Accordingly, the best way to promote security is to ensure the Network Security Reforms are consistent with an open, thriving and competitive marketplace.

1.2 Effective reforms would address the role of all stakeholders

As noted above, we understand and support the imperative of protecting national security.

¹² Michael S Schmidt, "Senators Force Weaker Safeguards Against Cyberattacks", *New York Times* (27 July 2012) available at <http://www.nytimes.com/2012/07/28/us/politics/new-revisions-weaken-senate-cybersecurity-bill.html>.

¹³ Steve Lohr, "When Innovation, Too, Is Made in China", *New York Times* (1 January 2011) available at <http://www.nytimes.com/2011/01/02/business/02unboxed.html>.

¹⁴ Tony Shepherd, President, Business Council of Australia, "Chasing the fast boat to Asia", *Sunday Morning Herald* (20 December 2011) available at <http://www.smh.com.au/business/chasing-the-fast-boat-to-asia-20111219-1p2dc.html>.

However, it is important the Network Security Reforms recognise that effective security involves inputs from many stakeholders – security is a responsibility which needs to be shared between governments, software suppliers, equipment vendors, network operators and end users. Network Security Reforms cannot be effective unless they form part of a broader strategy which addresses the responsibilities of each of these stakeholders in an end-to-end model (and covering security at the infrastructure, services and application layers). As the International Telecommunications Union has recognised:

*Security must not only be a thread of concern for each product or service, but must be developed in a manner that promotes the interweaving of security capabilities in the overall end-to-end security solution.*¹⁵

We note that many of the recently reported recent network security breaches in Australia have resulted from human errors or deliberate breaches by internal staff – rather than inherent weaknesses in network architecture or equipment.¹⁶ The Australian Government's Defence Signals Directorate has also indicated that at least 85% of the targeted cyber intrusions that it responded to in 2010 could have been prevented by following just four mitigation strategies, being:

- patching applications;
- patching operating system vulnerabilities;
- minimising the number of users with administrative privileges; and
- "white-listing" applications so that unapproved programs are unable to run.¹⁷

This suggests that even government users could take basic steps to prevent

security intrusions – and that responsibility for security should not lie wholly with carriers/CSPs or vendors.

Further, the globally interconnected nature of today's telecommunications means that there is a limit to the ability of domestic regulation to achieve security outcomes on an end-to-end basis. For example, Australian internet traffic is estimated to grow over four-fold from 2011 to 2016, a compound annual growth rate of 36%.¹⁸ The vast majority of growth is in international connectivity: for example, regionally, international bandwidth requirements grew by 47% between 2007 and 2011.¹⁹ This means that the majority of Australian network traffic will be vulnerable to unauthorised access at a point *outside* Australia and cannot be entirely protected by any reforms enacted by the Australian Government.

In this context, there is a clear limit to the effectiveness of Network Security Reforms which are aimed solely at Australian carriers/CSPs. We recognise that reforms directed at carriers/CSPs are worthwhile and should be pursued.

¹⁵ ITU-T, *Recommendation X.805 Security Architecture for Systems Providing End-to-End Communications* (10/03).

¹⁶ See, eg, ABC News, *Medicare privacy breaches 'only the beginning'* (3 March 2010) available at <http://www.abc.net.au/news/2010-03-02/medicare-privacy-breaches-only-the-beginning/347648> and ABC News, *Vodafone says security breach a 'one-off'* (10 January 2011) available at <http://www.abc.net.au/news/2011-01-09/vodafone-says-security-breach-a-one-off/1899268>.

¹⁷ Australian Government Defence Signals Directorate, *Top 35 Mitigation Strategies* (2012) available at <http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm>.

¹⁸ Cisco, *VNI Forecast Highlights: Australia* (2012) available at http://www.cisco.com/web/solutions/sp/vni/vni_forecast_highlights/index.html#%7ECountry.

¹⁹ TeleGeography, *International Bandwidth Demand Grows 45 Percent* (18 July 2012) available at <http://www.telegeography.com/press/marketing-emails/2012/07/18/international-bandwidth-demand-grows-45-percent/index.html>.

However, we suggest that they form part of a broader strategy to address security vulnerabilities on an end-to-end basis. This would include greater inter-governmental co-operation, the further development of global security standards, a greater focus on educating and monitoring access to telecommunications systems and data, promoting a more coordinated approach to security issues by carriers/CSPs and vendors, as well as better end user education.

In our view, the Network Security Reforms should be part of a holistic solution to improve network security standards.

Effective Network Security Reforms need to form part of a broader strategy which will address the role of all stakeholders in Australia and elsewhere.

1.3 Effective reforms should be dynamic, flexible and outcomes-based

Protecting network security is a dynamic process – it needs to be flexible and allow industry players to quickly respond to new and unanticipated types of security threats.

We agree with the concerns previously expressed by other members of the Australian telecommunications industry that it is not appropriate for the Government to impose prescriptive technical requirements. We therefore welcome the Discussion Paper's preference for an

approach that avoids the need for government approval of network architecture at a technical or engineering level and instead focuses on the security outcome, leaving industry to choose the most effective way to achieve it.²⁰

In our view a dynamic, outcomes-based approach has the following advantages.

(a) Flexible, outcomes-based regulation will be more effective

(a) Flexible, outcomes-based regulation will be more effective

Detailed and prescriptive regulation is not well suited to the emerging security challenges facing telecommunications networks worldwide. This is because network security standards which mandate the use of particular technologies or standards can be quickly rendered inadequate or redundant.

We note that these same concerns have been expressed in the US. The US Telecommunications Industry Association has noted, for example, that

*imposing rigid regulatory requirements that by their nature will be unable to keep up with rapidly evolving technologies will require industry to focus on meeting obsolete security requirements rather than the actual threat at hand, which will in effect make critical infrastructures and the customers that they serve less secure.*²¹

(b) Carriers/CSPs are best placed to identify appropriate compliance strategies

In our view, the Discussion Paper is correct in noting that carriers/CSPs themselves will be best placed to identify the most effective and efficient

²⁰ Discussion Paper, p 35.

²¹ Telecommunications Industry Association, *Innovation White Paper: Securing the Network* (24 July 2012) available at <http://www.tiaonline.org/policy/white-papers>.

way to achieve compliance rather than Government dictating particular technical solutions to be adopted.²²

In our experience as an equipment vendor, carriers/CSPs can comply with an obligation to exercise "competent supervision" and "effective control" over their networks (as referred to in section 3.2 of the Discussion Paper) in many ways, including for example through:

- implementing hardware/software solutions;
- taking measures to address personnel risks (such as monitoring of network use and human "checks and balances"); and
- limiting electronic access to sensitive information/data and physical access to network components.

Furthermore, carriers'/CSPs' typical contractual arrangements with vendors will normally include significant technical and security requirements which apply to the vendor's equipment and will provide the carrier/CSP with a full suite of indemnities, suspension and termination rights in the event of a breach by the vendor.

The most appropriate technologies and strategies to achieve security objectives will depend on many factors including the network topology, the existing technology, the costs of the solutions and capital available. Equally, the available solutions will change over time due to market and technological developments. In our view, an outcomes-based approach allows carriers/CSPs to adopt the solutions which are most appropriate for their networks.

(c) Carriers/CSPs will have increased regulatory certainty, more

autonomy over compliance and greater ability to manage costs

An outcomes-based approach will provide carriers/CSPs with flexibility to achieve the Government's desired outcomes in the most efficient way possible. We believe that that an outcomes-based approach is the only option that complies with the Discussion Paper's principle that the regulatory system "*not be resource-intensive for industry to comply with*".²³

Finally, we note that carriers/CSPs are familiar with outcomes-based legislation in Australia and that it has been successfully adopted in areas such as interception capability requirements (see further section 2.3 below). We believe outcomes-based legislation is tried, tested and effective.

We commend the approach proposed in the Discussion Paper; we believe effective Network Security Reforms should reflect a flexible, outcomes-based approach.

2 Refining the Network Security Reforms

While we are supportive of the proposed Network Security Reforms, in our view some aspects of the approach outlined in the Discussion Paper would limit the reforms' effectiveness.

²² Discussion Paper, p 35.

²³ Discussion Paper, p 34.

2.1 **Greater emphasis is needed on applying security standards in a technology neutral and vendor neutral way**

We note that the Discussion Paper proposes introducing obligations based on the concepts of “competent supervision” and “effective control”. We support these as obligations and they appear to be technology neutral and vendor neutral.

However, the Terms of Reference suggest that the Network Security Reforms are intended to mitigate “*the risks posed to Australia’s communications networks by certain foreign technology and service suppliers*”.²⁴ In this context, we continue to have concerns about:

- the lack of an unequivocal commitment in the Discussion Paper to security standards being technology and vendor neutral; and
- the risk that apparently neutral standards will be applied by regulators in a way that discriminates against vendors based on their country of origin and not on a proper assessment of security risk.

An important safeguard to ensure the competitive neutrality of any reforms is that affected stakeholders have the opportunity to understand and address specific concerns – rather than being subjected to regulations which are based on rumours and accusations instead of objective evidence and legitimate security concerns.

Application of the apparently neutral obligations of “competent supervision” and “effective control” in a way that discriminates against vendors from a particular country – especially if there is no right of review or response – could significantly affect the ability of those vendors to compete effectively in Australia. In our view, such regulatory risks could also affect the attractiveness of Australia as an investment destination and the willingness of foreign firms to do business in

(a) Open access for vendors would be beneficial to network security

We believe open access for vendors would be beneficial to competition and innovation – which would enhance security. As noted in section 1.1 above, thriving competition offers the most compelling incentives for all stakeholders to protect network security. For example, in the highly competitive equipment vendor market security issues play a critical role in establishing a competitive edge. Competition promotes a far greater diversity of products and services, including security products and services.

In Australia we have supplied network equipment to many of Australia's major carriers and we are proud of our reputation as a competitor in the market. We believe competition has led to substantial improvements in network security – both for our own products and for the industry as a whole.

Regulation which decreases competition would ultimately result in sub-optimal security outcomes.

²⁴ Discussion Paper, p 7.

(b) Open access for vendors increases the availability of telecommunications services and benefits of the digital economy

Vendor competition also delivers better prices for carriers/CSPs and this leads directly to lower prices for government, business and consumer end users.

We believe the vibrancy of the telecommunications equipment market in Australia has led to real benefits for Australian consumers in terms of price and innovation. For example, the Australian China Business Council has noted the

strong evidence pointing to the positive effect of trade on prices across a range of categories including telecommunications ... contributing to further downward pressure on prices in Australia.²⁵

Indeed, the Council has noted that

Trade with China has helped keep inflation low. Over the past few years significant increases have been observed in the prices of sectors such as housing, health and education products. However, price deflation has been evident in telecommunications equipment and clothing – two significant imports from China. From June 2007 to June 2011, telecommunications equipment import prices decreased at an annual average rate of 10 per cent, while clothing import prices decreased at 0.6 per cent. This compares with an increase in the consumer price index of 3.2 per cent within the same period.²⁶

The Council has also noted that:

The Council has also noted that:

Analysis by the ABS ... suggests that relatively low average annual rates of price inflation for telecommunication services over the past decade (0.9 per cent) may have contributed to the comparatively strong growth observed in per capita consumption of communication services. The cheaper mobile phones made in China has facilitated the social revolution in communication by Australian households.²⁷

We believe the importance of open markets and their contribution to lower prices and increased use of telecommunications services in Australia should be an important consideration for the Committee.

We believe access to innovative, market-leading technologies from leading global corporations such as Huawei is essential for Australian businesses: enabling them to grow, add value and export back into global supply chains and technology markets.

We also believe discriminatory regulation risks resulting in higher end user costs, less equipment availability and reduced innovation. This should be particularly important given the cost of living pressures facing Australians and the level of government investment in

²⁵ Australia China Business Council, *How China Trade Benefits Australian Households* (2012 update) p 3.

²⁶ Australia China Business Council, *How China Trade Benefits Australian Households* (2012 update) p 10.

²⁷ Australia China Business Council, *How China Trade Benefits Australian Households* (2012 update) p 30.

telecommunications infrastructure, which is aimed at improving Australians' access to affordable telecommunications.

(c) Implications for Australia's commitment to free trade

Approaches that target particular vendors or vendors from particular countries could also raise concerns about Australia's World Trade Organization (**WTO**) commitments, which require any barriers to trade to be no more trade-restrictive than necessary to fulfil the legitimate objective of protecting national security.

Under the *General Agreement on Tariffs and Trade (GATT)*, WTO members are essentially required not to discriminate against imported products on the basis of their country of origin. If the Network Security Reforms result in discrimination against vendors on the basis of their country of origin, it is likely that this would place Australia in breach of its WTO obligations under the GATT.

In particular, we note that the "national security" exceptions to this obligation apply in very limited circumstances. These exceptions are unlikely to support the discriminatory application of domestic regulation in a way that imposes unfair barriers on certain foreign vendors.²⁸

We believe similar concerns would arise in relation to Australia's commitments under the *Agreement on Technical Barriers to Trade*.

(d) Open access is the only rational approach given the complexity of the global supply chain

Finally, we note that an approach which targets vendors from particular countries would be impossible to rationally enforce given:

- the complexity of the global supply chain;
- that every major telecommunications equipment provider has substantial manufacturing and R&D bases in China; and
- that major telecommunications vendor have very similar global supply chain structures.

While the Discussion Paper may have focused on telecommunications networks, it needs to consider all technology from all vendors.

A single piece of equipment, such as a laptop, can include components from all over the world, from Canada, Ireland, Poland, Italy, the Czech Republic, the Slovak Republic all the way to China, Israel, Japan, Malaysia, the Philippines, Singapore, South Korea, Taiwan, Thailand, Vietnam and many others.

The Chinese city of Chengdu has 16,000 companies registered and 820 of them are foreign-invested companies.²⁹ Of these, 189 are Fortune 500 companies. Household brand names such as Intel, Microsoft, SAP, Cisco, Oracle, BAE, Ericsson, Nokia, SAP, Boeing, IBM and Alcatel-Lucent are all located there to name but a few.

²⁸ Namely, in relation to fissionable materials, traffic in arms or measures taken in times of war or other emergency in international relations: *GATT* art XXI.

²⁹ ChengDu Hi-Tech Industrial Development Zone, *West Park*, available at http://www.chengduhitech.co.uk/Location/West_Park.asp.

Every major telecommunications equipment provider has a substantial base in China. Alcatel-Lucent has its largest manufacturing base globally in China and is backed by a Chinese Government State Owned Enterprise;³⁰ Ericsson's joint-venture Nanjing Ericsson Panda Communications Co. has become the largest supply centre of Ericsson in the world;³¹ Nokia-Siemens has 14 wholly owned or joint ventures in China, and its factory in Suzhou manufactures a third of its global production of wireless network products.³²

Cisco also has a huge presence in China, with R&D centres in six major cities. Over 25% of all Cisco products are produced by Chinese partners, and the company announced a US\$16 billion investment in China that includes training 100,000 network engineers with China's Education Ministry and the opening of 300 centres at vocational colleges to train students in networking technologies.³³

Conversely, in terms of Huawei's supply chain diversity, about two thirds of our components come from suppliers outside of China (32% from the US and 32% from Taiwan and Europe).

Given this context, making distinctions between vendors based on their country of origin is neither rational nor effective. Indeed, the US Telecommunications Industry Association has noted that:

"The global ICT industry depends on a globally flexible supply chain, characterised by intense competition and fluctuation in price and supply of different inputs. Indeed, market demands are such that it would be impractical for the commercial sector to eliminate the use of global resources or a distributed supply chain model. As a result, TIA believes the focus of security concerns should be in how a product is made – not where".³⁴

We believe that the Network Security Reforms need to be applied in a competitively neutral way and that this concept should be hard-wired into any legislative reforms. In this respect, we note that of the key countries which have enacted network security reforms (which are outlined in the Annexure), *none* of those countries have adopted laws which are technology or vendor specific.

2.2 There needs to be a clear emphasis on risk assessment

It is also important that the obligations are proportionate – they should balance the reduced network security risks against the costs which would be imposed on carriers/CSPs. While the Discussion Paper notes that compliance would be assessed “based on a risk assessment to inform the level of engagement required”,³⁵ there is no indication that the security obligations themselves would reflect a proportionate, risk management approach.

³⁰ “ASB chairman seeks bigger, global role”, *China Daily* (17 November 2011) available at http://www.china.org.cn/business/2011-11/17/content_23943450.htm.

³¹ Panda Electronics, *Nanjing Ericsson Panda Communication Co Ltd*, available at <http://www.panda.cn/SJTCMS/html/pandastock/stocken200811/28647428.asp>.

³² Nokia Siemens Networks, *Nokia Siemens Networks celebrates another milestone in China*, 16 December 2011, available at <http://blogs.nokiasiemensnetworks.com/news/2011/12/16/nokia-siemens-networks-celebrates-another-milestone-in-china/>.

³³ Joe McDonald, “Cisco Announces \$16B China Expansion”, *USA Today* (11 January 2007) available at http://www.usatoday.com/tech/products/2007-11-01-425344141_x.htm.

³⁴ Telecommunications Industry Association, *Innovation White Paper: Securing the Network* (24 July 2012) available at <http://www.tiaonline.org/policy/white-papers>.

³⁵ Discussion Paper, p 36.

In our view it would not be rational to impose significant new costs on the Australian telecommunications industry (costs which will inevitably be passed through to Australian businesses and consumers) in circumstances where there will be little impact on overall security – for example, because of weaknesses in overseas telecommunications networks or end users' failure to adopt simple security measures.

Any requirements imposed need to be based on the level of risk and a realistic evaluation of the effectiveness and cost of implementing security measures. It also needs to recognise that even if carriers/CSPs are adopting "competent supervision" and "effective control" over a network, it will not be possible to guarantee security outcomes given:

- as noted above, there are many other stakeholders involved in ensuring security outcomes – including end users themselves;
- the complexity and scale of telecommunications equipment and software is continuing to increase drastically. For example, the move from closed, dedicated telecommunications infrastructure to IP-based systems and open signalling protocols means that there are increasing opportunities for vulnerabilities; and
- the sheer number of security vulnerabilities and instances of breaches is increasing exponentially. For example, in 2011, the incidence of smartphone malware increased 7 times over that in 2004.³⁶

Even Governments and large enterprises with significant resources devoted to IT security have suffered from cyber-attacks and unauthorised intrusions into their networks.³⁷ These breaches demonstrate that security breaches may occur despite "best efforts" being undertaken. It is precisely for these reasons that hypersensitive communications such as those of the Department of Defence are

carried over secure private networks instead of public networks.

In the Annexure to our submission, we have outlined the regulatory approaches taken by other countries to improve telecommunications network security. We note that some countries have limited their network security regulation to networks which serve critical functions (such as power grids). Each country which has adopted network security laws which apply to public telecommunication networks specifically requires network operators to adopt a risk management approach – such as by reference to what is “appropriate” or “state of the art” – rather than requiring them to guarantee complete security.

We believe this is the only practical approach to managing the challenges of network security and that the Network Security Reforms should incorporate a concept of proportionality (for example by requiring carriers/CSPs to take reasonable steps to achieve the required security outcomes).

2.3 There should not be a government role in reviewing or approving procurement decisions or network designs

We have significant concerns about the proposal to oblige carriers/CSPs to provide information to the Government, in advance, about significant business and procurement decisions and network designs.³⁸

³⁶ F-Secure, *Mobile Threat Report* (Q4 2011) p 7, available at http://www.f-secure.com/weblog/archives/Mobile_Threat_Report_Q4_2011.pdf.

³⁷ CRN, *Hackers claim Aus government email breach* (9 November 2011) available at <http://www.crn.com.au/News/279565.hackers-claim-aus-government-email-breach.aspx>.

³⁸ Term of Reference 16(b) or, as set out in the Discussion Paper, “an obligation for [carriers]/CSPs to provide Government, when requested with information to assist in the assessment of national security risks to telecommunications infrastructure”: Discussion Paper, p 34.

As noted above, carriers/CSPs have a critical business interest in ensuring their networks are secure. Security is critical to winning business in a competitive telecommunications market.

Australian public network operators such as Telstra, Optus and VHA are tier 1 operators with significant experience managing and a keen appreciation of national security issues. To the extent the Australian Government is concerned about a "a lack of awareness of national security risks"³⁹ on the part of carriers/CSPs, we support the Discussion Paper's proposal to deal with this problem through engagement by the Government with carriers/CSPs to share knowledge and disseminate information on an "as needs" basis. This is preferable to a regime where significant procurement decisions must be notified to the Government as proposed.

(a) **The proposal is not outcomes-based**

This regulatory approach misses the point that carriers/CSPs are far better at making procurement decisions and that they have a critical commercial interest in making their networks secure. Any suggestion that Government approval be required of carrier/CSP procurement decisions is anathema to a modern, competitive telecommunications industry.

Consistent with the rationale for an "outcomes-based" approach, we believe compliance needs to be assessed on results and without undue scrutiny of carrier/CSP legitimate business decisions. We believe this type of scrutiny would discourage carriers/CSPs from being able to make rational, timely commercial judgments about managing risk.

(b) **The proposal goes well beyond what is required in other jurisdictions**

A notification obligation would go far beyond what has been adopted in other jurisdictions. We are not aware of any developed jurisdiction which requires network operators to seek Government approval for procurement decisions or network designs.

The European approach has been to:

- permit regulators to request information from operators to assess operators' compliance with security standards; and
- impose an obligation on operators to notify regulators only in the event of an actual security incident.

We believe this is a more proportionate and workable approach.

There are existing reporting regimes in Australia which could be applied and which would better reflect an outcomes-based approach. For example, the *Telecommunications (Interception and Access) Act* provides for carriers/CSPs to provide annual interception capability plans so that the Government can be satisfied that their networks can be intercepted for law enforcement. In our view it would be far more appropriate and less invasive for these types of alternatives to be considered. We request the Committee give consideration in its report to options such as:

- "exception"-based reporting system (as adopted in the European Union); and/or

³⁹ Discussion Paper, p 33.

- regular reporting about the provision of high level information about risk identification and mitigation strategies (similar to the model adopted in Australia in respect of interception capability).

Alternatively, we consider that accreditation of a network's security via industry bodies such as Communications Alliance may be a viable alternative, noting that the Discussion Paper expressly contemplates "*a role for third parties in providing audit and assurance services*".⁴⁰

If the Committee believes additional measures are justified to meet network security goals, we believe independent verification of vendor hardware and software for use in critical networks may be an alternative (as has been adopted for Huawei equipment being used by BT in the United Kingdom). However such verification would at the very least need to:

- apply to all vendors in a non-discriminatory fashion;
- be undertaken by independent third parties; and
- ensure any audits or verification are performed efficiently.

2.4 The enforcement regime should be proportionate and appropriate

As the Discussion Paper notes, there are already relevant enforcement mechanisms and national security provisions in the Telco Act. In particular we note that:

- carriers/CSPs are required to do their best to prevent their networks and facilities from being used to commit offences and to assist authorities to safeguard national security;⁴¹

- carriers/CSPs may be requested to suspend the supply of a carriage service where reasonably necessary to prevent or reduce the likelihood of certain emergencies;⁴²
- the ACMA has a broad power to give carriers/CSPs binding directions (including about national security matters);⁴³ and
- the Attorney-General may direct a carrier/CSP not to use or supply a carriage service, if the Attorney-General considers that the use or supply is or would be prejudicial to security.⁴⁴

Accordingly we do not see a need for Network Security Reforms to involve a significant overhaul of the enforcement regime – particularly at the harsher end of the scale. In our view, only incremental changes to the enforcement mechanisms in the Telco Act are required.

For example, we note that the ACMA already has powers to give directions to a carrier/CSP “in connection with performing any of the ACMA's telecommunications functions or exercising any of the ACMA's telecommunications powers”.⁴⁵ However, we agree with the Discussion Paper's suggestion that a power of direction should only be used in the event of a breach,

⁴⁰ Discussion Paper, p 37.

⁴¹ Telco Act s 313.

⁴² Telco Act s 315.

⁴³ Telco Act s 581(1).

⁴⁴ Telco Act s 581(3).

⁴⁵ Telco Act s 581.

after close consultation with the carriers/CSP involved and applying the safeguards set out in the Discussion Paper.⁴⁶

We also acknowledge that it may also be appropriate for a Court to order financial penalties in the event of a breach. However, in our view it would be essential that a “breach” is defined as a failure by the carrier/CSP to take reasonable steps to ensure “competent supervision” and “effective control” over their network. This is consistent with similar legislation enacted in Europe, which refers to whether risks are “appropriately” managed or takes into account whether mitigation measures are “state of the art”. If a security issue is undetectable, entirely new and could not have been prevented by taking reasonable steps, in our view a carrier/CSP should not be liable so long as it took all reasonable remedial steps once the issue was detected.

2.5 Should the regime apply to existing network infrastructure?

Finally, we note that the Discussion Paper states that the new obligations:

*will require the application of mitigation measures to existing infrastructure. The security obligations would apply to existing and new infrastructure. Government recognises that it would need to work closely with industry to ensure that there is a reasonable transition period.*⁴⁷

We understand that carriers/CSPs are extremely concerned about the costs and technical complexity of applying the proposed regulatory regime to existing infrastructure. We appreciate these concerns and believe that the Committee should consider whether it would be appropriate for regulation to impose significant additional costs on investments which have already been made.

3 Huawei and Cyber Security

3.1 Cyber Security as a Global Corporate Policy

3.1 Cyber Security as a Global Corporate Priority

Huawei has always understood that to provide the level of confidence required in a small number of markets by customers who have been “challenged” by their local or regional political or commercial environments to “buy local” or “buy Western” may require us to provide independent assessments of our products and processes along with dedicated localisation to ensure that the integrity of the supply and support flow is maintained to a high degree of security assurance.

We have established and implemented an end-to-end global cyber security assurance system. We emphasise that our commitment to cyber security will never be outweighed by the consideration of commercial interests. It is our primary responsibility and guiding principle to ensure the stable and secure operation of our customers’ network and business (especially in times of natural disasters such as earthquakes and tsunamis and other emergencies); we understand that cyber security concerns of the industry and society are increasing.

3.2 Designing security from within – “built-in” not “bolted-on”

- Huawei has established standardised business processes globally and has identified Key Control Points (**KCPs**) and Global Process Owners (**GPOs**) for each process. In addition, Huawei has established a Global Process Control Manual and a Segregation of Duties Matrix that are applicable to all subsidiaries and business units. The GPOs are responsible for ensuring the overall internal control effectiveness, in light of changes in operational environment and risk exposures.

⁴⁶ For example, that directions would be preceded by engagement with the relevant carrier/CSP and a graduated suite of other enforcement mechanisms: Discussion Paper, p 37.

⁴⁷ Discussion Paper, p 39.

- From a governance perspective, there is a standing Board Committee dedicated to cyber security chaired by a Deputy Chairman. On this Board sits the main Board Members and Global Process Owners who have a role in ensuring that cyber security requirements are imbedded in processes, policies and standards and that they are executed effectively. If there is any conflict, or resource issue, then this committee has the power, remit and seniority to make decisions and change the business without reference to anyone else.
- Huawei Auditors use the Key Control Points and the Global Process Control manual to ensure processes are executed and that they are effective. Audits, external inspections and third-party reviews all validate what is happening against what should happen. Individual personal accountability and liability (the rules and regulations) are built into Huawei's Business Conduct Guidelines that specify how we must behave in our daily operations. Every person is updated through online exams every year to keep knowledge current and this forms part of our Internal Compliance Programme.

3.3 Going Forward - Together

Guiding Principles

1. **IT'S GLOBAL:** Efforts to improve cyber security must properly reflect the borderless, interconnected and global nature of today's cyber environment in terms of governance, laws, standards and sanctions
2. **IT'S THE LAW:** Efforts to harmonise and align international laws, standards, definitions and norms must be undertaken, accepting the challenges of cultural differences
3. **IT'S COLLABORATIVE:** Efforts to improve cyber security must leverage public-

3. **IT'S DOING THE BASICS:** Efforts to improve basic cyber security "hygiene" must be collectively prioritised to drive the entry point of successful attack to a much higher point
4. **IT'S STANDARDS-BASED:** Efforts to design, agree on and implement international standards and benchmarks of ICT vendors should set the highest, not lowest, requirements and standards
5. **ITS VERIFICATION-BASED:** Efforts to design, develop and implement global independent verification methodologies that ensure products conform to the agreed standards and benchmarks should be mandated
6. **IT'S EVIDENCE-BASED:** Efforts to improve cyber security must be based on evidence of risk, evidence of the attacker and evidence of loss or impact – we should focus on facts, not fiction
7. **IT'S DOING THE BASICS:** Efforts to improve basic cyber security "hygiene" must be collectively prioritised to drive the entry point of successful attack to a much higher point

This submission favours and supports international collaboration, openness and trust as the foundation for a world where technology can continue to drive economic and social improvement for the majority of the seven billion citizens on the planet.

Annexure: comparison of public telecommunications

Jurisdiction	Security obligation	Notification obligations
<p>EU (Directive 2009/140/EC)</p>	<p>Providers of electronic communications networks and services should be required to take measures to safeguard their integrity and security in accordance with the assessed risks, taking into account the state of the art of such measures.</p>	<p>Both the European Network and Information Security Agency and the national regulators should take the necessary means to perform their duties, including powers to require sufficient information in order to assess the level of security of networks or services as well as comprehensive and reliable information about actual security incidents that have had a significant impact on the operation of networks or services.</p>
<p>UK (<i>Electronic Communications and Wireless Telegraphy Regulations 2011</i>)</p>	<p>Network and service providers must take technical and organisational measures appropriately to manage risks to the security of public electronic communications networks and services.</p> <p>The measures must include measures to prevent or minimise the impact of security incidents on end-users.</p> <p>Network providers must also take:</p> <ul style="list-style-type: none"> • measures to prevent or minimise the impact of security incidents on interconnection of public electronic communications networks; and 	<p>Network providers must notify Ofcom of:</p> <ul style="list-style-type: none"> • a breach of security; and • a reduction in the availability of a public electronic communications network which has a significant impact on the operation of a public electronic communications service. <p>Service providers must not notify Ofcom of a breach of security which has a significant impact on the operation of a public electronic communications service.</p> <p>Ofcom may notify the public electronic communications regulators, regulatory authorities of other member States and the European Network and Information Security Agency.</p>

Network security obligations in selected jurisdictions

	Verification obligations	Penalties
<p>and cy and uld have form their obtain der to of ll as e data ents that act on the ervices.</p>	<p>No specific reference to audits.</p>	<p>National regulatory authorities should have the power to issue binding instructions relating to technical implementing measures.</p> <p>In order to perform their duties, they should have the power to investigate cases of non-compliance and to impose penalties.</p>
<p>ntify id ability, act on a cations ify rity which the onic lic, other orities in ie ormation</p>	<p>Ofcom may carry out or arrange an audit of the measures taken by a network provider or a service provider at the provider's own cost.</p>	<p>Penalties may include:</p> <ul style="list-style-type: none"> • a fine of up to 10% of turnover (max £2 million); • suspension of the provider's entitlement to provide electronic communications networks or services; • payment of compensation to provider's customers; and • liability for any civil claims.

Jurisdiction	Security obligation	Notification obligations
	<ul style="list-style-type: none"> all appropriate steps to protect, so far as possible, the availability of the provider's public electronic communications network. 	Security Agency.
<p>Ireland (<i>European Communities (Electronic Communications Networks And Services) (Privacy And Electronic Communications) Regulations 2011</i>)</p>	<p>An undertaking providing a publicly available electronic communications network or service shall take appropriate technical and organisational measures to safeguard the security of its services, if necessary, in conjunction with undertakings upon whose networks such services are transmitted. These measures shall ensure the level of security appropriate to the risk presented having regard to the state of the art and the cost of their implementation.</p> <p>The measures referred to must at least:</p> <ul style="list-style-type: none"> ensure that personal data can be accessed only by authorised personnel for legally authorised purposes, protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or 	<p>In the case of a particular breach of the security of the communications network, the undertaking providing the publicly available electronic communications service must inform its subscribers concerning such risk without delay, and, where the risk lies outside the scope of the measures to be taken by the relevant service provider, indicate the possible remedies including the likely consequences of the breach.</p> <p>There are other notification provisions which are specific to personal data.</p>

	Verification obligations	Penalties
<p>risk of a e public the publicly communications scribers ut delay side the e taken by er, any g an ts</p> <p>1 fic to</p>	<p>The regulator may audit the measures taken by an undertaking providing publicly available electronic communications services and issue recommendations about best practices concerning the level of security which those measures should achieve</p>	<p>Penalties may include:</p> <ul style="list-style-type: none"> • a fine of up to €250,000; • a court order requiring data or material to be forfeited or erased; and • a direction to undertake specific measures or refrain from some activity.

Jurisdiction	Security obligation	Notification obligations
	disclosure, and <ul style="list-style-type: none"> • ensure the implementation of a security policy with respect to the processing of personal data. 	
New Zealand	None, however government agencies must comply with the NZ Inf	
Canada	None.	
Singapore	None, however the regulator has issued a <i>Secure and Resilient Inte</i>	
Malaysia	None, however a Security, Trust and Governance Department is ta	
United States	There are no legislative provisions directly creating security obliga infrastructure. Additionally, the FCC in practice requires foreign e Security Agreement.	
South Africa	None, however security obligations apply to certain "critical" data	

	Verification obligations	Penalties
Information Security Manual.		
<i>Internet Infrastructure Code of Practice.</i>		
linked with ensuring the reliability and the security of Malaysian networks.		
tions. However, there are certain Executive Directives related to protection of critical entities which acquire 25% of shares in a radio-telecoms licensee to enter into a Network		
cases (which may include telecommunications databases).		



Submission No 185

Inquiry into potential reforms of National Security Legislation

Name: Dr Vivienne Thom

Organisation: Inspector General of Intelligence and Security

Parliamentary Joint Committee on Intelligence and Security



Inquiry into potential reforms of national security legislation

Submission to the Parliamentary Joint Committee on Intelligence and Security

Dr Vivienne Thom
Inspector-General of Intelligence and Security

23 August 2012

Contents

Executive summary	3
Background.....	4
Role of the Inspector-General of Intelligence and Security.....	4
Basis of this submission	5
<i>Telecommunications (Interception and Access) Act 1979</i>	6
ToR 1 – Strengthening the safeguards and privacy protections under the lawful access to communications regime in the <i>Telecommunications (Interception and Access) Act 1979</i>	6
ToR 2 – Reforming the lawful access to communications regime.	8
ToR 3 – Streamlining and reducing complexity in the lawful access to communications regime.	9
ToR 4 – Modernising the TIA Act’s cost sharing framework	9
ToR 8 – Streamlining and reducing complexity in the lawful access to communications	9
ToR 9 – Modernising the Industry assistance framework	10
ToR 14 – Reforming the Lawful Access Regime	10
ToR 15 – Modernising the Industry assistance framework	12
<i>Australian Security Intelligence Organisation Act 1979</i>	14
ToR 5 – Amending the ASIO Act to modernise and streamline ASIO’s warrant provisions	14
ToR 6 – Modernising ASIO Act employment provisions	16

ToR 6 – Modernising ASIO Act employment provisions:..... 16

ToR 10 – Amending the ASIO Act to create an authorised intelligence operations scheme..... 17

ToR 11 – Amending the ASIO Act to modernise and streamline ASIO’s warrant provisions to: 19

ToR 12 – Clarifying ASIO’s ability to cooperate with the private sector. 21

ToR 13 – Enabling ASIO to refer breaches of section 92 of the ASIO Act to authorities 21

ToR 17 – Amending the ASIO Act to modernise and streamline ASIO’s warrant provisions: 21

Intelligence Services Act 2001 23

 ToR 7 – Clarifying the DIGO’s authority to provide assistance to approved bodies. 23

 ToR 18 – Amending the *Intelligence Services Act 2001* 23

Telecommunications Act 1997..... 26

 ToR 16 – Amending the Telecommunications Act to address security and resilience risks..... 26

Executive summary

The terms of reference for this inquiry set out a range of high-level proposals to ensure that Australian law enforcement, intelligence and security agencies are equipped to effectively perform their functions and cooperate effectively given the advances in technology, the changes to the ways that technology is used, and the need for increased cooperation between agencies.

This submission acknowledges these challenges and supports the need for the legislation to be reformed to ensure that it meets current and future requirements. The submission focuses on the requirement to address the needs of national security while ensuring that any response is proportional to the threat, safeguards the privacy of individuals, and includes effective accountability and oversight regimes.

The submission highlights the following issues that arise from the proposals:

1. Proposals to simplify, streamline or reduce administrative burdens must be examined closely to ensure that any proposals to standardise tests and thresholds for the use of powers take into account the nature of each of these powers and the level of intrusiveness. While having a single test might be administratively convenient it could allow the use of more intrusive powers where less intrusive ones are appropriate.
2. Proposals to increase the scope of existing powers or their duration need to ensure that safeguards exist such that the extended scope or longer timeframes do not become the norm, and that the warrants are not unduly broad and are executed reasonably and in accordance with the specifics of the legislation as well as the overarching privacy and

proportionality objectives.

3. Proposals that effectively transfer the level of decision-making from ministerial level to within an agency need to consider appropriate reviews within the agency, provide for independent scrutiny and consider external reporting requirements.
4. Proposals to increase the retention or sharing of data and personal information need to take account of the security, record-keeping and destruction requirements that are necessary to safeguard privacy and ensure that there is adequate oversight in place.
5. The proposal for ASIO to conduct authorised operations needs to ensure an appropriate balance between the requirement to protect sensitive national security information with the benefits of independent authorisation and detailed oversight and public reporting.

The Office of the Inspector-General of Intelligence and Security will continue to review activities of intelligence and security agencies to ensure that that each agency acts legally and with propriety, complies with ministerial guidelines and directives, and respects human rights. The proposed reforms are not insignificant and continuing proper oversight will be essential if Parliament and the public are to be assured that agencies use these powers appropriately. Although current funding for the office is adequate, the proposed reforms would require additional funding for the office to continue to perform its role effectively.

Background

Role of the Inspector-General of Intelligence and Security

The Inspector-General of Intelligence and Security (IGIS) is an independent statutory officer who reviews the activities of the agencies which collectively comprise the Australian Intelligence Community (AIC):

- Australian Security Intelligence Organisation – ASIO
- Australian Secret Intelligence Service – ASIS
- Defence Signals Directorate – DSD
- Defence Imagery and Geospatial Organisation – DIGO
- Defence Intelligence Organisation – DIO
- Office of National Assessments – ONA.

The Office of the IGIS is situated within the Prime Minister's portfolio and reports to the Special Minister for State for the Public Service and Integrity for administrative purposes; however, the IGIS is not subject to general direction from the Prime Minister, or other Ministers, on how responsibilities under the IGIS Act should be carried out.

The primary role and functions of the IGIS are set out in sections 8, 9 and 9A of the *Inspector-General of Intelligence and Security Act 1986* (the IGIS Act). This Act provides the legal basis for the IGIS to conduct inspections of the AIC agencies and to conduct inquiries, of varying levels of formality, as the need arises.

The overarching purpose of these activities is to ensure that each AIC agency acts legally and with propriety, complies with ministerial guidelines and directives, and respects human rights. A significant proportion of the resources of the office are directed towards on-going inspection and monitoring activities, so as to identify issues, including about the governance and control frameworks within agencies, before there is a need for major remedial action.

The inspection role of the IGIS is complemented by an inquiry function. The IGIS has own motion powers to investigate matters and conduct inquiries in addition to considering requests from Ministers and complainants. In undertaking inquiries the IGIS has strong investigative powers including the power to obtain information and can require any person to answer questions and produce relevant documents, take sworn evidence, and enter agency premises. IGIS inquiries are conducted in private because they almost invariably involve highly classified or sensitive information, and the methods by which it is collected.

Although the primary focus of the IGIS relates to the activities of the AIC agencies, an amendment to the legislation made in late 2010 allows the Prime Minister to request the IGIS to inquire into an intelligence or security matter relating to any Commonwealth agency. This provision has been used twice.

Basis of this submission

In general, it is not the role of the IGIS to comment on current or proposed government policy. However, there are some matters on which I have particular experience because of my oversight of the activities of the AIC. This experience may assist a body such as the Parliamentary Joint Committee on Intelligence and Security (the Committee) in considering legislative proposals. It follows then that my comments are focused on whether the proposals:

- have proper accountability and oversight mechanisms
- pose risks to legality or propriety
- are consistent with human rights
- address issues that I am aware of through my examination of agency operations.

I have a particular interest in whether proposed policies place sufficient weight on maintaining the privacy of individuals, and whether proposals reflect the concept of proportionality – that is, that the means for obtaining information must be proportionate to the gravity of the threat posed and the likelihood of its occurrence. As the exercise of agency powers will in the vast majority of cases not be apparent to the subject, and as they are by their nature often highly intrusive, these powers should only be considered for use when other, less intrusive, means of obtaining information are likely to be ineffective or are not reasonably available.

I have complete access to all documents of the AIC agencies and am often proactively briefed about sensitive operations. It is my expectation that AIC agencies will be forthright in briefing me on any legal and propriety issues that arise in operational planning or activity. This familiarity with agency operations and capabilities also allows me to give my views about some of the challenges outlined in

the discussion paper.¹

My comments are necessarily limited to the agencies and type of activities that I oversight. I cannot comment on these proposed legislative amendments insofar as they relate to the activities of law enforcement agencies, or the impact upon the telecommunications sector.

In addressing the terms of reference and commenting on the proposals, this submission also sets out some of the current oversight arrangements that are in place.

While this submission mentions some international comparisons these are indicative only as I have not conducted a comprehensive comparison.

This submission is structured to address the terms of reference by addressing each piece of legislation in turn. Numbers in the headings align with the numbering in the terms of reference (ToR). Relevant parts of the discussion paper are cross referenced.

¹ *Equipping Australia against emerging and evolving threats*,
http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=picis/nsi2012/additional/discussion%20paper.pdf, accessed 14 August 2012

Telecommunications (Interception and Access) Act 1979

ToR 1 – Strengthening the safeguards and privacy protections under the lawful access to communications regime in the *Telecommunications (Interception and Access) Act 1979*.

This would include the examination of:

- a. the legislation's privacy protection objective
- b. the proportionality tests for issuing of warrants
- c. mandatory record-keeping standards
- d. oversight arrangements by the Commonwealth and State Ombudsmen

The discussion paper suggests that it may be timely to revisit whether the privacy framework within the *Telecommunications (Interception and Access) Act 1979* (TIA Act) remains appropriate. It proposes 'reviewing the current checks, balances and limitations on the operation of interception powers will ensure that the privacy needs of contemporary communications users are appropriately reflected in the interception regime'.² The paper does not set out specific proposals as to how this is to be achieved.

The discussion paper notes that community views about access to communications may have changed along with their use and expectations of technology.³ It is certainly true that many in the community share personal data including their current location, email content, photographs, data of personal contacts, personal interests and buying patterns. It is not clear to what extent this sharing is conscious. In my view, it would not be appropriate to extrapolate from this behaviour to conclude that there is any diminished interest in the community about privacy issues and the desirability of having limits on government collection of information. It is clear to me from complaints to my office

having limits on government collection of information. It is clear to me from complaints to my office that there is still widespread concern in the community about covert, albeit lawful, access to personal information by intelligence and security agencies and the recording and communication of that information.

In light of this, any changes to the current system of checks, balances and limitations would require compelling arguments and should be given very serious consideration.

The paper also states that consideration is being given to 'introducing a privacy focused objects clause that clearly underpins this important objective of the legislation and which guides interpretation of obligations under the Act'.⁴

Although the primary objective of the TIA Act is to prohibit interception of telecommunication or access to stored communication except in certain prescribed and regulated circumstances, the range of exceptions has grown and, if the proposals in the discussion paper are accepted by Parliament, the ways in which interception can occur will continue to expand. A privacy-focused objects clause may address this apparent imbalance and ensure that the legislation is interpreted with the emphasis on protecting communications and privacy rather than facilitating exemptions.

The terms of reference also contemplate examining the proportionality tests for the issue of warrants. As discussed under ToR 2(b) below, any proposal to rationalise the types of warrants or

² Discussion paper, page 23

³ Discussion paper, page 23

⁴ Discussion paper, page 23

align thresholds will need to be examined carefully to ensure that it does not compromise proportionality tests or privacy objectives.

The discussion paper addresses record keeping and accountability obligations for law enforcement agencies.⁵ These agencies are required to keep records relating to documents associated with the warrants issued and particulars relating to warrant applications and each time lawfully intercepted information is used, disclosed, communicated, entered into evidence or destroyed.

Chief officers of law enforcement agencies are required to report to the Attorney-General on the use and communication of intercepted information and the Attorney-General must table a statistical report in Parliament. The Commonwealth Ombudsman oversees the use of TIA powers by Commonwealth law enforcement agencies and reporting requirements are set out in the TIA Act.

The oversight regime for ASIO is not specified in the TIA Act but, in practice, my office oversees ASIO's use of TIA powers under the inspection function in the IGIS Act. To assist the Committee in understanding the way this oversight occurs I have summarised the current inspection regime below:

Warrant related papers are examined so that we may be properly satisfied that:

- the intelligence or security case that ASIO has made in support of the application is soundly based and that all necessary legislative requirements have been met
- the individuals identified in each warrant are actually identical with, or closely linked to, persons of security interest (this is particularly relevant where a 'B-

Party' telecommunications interception warrant is being sought⁶)

- appropriate internal and external approvals for the request have been obtained
- the Director-General of Security has identified in writing those individuals who may execute the warrant, or communicate information obtained from the warrant
- written reports to the Attorney-General on the outcome of executed warrants are factual and provided in a timely manner
- the activity concerned did not begin before, or continue after, the period authorised by the warrant
- in the small number of cases where unauthorised collection has occurred, that prompt and appropriate remedial action has been undertaken.

In addition to our regular warrants inspections OIGIS staff undertake spot audits of ASIO's interception management systems. The purpose of these checks is to gain independent assurance that ASIO's collection activities are only occurring in accordance with the terms of a relevant warrant and related investigative authorities.

If any issues with warrants are identified, they are raised with the Director-General of Security to ensure that appropriate action is taken. Where appropriate I can also advise the Attorney-General of any concerns. I also include a summary of inspection activity in my

⁵ Discussion paper, pages 25-26

⁶ A so-called 'B-party' warrant allows ASIO to access the services of associates of persons of security interest see s. 9(1)(b) of the TIA Act

annual report. Generally the standard of warrant materials is very high and the error rate is low.⁷

Comprehensive record-keeping in ASIO is essential to ensure ASIO complies with the legislation and to enable effective oversight. Any proposal to change the record-keeping regime must consider the accountability requirements.

ToR 2 – Reforming the lawful access to communications regime.

- a. reducing the number of agencies eligible to access communications information

I have no comment on this proposal.

- b. the standardisation of warrant tests and thresholds

The discussion paper refers to four warrants for law enforcement agencies to access the content of communications and the types of offences for which a warrant can be obtained. The paper does not give much detail in relation to ASIO warrants, stating that 'ASIO's ability to intercept communications supports its functions relating to security'⁸. ASIO can currently obtain two types of telecommunication interception warrants from the Attorney-General to further its security functions: a telecommunications service warrant and a named person warrant.⁹ These can include authority to intercept 'B-party' services.¹⁰ ASIO can also obtain three types of warrants that relate to foreign intelligence including a service warrant and a named person warrant.¹¹ ASIO warrants automatically authorise access to stored communications.¹² Senior ASIO officers can authorise access to existing or prospective data.¹³

The tests and thresholds for each of the current ASIO warrants vary, corresponding to the intrusiveness of the warrant. For example a named person warrant is only available where a service warrant would be 'ineffective'¹⁴ and a 'B-party' warrant is only available where ASIO has exhausted all other practicable methods or interception would not otherwise be possible.¹⁵

In my 2010-11 annual report I noted that, in respect of 'B-Party' warrants:

In the course of our warrant inspections during 2010–11, OIGIS staff accessed and reviewed every 'B-Party' warrant which ASIO obtained. On the basis of these activities I am satisfied that this type of warrant continues to be used sparingly, and only where the special circumstances of each case dictated that it was appropriate and necessary.¹⁶

Broadly speaking, requests for warrants (other than B-Party warrants) to intercept communications in pursuit of ASIO's security function need to explain why the interception is *necessary* and why it is

⁷ Inspector-General of Intelligence and Security Annual Report 2010-2011, pages 27-29

⁸ Discussion paper, page 24

⁹ See ss. 9 and 9A of the TIA Act

¹⁰ A so-called 'B-party' warrant allows ASIO to access the services of associates of persons of security interest

¹¹ See s. 17(1)(e) of the ASIO Act and ss. 11A, 11B and 11C of the TIA Act.

¹² See s. 109 of the ASIO Act

¹³ This 'data' does not include the content of a communication. See ss. 175 and 176 of the TIA Act

¹⁴ See ss. 9A(1)(c) and 11B(1)(b)(iii) of the TIA Act

¹⁵ See s. 9(3) of the TIA Act

¹⁶ Inspector-General of Intelligence and Security Annual Report 2010-2011, page 28

reasonably suspected that the individual being targeted is engaged, or likely to be engaged, in activities prejudicial to security.¹⁷ For access to data the threshold is only that it be *in connection with* ASIO's function.¹⁸

By way of comparison, the threshold that needs to be met in the UK is that a proposed activity under a warrant needs to be *necessary* in the interests of national security and the conduct *proportionate* to what is sought to be achieved¹⁹. In Canada the judge issuing the warrant must be satisfied the warrant is *required* to enable investigation of a threat to security and that other investigative procedures have been tried and failed or are unlikely to succeed.²⁰ In the US interception is only conducted under court orders and, amongst other things, for the Federal Bureau of Investigations to obtain a warrant to intercept communications the judge must be satisfied that a particular serious offence is, or is about to be, committed, the court also plays a role in the ongoing supervision of the warrant.²¹

Any proposals to standardise security warrant tests and thresholds must take into account the nature of each of these warrants and the level of intrusiveness. A single test could allow the use of more intrusive powers where less intrusive ones are appropriate.

ToR 3 – Streamlining and reducing complexity in the lawful access to communications regime.

- a. simplifying the information sharing provisions that allow agencies to cooperate
- b. removing legislative duplication

The discussion paper suggests that simplifying the current information-sharing provisions would support co-operative arrangements between the agencies and that further consideration could be

given to the ways in which information sharing amongst agencies could be facilitated.²² There is no specific discussion of how this proposal would affect ASIO. I am not aware of specific legislative impediments to ASIO sharing information with other agencies that I oversight but I would note that any proposal to increase the sharing of information between agencies should address the security, record-keeping and destruction requirements that are necessary to safeguard privacy.

ToR 4 – Modernising the TIA Act’s cost sharing framework

- a. align industry interception assistance with industry regulatory policy
- b. clarify ACMA’s regulatory and enforcement role

I have no comments on these proposals.

ToR 8 – Streamlining and reducing complexity in the lawful access to communications

- a. creating a single warrant with multiple TI powers

Having multiple sets of warrant applications for a single investigation is administratively inconvenient for ASIO and does not necessarily provide the Attorney-General with a clear view of

¹⁷ See ss. 9(2)(b) and 9A(2)(c) of the TIA Act

¹⁸ This ‘data’ does not include the content of a communication. See ss. 175(3) and 176(4) of the TIA Act

¹⁹ See ss. 5(2) and (3) of the Regulation of Investigatory Powers Act 2000 (UK)

²⁰ See s. 21 of the Canadian Security Intelligence Services Act (R.S.C, 1985, c. C-23)

²¹ See for example Electronic Communications Privacy Act (18 USC ch 119)

²² Discussion paper, page 25

the totality of proposed activities. Any proposal to streamline this and give the Attorney-General a better picture of the situation is worthy of consideration but issues of proportionality and levels of authorisation will need careful consideration.

My understanding is that currently ASIO could legally combine multiple warrant applications into a single 'bundle' for the Attorney-General to consider. However, as discussed under ToR 2 above, there are currently different thresholds and tests depending on the intrusiveness of what is proposed. The warrant application bundle would need to set out how each test was satisfied so that the Attorney-General could make a decision about the use of each warrant type.

One interpretation of the proposal in the discussion paper could be that the Attorney-General is to be asked only to agree broadly to 'interception' against a particular individual, group or premises for a specified period and to then allow the Director-General of Security or a delegated ASIO officer to decide what form that interception should take during the warrant period (including whether B-Party interception is appropriate). I note that a 'named person warrant' currently allows the Director-General of Security to add or remove services from interception coverage during the life of the warrant to enable interception of communications made by or to the specified individual.²³ Any proposal to effectively further transfer the level of decision making from Ministerial level to within an agency needs to ensure that appropriate reviews take place within the agency, make allowance for independent scrutiny and consider external reporting requirements.

If such a proposal was implemented my office would monitor whether the use of the more intrusive powers increased with time.

It is also not clear how ToR 8 combines with ToR 14 (characteristic-based interception) and whether characteristics would also be able to be varied without reference to the Attorney-General.

ToR 9 – Modernising the Industry assistance framework

- a. Implement detailed requirements for industry interception obligations
- b. extend the regulatory regime to ancillary service providers not currently covered by the legislation
- c. implement a three-tiered industry participation model

I have no comments on these proposals.

ToR 14 – Reforming the Lawful Access Regime

- a. expanding the basis of interception activities

I understand this reform to be proposing what is described in the discussion paper as a warrant regime that is 'focused on better targeting the characteristics of a communication that enable it to be isolated from communications that are not of interest'.²⁴

My understanding is that the proposal would not actually enable agencies to collect communications that they cannot currently legally collect under a warrant or a combination of service, device and named person warrants. However the proposed scheme would enable the

²³ See ss. 9A and 11B of the TIA Act

²⁴ Discussion paper, page 25

warrant to be specific about particular characteristics of communications to be provided and thereby potentially oblige the carriers to sort those from other telecommunications traffic that could be covered by the existing warrants. I am also advised that ASIO considers the proposal would be administratively more efficient than having to potentially obtain a combination of other warrants; I have no reason to doubt this.

A key issue to be considered in this proposal is whether the warrants would be limited to interception based on the 'characteristics' described in the initial warrant (similar to a service warrant) or whether ASIO would itself be able to vary the warrant to add or remove 'characteristics' (similar to a named person warrant). If the proposal is for the latter then there needs to be certainty as to the parameters within which 'characteristics' can be added.

In the UK, for example, the relevant agency can vary the 'characteristics' upon which interception for national security purposes is undertaken but each warrant is limited to interception against one person or premises.²⁵ My understanding is that in the US and Canada the court order authorising the interception is to specify the person or premises and can be made by reference to a 'type of communications' but these 'types' cannot be later unilaterally be varied by the agency.²⁶

If the proposed warrant is not limited to a specified person or premises and allows ASIO to add and remove 'characteristics' during the life of the warrant it would substantially change the balance between what is currently decided by the Attorney-General and what is within the authority of the Director-General of Security. Such a change should take into account the need for effective internal and external review and consider reporting requirements. If the proposed change was limited to interception against a specified person it would be more akin to the current named person warrants.²⁷

A further issue is the technological capacity to actually undertake this type of 'characteristic'-based interception – including whether the carriers should be responsible for collecting, processing and delivering the communications of interest or whether the agencies should be permitted to collect and retain large amounts of information in order to find the communications of interest. It is outside my area of focus to comment on the technology, cost or burden sharing aspects of the proposal. However I would expect to see any regime include appropriate measures to ensure that the content of communications which were not the specific target of the warrant were not retained longer than necessary for 'sorting' and to ensure that such information is kept secure.

One of the important accountability and oversight requirements of the current regime is the requirement that ASIO provide a report to the Attorney-General after the expiration or revocation of each warrant. The report must include details of the telecommunications service to or from each intercepted communication was made as well as the extent to which the warrant has assisted ASIO

²⁵ See ss. 8(1) and 10(6) of the Regulation of Investigatory Powers Act 2000 (UK)

²⁶ See for example s. 21 of the Canadian Security Intelligence Services Act (R.S.C, 1985, c. C-23) and Electronic Communications Privacy Act (18 USC ch 119). However note that this submission is not based on a detailed study of the relevant overseas legislation

²⁷ Named person warrants can currently allow the Attorney-General to authorise interception of communications made to or from any service used by the specified person (see for example s. 9A(1)(b)(i) of the TIA Act). During the life of such a warrant the Director-General can add or remove any such services from interception coverage. However the Director-General cannot currently add a service used by a third person without a specific B-Party warrant nor can the Director-General add or remove services to be intercepted based only on proximity to a location.

in carrying out its functions.²⁸ This measure would be particularly important in maintaining oversight and accountability of any discretion to add new characteristics for interception.

ToR 15 – Modernising the Industry assistance framework

- a. establish an offence for failure to assist in the decryption of communications
- b. institute industry response timelines

I have no comments on these proposals.

- c. tailored data retention periods for up to 2 years for parts of a data set, with specific timeframes taking into account agency priorities, and privacy and cost impacts

This office has an interest in the amount of information retained by ASIO and the security of that information. However, I do not have a role in relation to what information is retained by carriers. In relation to the retention of data by ASIO the 2009-10 IGIS annual report noted:

Our interest in ASIO's retention and destruction of data arises from the Attorney-General's Guidelines which were issued to ASIO by the then Attorney-General, the Hon. Philip Ruddock MP, in October 2007 (the 2007 Guidelines). These guidelines replaced earlier guidance issued by the then Attorney-General, the Hon. Michael Duffy MP, in December 1992 (the 1992 Guidelines).

Around the time that the 2007 Guidelines were issued, [the then IGIS] commented that while he was supportive of many of the changes, the office would take a close interest in ASIO's information management governance framework, with a particular focus on what data ASIO retains or destroys in future inspections.

This is a difficult issue because the real significance of some (but not all) data may only become apparent when it is correlated with other data which becomes available subsequently. At the same time, ASIO is required to comply with Ministerial Guidelines which preclude ASIO from retaining high volumes of data, including significant data holdings which prove to have no relevance to organisational objectives.

The 1992 Guidelines contained an express prohibition on so-called 'speculative data matching' which does not appear in the 2007 Guidelines. Instead, the 2007 Guidelines are more permissive as to what data ASIO may collect, including as 'reference' data, although this is subject to the general limitation that material be 'relevant to security'.

Data sets are only one element of the information which ASIO collects. In relation to other material there is also the question of what should be done with individual records over time, particularly data which proves not to be, or to no longer be, relevant to security.

Clause 11.2 of the 2007 Guidelines state that: *Where an inquiry or investigation concludes that a subject's activities are not, or are no longer, relevant to security, the records of that inquiry or investigation shall be destroyed under disposal schedules agreed to between ASIO and the National Archives of Australia.*

There is a requirement on broadly similar lines in the *Telecommunications (Interception and Access) Act 1979* for intercepted material (section 14), and in the *Australian Security Intelligence Organisation Act 1979* in relation to certain records obtained under warrant (sections 31 and 34ZL).

²⁸ See s. 17(1) of the TIA Act

The challenge continues to be to ensure that ASIO performs its functions to full effect and within the legislative framework.²⁹

I continue to monitor ASIO's data retention and destruction policies and practices. OIGIS staff also undertake spot audits of ASIO's interception management systems. The purpose of these checks is to gain independent assurance that ASIO's data collection and retention activities are only occurring in accordance with the terms of a supporting special powers warrant and related investigative authorities.

It is not clear from the discussion paper what safeguards will be put in place if carriers have an increased obligation to retain data. In our inspection work we note that most errors relating to telecommunication intercept occur as a result of service provider error:

During 2010–11 this office either identified, or had brought to our attention by relevant ASIO staff, nine instances in which an error had occurred in the course of telecommunications interception activities ... Of these nine errors two were directly attributable to ASIO and seven occurred as the result of actions which relevant telecommunications service providers either took or failed to take.

While any mistake or error is regrettable, it is important to clearly recognise that most of the errors we identified were not directly within ASIO's control ...

In some of the cases where a problem was identified, a combination of technical, product delivery and administrative errors in preparation for, or subsequent to, the execution of these warrants led to collection occurring against persons who were not the intended target of these warrants, or the potential existed for such collection to occur.

In one instance intercepted material which was intended to be delivered to ASIO was misdelivered to

a law enforcement agency which had simultaneously obtained telecommunications warrants on the same person of interest.

In several other instances appropriate preliminary checks had been undertaken by ASIO to properly identify the telecommunications services being used by persons of interest only for that information to subsequently be found to be inaccurate.

In at least one case the telecommunications service which ASIO wished to intercept was disconnected in the period between when subscriber checks were undertaken and when the warrant was issued. Although ASIO should have received advice from the telecommunications service provider that the targeted service had been disconnected, this advice was not provided. After a quarantine period during which the service in question was not allocated, it was then reallocated to an individual with no connection to any matters of security interest.³⁰

I note that the number of errors is low compared to the number of service intercepted and that despite best efforts administrative and technical errors will almost inevitably occur. But these observations do highlight the need for safeguards to be put in place if the obligations placed on carriers are increased.

²⁹ Inspector General of Intelligence and Security Annual Report 2009-2010, pages 18-19

³⁰ Inspector-General of Intelligence and Security Annual Report 2010-11, page 28

Australian Security Intelligence Organisation Act 1979

ToR 5 – Amending the ASIO Act to modernise and streamline ASIO’s warrant provisions

- a. to update the definition of ‘computer’ in section 25A

The discussion paper sets out the difficulties of the current provision and suggests amending the legislation so that a computer access warrant may be issued in relation to ‘a computer, computers on a particular premises, computers connected to a particular person or a computer network’.³¹

Computing technology and usage patterns have changed and continue to change, however the proposed response may introduce further issues. For example, the term ‘computers connected to a computer network’ is potentially very broad in scope. It is difficult to contemplate when it would be reasonable to access *all* computers connected to a network in the absence of further limitations. Similarly ‘computers on a particular premises’ could inadvertently include computers that can have no connection whatsoever with the individual of interest.

My understanding is that the ‘mischief’ that the proposed change is seeking to overcome is much narrower than the potential breadth of the proposal in the discussion paper. I am advised that the ‘mischief’ arises where a warrant is executed on a specific premises and the subsequent search reveals not only the computer system that was expected to be found but also additional computers that are not in some way connected to the computer system specified in the warrant.³² The circumstances may be such that ASIO believes it is likely that the individual of security interest may have saved relevant information on the separate computer or computer systems as well as those originally covered by the warrant. In this scenario it would be administratively more convenient for ASIO to be able to obtain access to all such computers without having to obtain further warrants

ASIO to be able to obtain access to all such computers without having to obtain further warrants (which may be impractical in the time available).

The drafting of any specific legislative proposal should be able to address this type of issue without a disproportionate increase to the scope of the existing warrant powers.

- a. Enabling warrants to be varied by the AG, simplifying the renewal of the warrants process and extending duration of search warrants from 90 days to 6 months.

Variation of warrants

The discussion paper notes that there is currently no provision to vary a warrant and that a new warrant is required when there is a 'significant change in circumstances'.³³ (The paper does not canvass whether s. 33(3) of the *Acts Interpretation Act 1901* applies, a provision which would generally allow a decision maker to vary an instrument that they have made.)

I note that the Attorney-General can always issue a new warrant where they consider it appropriate to do so. Further, if the 'significant change in circumstances' amounts to 'the grounds on which the warrant was issued have ceased to exist' then s. 13 of the TIA requires that the Attorney-General be advised forthwith and interception discontinued thereby contemplating that a new warrant would be required to continue interception.

³¹ Discussion paper, page 41

³² Warrants can currently authorise access to more than one computer or device where those computers form part of one system (see s. 25A and the definition of a 'computer' in s. 22 of the ASIO Act)

³³ Discussion paper, page 41

The paper proposes a renewal process instead of a new warrant being required in instances where there has been no change to the intelligence case.³⁶ The paper notes that currently ASIO 'must apply for a new warrant which necessitates restating the intelligence case and completely reassessing the legislative threshold in instances where there has not been a significant change to either, and the assessment of the intelligence case remains unchanged'.³⁷

Section 30 of the ASIO Act would seem to require ongoing monitoring of the intelligence case and need for the warrant. Section 30 requires that if 'the Director-General is satisfied that the grounds on which the warrant was issued have ceased to exist, the Director-General shall forthwith inform the Minister accordingly and take such steps as are necessary to ensure that action in pursuance of the warrant (other than the recovery of a listening device or tracking device) is discontinued'.

My experience is that ASIO actively monitors changes in circumstances and is generally prompt in ensuring that action under a warrant is discontinued when the grounds for a warrant have ceased to exist. My understanding is that there is no intention in ASIO to reduce the scrutiny given to the intelligence case on renewal or re-issue of warrants or the ongoing monitoring of the grounds for the warrant – these essential internal assurance processes may limit the 'streamlining' benefits the proposed amendment could deliver.

³⁴ Discussion paper, page 42

³⁵ See Schedule 10 of the *Anti-terrorism Act (No. 2) 2005*

³⁶ Discussion paper, page 43

³⁷ Discussion paper, page 42

Duration of warrants

The discussion paper suggests extending the maximum duration of a search warrant from 90 days to six months to be consistent with other types of warrants and to provide operational benefits as there have been some instances where ASIO was unable to execute the warrant within 90 days.³⁴ I note that the maximum duration of a warrant was increased from 28 days to the current 90 days in 2005.³⁵

In my view, it would be unusual, with the exception of one type of search, for ASIO to not be able to execute a search warrant of a premises within 90 days. If that period is extended to six months then this should clearly be set as the *maximum possible* duration – not the default standard for all warrants. If this provision was enacted I would monitor search warrant requests closely to see whether the duration of each warrant request was considered on an individual basis to ensure it was valid for an appropriate time, which would usually be less than six months.

I am aware of one general category of warrants where there is sometimes difficulty executing the warrant within 90 days. To ensure the legislative response is proportionate it may be preferable to allow this particular category of search warrants to be extended rather than all search warrants.

Noting ToR 11(a) (establishing a named person warrant for multiple ASIO Act powers) it may be that the policy reason behind the change from 90 days to 6 months is directed at administrative ease and consistency for such warrants. However my view is that administrative ease and consistency are, in themselves, not compelling reasons to increase warrant powers or extend their duration.

Renewal of warrants

Current provisions also require ASIO to provide a report to the Attorney-General on the outcome of every warrant which is issued to it.³⁸ This is an important accountability step, and one that I would expect to continue if a warrant was renewed rather than a new warrant being issued.

ToR 6 – Modernising ASIO Act employment provisions:

- a. providing for officers to be employed under a concept of a 'level,' rather than holding an 'office.'
- b. Making the differing descriptions denoting persons as an 'employee' consistent
- c. Modernising the Director-General's powers in relation to employment terms and conditions
- d. Removing an outdated employment provision (section 87 of the ASIO Act)
- e. Providing additional scope for further secondment arrangements

The changes relating to the 'requirement to hold an office', 'descriptors of employees in the ASIO Act', 'special provisions relating to ASIO employees' and 'modernising the Director-General's powers in relation to employment terms and conditions' appear directed at bringing ASIO employment provisions in-line with other Commonwealth government employees.³⁹ I have no comment on these proposals other than to note that I expect that I will continue to have general oversight of the ASIO redress of grievance procedures⁴⁰ and to deal with complaints from ASIO employees about promotion, termination, discipline and remuneration matters.⁴¹

The proposed change relating to secondments may significantly change what powers individuals can exercise. For example, currently an ASIS staff member 'seconded' to ASIO or who is cooperating with ASIO under a s. 13 A ISA arrangement may not undertake an activity for the purpose of producing intelligence on an Australian person without the approval of the Foreign Minister unless

the staff member is on leave without pay from their 'home' agency and has been employed by ASIO. Under the proposed changes an individual might 'switch' from being an ASIS staff member, who is not permitted to produce intelligence on an Australian without ministerial authorisation, to being an ASIO staff member who is permitted to do so. Though while on 'secondment' individuals would not be able to rely on powers specific to their 'home' agency so for example ASIS staff members 'seconded' to ASIO could not carry weapons or rely on the partial immunity in s14 of the ISA.

If the secondment proposal is adopted I would be looking to ensure that the changes are applied in such a way that it is clear to individual officers which agency they are undertaking an activity for and that 'secondments' are a true change in working arrangements for a reasonable period. In my view it would not be proper for such a mechanism to be used to circumvent limits placed on employees in other legislation. For example it would not be proper for an ASIS staff member to be 'seconded' to ASIO for a day or two to enable them to perform an activity that they would otherwise not be permitted to undertake. My understanding is that this is not a practice the agencies intend to adopt.

Careful consideration also needs to be given to how the proposed secondment provisions would interact with the proposed authorised operations regime (ToR 10).

My understanding is that there is no intention for 'secondments' to apply outside of Australian Government agencies (note ToR 12 – ASIO cooperating with the private sector).

³⁸ See s 34 of the ASIO Act

³⁹ Discussion paper, pages 42-43

⁴⁰ See s. 8(1)(b) of the IGIS Act

⁴¹ See s. 8(6) of the IGIS Act

ToR 10 – Amending the ASIO Act to create an authorised intelligence operations scheme.

This will provide ASIO officers and human sources with protection from criminal and civil liability for certain conduct in the course of authorised intelligence operations.

The discussion paper states that ASIO has a requirement:

... to covertly gain and maintain close access to highly sensitive information. This activity often involves engaging and associating closely with those who may be involved in criminal activity and therefore has the potential to expose an ASIO officer or human source to criminal or civil liability in the course of their work.⁴²

An example is cited where, in the course of collecting covert intelligence in relation to a terrorist organisation, an ASIO officer or source may be open to criminal liability under the Criminal Code if they receive training from that organisation.

Intelligence and security agencies must act lawfully. It is not acceptable for agencies to operate in 'grey areas'. If Parliament decides to permit ASIO employees and sources to engage in activity that may otherwise be illegal then, in my view, there should be a carefully considered regime to regulate this.

The paper suggests that an authorised intelligence operations scheme would be 'similar to' the controlled operations scheme that operates in relation to the Australian Federal Police (AFP), the Australian Crime Commission (ACC) and the Australian Commission for Law Enforcement Integrity (ACLEI) under the *Crimes Act 1914* (Crimes Act). It is useful to briefly set out some of the key features of that scheme:

A controlled operation is a covert operation carried out by law enforcement officers for the purpose of obtaining evidence that may lead to the prosecution of a person for a serious offence. The operation may result in law enforcement officers and other approved persons engaging in conduct that would otherwise constitute an offence. Specific and detailed external oversight and reporting mechanisms are set out in the legislation.

Generally, controlled operations may be approved in the first instance by designated Senior Executive Service officers (except for major controlled operations in the AFP which must be authorised by the Commissioner or Deputy Commissioner).⁴³ The initial period generally cannot exceed three months. The operation may only be extended past three months up to a maximum of 24 months with the approval of a nominated member of the Administrative Appeals Tribunal (AAT).⁴⁴ This provides an independent external review of the case for an ongoing controlled operation every three months.

The Chief officer of the law enforcement agency must provide detailed reports to the Minister and the Commonwealth Ombudsman.⁴⁵ The annual report of operations must be tabled in Parliament (excluding sensitive matters).

⁴² Discussion paper, page 46

⁴³ See s. 15GF of the *Crimes Act 1914*

⁴⁴ See s. 15GT of the *Crimes Act 1914*

⁴⁵ See ss. 15HM and 15HN of the *Crimes Act 1914*

The Commonwealth Ombudsman is required to inspect the controlled operations records of the AFP, the ACC and ACLEI at least once every twelve months.⁴⁶ The Ombudsman is required to submit a report to the Minister and the report is tabled in Parliament.⁴⁷

The discussion paper states that any scheme for ASIO would need 'appropriate modifications'.⁴⁸ The proposal is that the Director-General of Security could issue authorised intelligence operation certificates which would provide protections from criminal and civil liability for specified conduct for a specified period (such as twelve months). The discussion paper is silent on how long any renewal could be for or what test would be applied to determine if a renewal was appropriate. Consistent with the law enforcement regime, the legislation would specify what conduct could not be authorised⁴⁹

The ability to give itself immunity from Australian law would be a significant new power for ASIO. Engaging in activities that would otherwise be illegal carries significant risk – particularly for human sources. I am aware that over a period of some years my office has received a small number of complaints from current and former ASIO human sources that demonstrate the complexity of the relationship. The paper does not explain why ASIO could not request the AFP or ACC to use existing powers to perform these functions, including where necessary authorising ASIO officers or sources under the existing schemes. Similarly, where such an activity was to occur outside Australia the scheme already provided for ASIS under s. 14 of the *Intelligence Services Act 2001* (the ISA) would appear relevant and the Committee may want to consider why such overseas activities could not be managed in conjunction with ASIS perhaps by way of ASIO staff and agents being made available to ASIS under the existing provisions.

I understand that there are operational impediments for ASIO in being required to operate under

schemes designed for law enforcement agencies, particularly where those schemes emphasise the collection of evidence or are designed for short-term operations. I am conscious too that ASIO considers it needs to develop and maintain sources over many years.

The proposed scheme for authorised operations by ASIO is silent on the issue of independent authorisation and detailed oversight or public reporting. Notwithstanding the sensitive matters relating to national security, the Committee may want to consider whether it would be desirable to have independent external review or ministerial approval of the intelligence case at regular intervals. This external review could be provided by suitably cleared members of the AAT.⁵⁰

The discussion paper does suggest that my office would have a role in oversight and inspection. This could be carried out under the IGIS Act but the Committee may also like to consider whether it would be preferable for the oversight and reporting regime to be set out in detail in the legislation, as is the case for controlled operations, to provide assurance that the scheme operates according to the legislation. Being notified that a scheme has been 'approved' may not necessarily be enough to maintain oversight, particularly where operations run for many years.

⁴⁶ See s. 15HS of the *Crimes Act 1914*

⁴⁷ See s. 15HO of the *Crimes Act 1914*

⁴⁸ Discussion Paper, page 46

⁴⁹ Discussion paper, pages 46-47

⁵⁰ Note that the *Administrative Appeals Tribunal Act 1975* (the AAT Act) and the ASIO Act make provision for the AAT to review sensitive ASIO security assessment decisions under special procedures intended to protect security – see s. 21AA of the AAT Act and Part IV, Division 4 of the ASIO Act.

Additional resources for my office could be required for my office to effectively oversight the proposed authorised operations scheme.

ToR 11 – Amending the ASIO Act to modernise and streamline ASIO’s warrant provisions to:

- a. Establish a named person warrant enabling ASIO to request a single warrant specifying multiple (existing) powers against a single target instead of requesting multiple warrants against a single target.

As far as I am aware there is no legal reason why ASIO cannot currently ‘bundle’ warrant applications so that the Attorney-General is asked to authorise the use of multiple powers in relation to a specific individual at the same time. Such an arrangement would, however, require the Attorney-General to consider the threshold and case for each individual power. See my comments in respect of ToR 8(a) – single TI warrants.

The discussion paper suggests that a single warrant could be issued covering all ASIO warrant powers where the relevant legislative thresholds are satisfied rather than requiring multiple warrants for an individual.⁵¹

The paper does not explain how the current different legislative tests and thresholds for the issuing of different types of warrants would be reconciled in a single warrant process or whether there is an intention to effectively transfer the decision as to what powers should be exercised from the Attorney-General to the Director-General of Security. The different types of warrants involve different activities and consequently different levels of intrusiveness (see also my comments above in respect of ToR 2(b) – standard TI warrant threshold). While a standardisation of tests and thresholds may be administratively convenient I would be concerned if there was, in effect, a

lowering of the thresholds without careful justification of the need to do this.

While such a scheme might be administratively simpler, there is the risk that the warrant would authorise activities that were not proportionate to the threat to security and may shift the balance between what is currently authorised by the Attorney-General and what is authorised by the Director-General – see my comments in respect of ToR 2(b) and 8(a) above.

b. Align surveillance device provisions with the *Surveillance Devices Act 2004*

The discussion paper proposes aligning the surveillance device provisions in the ASIO Act with the more modern *Surveillance Devices Act 2004* to overcome impediments to cooperation with law enforcement partner agencies.⁵²

While cooperation is desirable, it is not clear what the specific changes would be. Any changes must also consider external review and oversight mechanisms. I note there are substantial differences between the current ASIO regime and warrants under the Surveillance Devices Act. For example Surveillance Device Act warrants are issued by eligible judges or nominated members of the AAT.⁵³ There are also specific provision in the Surveillance Devices Act relating to reporting and oversight by the Ombudsman.⁵⁴

⁵¹ Discussion paper, page 47

⁵² Discussion paper, page 47

⁵³ See s. of the *Surveillance Devices Act 2004*

⁵⁴ See ss. 49 to 61 of the *Surveillance Devices Act 2004*

If the proposal is only to modernise the language of the ASIO Act – which for example rather confusingly includes a device for recording images within the definition of a 'listening device'⁵⁵ – then this is a more focussed proposal that does not raise propriety concerns.

- c. Enable the disruption of a target computer for the purposes of a computer access warrant

The ASIO Act currently restricts ASIO from doing anything under a computer access warrant that adds, deletes or alters data or interferes with, interrupts or obstructs the lawful use of the target computer by other persons.⁵⁶ The discussion paper suggests an amendment such that the prohibition would not apply to activity that is proportionate to what is necessary to execute the warrant.

I understand that the proposal is to enable ASIO to do only what is necessary to *covertly* retrieve the information sought under the warrant. That is, the primary purpose of any disruption would be to avoid disclosing to the person or group under surveillance that ASIO was monitoring them. This seems to be a reasonable solution to current operational problems.

As this proposal could directly affect the activities of persons unrelated to security interests it would be essential to have to clearly justify the case as to why it is appropriate to affect any lawful use of the computer. The reasons would need to balance the potential consequences of this interference to the individual(s) with the threat to security. There should be appropriate review and oversight mechanisms with particular attention to the effect of any disruption on third parties.

- d. Enable person searches to be undertaken independently of a premises search

The ASIO Act does not provide specific person search powers for ASIO, although a warrant to search

a premises can also specify, if appropriate, that the warrant provides the power to search a person who is at or near the premises where there are reasonable grounds to believe that the person has, on his or her person, records or other things relevant to security matters. This needs to be specified in the warrant.⁵⁷

The discussion paper states that it is not always feasible to execute a search warrant on a person of interest while they are 'at or near' the premises specified in the warrant. The paper proposes addressing 'the existing limitation' by enabling ASIO to request a warrant to search a specified person.⁵⁸

It seems that the current provisions consider the search of the person as incidental to the search of the premises. A proposal to introduce a warrant to search a specified person is not an extension of the existing power to search premises but is rather a proposal to introduce a new class of warrant. This will require careful consideration of the restrictions and conditions that should apply.

I am aware of one category of activities where ASIO currently relies on premises search warrants to achieve what is in effect a person search. While I do not have concerns about the legality of the current approach, from an oversight and transparency perspective it would be preferable for the legislation to provide a specific mechanism for person searches with appropriate limits rather than using a premises search warrant for this purpose.

⁵⁵ See s. 22 of the ASIO Act

⁵⁶ Discussion paper, page 48

⁵⁷ See s. 25 of the ASIO Act

⁵⁸ Discussion paper, page 48

Care needs to be taken that those undertaking a person search have appropriate training and qualifications. To this end it may be preferable to require that, were possible, such searches are undertaken by law enforcement officers who have specific training in this regard.

- e. Establish classes of persons able to execute warrants

The discussion paper proposes that the Direct-General of Security should be able to specify a class of person to execute a warrant rather than named individuals. While this could be operationally effective, it would be essential for ASIO to ensure that all officers in a particular class were fully trained and understood the limits of their authorisation. As noted above in relation to ToR 11(d) there may be cases where the best qualified officers to conduct a particular search are law enforcement officers.

ToR 12 – Clarifying ASIO's ability to cooperate with the private sector.

The discussion paper proposes amending s 19(1) of the ASIO Act to avoid any doubt about ASIO's ability to cooperate with the private sector.⁵⁹

My office regularly inspects the files of ASIO's interactions with, for example, State law enforcement agencies. We also have the ability to review ASIO's cooperation with private sector entities if appropriate.

ToR 13 – Enabling ASIO to refer breaches of section 92 of the ASIO Act to authorities

I have no comment on this proposal.

ToR 17 – Amending the ASIO Act to modernise and streamline ASIO’s warrant provisions:

- a. Using third party computers and communications in transit to access a target computer under a computer access warrant

The discussion paper proposes amending the ASIO Act to enable a third party computer or communication in transit to be used by ASIO to lawfully access a target computer.⁶⁰

Any such change must ensure that the impact on the third party, including privacy implications as well as any impact on the security or lawful use of the third party computer are considered carefully in the approval process.

Currently the TIA Act allows ASIO to obtain a warrant from the Attorney-General to intercept communications via a third party only where all other practicable methods have been exhausted or where it would not otherwise be possible to intercept the relevant communications.⁶¹ This appears to be an appropriate safeguard.

⁵⁹ Discussion paper page 49

⁶⁰ Discussion paper, page 50

⁶¹ See s. 9(3) of the TIA Act

- b. Clarifying that the incidental power in the search warrant provision authorises access to third party premises to execute a warrant

The discussion paper proposes 'clarification' of the scope of the powers incidental to the execution of a search or computer warrant in respect of entry to a third party's premises.⁶²

Any such change must ensure that the impact on the third party, including privacy implications as well as the potential for any damage to property, is considered carefully. If this entry is pre-planned – for example as access to a premises – it could be specified and authorised in the warrant documentation.

My understanding is that the operational driver behind the proposed amendment is to allow for an unplanned or unforeseen emergency exiting by ASIO officers who are covertly executing a warrant. This limitation could to be set out in the legislation.

- c. Clarifying that reasonable force may be used at any time during the execution of a warrant, not just on entry.

The current drafting of the ASIO Act suggest that the use of force is limited to authorisation of entry measures.⁶³ The discussion paper suggest that 'the provisions relating to the use of force are not limited in such a way' and proposes an amendment to 'correct' this is a 'drafting anomaly'.⁶⁴

It is not clear whether this is in fact a 'drafting anomaly' but, in any event, to broaden the use of force to include *all* warranted activities could enable ASIO to use force in conducting person searches.

My understanding is that the policy intention behind the proposed amendment relates only to secondary use of force by ASIO officers against 'things' when conducting premises searches. For example force may be required to initially get through the front door and further force may be needed to, for example, open a locked drawer. I understand that there is no intention to authorise ASIO officers to use force to conduct person searches.

From time to time my office has received complaints about searches of premises. This is a highly intrusive activity and I will continue to monitor ASIO's activities in this regard.

d. Introducing an evidentiary certificate regime.

I have no comments on this proposal

⁶² Discussion paper, page 50

⁶³ See, for example, heading above s. 25(7) of the ASIO Act

⁶⁴ Discussion paper, page 50

Intelligence Services Act 2001

ToR 7 – Clarifying the DIGO's authority to provide assistance to approved bodies.

The discussion paper proposes amendments to DIGO's function under s. 6B(e) of the ISA to ensure that DIGO has clear legislative support to undertake its geospatial and imagery related functions, and include an express reference to specialised imagery and geospatial technologies.⁶⁵

I do not need to comment on what might have been the original parliamentary intention or whether there is actually any ambiguity in the current legislation, but I will note that I have no propriety concerns with the view that DIGO should be able to provide Commonwealth and State authorities and other approved bodies, assistance in relation to the production and use of all imagery and geospatial products or assistance with the use and application of specialised imagery and geospatial technologies. If such assistance was also for the specific purpose of producing intelligence on an Australian person my expectation is that DIGO would continue to be required to obtain ministerial authorisation. I also expect DIGO to continue to apply the Privacy Rules made under s. 15 of the ISA to any disclosure of intelligence about an Australian person, regardless of which function the intelligence was collected under.

ToR 18 – Amending the *Intelligence Services Act 2001*

The ministerial authorisations scheme ensures appropriate ministerial oversight of the most sensitive functions of the foreign intelligence agencies including setting out the limited circumstances in which it is permissible for those agencies to undertake an activity for the specific purpose of producing intelligence on an Australian person. Two changes are proposed

purpose of producing intelligence on an Australian person. Two changes are proposed.

- a. Add a new ministerial authorisation ground where the Minister is satisfied that a person is, or is likely to be, involved in intelligence or counter-intelligence activities.

The first change concerns the addition of a new provision which would allow the Minister to authorise the production of intelligence on an Australian person who is, or is likely to be, involved in intelligence or counter-intelligence activities.⁶⁵ The proposed change is consistent with the structure of existing approval mechanisms. I have no propriety concerns with the proposed change. Oversight of the use of such a provision could be managed in the same way that this office inspects the exercise of other actions based on similar approvals by the relevant Minister.

- b. Enable the Minister of an agency under the ISA to authorise specified activities which may involve producing intelligence on an Australian person or persons where the agency is cooperating with ASIO in the performance of an ASIO function pursuant to a section 13A arrangement. A ministerial authorisation will not replace the need to obtain a warrant where one is currently required.

ASIO collects intelligence relevant to 'security'.⁶⁷ ASIS collects intelligence about the capabilities, intentions or activities of people or organisations outside Australia.⁶⁸ While the statutory functions

⁶⁵ Discussion paper, page 44

⁶⁶ Discussion paper, pages 51-52

⁶⁷ See s. 17(1)(a) of the ASIO Act

⁶⁸ See ss. 6(1)(a) and (b) of the ISA

of ASIO and ASIS overlap significantly, the mechanisms to ensure ministerial control over the production of intelligence on Australian persons differ substantially.

ASIO can collect intelligence about an Australian of security interest who is overseas based on internal approvals whereas ASIS would in all cases require the approval of the Minister for Foreign Affairs and the agreement of the Attorney-General to do the same thing.⁶⁹ This means that, in some instances, the level of protection for the privacy of individual Australians may depend on which agency is collecting the intelligence. Through my experience in the oversight of the agencies I am aware of the operational difficulties and anomalies of the current regime and can see the need for change.

The discussion paper does not specify what types of 'activities' could be approved, whether they may only occur overseas, which minister(s) would give the approval, how long the approval would be for, or on what basis it could be approved or renewed. However, my understanding is that intention is that the Minister for Foreign Affairs could issue authorisations to 'pre-approve' ASIS conducting an 'operation' that may involve collecting intelligence on any Australian provided that activity is being done for the purpose of assisting ASIO.

If an 'activity' is to be defined by reference to a particular operation there would be scope for the approvals to become quite broad. As a result it is possible that such authorisations could, in effect, become an almost blanket approval for ASIS, like ASIO, to produce intelligence on Australian persons for any purposes relating to security without further specific approval. Indeed, unless a broad range of activities were pre-approved and renewed on an ongoing basis the current difficulties with delay in obtaining an authorisation may continue.

I note that the proposal does include a reference to the need to obtain an individual ministerial authorisation where it could be sought. While, in principle, this is a good idea and seeks to maintain some of the current system of safeguards, it may have unintended consequences that could result in a continuation of current operational issues and make the scheme difficult to effectively oversight.

The existing threshold for a ministerial authorisation in security related cases is that the Minister must be satisfied that an individual is, or is likely to be, involved in an activity that is, or is likely to be, a threat to security.⁷⁰ This is not a high threshold. However my experience is that the cases that ASIS usually pursues are the more serious ones which go well above this threshold.

If the proposal requires a ministerial authorisation to be sought at renewal whenever this relatively low threshold is met, ASIS will need to ensure that each time an 'activity authority' is renewed every case is assessed to determine whether, for each individual, the legal threshold for an individual authorisation has been met. ASIS would have to stop collecting intelligence while an authorisation is obtained at the exact time it is assessed that the individual is of potential security interest. This problem may be particularly apparent where the individual comes to attention only towards the end of the authorisation period.

⁶⁹ See ss. 8(1)(a)(i) and 9(1A)(b) of the ISA. Note that in any case if the activity was in Australia and required a warrant it could not be undertaken by either agency in the absence of a warrant. This includes, for example, if ASIO was to obtain intelligence about an Australian who is overseas by intercepting the calls made by that person to another person in Australia via the Australian telecommunications network.

⁷⁰ See s. 9(1A)(a)(iii) of the ISA

It is possible that the problem of the inconsistency of legal frameworks outlined above could be addressed in a different way that might lead to a more consistent outcome. For activities inside Australia all of the agencies are currently bound by the common standard that requires ministerial approval (in the form of a warrant) or some other form of approval under legislation (for example, an authority to collect telecommunications data) for particularly intrusive activities. The Committee might want to consider whether this standard should be maintained to protect the privacy of *Australian persons* wherever they are. It may be appropriate to require that any intelligence or security agency that is undertaking an activity for the purpose of producing intelligence on an Australian person overseas should obtain the equivalent to the approval that ASIO would require if the activity was conducted in Australia (so for example Ministerial level approval for actions that would require a warrant and equivalent approvals for other actions that ASIO needs to have authorised under legislation).

So, for example, under such a scheme if DSD was to intercept the communications of an Australian person outside Australia a ministerial authorisation might be required. If ASIS or ASIO was to use a listening device to collect intelligence on an Australian outside Australia a ministerial authorisation might be required. However, if ASIS or ASIO was to ask an agent what they know about an Australian person who may be allegedly involved in terrorist activity or to task an agent to try to find out if any Australian persons are present at a terrorist training camp, specific ministerial authorisation would not be required.

My office would be required to monitor any changes to ministerial authorisation requirements and to continue to pay very close attention to any activity against an Australian person. In both my 2009-10 and 2010-11 annual reports I have noted that there is overall a very high level of compliance by the agencies with ministerial authorisation and warrant requirements.

the agencies with ministerial authorisation and warrant requirements.

- b. Enable ASIS to provide training in self-defence and the use of weapons to a person cooperating with ASIS.

Currently ASIS cannot provide training in the use of weapons to individuals who are not ASIS staff members. This restricts joint training exercises. The discussion paper proposes amendment to allow ASIS to cooperate in training with law enforcement and military personnel as well as a limited number of approved overseas authorities.⁷¹

Generally I am satisfied that the powers afforded to ASIS under Schedule 2 of the ISA are reasonable given the high threat environments in which it conducts some of its more sensitive activities, that the numbers of individuals who are authorised to use weapons is quite small and these authorisations are not being misused. I have been briefed on the need for joint training activities and have no propriety concerns with what has been proposed. If the proposed amendments are made I will monitor their implementation.

⁷¹ Discussion paper, page 54

Telecommunications Act 1997

ToR 16 – Amending the Telecommunications Act to address security and resilience risks

1. Amending the Telecommunications Act to address security and resilience risks posed to the telecommunications sector. This would be achieved by:
 - a. by instituting obligations on the Australian telecommunications industry to protect their networks from unauthorised interference
 - b. by instituting obligations to provide Government with information on significant business and procurement decisions and network designs
 - c. Creating targeted powers for Government to mitigate and remediate security risks with the costs to be borne by providers
 - d. Creating appropriate enforcement powers and pecuniary penalties

I have no comments on these proposals



Submission No 189

Inquiry into potential reforms of National Security Legislation

Organisation: Telstra
George Street Sydney
NSW 2000 Australia

Parliamentary Joint Committee on Intelligence and Security



**PJCIS INQUIRY ON REFORMS TO NATIONAL SECURITY
LEGISLATION**

SUBMISSION BY TELSTRA

TELSTRA CORPORATION LIMITED (ABN 33 051 775 556)

PAGE 1/26

PJCIS Submission (continued)



Contents

A.	Introduction	3
B.	Executive Summary	3
C.	Telecommunications (Interception and Access) Act 1979	5
1.	Strengthening the safeguards and privacy protections under the lawful access to communications regime in the TIA Act	5
2.	Reforming the lawful access to communications regime	6
3.	Streamlining and reducing complexity in the lawful access to communications regime	6
4.	Modernising the TIA Act's cost sharing framework	7
8.	Streamlining and reducing complexity in the lawful access to communications regime	8
9.	Modernizing the industry assistance framework	8
14.	Reforming the Lawful Access Regime	9
15.	Modernising the industry assistance framework	10
D.	Telecommunications Act 1997	12
16.	Amending the Telecommunications Act to address security and resilience risks posed to the telecommunications sector	12
E.	Australian Security Intelligence Organisation Act 1979	13
5.	Amending the ASIO Act to modernise and streamline ASIO's warrant provisions	13
11.	Amending the ASIO Act to modernise and streamline ASIO's warrant provisions to	14

11. Amending the ASIO Act to modernise and streamline ASIO's warrant provisions to	14
12. Clarifying ASIO's ability to cooperate with the private sector	14
17. Amending the ASIO Act to modernise and streamline ASIO's warrant provisions by	15
ATTACHMENT 1	16

Note: Submission Sub-section numbers correspond to Terms of Reference numbering.

PJCIS Submission (continued)



A. Introduction

Telstra welcomes the opportunity to respond to the PJCIS inquiry into potential reforms of national security legislation. We are a major builder and supplier of telecommunications networks and services with a large customer base and a long history of providing lawful assistance to security and law enforcement agencies. We are keen to share our insights on the issues and proposals contained within the PJCIS inquiry's Terms of Reference and Discussion Paper.

The proposed changes will require that a framework be established that balances our important obligations to protect the privacy of our customers against the equally important need to provide cost effective support to national security and law enforcement requirements in a timely, effective and sustainable way. Detailed consultation and thorough consideration is required before any changes are made.

B. Executive Summary

Telstra recognises the need to ensure that regulation remains relevant and appropriate to support critical national security and law enforcement requirements in a rapidly changing social and technological environment. However, consistent with the Government's Principles of Best Practice Regulation, in addition to identifying specific national security and law enforcement needs the proposed reforms should also be thoroughly evaluated against alternative reform options to ensure the proposals with greatest net benefits are adopted.

All reform proposals in this area will need to balance the public interest objectives, implementation costs to industry and ultimately customers, the need to maintain high levels of network integrity and legitimate community concerns about the security and privacy of customer information. In this context, public interest must be broadly defined and ensure that protection measures do not have the effect of impeding the delivery of high quality and innovative services to customers on Telstra's networks.

impeding the delivery of high quality and innovative services to customers on Telstra's networks.

Consistent with best practice policy-making, Telstra understands that the Government's approach to the issues raised in the Discussion Paper will be principles-based and seek to strike an appropriate balance between several legitimate, but at times opposing, principles. In Telstra's view, the key principles are:

- Reforms must support critical, identified and specific national security and law enforcement requirements in a rapidly changing social and technological environment;
- The public interest benefits of the reforms must outweigh their cost to government, industry and consumers;
- Reforms must be framed in ways that promote transparency and raise public awareness levels regarding why specific, identified requirements are sought/necessary;
- The highest possible levels of protection for the privacy and security of customer communications, personal information and data should be provided, with transparency as to the circumstances in which such information may be accessed and used for public interest purposes;
- The allocation of financial costs, and operational, legal and reputational risks associated with implementing such reforms as between Government, its LENSAs (Law Enforcement and National Security Agencies), C/CSPs (carriers/carriage service providers), customers and the community more broadly should be allocated to the entities that benefit from them;
- The way changes are implemented should be competitively neutral and applied equally to all service providers to avoid distorting market outcomes and to reduce the opportunity for users to evade the intended outcomes of the changes;
- There must be recognition of the high levels of C/CSP and consumer reliance on communication networks and applications and minimise any impacts on or risks to network access, capacity and innovation;
- Seek to adopt relevant examples of best international practice in law enforcement and national security including from C/CSPs, from LENSAs and on policy/legislative reform;

PJCIS Submission (continued)

IT'S HOW
WE CONNECT



-
- Reforms that place new and amended obligations on C/CSPs must be clear and unambiguous so that C/CSPs and their staff do not face any legal risks from complying with these obligations;
 - The role of industry under lawful interception legislation should remain strictly limited to providing access to the intercepted material, and not extend to investing capital in capability to process or interpret data or requiring C/CSP personnel to undertake these tasks. Processing interception data is the role of the LENSAs. Telstra does not have the capability to process or interpret interception data. To place C/CSPs in the role of interpreting intelligence data potentially jeopardises the integrity of the intercepted data and creates a real risk that it opens up agencies to further legal challenges from a defendant in a criminal prosecution;
 - It is important for the Committee to understand that, were they to be implemented, many of the proposals in the Discussion Paper would entail the imposition of new or additional costs on C/CSPs. Ultimately, the committee should recognise that the greater the implementation and administration costs that are imposed on C/CSPs under these proposals, the greater the likelihood that these costs will be passed onto consumers in the form of higher bills for telecommunications services; and
 - To effectively implement these principles Telstra suggests that the Government partner with industry and relevant consumer interest groups in determining the most appropriate and effective ways of addressing these critical public interests. This collaborative approach will provide the appropriate levels of expertise to develop options and test alternate approaches before final decisions are taken, and will assist in building a broader recognition of drivers for change and support for solutions.

Committee members are encouraged to read Telstra's submission through the prism of these principles.

There are many issues canvassed in the Discussion Paper, but our submission is focused on the following issues:

- **Telecommunications interception reform** – Telstra welcomes proposals to streamline processes, but is concerned to ensure that allocation of new responsibilities and associated costs and risks accords with the above principles.
- **Data retention** – Telstra appreciates the objectives but would like to discuss more cost effective options to address the issues raised, consistent with the principles we have articulated above.
- **Telecommunication sector security reform** – Telstra supports measures to ensure that C/CSPs have appropriate incentives to focus resources on network security and believes this can be achieved through the modification of some of the proposed measures to avoid adverse impacts on our ability to undertake efficient procurement and network design and operations.

Attachment 1 of our submission is a summary table where we have brought together responses, where appropriate, on all issues canvassed in the terms of reference.

Below are our detailed responses. Our submission addresses each of the proposals grouped under a particular Act, in the following order:

- *Telecommunications (Interception and Access) Act 1979*
- *Telecommunications Act 1997*
- *Australian Security Intelligence Organisation Act 1979*

Telstra has not provided comment on any of the proposals canvassed for the *Intelligence Services Act 2001*.

PJCIS Submission (continued)



C. Telecommunications (Interception and Access) Act 1979

1. Strengthening the safeguards and privacy protections under the lawful access to communications regime in the TIA Act

a. The legislation's privacy protection objective

Telstra supports the proposal to strengthen the safeguards and privacy protections under the lawful access to communications regime in the TIA Act (*Telecommunications (Interception and Access) Act 1979*) to ensure the protection and privacy of a customer's communications. Telstra also supports the need for consistency and alignment between the TIA Act and the Telco Act (*Telecommunications Act 1997*) for lawful interception, stored communications and any other customer data or information requested by Government.

Aligning the powers of both the Telco Act and TIA Act will assist in avoiding situations where C/CSPs are caught between legal obligations to protect customer information under the Telco Act (Part 13) and the legal obligations to provide assistance to LENSAs under the TIA Act. We recommend a simplification of those parts of the two Acts that compel C/CSPs to provide assistance to LENSAs in the public interest, while ensuring that approval thresholds for access are high enough to protect every consumer's right to privacy.

Any reforms should promote transparency and raise public awareness levels of how and why such information may be accessed and used for public interest purposes.

b. The proportionality tests for issuing of warrants

The proportionality testing of warrants will need to be consistent, practical and understandable by

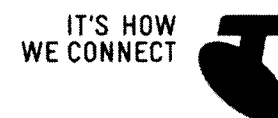
The proportionality testing of warrants will need to be consistent, practical and understandable by those required to implement them. Telstra remains concerned that ambiguity between the roles of agencies and requirements for C/CSPs to complete added steps will add unnecessary and avoidable complexity. There is a real need for these types of proposals to be further evaluated.

The scope of some of the proposed changes to lawful warrants will blur the boundaries between the part of the interception process traditionally conducted by the C/CSPs and that carried out by the LENSAs. This will require a review of the proportionality tests for the existing warrant authorisation and evidentiary certificate regime (and a review of costs arrangements) as well as for any new types of warrants, particularly where C/CSPs may no longer simply be enabling a lawfully issued interception warrant. The new types of warrants that have been proposed in the Discussion Paper may require C/CSPs to undertake processing which could be construed to be a form of interception if the C/CSP is required to record or store the material at some stage of the interception process (for example, in case of decryption).

c. Mandatory record-keeping standards

Telstra understands the desire for a reporting and record-keeping regime, but believes that the potential benefits of such proposals must explicitly and rigorously be evaluated against the costs associated with the implementation. The reporting regime needs to be simple and demonstrate to the public that the intended safeguards and privacy protections are working. At the same time the regime must not be administratively burdensome for both C/CSPs and LENSAs. Although the current record-keeping requirements are not overly onerous on C/CSPs, the regime does need an overhaul to achieve the intended outcomes. The existing obligation could be made more relevant to both LENSAs and C/CSPs, e.g. it is very difficult for a C/CSP to predict what products and services it will launch in 2-5 years' time and whether or not those services will have an impact on the C/CSP's legal interception capability.

PJCIS Submission (continued)



d. Oversight arrangements by the Commonwealth and State Ombudsmen

Telstra agrees that there must be consistent and practical arrangements put in place to enable oversight by both Commonwealth and State Ombudsmen aimed at strengthening the safeguards and privacy protections under the TIA Act and the Telco Act to ensure the security and privacy of customer communications.

2. Reforming the lawful access to communications regime

a. Reducing the number of agencies eligible to access communications information

In principle Telstra supports this proposal, acknowledging the levels of rich communications data now available and likely to be the subject of a broader number of LNSA requests in the future.

Telstra believes there is some merit in adopting a two-tiered communications data access regime to address potential risks of allowing access to customer data for the investigation of lesser offences. Under this type of regime, data readily available through C/CSP customer information systems could be provided under the current threshold test and would potentially remain accessible to a larger number of enforcement agencies and LNSAs.

Under this construct, access to more intrusive communications data, e.g. URLs, IP addresses or 'created' tailored data sets proposed under the data retention regime, would only be provided to a limited number of LNSAs and would require higher approval thresholds to be satisfied.

b. The standardization of warrant tests and thresholds

Telstra supports the proposed changes to further limit the number of LENSAs able to request access to communications data given the increased richness of telecommunications information, and the potential for a wide range of non-criminal LENSAs to access to such information. Telstra does not believe the public interest requires the disclosure of personal information to non-criminal LENSAs such as bodies that can impose a pecuniary penalty.

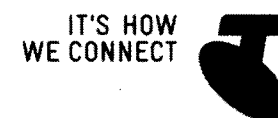
Currently, non criminal LENSAs can access historical data (that is, existing information or documents in the enforcement of a law imposing a pecuniary penalty or protection of public revenue) under section 179 of the TIA Act. In contrast the approval threshold to access prospective call data imposes an effective limitation – it may only be authorised by a criminal law-enforcement agency when it is considered reasonably necessary for the investigation of an offence that is punishable by imprisonment for at least three years.

3. Streamlining and reducing complexity in the lawful access to communications regime

a. Simplifying the information sharing provisions that allow agencies to cooperate

Telstra would need to understand how this might work in practice and what, if any, legal and reputational implications might arise under such arrangements before we could express a view on this proposal. For example, if Telstra releases communications data or interception content to one agency under a lawful warrant and then that information is provided by the approved LENSA to one or more other LENSAs (who in turn rely upon the data in evidentiary proceedings), what appropriate processes would need to be established to address the continuity of evidence issues?

PJCIS Submission (continued)



b. Removing legislative duplication

Telstra supports the removal of duplication and ambiguity between what C/CSPs are obliged to provide under the TIA Act and what LENSAs expect C/CSPs to provide under Section 313 of the Telco Act (i.e. "reasonably necessary assistance"). Section 313 enables LENSAs to request C/CSPs to provide a wide variety of assistance on the production of a lawful request but at present there is no clear delineation between what information must be provided under the TIA Act and what can be provided under Section 313.

4. Modernising the TIA Act's cost sharing framework

a. Aligning industry interception assistance with industry regulatory policy

At present a C/CSP's role in the 'lawful request' process is solely to deliver telecommunications data in compliance with a coercive instrument.

The capital "*cost of developing, installing and maintaining interception capability*" is borne by C/CSPs. C/CSPs are currently entitled to recover costs from LENSAs on a 'no cost - no profit' basis. In practice this means that C/CSPs are investing their shareholders' capital for sub-economic returns, and may not necessarily even recover their full operational costs in complying with existing legislation from the beneficiaries of these arrangements (i.e. national security and law enforcement agencies).

In attempting to assess the financial impact and requirements of future compliance, Telstra submits there is currently much ambiguity around the structure and likely costs associated with these proposals (e.g. initial system build and ongoing maintenance costs and how they will be addressed).

Under current arrangements, almost all of the retained data C/CSPs currently provides to LENSAs

has to be 'mined' via manual interrogation of operational and business support systems as opposed to simply electronically accessing telecommunications data from our networks. Any new security related measures which impose additional costs on C/CSPs beyond those absolutely necessary to achieve the legitimate requirements for maintaining security must be subject to a cost benefit.

Telstra submits that C/CSPs should be able to recover their economic costs of developing, installing and maintaining an interception and delivery capability. The imposition of an economic cost recovery model will also mean that LENSAs will need to demonstrate a level of rigor in their application for lawful assistance from C/CSPs.

b. Clarifying the ACMA's regulatory and enforcement role

The ACMA's current role would appear to have diminished over time and particularly so after the Blunn Review when parts of the Telco Act were transferred to the TIA Act. Telstra believes there needs to be clarification as to what role ACMA will have in future in monitoring compliance by C/CSPs with the Telco Act and TIA Act in respect to national security and law enforcement.

The Discussion Paper does not suggest what types of additional powers may be contemplated. Telstra would recommend that whatever agency is given this enforcement role its primary focus should be on undertaking an active role in education and dispute resolution, with any penalty enforcement role being secondary.

PJCIS Submission (continued)



8 Streamlining and reducing complexity in the lawful access to communications regime

a. Creating a single warrant with multiple TI powers

Telstra supports simplifying the warrant regime. This could be achieved by introducing a single and more precisely targeted warrant that provides unambiguous direction to C/CSP staff required to assist.

The proposed reforms that define attributes or 'non-traditional' service identifiers for warrants in a manner that focuses on characteristics of communication would represent a substantial shift of interception technology complexity and cost of interception from Government to C/CSPs. Implementation of such a change will require careful consideration to avoid unintended consequences particularly where services may be carried by a C/CSP, but are not managed or operated by the C/CSP, e.g. OTT (Over the Top) applications and services (Whatsapp and Skype), where a C/CSP may not be able to guarantee reliable interception or provide a carrier evidentiary certificate given the uncertainty regarding how the communications may be identified or carried within the C/CSP's network.

The ability to identify communications by attributes rather than services or technologies would require sophisticated equipment that, due to the size and diversified nature of C/CSP networks, may need to be installed at various locations through a C/CSP's networks. The economic cost for this capability cannot be determined without more detail. However based on experience it is reasonable to assume that the total cost will be substantial.

If the creation of a single warrant puts C/CSPs in a position of having to interpret warrants based on vague or incomplete details or attributes of the person of interest, the type of data or the services subscribed to by the person of interest to a LNSA, Telstra would not be able to support this

proposal. The proposal for a single (all encompassing) type of warrant will also impact on a C/CSP's warrant management systems and introduce complexity in processes for delivering the required sets of data.

For these reasons single warrants will need to continue to include details of the specific attributes and services required to be intercepted or the type data being requested and not be open to misinterpretation by C/CSP employees. C/CSPs should continue to have the right (and the legal protection) to reject a request from a LENSA that has not met the specific pre-requisites.

The introduction of a single and more precisely targeted warrant may also require the introduction of a secure electronic warrant system to ensure the efficiencies of a single warrant system are delivered. Electronic warrants would benefit both LENSAs and C/CSPs in providing a streamlined system for serving, receiving, filing and managing warrants. A secure electronic warrant system that is used by all LENSAs and C/CSPs may also assist in reducing costs and response times for lawful requests as well as standardising the information in single warrants which would potentially reduce the incidence of vague, incomplete, or ambiguous directions on a warrant.

9. Modernizing the industry assistance framework

a. Implement detailed requirements for industry interception obligations

Telstra believes the proposed model of tiered participation based on participant status creates the potential for criminals and terrorists to bypass interception arrangements through the selection of their C/CSP. In relation to the new security compliance framework that the Discussion Paper suggests in relation to C/CSPs considered to be a higher security risk, it is not clear how LENSAs would make a determination on how compliance assessments and audits could apply. The proposal also raises questions about whether a C/CSP with larger market share might be considered to be higher risk simply because it carries more traffic.

PJCIS Submission (continued)

IT'S HOW
WE CONNECT



In this regard Telstra is concerned that the Discussion Paper suggests the “level of engagement” would be informed by factors such as market share and customer base, meaning larger operators are likely to receive more scrutiny. Telstra maintains that market share and size of customer base is not an appropriate base on which to assess a company as being of ‘higher risk’. A regulatory regime that clearly signals that small providers will have no interception capabilities invites criminals and terrorists to use such small C/CSPs. A more effective regime would be to focus the supply of interception capabilities on mass market and access services where interception is most likely to be utilised and be more effective.

b. Extend the regulatory regime to ancillary service providers not currently covered by the legislation

Telstra believes further work would need to be undertaken in this regard and final proposals would need to be able to demonstrate a practical, fair and reasonable approach on C/CSP compliance.

This proposal indicates that interception-type obligations could be extended beyond Australian based C/CSPs to cover website/application and overseas based providers, such as social media operators, webmail services and cloud computing providers. An ancillary effect of this extension to Australian C/CSPs would be that any products that the C/CSP was offering that covered these types of services such as webmail or OTT applications (Whatsapp, Viber and TU ME) and which have not previously been subject to lawful interception obligations other than for the carriage element would also be caught. In some cases local C/CSPs may not be aware of what services are being used by customers, i.e. VoIP services such as Skype.

c. Implement a three-tiered industry participation model

Telstra believes these proposals run the risk of creating an uneven playing field, where the compliance burden would rest disproportionately with larger C/CSPs and the effectiveness of the overall regime is undermined by allowing criminals or terrorists to avoid interception arrangements by acquiring services from smaller C/CSPs.

In relation to the interception cost sharing framework, the Discussion Paper indicates that a new tiered model may be introduced where larger C/CSPs are expected to have a comprehensive interception capability (presumably at a greater cost) while smaller C/CSPs may only be required to have a minimum level capability (presumably at a lower cost). While the Discussion Paper states that one of its aims is to maintain "competitive neutrality" in the industry, it is hard to see how tiered compliance obligations are consistent with this aim. As such, Telstra does not support this proposal.

This tiered approach would also create the perverse outcome in which criminals or terrorists actively avoided using a Tier 1 C/CSP's services in favour of Tier 3 C/CSP that are not required to comply with the new legislation/regulation.

14. Reforming the Lawful Access Regime

a. Expanding the basis of interception activities

If the intent of this proposal is intended to be consistent with that outlined under 9b, namely "*to extend the regulatory regime to ancillary service providers not currently covered by the legislation*", Telstra would require further information before it could understand how this might work in practice. Telstra would support an expansion, assuming that the proposed changes are implemented in a competitively neutral manner and applied equally to all service providers to avoid distorting market outcomes and to reduce the opportunity for criminals to evade the intended outcomes of the changes.

PJCIS Submission (continued)



15. Modernising the industry assistance framework

a. Establish an offence for failure to assist in the decryption of communications

It is Telstra's position that the level of assistance that can reasonably be expected to be provided by C/CSPs should be carefully defined and limited in any event, but all the more so if an offence of failure to assist is to be created. For example, Telstra believes it would be unreasonable for a C/CSP to be required to:

- Decrypt services where the CSP is merely on-selling relevant services for a particular vendor (ie Blackberry). In this context, it would be reasonable for Government to obtain encryption keys from the relevant vendor of that product;
- Weaken or dilute or interfere with the encryption on a communications service in a way that would affect customers other than the authorised interception target;
- Weaken or dilute or interfere with the encryption on a communications service in a way that would affect the reputation or perception of the value of a third-party product (for example, leading to a belief that a CSP or vendor product is less secure than a competitor's product);
- Increase the risk that privacy of other customers will be compromised; or
- Conduct extensive storage and processing of communications to facilitate post-processing or decryption of communications prior to delivery to an agency. As previously stated in this submission, C/CSPs should not be expected to interpret or reconstruct the contents of a communication.

Some of the proposed changes reflect a shift of the interception burden from LENSAs to C/CSPs. As well as developing the capability to enable interception, C/CSPs would also be required to partially process intercepts before delivery to LENSAs to create communications data and also to assist in decryption. The changed process will mean that the enhanced and more intrusive interception role

and actions of a C/CSP would be subject to greater scrutiny and may be more likely to be challenged in evidentiary proceedings. Telstra does not support any proposed change to legislation where the interception burden on C/CSPs becomes one of 'processing' or 'creating' communications data.

b. Institute industry response timelines

Telstra submits that for Government to mandate 'response timelines' would also require Government to spend significant funds to support the introduction of a fully automated request management system (as discussed in 8a) for use by LENSAs and C/CSPs otherwise the LENSAs would not obtain the benefits intended from this proposal.

C/CSPs invest in communications networks and systems which are optimised for the efficient carriage of communications products and services between geographic locations. The OSS (Operations Support Systems) and BSS (Business Support Systems) systems that are used by C/CSPs to operate and manage these networks and systems generate information (i.e. customer information and billing records) which is valuable to Government in serving the public interest and maintaining customer privacy.

The proposal to introduce response times into the delivery of customer data and intercepted material introduces a level of complexity perhaps not fully considered, in that almost all of the retained data C/CSPs currently provide to LENSAs has to be 'mined' via manual interrogation of BSS and OSS systems as opposed to simply accessing telecommunications data from C/CSP networks and systems using standard on-line access tools.

Before response timelines could be introduced, LENSAs would need to be provided with enhanced capability (i.e. an automated streamlined electronic system) for serving, receiving, filing and managing warrants and the receipt of intercepted material and communications data. The current electronic delivery system (SedNode) requires manual intervention to enable processing of communications data by C/CSPs.

PJCIS Submission (continued)



c. Tailored data retention periods for up to 2 years for parts of a data set, with specific timeframes taking into account agency priorities, and privacy and cost impacts

The proposed arrangements are likely to be very costly and raise substantial security and privacy questions that will need to be answered.

Scope of data to be retained

Capturing meta data created by C/CSPs' communications systems and having to catalogue, store, retrieve and make available such information for possible use by LENSAs for up to two years (including data that passes through a C/CSP's network) raises a wide range of issues that we believe require detailed consultation and thorough consideration before any changes are made.

Telstra believes the proposed changes to retain a larger amount of telecommunications data will blur the boundaries between the interception process traditionally conducted by the C/CSPs and that carried out by the LENSAs.

In Telstra's view, to comply with any data retention regime we may need to routinely intercept and process large volumes of non-target customer communications to inspect, identify, and extract the required communications data from within the communications stream. C/CSPs, and nominated C/CSP personnel, would then need to be approved, similar to the agency interception authorities, to carry out this 'bulk' interception and communications processing. Presumably this would also require the introduction of a new compliance regime where C/CSPs may need to be subject to similar oversight and reporting obligations to the intercepting LENSAs.

The changed process will mean that the enhanced and more intrusive interception role and actions of

a C/CSP would be subject to greater scrutiny and may be more likely to be challenged in evidentiary proceedings. It is Telstra's view that the expansion of interception related activities to C/CSP staff would not be appropriate.

Challenges of retaining large data sets

Telstra believes that an effective and fair data retention regime must recognise there is an increased risk to privacy that C/CSPs will need to manage, and the regime should provide indemnity or relief to C/CSPs if such data is compromised despite the best efforts by C/CSPs to avoid that happening.

With very few exceptions, the current communications data that C/CSPs provide to the LENSAs can be validated, by defence counsel, by comparison with a defendant's telecommunications service account ('bill'). This will no longer be the case with 'created' communications data and Telstra believes that prosecutors are highly likely to be challenged in court to substantiate the accuracy of the data in evidentiary proceedings.

Cost of creation and retention of telecommunications data

Telstra believes that the costs involved in any new data creation and retention regime will be significant and we will need to undertake large scale and detailed technical feasibility studies in order to understand what network, IT, vendor changes would be necessary and the costs of implementation and compliance with any new data creation and retention regime.

Telstra recognises the need to ensure that legislation and regulations remain relevant and appropriate to support critical national security and law enforcement requirements in a rapidly changing environment. The potential reforms must be effective in helping to achieve the Government's objectives and the benefits of the reforms must outweigh the costs.

By way of comparison, in July 2011, in Telstra's response to the parliamentary committee inquiry into the *Cybercrime Legislation Amendment Bill 2011* (therefore, a much smaller scale of data extraction

PJCIS Submission (continued)



and preservation), we submitted that that C/CSPs would need to budget for a range of significant modifications and that preservation of stored communications for up to 180 days *'will have a major impact on these networks and systems'*.¹

Therefore it is impossible for Telstra to speculate on the significant costs or timeframes for compliance until Government has settled on the final form of any data retention regime.

D. Telecommunications Act 1997

16. Amending the Telecommunications Act to address security and resilience risks posed to the telecommunications sector

Telstra agrees that there is a need for C/CSPs to be more aware of the security threats to their customer's data and networks and that there are strong arguments for a partnership² with Government to share information on potential threats to C/CSP's customer data and networks. However we believe C/CSPs should retain the discretion to assess the risks and make informed decisions based on their knowledge taking into account any advice available from Government in relation to enhancing the security, integrity and resilience of their telecommunications infrastructure.

The proposals as currently crafted would create ambiguity and uncertainty as to what is expected of C/CSPs. Any proposed regime should minimise regulatory hurdles and provide incentives for C/CSPs to act in partnership with Government. Otherwise there is a risk that C/CSPs would not be able to finalise investment decisions or complete due diligence activities whilst waiting on Government decisions about network design and technology choices, acquisitions including overseas acquisitions and equipment purchases. These proposals will require extensive consultation in order to establish a fair, well-defined and balanced regime if the Government is to proceed.

In summary, Telstra's views on the key issues include:

There are already regulated processes under which C/CSPs are required to provide notifications of additions/amendments to our network (either onshore or offshore), procurement or other business arrangements to AGD including the IC Plan (Interception Capability Plan) process and S202B under the *Telecommunications (Interception and Access) Act 1979*. We are concerned that if additional obligations are imposed on local C/CSPs that add to their costs and reduce efficiency with no demonstrated benefit to their customers or their business, we may see the migration of services offshore which would be contrary to Government objectives.

The proposed amendments impose a significant impost on C/CSPs normal operations and procurement activities as well as reducing vendor competition raising overall procurement costs for Australian-based C/CSPs. At face value it would appear that C/CSPs would need to accept government advice on what equipment they could or could not procure, how C/CSPs could or could not configure their networks and systems and possibly how they conduct their day-to-day business activities. It would also appear that this proposed obligation will only apply to a few "nominated" C/CSPs, such that the impost would not be competitively neutral. Telstra does not support this approach.

The proposed amendments appear to offer "risk assessments" to be undertaken by the Government for sensitive procurement or network modifications. What is not clear is whether these "risk assessments" would be subject to legislated timeframes so as to avoid delaying procurement or

¹ Telstra's submission to the Parliament's Joint Select Committee on Cyber-Safety, 26 July 2011, page 2

² This partnership could be modelled on the US Government's Joint Cybersecurity Services Pilot which is intended to share classified National Security Agency cyberthreat intelligence with the private sector and is expected to be extended to network providers.

<http://www.smh.com.au/it-pro/security-it/symantecs-move-to-end-chinese-joint-venture-linked-to-cyberthreats-20120327-1vwb7.html>

PJCIS Submission (continued)



network design activities. It is also unclear if C/CSPs will have to implement the suggested outcomes of the "risk assessments" and if there are any penalties for not doing so.

Understanding there are risks that "nominated" C/CSPs may be seen as undertaking anti-competitive behavior if "risk assessments" recommendations limit carriage of competitor traffic, Government protections will be required from civil actions for those "nominated" C/CSPs who do implement the recommendations of the "risk assessments".

Telstra suggests that C/CSPs should be able to obtain reliable and trustworthy advice from Government to assist them in making informed decisions as an alternative. This could apply through a number of mechanisms including:

- a) TISN (Trusted Information Sharing Network). Telstra already interacts with Government on national security issues through the TISN and believes that the TISN should be used more constructively in the sharing with C/CSPs of up-to-date and sensitive information on threats and vulnerabilities. TISN would also provide a 24/7 service to C/CSPs seeking security and threat advice;
- b) A program that supports financial and commercial incentives for C/CSPs that would benefit both Government and customers if C/CSPs were to:
 - I. implement the recommendations of the "risk assessments" from Government;
 - II. immediately report (no fault, no blame or penalty in reporting) security breaches/security attacks to CERT rather than rely on voluntary reporting; and
 - III. embed in their network and business management processes a set of guidelines developed by Government covering information on what, how and where C/CSPs would need to configure (or make additions/amendments) to networks, procurement or other business arrangements to enhance the security, integrity and resilience of

their telecommunications infrastructure. This would limit the number of notifications required and potential risk assessments needed.

Telstra believes the most sensible way to provide these incentives would be through the Government's own procurement practices – i.e. Government to specify in requests for proposal/tender their security, resilience and integrity requirements for IT and communications services supplied to Government by C/CSPs.

E. Australian Security Intelligence Organisation Act 1979

5. Amending the ASIO Act to modernise and streamline ASIO's warrant provisions

Telstra agrees with the proposal to update the definition of 'computer'. The definition must also be consistent with the Criminal Code, Telecommunications and TIA Acts to avoid inconsistency and risks of error in interpretation.

The proposal to vary, simplify and extend the duration of warrants would have a direct impact on the warrant management systems used by C/CSPs. Consideration would need to be given to the impacts on existing interception warrants, the types of variations requested by the Attorney-General and C/CSP's resources required to manage the variations.

PJCIS Submission (continued)



11. Amending the ASIO Act to modernise and streamline ASIO's warrant provisions to:

- a. Establish a named person warrant enabling ASIO to request a single warrant specifying multiple (existing) powers against a single target instead of requesting multiple warrants against a single target.**

While Telstra supports simplifying the warrant regime and the use of a named person warrant, it should not be put in the position of having to interpret warrants based on vague or incomplete details of either the person of interest or their services. Telstra believes warrants must continue to include details of the specific services required to be intercepted. The proposal will also impact on C/CSP's warrant management system and processes required to deliver all information requested from multiple services and systems on the single target warrant.

- c. Enable the disruption of a target computer for the purposes of a computer access warrant**

ASIO or any other LENSA must be able to demonstrate that such action is consistent with any lawful request. If such a change to legislation is contemplated, Telstra would expect that ASIO provide C/CSPs with full indemnity in relation to proceedings brought by a third party in relation to this form of interception.

- e. Establish classes of persons able to execute warrants**

Telstra agrees that the classes of persons who are eligible to execute a warrant will need to be clearly defined as to what types of warrants they can authorise and under what law. Careful consideration will also need to be given to the appropriate levels of oversight and record keeping. A list of persons will then need to be conveyed to C/CSPs to reduce any risk of harm, unauthorised interception or breaches

of customer privacy by persons who are not eligible to execute a warrant.

12. Clarifying ASIO's ability to cooperate with the private sector

Telstra supports closer cooperation between ASIO (and other LENSAs) and the private sector where there is a sound mutual interest. Whether this is through continued participation in industry forums such as CSER (Communications Security Enforcement Roundtable) and BGAG (Business Government Advisory Forum) or forums such as the TISN, Telstra believes that closer cooperation will assist both LENSAs and C/CSPs in their respective goals while balancing legitimate privacy concerns.

Telstra supports the proposition that LENSAs "*capabilities must keep ahead of terrorists, agents of espionage and organised criminals who threaten national security and the safety*" of Australians. The Discussion Paper suggests there is a technology gap in LNSA capability and Telstra supports Government taking action to increase the technical capabilities within LENSAs.

LENsAs will need advanced technical skills to stay abreast of the interception challenge, understanding what knowledge or intelligence could be derived, how to target the necessary information, what information is possible to extract, the complexities and capabilities of new social communications services, the increasing volumes of internet data, and how to deal with encryption and private networks. Intercepting new types of services, and access to richer communications data provides greater operational opportunities, but with the obvious comment that more information will take longer to 'mine' to find the valuable information from a LNSA perspective.

The National Interception Technical Assistance Centre (NiTAC) was created in 2010 to help ASIO deal with the technological and legal problems of intercepting online communications. Operating as a two year trial, the intention was for NiTAC to identify future requirements for all telecommunications interceptions.

PJCIS Submission (continued)

IT'S HOW
WE CONNECT



A properly structured, managed and resourced NiTAC, with active contribution and support from key Federal and State LENSAs, would help overcome many practical problems that cannot be solved by C/CSPs and regulation. But for this to work, Government and LENSAs need to understand what role Federal agencies, such as DSD, ASIO and AFP and the major state law enforcement agencies can and should play and how to make the NiTAC effective in lifting the technical capabilities of LENSAs.

This may require a shift in thinking for Government and LENSAs and may also require amendment to the oversight mechanisms by different Departments; State Ombudsman; Commonwealth Ombudsman; and the Inspector General of Intelligence and Security (IGIS). Telstra notes the complex public policy and legislative challenges that may currently constrain cooperation between different LENSAs, however, the magnitude of the technology challenges and the importance of maintaining such an important investigate capability requires a commitment by Government to review all alternative solutions, including how to best make use of existing Government resources.

Industry could also play a role in partnering with NiTAC by:

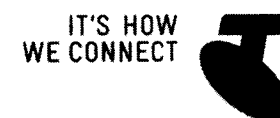
- I. Seconding suitably qualified LENSA staff into C/CSPs' positions to gain knowledge on how C/CSPs develop and deploy advanced communications products, services and networks;
- II. Explore opportunities for C/CSPs to rotate staff into NiTAC for short periods to provide technology training and in understanding how C/CSPs operate; and
- III. Establish partnerships with equipment vendors and carriers to explore the capabilities of new technologies and understand how C/CSPs deploy the technologies in their networks (similar to US Electronic Warfare Associates or the UK Cyber Security Evaluation Centre (BT)).

17. Amending the ASIO Act to modernise and streamline ASIO's warrant provisions by:

a. Using third party computers and communications in transit to access a target computer under a computer access warrant.

Telstra believes C/CSPs will need to be indemnified from consequences that may arise from the execution of the warrant in a range of circumstances. This will include situations where ASIO is seeking assistance from C/CSPs, including requesting that C/CSPs use computers operated by C/CSPs or used by C/CSP customers who are not the target of the warrant, or that requires C/CSPs to permit ASIO to use computers operated by C/CSPs or C/CSP customers. This includes potential breaches of customer privacy or service levels and resulting commercial damages and C/CSPs would need to be able to exercise a right of refusal.

PJCIS Submission (continued)



ATTACHMENT 1

ToR	Proposal	Response
1a	the legislation's privacy protection objective	<p>Telstra supports the proposal to strengthen the safeguards and privacy protections under the lawful access to communications regime in the TIA Act (<i>Telecommunications (Interception and Access) Act 1979</i>) to ensure the protection and privacy of a customer's communications. Telstra also supports the need for consistency and alignment between the TIA Act and the Telco Act (<i>Telecommunications Act 1997</i>) for lawful interception, stored communications and any other customer data or information requested by Government.</p> <p>We recommend a simplification of those parts of the two Acts that compel C/CSPs to provide assistance to LENSAs in the public interest, while ensuring that approval thresholds for access are high enough to protect every consumer's right to privacy.</p> <p>Any reforms should promote transparency and raise public awareness levels of how and why such information may be accessed and used for public interest purposes.</p>
1b	the proportionality tests for issuing of warrants	<p>The proportionality testing of warrants will need to be consistent, practical and understandable by those required to implement them. Telstra remains concerned that ambiguity between the roles of agencies and requirements for C/CSPs to complete added steps will add unnecessary and avoidable complexity. There is a real need for these types of proposals to be further evaluated.</p>

		<p>The scope of some of the proposed changes to lawful warrants will blur the boundaries between the part of the interception process traditionally conducted by the C/CSPs and that carried out by the LENSAs. This will require a review of the proportionality tests for the existing warrant authorisation and evidentiary certificate regime (and a review of costs arrangements) as well as for any new types of warrants, particularly where C/CSPs may no longer simply be enabling a lawfully issued interception warrant.</p>
1c	mandatory record- keeping standards	<p>Telstra understands the desire for a reporting and record-keeping regime, but believes that the potential benefits of such proposals must explicitly and rigorously be evaluated against the costs associated with the implementation. The reporting regime needs to be simple and demonstrate to the public that the intended safeguards and privacy protections are working. At the same time the regime must not be administratively burdensome for both C/CSPs and LENSAs.</p> <p>Although the current record-keeping requirements are not overly onerous on C/CSPs, the regime does need an overhaul to achieve the intended outcomes. The existing obligation could be made more relevant to both LENSAs and C/CSPs, e.g. it is very difficult for a C/CSP to predict what products and services it will launch in 2-5 years' time and whether or not those services will have an impact on the C/CSP's legal interception capability.</p>
1d	oversight arrangements by the Commonwealth and State	<p>Telstra agrees that there must be consistent and practical arrangements put in place to enable oversight by both</p>

PJCIS Submission (continued)



ToR	Proposal	Response
	Ombudsmen	Commonwealth and State Ombudsmen aimed at strengthening the safeguards and privacy protections under the TIA Act and the Telco Act to ensure the security and privacy of customer communications.
2a	reducing the number of agencies eligible to access communications information	<p>In principle Telstra supports this proposal, acknowledging the levels of rich communications data now available and likely to be the subject of a broader number of LENSA requests in the future.</p> <p>Telstra believes there is some merit in adopting a two-tiered communications data access regime to address potential risks of allowing access to customer data for the investigation of lesser offences. Under this type of regime, data readily available through C/CSP customer information systems could be provided under the current threshold test and would potentially remain accessible to a larger number of enforcement agencies and LENSAs.</p>
2b	the standardisation of warrant tests and thresholds	<p>Telstra supports the proposed changes to further limit the number of LENSAs able to request access to communications data given the increased richness of telecommunications information, and the potential for a wide range of non-criminal LENSAs to access to such information. Telstra does not believe the public interest requires the disclosure of personal information to non-criminal LENSAs such as bodies that can impose a pecuniary penalty.</p> <p>Currently, non criminal LENSAs can access historical data (that is, existing information or documents in the enforcement of a law</p>

		<p>imposing a pecuniary penalty or protection of public revenue) under section 179 of the TIA Act. In contrast the approval threshold to access <i>prospective</i> call data imposes an effective limitation – it may only be authorised by a criminal law-enforcement agency when it is considered reasonably necessary for the investigation of an offence that is punishable by imprisonment for at least three years.</p>
3a	simplifying the information sharing provisions that allow agencies to cooperate	<p>Telstra would need to understand how this might work in practice and what, if any, legal and reputational implications might arise under such arrangements before we could express a view on this proposal. For example, if Telstra releases communications data or interception content to one agency under a lawful warrant and then that information is provided by the approved LENSA to one or more other LENSAs (who in turn rely upon the data in evidentiary proceedings), what appropriate processes would need to be established to address the continuity of evidence issues?</p>
3b	removing legislative duplication	<p>Telstra supports the removal of duplication and ambiguity between what C/CSPs are obliged to provide under the TIA Act and what LENSAs expect C/CSPs to provide under Section 313 of the Telco Act (ie "<i>reasonably necessary assistance</i>"). Section 313 enables LENSAs to request C/CSPs to provide a wide variety of assistance on the production of a lawful request but at present there is no clear delineation between what information must be provided under the TIA Act and what can be provided under Section 313.</p>
4a	align industry interception	<p>At present a C/CSP's role in the 'lawful request' process is solely to deliver telecommunications data in compliance with a coercive</p>

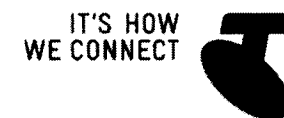
PJCIS Submission (continued)



ToR	Proposal	Response
	<p>assistance with industry regulatory policy</p>	<p>instrument.</p> <p>The capital “<i>cost of developing, installing and maintaining interception capability</i>” is borne by C/CSPs. C/CSPs are currently entitled to recover costs from LENSAs on a ‘no cost - no profit’ basis. In practice this means that C/CSPs are investing their shareholders’ capital for sub economic returns, and may necessarily even recover their full operational costs in complying with existing legislation from the beneficiaries of these arrangements (i.e. national security and law enforcement agencies).</p> <p>In attempting to assess the financial impact and requirements of future compliance, Telstra submits there is currently much ambiguity around the structure and likely costs associated with these proposals (e.g. initial system build and ongoing maintenance costs and how they will be addressed).</p> <p>Telstra submits that C/CSPs should be able to recover their economic cost of developing, installing and maintaining an interception and delivery capability. The imposition of a full economic cost recovery model will also mean that LENSAs will need to demonstrate a level of rigor in their application for lawful assistance from C/CSPs.</p>
4b	<p>clarify ACMA’s regulatory and enforcement role</p>	<p>The ACMA’s current role would appear to have diminished over time and particularly so after the Blunn Review when parts of the</p>

	enforcement role	<p>Telco Act were transferred to the TIA Act. Telstra believes there needs to be clarification as to what role ACMA will have in future in monitoring compliance by C/CSPs with the Telco Act and TIA Act in respect to national security and law enforcement.</p> <p>The Discussion Paper does not suggest what types of additional powers may be contemplated. Telstra would recommend that whatever agency is given this enforcement role its primary focus should be on undertaking an active role in education and dispute resolution with any penalty enforcement role becoming secondary.</p>
5a	to update the definition of 'computer' in section 25A	Telstra agrees with the proposal to update the definition of 'computer'. The definition must also be consistent with the Criminal Code, Telecommunications and TIA Acts to avoid inconsistency and risks of error in interpretation.
5b	Enabling warrants to be varied by the AG, simplifying the renewal of the warrants process and extending duration of search warrants from 90 days to 6 months.	The proposal to vary, simplify and extend the duration of warrants would have a direct impact on the warrant management systems used by C/CSPs. Consideration would need to be given to the impacts on existing interception warrants, the types of variations requested by the Attorney-General and C/CSP's resources required to manage the variations.
6a	Providing for officers to be employed under a concept of a 'level,' rather than holding an 'office.'	No comment provided

PJCIS Submission (continued)



ToR	Proposal	Response
6b	Making the differing descriptions ('officer,' 'employee' and 'staff') denoting persons as an 'employee' consistent	No comment provided
6c	Modernising the Director- General's powers in relation to employment terms and conditions	No comment provided
6d	Removing an outdated employment provision (section 87 of the ASIO Act)	No comment provided
6e	Providing additional scope for further secondment arrangements	No comment provided
7	Amending the Intelligence Services Act 2001 to clarify the Defence Imagery and Geospatial Organisation's authority to provide assistance	No comment provided

	to approved bodies.	
8a	Creating a single warrant with multiple TI powers	<p>Telstra supports simplifying the warrant regime. This could be achieved by introducing a single and more precisely targeted warrant that provides unambiguous direction to C/CSP staff required to assist.</p> <p>Implementation of such a change will require careful consideration to avoid unintended consequences particularly where services may be carried by a C/CSP, but are not managed or operated by the C/CSP, e.g. OTT (Over the Top) applications and services (Whatsapp and Skype), where a C/CSP may not be able to guarantee reliable interception or provide a carrier evidentiary certificate given the uncertainty regarding how the communications may be identified or carried within the C/CSP's network.</p> <p>If the creation of a single warrant puts C/CSPs in a position of having to interpret warrants based on vague or incomplete details or attributes of the person of interest, the type of data or the services subscribed to by the person of interest to a LENSA, Telstra would not be able to support this proposal.</p> <p>The introduction of a single and more precisely targeted warrant may also require the introduction of a secure electronic warrant system to ensure the efficiencies of a single warrant system are delivered. Electronic warrants would benefit both LENSAs and C/CSPs in providing a streamlined system for serving, receiving, filing and managing warrants.</p>

PJCIS Submission (continued)



ToR	Proposal	Response
9a	Implement detailed requirements for industry interception obligations	<p>Telstra believes the proposed model of tiered participation based on participant status creates the potential for criminals and terrorists to bypass interception arrangements through the selection of their C/CSP. The proposal also raises questions about whether a C/CSP with larger market share might be considered to be higher risk simply because it carries more traffic.</p> <p>In this regard Telstra is concerned that the Discussion Paper suggests the “level of engagement” would be informed by factors such as market share and customer base, meaning larger operators are likely to receive more scrutiny.</p> <p>A more effective regime would be to focus the supply of interception capabilities on mass market and access services where interception is most likely to be utilised and be more effective.</p>
9b	extend the regulatory regime to ancillary service providers not currently covered by the legislation	<p>Telstra believes further work would need to be undertaken in this regard and final proposals would need to be able to demonstrate a practical, fair and reasonable approach on C/CSP compliance.</p> <p>This proposal indicates that interception-type obligations could be extended beyond Australian based C/CSPs to cover website/application and overseas based providers, such as social media operators, webmail services and cloud computing providers. An ancillary effect of this extension to Australian C/CSPs would be that any products that the C/CSP was offering</p>

		<p>that covered these types of services such as webmail or OTT applications (Whatsapp, Viber and TU ME) and which have not previously been subject to lawful interception obligations other than for the carriage element would also be caught. In some cases local C/CSPs may not be aware of what services are being used by customers, i.e. VoIP services such as Skype.</p>
9c	<p>implement a three- tiered industry participation model</p>	<p>Telstra believes these proposals run the risk of creating an uneven playing field, where the compliance burden would rest disproportionately with larger C/CSPs and the effectiveness of the overall regime is undermined by allowing criminals or terrorists to avoid interception arrangements by acquiring services from smaller C/CSPs.</p> <p>In relation to the interception cost sharing framework, the Discussion Paper indicates that a new tiered model may be introduced where larger C/CSPs are expected to have a comprehensive interception capability (presumably at a greater cost) while smaller C/CSPs may only be required to have a minimum level capability (presumably at a lower cost). As such, Telstra does not support this proposal.</p>
10	<p>Amending the ASIO Act to create an authorised intelligence operations scheme. This will provide ASIO officers and human sources with protection from criminal and civil liability for certain conduct</p>	<p>No comment provided</p>

PJCIS Submission (continued)



ToR	Proposal	Response
	in the course of authorised intelligence operations.	
11a	Establish a named person warrant enabling ASIO to request a single warrant specifying multiple (existing) powers against a single target instead of requesting multiple warrants against a single target	While Telstra supports simplifying the warrant regime and the use of a named person warrant, it should not be put in the position of having to interpret warrants based on vague or incomplete details of either the person of interest or their services. Telstra believes warrants must continue to include details of the specific services required to be intercepted. The proposal will also impact on C/CSP's warrant management system and processes required to deliver all information requested from multiple services and systems on the single target warrant.
11b	Align surveillance device provisions with the Surveillance Devices Act 2007	No comment provided
11c	Enable the disruption of a target computer for the purposes of a computer access warrant	ASIO or any other LENSA must be able to demonstrate that such action is consistent with any lawful request. If such a change to legislation is contemplated, Telstra would expect that ASIO provide C/CSPs with full indemnity in relation to proceedings brought by a third party in relation to this form of interception.
11d	Enable person searches to be undertaken independently of a premises search	No comment provided

11e	Establish classes of persons able to execute warrants	Telstra agrees that the classes of persons who are eligible to execute a warrant will need to be clearly defined as to what types of warrants they can authorise and under what law. Careful consideration will also need to be given to the appropriate levels of oversight and record keeping. A list of persons will then need to be conveyed to C/CSPs to reduce any risk of harm, unauthorised interception or breaches of customer privacy by persons who are not eligible to execute a warrant.
12	Clarifying ASIO's ability to cooperate with the private sector	<p>Telstra supports closer cooperation between ASIO (and other LENSAs) and the private sector where there is a sound mutual interest. Whether this is through continued participation in industry forums such as CSER (Communications Security Enforcement Roundtable) and BGAG (Business Government Advisory Forum) or forums such as the TISN, Telstra believes that closer cooperation will assist both LENSAs and C/CSPs in their respective goals while balancing legitimate privacy concerns.</p> <p>Telstra supports the proposition that LENSAs "<i>capabilities must keep ahead of terrorists, agents of espionage and organised criminals who threaten national security and the safety</i>" of Australians.</p> <p>LENsAs will need advanced technical skills to stay abreast of the interception challenge, understanding what knowledge or intelligence could be derived, how to target the necessary information, what information is possible to extract, the complexities and capabilities of new social communications services, the increasing volumes of internet data, and how to deal</p>

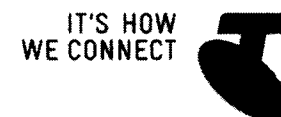
PJCIS Submission (continued)



ToR	Proposal	Response
		<p>with encryption and private networks.</p> <p>The National Interception Technical Assistance Centre (NiTAC) was created in 2010 to help ASIO deal with the technological and legal problems of intercepting online communications.</p> <p>A properly structured, managed and resourced NiTAC, with active contribution and support from key Federal and State LENSAs, would help overcome many practical problems that cannot be solved by C/CSPs and regulation. But for this to work, Government and LENSAs need to understand what role Federal agencies, such as DSD, ASIO and AFP and the major state law enforcement agencies can and should play and how to make the NiTAC effective in lifting the technical capabilities of LENSAs.</p> <p>This may require a shift in thinking for Government and LENSAs and may also require amendment to the oversight mechanisms by different Departments; State Ombudsman; Commonwealth Ombudsman; and the Inspector General of Intelligence and Security (IGIS).</p>
13	Amending the ASIO Act to enable ASIO to refer breaches of section 92 of the ASIO Act (publishing the identity of an ASIO officer) to authorities for	No comment provided

	investigation	
14a	expanding the basis of interception activities	<p>If the intent of this proposal is intended to be consistent with that outlined under 9b, namely <i>"to extend the regulatory regime to ancillary service providers not currently covered by the legislation"</i>, Telstra would require further information before it could understand how this might work in practice. Telstra would support an expansion, assuming that the proposed changes are implemented in a competitively neutral manner and applied equally to all service providers to avoid distorting market outcomes and to reduce the opportunity for criminals to evade the intended outcomes of the changes.</p>
15a	establish an offence for failure to assist in the decryption of communications	<p>It is Telstra's position that the level of assistance that can reasonably be expected to be provided by C/CSPs should be carefully defined and limited in any event, but all the more so if an offence of failure to assist is to be created. For example, Telstra believes it would be unreasonable for a C/CSP to be required to decrypt services where the CSP is merely on-selling relevant services for a particular vendor (ie Blackberry). In this context, it would be reasonable for Government to obtain encryption keys from the relevant vendor of that product.</p> <p>Some of the proposed changes reflect a shift of the interception burden from LENSAs to C/CSPs. As well as developing the capability to enable interception, C/CSPs would also be required to partially process intercepts before delivery to LENSAs to create communications data and also to assist in decryption.</p>

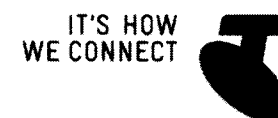
PJCIS Submission (continued)



ToR	Proposal	Response
		<p>Telstra does not support any proposed change to legislation where the interception burden on C/CSPs becomes one of 'processing' or 'creating' communications data.</p>
15b	<p>institute industry response timelines</p>	<p>Telstra submits that for Government to mandate 'response timelines' would also require Government to spend significant funds to support the introduction of a fully automated request management system (as discussed in 8a) for use by LENSAs and C/CSPs otherwise the LENSAs would not obtain the benefits intended from this proposal.</p> <p>Before response timelines could be introduced, LENSAs would need to be provided with enhanced capability (i.e. an automated streamlined electronic system) for serving, receiving, filing and managing warrants and the receipt of intercepted material and communications data. The current electronic delivery system (SedNode) requires manual intervention to enable processing of communications data by C/CSPs.</p>
15c	<p>tailored data retention periods for up to 2 years for parts of a data set, with specific timeframes taking into account agency priorities, and privacy and cost impacts</p>	<p>The proposed arrangements are likely to be very costly and raise substantial security and privacy questions that will need to be answered.</p> <p>Telstra believes the proposed changes to retain a larger amount of telecommunications data will blur the boundaries between the interception process traditionally conducted by the C/CSPs and that carried out by the LENSAs.</p>

		<p>Telstra believes that an effective and fair data retention regime must recognise there is an increased risk to privacy that C/CSPs will need to manage, and the regime should provide indemnity or relief to C/CSPs if such data is compromised despite the best efforts by C/CSPs to avoid that happening.</p> <p>Telstra believes that the costs involved in any new data creation and retention regime will be significant and we will need to undertake large scale and detailed technical feasibility studies in order to understand what network, IT, vendor changes would be necessary and the costs of implementation and compliance with any new data creation and retention regime.</p> <p>Telstra recognises the need to ensure that legislation and regulations remain relevant and appropriate to support critical national security and law enforcement requirements in a rapidly changing environment. The potential reforms must be effective in helping to achieve the Government's objectives and the benefits of the reforms must outweigh the costs.</p> <p>Therefore it is impossible for Telstra to speculate on the significant costs or timeframes for compliance until Government has settled on the final form of any data retention regime.</p>
16a	by instituting obligations on the Australian telecommunications industry to protect their networks from unauthorised	Telstra agrees that there is a need for C/CSPs to be more aware of the security threats to their customer's data and networks and that there are strong arguments for a partnership with Government in advising us of the threats to our customer data and networks. However we believe C/CSPs should retain the discretion to assess

PJCIS Submission (continued)



ToR	Proposal	Response
	interference	<p>the risks and make informed decisions based on their knowledge taking into account any advice available from Government in relation to enhancing the security, integrity and resilience of their telecommunications infrastructure.</p> <p>The proposals as currently crafted would create ambiguity and uncertainty as to what is expected of C/CSPs. Any proposed regime should minimise regulatory hurdles and provide incentives for C/CSPs to act in partnership with Government. Otherwise there is a risk that C/CSPs would not be able to finalise investment decisions or complete due diligence activities whilst waiting on Government decisions about network design and technology choices, acquisitions including overseas acquisitions and equipment purchases. These proposals will require extensive consultation in order to establish a fair, well-defined and balanced regime if the Government is to proceed.</p> <p>Telstra understands that the Government has concerns in relation to securing Australian telecommunications data and networks from cyber crime and related criminal threats, and we believe we are well placed to assist the Government to develop a practical framework that can focus on the real problems, while achieving the right incentive structure and value proposition for C/CSPs.</p>
16b	by instituting obligations to provide Government with information on significant	There are already regulated processes under which C/CSPs are required to provide notifications of additions/amendments to our network (either onshore or offshore), procurement or other

	information on significant business and procurement decisions and network designs	<p>business arrangements to AGD including the IC Plan (Interception Capability Plan) process and S202B under the TIA Act.</p> <p>The proposed amendments impose a significant impost on C/CSPs normal operations and procurement activities as well as reducing vendor competition raising overall procurement costs for Australian-based C/CSPs. Telstra does not support this approach.</p> <p>The proposed reforms would need to include clear Government protections from civil actions for C/CSPs who do implement the recommendations of the reforms.</p>
16c	Creating targeted powers for Government to mitigate and remediate security risks with the costs to be borne by providers	<p>While the Discussion Paper indicates that directions would only be given after an appropriate period of discussion and engagement with the C/CSP, C/CSPs would be concerned about the prospect of very prescriptive directions, which would limit flexibility and commercial viability around their security solutions and the cost of any remedial action and what the consequences would be to C/CSPs who fail to remediate Government specified security risks. Telstra would not support this proposal.</p> <p>There would also need to be a framework that would include clear mechanisms to enable an independent judicial review or appeal process to deliver timely, balanced, and equitable decisions on Government imposed binding directions or specific mitigation action to reduce the likelihood of drawn out litigation in relation to contentious rulings or decisions.</p>

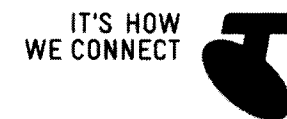
PJCIS Submission (continued)



ToR	Proposal	Response
		<p>Telstra believes the most sensible way to provide these incentives would be through the Government's own procurement practices – i.e. Government to specify in requests for proposal/tender their security, resilience and integrity requirements for IT and communications services supplied to Government by C/CSPs.</p>
16d	<p>Creating appropriate enforcement powers and pecuniary penalties</p>	<p>The proposal to introduce new security compliance obligations on C/CSPs to maintain "competent supervision" and "effective control" over their networks could require C/CSPs to change the way they manage relationships with existing vendors and suppliers.</p> <p>The Discussion Paper indicates that Government will provide general guidelines, advice and briefings, but despite this the standard of security compliance required may still be changeable and difficult for C/CSPs to manage. The proposal may also bring C/CSPs into conflict with existing corporate obligations, particularly those relating to impacts in the marketplace and the continuous disclosure of information to the financial markets.</p> <p>It would also be challenging to retrofit these requirements to existing long-term commercial arrangements that C/CSPs may already have in place with key vendors and suppliers (e.g. in order to comply it may be necessary to renegotiate the security aspects of outsourcing agreements that are currently in place). Telstra would</p>

		not support this proposal.
17a	Using third party computers and communications in transit to access a target computer under a computer access warrant	Telstra believes C/CSPs will need to be indemnified from consequences that may arise from the execution of the warrant in a range of circumstances. This will include situations where ASIO is seeking assistance from C/CSPs, including requesting that C/CSPs use computers operated by C/CSPs or used by C/CSP customers who are not the target of the warrant, or that requires C/CSPs to permit ASIO to use computers operated by C/CSPs or C/CSP customers. This includes potential breaches of customer privacy or service levels and resulting commercial damages and C/CSPs would need to be able to exercise a right of refusal.
17b	Clarifying that the incidental power in the search warrant provision authorises access to third party premises to execute a warrant	No comment provided
17c	Clarifying that reasonable force may be used at any time during the execution of a warrant, not just on entry	No comment provided
17d	Introducing an evidentiary certificate regime	No comment provided

PJCIS Submission (continued)



ToR	Proposal	Response
18a	Add a new ministerial authorisation ground where the Minister is satisfied that a person is, or is likely to be, involved in intelligence or counter- intelligence activities	No comment provided
18b	Enable the Minister of an Agency under the IS Act to authorise specified activities which may involve producing intelligence on an Australian person or persons where the Agency is cooperating with ASIO in the performance of an ASIO function pursuant to a section 13A arrangement. A Ministerial Authorisation will not replace the need to obtain a warrant where one is currently required	No comment provided
18c	Enable ASIS to provide training in self- defence and the use of	No comment provided

	weapons to a person cooperating with ASIS	



Submission No 209

Inquiry into potential reforms of National Security Legislation

Organisation: ASIO

Parliamentary Joint Committee on Intelligence and Security

National Security Legislation Reform

The Parliamentary Joint Committee on Intelligence and Security has been asked to examine a package of national security ideas comprising proposals for telecommunications interception reform, telecommunications sector security reform and Australian intelligence community legislation reform. The terms of reference and a discussion paper which provide explanation of the reform proposals have been published on the Committee's website.

The reform proposals are about properly equipping our law enforcement, security and intelligence professionals to do the job that Australians have entrusted to them. They are also about continuing to ensure that the Australian telecommunications sector is properly protected.

In this document ASIO discusses data retention and why this is considered necessary in the context of the *Telecommunications (Interception and Access) Act 1979* (the TIA Act) and the security intelligence functions of ASIO.

Modernisation of the Telecommunications (Interception and Access) Act

What do we use Telecommunications Interception (TI) for?

TI is a critical operational tool for security, law enforcement and integrity agencies. It cannot easily, or without considerable cost or risk, be substituted with any combination of alternative investigative techniques.

For ASIO and law enforcement agencies, TI provides a unique, low risk and cost effective tool for

For ASIO and law enforcement agencies, it provides a unique, low risk and cost effective tool for collecting intelligence and evidence. It can only be used in very specific circumstances. For ASIO, this threshold is very high. ASIO must be confident that there is a link between the telecommunications activity to be intercepted and activities that are intended to do harm to Australia or its people. Furthermore, ASIO rules dictate that interception can only be carried out after consideration of the proportionality between the nature and seriousness of the threat, the degree of intrusion and the overall impact on privacy. The independent Inspector General of Intelligence and Security routinely inspects ASIO's TI operations to ensure this is the case.

Communications material is vital in two respects:

1. the actual content of telecommunications, telephone conversations, emails and messages which forms the basis for intelligence assessment and investigations and may be used as evidence in court proceedings. The actual content may be collected only on the basis of a warrant.
2. the so called 'meta-data' or 'communications associated data (CAD)' which is essentially information generated alongside the communication and is identifying information about the originator, recipient, location and timing of calls, etc. This data is vital to law enforcement and security intelligence agencies for pre-warrant checks, investigative leads, intelligence and evidentiary corroboration, etc. It may also be used in evidence. Collection of this telecommunications data, as opposed to content, does not require a warrant.

Current TI Regime

All carriers and carriage service providers (C/CSPs) have an obligation under the TIA Act to install and maintain an interception capability within their networks and to make that capability available to authorised interception agencies. That capability may include access both to the actual content of the communication (but only under warrant) and to CAD.

The interception model in Australia is currently based on a service or equipment identifier. These identifiers include telephone numbers, email addresses, or unique numbers attached to telecommunications hardware (e.g. mobile phone handsets, or individual computers, etc). Warrants for interception of content within telecommunications networks can only be issued on the basis of these network identifiers.

Agencies currently intercept on the basis of those network identifiers via the following warrant types:

- *Telecommunications service warrant*
A telecommunications services warrant enables authorised agencies to intercept communications from a specified telecommunications service (e.g. mobile phone) either because it is being used by a person reasonably suspected of engaging in activities prejudicial to security or the service itself is being used for purposes prejudicial to security.
- *Telecommunications service (B-party) warrant*

Where the service of the person involved in activities prejudicial to security cannot be identified or intercepted, ASIO may request interception of services belonging to another person known to communicate with the person of interest.

- *Named person warrant*

Where it is ineffective to rely on a telecommunications service warrant to obtain the requisite intelligence, ASIO may request authority to intercept all telecommunications services that are used by the person of interest.

There are two categories of this named person warrant – named person (services) and named person (devices). The former authorises interception of all known telecommunications services (for example, home phone, business phone, mobile phone, facsimile, and email) whereas the latter authorises interception of specified devices connected to the person (e.g. multiple mobile phone handsets).

Current protections for access to communications and to data

ASIO is, appropriately, subject to significant oversight and accountability mechanisms. These, combined with specific protections under the current Telecommunications Interception regime provide a high level of assurance to the Australian community that its security intelligence service acts responsibly and with proportionality. These protections include:

- ASIO may only listen to or record (ie intercept) the content of communications passing over the Australian telecommunications network under the authority of a warrant issued by the Attorney-General or where otherwise authorised under the Telecommunications (Interception and Access) Act.
- ASIO may also only access the content of stored communications held on a carrier/carriage service provider's equipment (such as emails, SMS and voice mail messages) under a warrant issued by the Attorney-General.
- The Attorney-General must be satisfied that the request meets the legal tests (for example, whether the telecommunications service to be intercepted is likely being used by a person engaged in activities prejudicial to security) before issuing a warrant.
- ASIO accesses telecommunications-associated data (i.e. not content) from carriers/carriage service providers under internal authorisations which may only be made where the relevant ASIO officer is satisfied that the disclosure of the data specified in the authorisation would be in connection with the performance of ASIO's legal functions (and for no other purpose).

- In all cases, before requesting a warrant or making an authorisation, consideration must have first been given to the requirements of the guidelines issued by the Attorney-General under the ASIO Act which include:
 - inquiries and investigations are to be undertaken using as little intrusion into individual privacy as possible;
 - wherever possible, the least intrusive techniques of information collection should be used before more intrusive techniques; and
 - any means used for obtaining information must be proportionate to the gravity of the threat posed and the probability of its occurrence.
- The Inspector-General of Intelligence and Security routinely undertakes inspections of warrants, warrant related document and authorisations for the disclosure of telecommunications data to ensure that ASIO acts within its legal authority and with propriety and reports on these issues in the Inspector-General's annual report.
- ASIO reports to the Attorney-General within three months of the expiry or revocation of a warrant on the extent to which the interception of communications under the warrant has assisted ASIO in carrying out its functions.

Communication Assisted Data (CAD) – data retention

In the context of TI reform “data” or CAD generally refers to *information about communications* – not the actual substance or content of those communications. For example: phone number xxxxxxxxx called number yyyyyyy at 10:00 on 12 September 2012; not what was said during the conversation.

For many years law enforcement and security agencies (as well as many others) have been able to request CAD from any carrier or carriage service provider. Agencies access to this information through an internal authorisation. This power already exists; a brand new power is not being sought.

Traditionally the telecommunications industry has retained the call data, and many still do, mainly for billing purposes. However, over time, technological and business changes have meant that industry has less need to retain the sort of CAD information agencies require. The main drivers are the increased use of Internet Protocol (IP) technology and the trend to charge customers based on volume (units of data sent or received) rather than by transaction (ie. call by call, message by message).

This situation is becoming more common around the world and has led many jurisdictions to consider mandatory retention of CAD for law enforcement and security purposes.

CAD is used by agencies to determine who communicated with whom, when, where to and where from. Its use is often the most appropriate and proportionate response to investigative leads. This information assists in a variety of ways, including an investigation and ensures individuals who are not relevant

information assists in refining/focusing an investigation and ensures individuals who are not relevant to the investigation can be ruled out at the earliest possible opportunity.

CAD is often received as important "lead" or "tip off" information. For example it may demonstrate that an Australian telephone number has been in contact with a member of a terrorist cell in a foreign country or that an Australian internet address has been the subject of cyber attack.

CAD may be used to corroborate intelligence or evidence, exclude or include persons in an investigation, or to provide locational information.

CAD data also provides a critically important part of broader security or law enforcement requirements. It can be used to help identify perpetrators or victims of malicious activity on the internet. It can be used to help locate victims of crime or individuals in distress.

To the extent possible, agencies are seeking greater certainty that the information needed to protect the community will be there when they need it. In that sense agencies are looking to access the same general information they have been accessing for many years; information that would enable them to trace the participants of a communication in retrospect, when the communication occurred and ideally where the parties were. It might include:

- data to identify the parties of a communication;
- data to identify the origin and destination of a communication;
- data to identify the date, time and duration of a communication;

- data to identify the type of communication (eg. phone call, email)
- data to identify users' communications equipment; and
- data to identify the location of parties to the communications.

In this context, agencies are not seeking access to the content of communications.

The period that CAD is available to law enforcement and security intelligence agencies has a direct impact on its utility for investigations. Investigations of serious criminal activity and threats to security are often long and complex. The identity of all persons of interest may not initially be known and often additional persons of interest will emerge as investigations unfold. The longer relevant data is available to access, the greater the potential utility for the agencies. Given complex investigations are measured in years rather than months, access to CAD for a minimum period of two years is proposed to ensure that agencies can undertake effective investigations in accordance with their functions. Shorter periods of access carry the risk that agencies may be less able to access the critical intelligence that they require to progress an investigation.

The European Union Data Retention Directive provides a useful outline of the types of data requested and is an important basis for discussion with Australian C/CSPs, agencies and other stakeholders: (<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:HTML>)

To ensure privacy protections remain appropriate it may be necessary to include new penalties for misuse of retained data as well as an appropriate scheme for the notification of data breaches.

Agencies would support the introduction of such measures provided that there were appropriate

agencies would support the introduction of such measures provided that there were appropriate exemptions in place to protect sensitive operational information.

Summary

- Any new regime should maintain the distinction between the interception of content and access to communications data.
- Any new regime should retain the current effective oversight and accountability mechanisms which help ensure interception capabilities are used for appropriate and legal purposes and only by the agencies authorised to conduct such activities in the public interest.
- From the point of view of security and law enforcement agencies retention of CAD information has important investigative advantages.

**Pages 545 to / à 547
are withheld pursuant to sections
sont retenues en vertu des articles**

15(1) - Subv, 16(1)(a)(iii), 16(1)(c)

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

**Pages 548 to / à 550
are withheld pursuant to sections
sont retenues en vertu des articles**

15(1) - Subv, 16(1)(a)(iii), 16(1)(c)

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

**Pages 551 to / à 555
are withheld pursuant to sections
sont retenues en vertu des articles**

15(1) - Subv, 16(1)(a)(iii), 16(1)(c)

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

**Pages 556 to / à 558
are withheld pursuant to sections
sont retenues en vertu des articles**

15(1) - Subv, 16(1)(a)(iii), 16(1)(c)

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

**Pages 559 to / à 560
are withheld pursuant to sections
sont retenues en vertu des articles**

15(1) - Subv, 16(1)(a)(iii), 16(1)(c)

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

Dvorkin, Corey

From: Grigsby, Alexandre
Sent: March-26-12 9:30 AM
To: Dvorkin, Corey; Green, Amanda; Matz, Mark; Bradley, Kees; Binne, Christine
Cc: Gordon, Robert; Dick, Robert
Subject: from the news summary: Huawei stopped from working on Australia's National Broadband project

Huawei stopped from working on Australia's National Broadband project

Although Huawei has been spreading itself fast and thick across Europe, Asia and India, the network company has now come up against a brick wall in Australia where it has been blocked from bidding on the country's \$37.5 billion national broadband (NBN) project.

The "prudent decision" was outlined by Australian Prime Minister Julia Gillard who cited concerns about cyber security.

Although she wouldn't go into too much detail as to why the Chinese company was targeted, a source close to the broadband deal told the Economic Times that the country feared attacks by China.

The source said the NBN would endeavour to connect around 93 percent of Australian homes to superfast fibre-to-the-home internet by 2017. It is seen as the future "backbone of Australia's information infrastructure," meaning that security surrounding the project must be tight.

Huawei has so far bowed out of the decision gracefully with a spokesman stating that it was hopeful of playing a role in the NBN in the future.

It said it would work hard to be open and transparent to show the country that its technology was trustworthy.

The spokesman added that individuals and governments around the world were still coming to terms "with the emergence of the new China which is an innovation leader." And although network security was an issue for all vendors, "the real risk [was] missing out on the innovation China has to offer."

However, we doubt Huawei will be crying into its pillow for much longer as it has deals for broadband networks in Britain, New Zealand, Singapore and Malaysia.

<http://news.techeye.net/security/huawei-stopped-from-working-on-australias-national-broadband-project>

Alexandre Grigsby
Analyst | Analyste
National Cyber Security Directorate | Direction générale de la cybersécurité nationale
Public Safety Canada | Sécurité publique Canada
tel: 613-949-4243

s.15(1) - Int'l

s.19(1)

Dvorkin, Corey

From: Matz, Mark
Sent: February-13-12 10:53 AM
To: Gordon, Robert; Green, Amanda; Dvorkin, Corey; Grigsby, Alexandre
Cc: Dick, Robert; Hatfield, Adam
Subject: RE: Canada - Huawei

From last week: PM at signing ceremony for Telus and Huawei.

<http://www.newswire.ca/en/story/918527/huawei-helps-bell-bring-lte-to-millions-of-canadians>

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

From: Gordon, Robert
Sent: February-12-12 2:28 PM
To: Matz, Mark; Green, Amanda; Dvorkin, Corey; Grigsby, Alexandre
Cc: Gordon, Robert
Subject: Fw: Canada - Huawei

FYI.

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

From: [REDACTED]
Sent: Sunday, February 12, 2012 10:09 AM
To: Gordon, Robert
Cc: [REDACTED]
Subject: RE: Canada - Huawei

Bob

See below. I'd like to catch up sometime next week to discuss the shape of the agenda and how we use the time on Wednesday-week.

When would you be free to speak?

I am switching to my other email address now and I will stop reading this one after Monday morning my time.

Regards

[REDACTED]

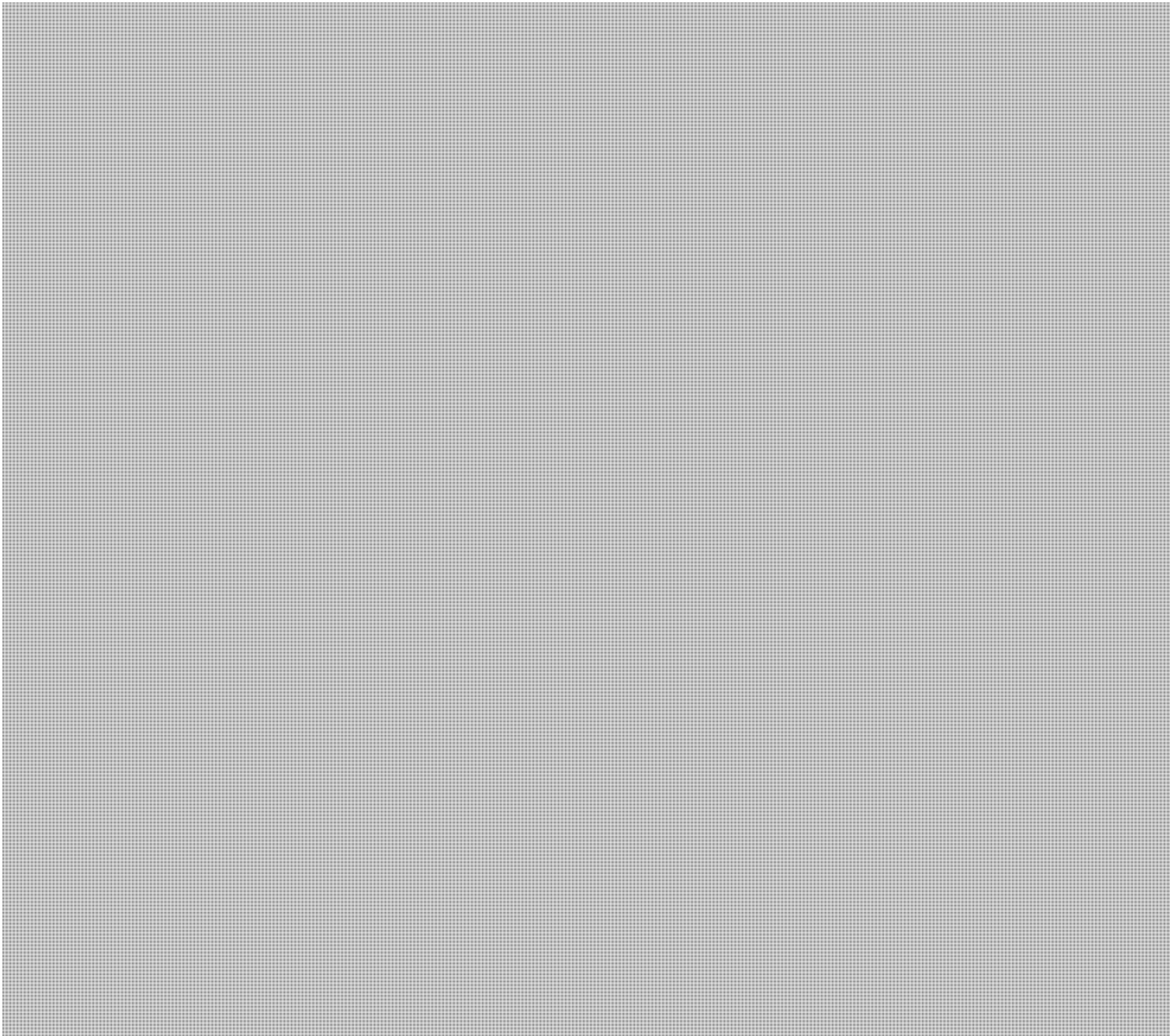
[REDACTED]

when in the building
when out of the building

[REDACTED]

s.15(1) - Int'l

s.19(1)



<http://www.ottawacitizen.com/touch/story.html?id=6135107> Does the U.S. know something about China we don't?
BY TERRY GLAVIN, FEBRUARY 10, 2012 To get just a glimpse into the perilous territory where Ottawa's clever China
enthusiasts have led us lately, you'd do well to know something about the unsettling tale of Huawei Technologies Co.
Ltd., headquartered in the Special Economic Zone of Shenzhen in the Chinese province of Guangdong. Huawei has more
than 120 staff at its gleaming new Canada Research & Development Centre in Ottawa, a head office in Markham, branch
offices in Montreal and Edmonton and partnerships with the University of Ottawa and Carleton University. It plans to
double its Ottawa staff in the next year.

Huawei's operations are also now under investigation by the U.S. State Department on charges of sanctions-busting in
Iran.

To properly consider the implications it might help to keep in the back of your mind the bitter and quickening
estrangement between Prime Minister Stephen Harper and U.S. President Barack Obama, the spectre of a shooting war
in the Strait of Hormuz, and missiles flying in the direction of Tel Aviv. You can count on war perhaps as soon as April if
the speculations of U.S. Defense Secretary Leon Panetta are anything to go by.

Huawei is an aggressive, high-performance and at least nominally private corporation. Its 100,000 workers are some of the brightest in the business. Huawei has about 400 employees in Canada and they have not been helped by suspicions in the U.S. that Huawei is a conduit for Chinese espionage. Neither has it helped that Huawei president Ren Zhengfei is a former People's Liberation Army major and Communist Party loyalist. Huawei's global branch bosses have made gallant efforts to allay everyone's concerns. They've failed pretty well everywhere but Ottawa.

While Prime Minister Stephen Harper was taking tea with Chinese President Hu Jintao this week, U.S. President Barack Obama was in Washington attending to the authorizations under a new, head-breaking, scaffold-building sanctions order that he signed only last Sunday. It's Washington's last-ditch prelude to a full-on Iranian oil embargo, and an embargo is the final Hail Mary before the bombs start flying.

Obama's executive order severely tightens a sanctions net that was already circling around another Chinese giant: Beijing's own Sinopec, also known as the China Petroleum & Chemical Corporation, also known around the Prime Minister's Office these days as Canada's lifeline to economic prosperity in China. This is seriously inconvenient. But back to Huawei.

Before the U.S. State Department investigation began, the U.S. House Intelligence Committee was already looking into whether Beijing's spies use networks like Huawei in ways that pose threats to the U.S. telecommunications infrastructure. The twist with the new State Department probe is that it's inquiring into whether Huawei has violated the U.S. Comprehensive Iran Sanctions law of 2010 by providing telecommunications technology used by the Khomeinist regime in Tehran to track dissidents. Huawei loudly professes its innocence.

But Huawei's partners in Iran, Zaeim Electronic Industries, name the Khomeinist regime's defence ministry and its intelligence branch on their client list, along with the fanatically pro-regime Islamic Revolutionary Guards Corps.

As national security concerns have been freezing Huawei out of the information-technology industry in the United States, Huawei has quickly expanded in Canada. While Huawei's American operations have fallen afoul of the U.S. Committee on Foreign Investment, Canada abolished its own Foreign Investment Review Agency years ago. While U.S. law lists the Islamic Revolutionary Guard Corps as a terrorist entity, Canadian law does not.

The U.S. National Security Agency and the U.S. Commerce Department have cited "national security" concerns to block Huawei's involvement in Homeland Security contracts and Huawei's dealings with American telecom giants. In Canada it's not clear whether any such firewalls would even be legal anymore.

Against the advice of intelligence experts, the federal cabinet approved amendments to the Investment Canada Act in September 2009 that hollowed out "national security" defences against foreign-power takeovers and investment intrigues. In the run-up to the amendments, David Emerson, Canada's trade minister at the time and now a major China investment adviser, was in China, telling everybody not to worry. By the time regulations were gazetted in Ottawa they didn't even contain a minimum regulatory explanation of what the words "national security" mean.

In the wake of the amendments, Beijing's state-owned corporations high-gearred their acquisitions program in Canada's energy sector, especially the Alberta oilsands. In April, 2010, Beijing's own Sinopec obtained a veto over whether any stepped-up bitumen production by the oilsands giant Syncrude would be upgraded and refined in the U.S. and Canada, or shipped offshore instead.

Less than a week later, Huawei Technologies, aided by a \$6.5 million grant from the Ontario government, officially opened its Canada R&D Centre in Ottawa. Huawei declared: "Research is global in nature and will be applied to all markets that Huawei serves (not just Canada)." A small problem: All global markets for Huawei include Iran.

After Sinopec let it be known that it was behind the proposed \$6-billion Enbridge Inc. pipeline from Alberta to awaiting supertankers at Kitimat, Prime Minister Harper quietly reversed a long-standing Conservative pledge to oppose shipping

bitumen offshore. The prime minister is now calling Sinopec's big Enbridge bitumen tube a project that's vital to Canada's national interests. After all, China is the future. A big problem: In Washington, Sinopec is not discussed in such flattering language.

Even before President Obama signed his new hardball executive order last Sunday, Sinopec was already at the corkline of the U.S. sanctions dragnet. It was under the older, looser rules that Sinopec's own Iranian oil buyer Zhuhai Zhenrong was busted last month after getting caught selling gasoline worth more than \$500 million back into Iran.

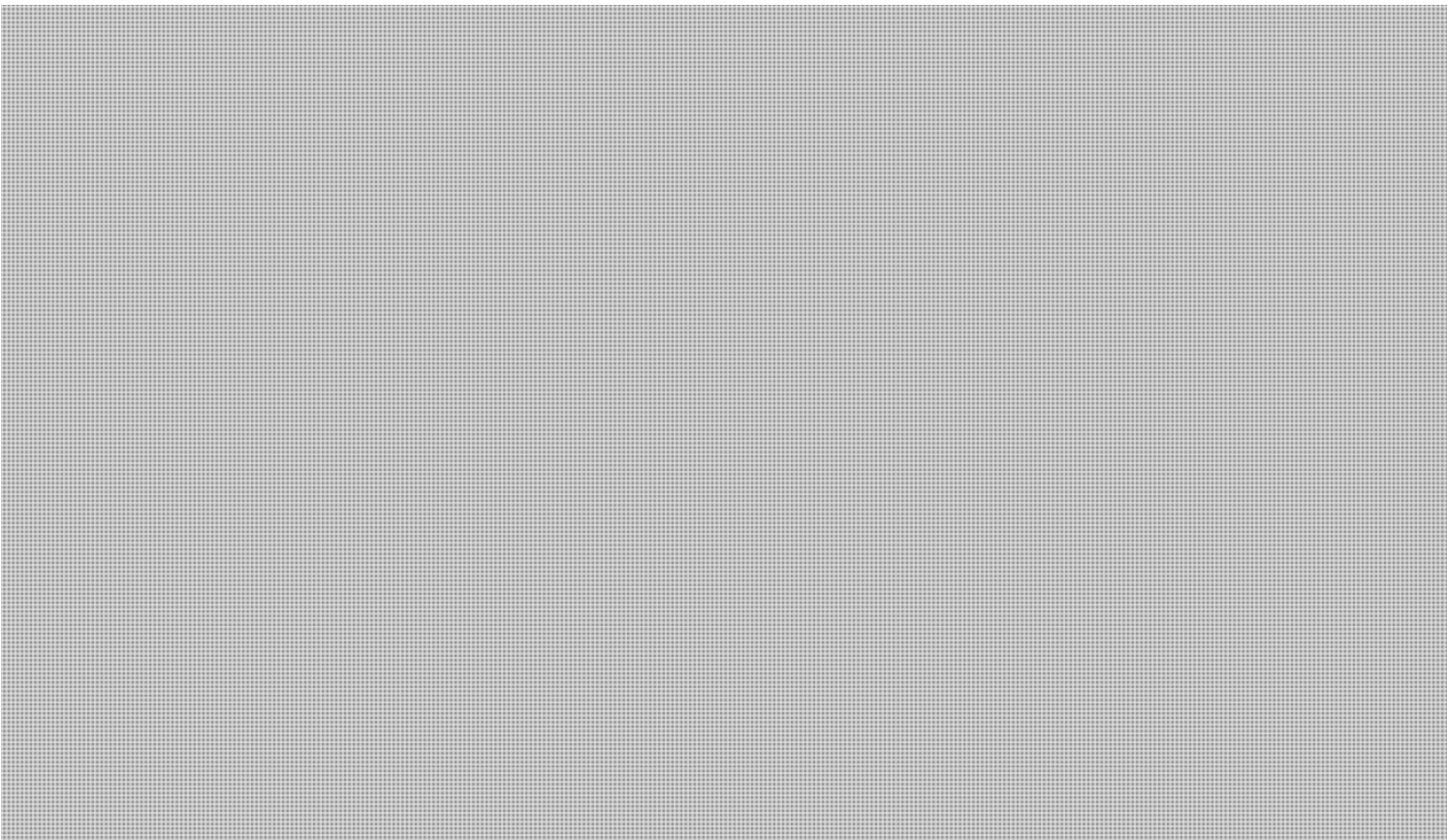
Canada talks a tough game on sanctions, but Sinopec and Zhuhai Zhenrong are still the two largest buyers of Iranian oil, and even after it got busted by the U.S. State Department last month, Zhuhai Zhenrong was poking around in Alberta's oilsands looking for greener pastures.

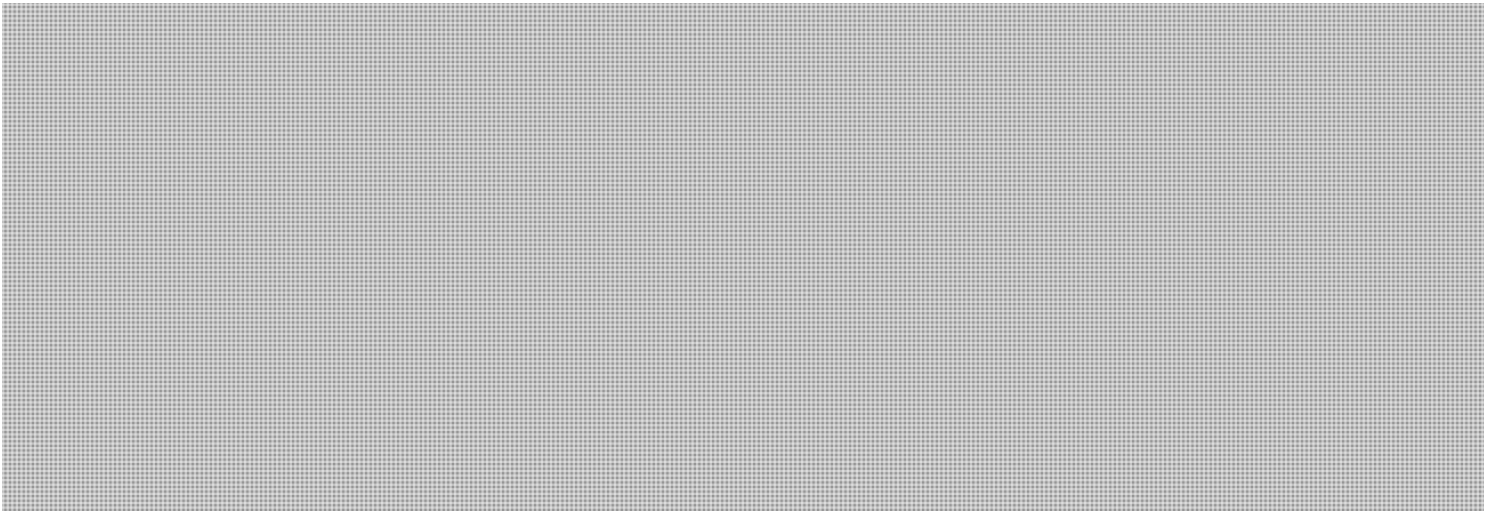
It was in Beijing last November that Huawei's Canada boss Sean Yang first announced plans for a major staffing increase at the Ottawa R&D Centre. On hand was former Liberal cabinet minister Martin Cauchon, whose career trajectory will be familiar to former federal cabinet ministers. He's now a big-money China deal broker. In what hindsight may render as merely an unfortunate choice of words, Cauchon said: "There is a saying that if you can't beat them, join them."

But that is the Conservative government's party line now. Sanctions are for chumps, China is the future, obeisance to Beijing is in Canada's vital national interests, and from now on the United States can suck eggs.

Terry Glavin is an award-winning author and journalist. His most recent book is *Come From The Shadows: The Long and Lonely Struggle for Peace in Afghanistan*.

s.15(1) - Int'l





s.15(1) - Int'l

Supply Chain Risk Mitigation

s.15(1) - Def
s.15(1) - Int
s.15(1) - Subv

Plunkett, Shawn

From: [redacted]@cse-cst.gc.ca]
Sent: Friday, June 15, 2012 4:19 PM
To: Lister, Michael (FAC); [redacted] (CSIS); Plunkett, Shawn; Soper, Lesley (PCOSANDI); Smith, Maggie M (CIC); Hatfield, Adam
Cc: [redacted] (CSE)
Subject: Supply Chain Risk Mitigation
Attachments: CERRID-#987336-v1-[redacted]_Supply_Chain_Risk_Mitigation_-_GC_Interdepartmental_June_2012.PPT

Classification: TOP SECRET//

DFAIT: For distribution to Chris MacLean and David Hartman

Hello all,

Please find attached a copy of the deck from this morning's meeting.

<<CERRID-#987336-v1-[redacted]_Supply_Chain_Risk_Mitigation_-_GC_Interdepartmental_June_2012.PPT>>

In addition, here are the [redacted] we referenced. Please let me know if you are having trouble retrieving [redacted]

Thank you,

[redacted signature]

IT Security Strategic Relationships Office / Bureau des relations stratégiques
Communications Security Establishment Canada / Centre de la sécurité des télécommunications Canada

10/17/2012

000567

000567



Communications Security
Establishment Canada

Centre de la sécurité
des télécommunications Canada



s.15(1) - Def
s.15(1) - Subv
s.16(2)(c)
s.21(1)(a)

Risk Mitigation

June 14, 2012

Director IT Security Strategic Relationships Office

Canada

OVERALL CLASSIFICATION IS TOP SECRET//



Communications Security
Establishment Canada

Centre de la sécurité
des télécommunications Canada



Present Concern

- s.15(1) - Def
- s.15(1) - Int
- s.15(1) - Subv
- s.16(2)(c)
- s.20(1)(b)
- s.20(1)(c)
- s.21(1)(a)

Canada



Intelligence Review

- Recent reports

- Huawei

-
-
-
-
-

- Conclusion

-

s.15(1) - Def
s.15(1) - Int
s.15(1) - Subv
s.16(2)(c)
s.20(1)(b)
s.20(1)(c)
s.21(1)(a)

OVERALL CLASSIFICATION IS TOP SECRET/



Communications Security
Establishment Canada

Centre de la sécurité
des télécommunications Canada



Risk Mitigation in Canada

- s.15(1) - Def
- s.15(1) - Int
- s.15(1) - Subv
- s.16(2)(c)
- s.20(1)(b)
- s.20(1)(c)
- s.21(1)(a)

Canada

OVERALL CLASSIFICATION IS TOP SECRET//



Communications Security
Establishment Canada

Centre de la sécurité
des télécommunications Canada



Risk Mitigations

- s.15(1) - Def
- s.15(1) - Int
- s.15(1) - Subv
- s.16(2)(c)
- s.20(1)(b)
- s.20(1)(c)
- s.21(1)(a)

- Conclusion:

Canada

OVERALL CLASSIFICATION IS TOP SECRET//



Communications Security
Establishment Canada

Centre de la sécurité
des télécommunications Canada



Risk Mitigations

s.15(1) - Def

s.15(1) - Int

s.15(1) - Subv

s.16(2)(c) •

s.20(1)(b)

s.20(1)(c)

s.21(1)(a)

•

•

•

•

•

Canada

OVERALL CLASSIFICATION IS TOP SECRET//



Communications Security
Establishment Canada

Centre de la sécurité
des télécommunications Canada



- s.15(1) - Def
- s.15(1) - Int
- s.15(1) - Subv
- s.16(2)(c)
- s.20(1)(b)
- s.20(1)(c)
- s.21(1)(a)

Canada

7

000574

000574

OVERALL CLASSIFICATION IS TOP SECRET/



Communications Security
Establishment Canada

Centre de la sécurité
des télécommunications Canada



s.15(1) - Def
s.15(1) - Int
s.15(1) - Subv
s.16(2)(c)

Canada

8

000575

000575

OVERALL CLASSIFICATION IS TOP SECRET//



Communications Security
Establishment Canada

Centre de la sécurité
des télécommunications Canada



s.15(1) - Def
s.15(1) - Int
s.15(1) - Subv

Update

s.20(1)(b)
s.20(1)(c)

•

•

•

•

•

Canada

9

000576

000576

OVERALL CLASSIFICATION IS TOP SECRET/



Communications Security
Establishment Canada

Centre de la sécurité
des télécommunications Canada



GC Considerations

- s.13(1)(a)
- s.13(1)(b)
- s.15(1) - Def
- s.15(1) - Int
- s.15(1) - Subv
- s.20(1)(b)
- s.20(1)(c)

•

•

•

•

Canada

OVERALL CLASSIFICATION IS TOP SECRET/



Communications Security
Establishment Canada

Centre de la sécurité
des télécommunications Canada



Risk Mitigation

s.15(1) - Def
s.15(1) - Int
s.15(1) - Subv
s.21(1)(a)

•

•

•

•

Canada

OVERALL CLASSIFICATION IS TOP SECRET//



Communications Security
Establishment Canada

Centre de la sécurité
des télécommunications Canada



- s.15(1) - Def
- s.15(1) - Int
- s.15(1) - Subv
- s.20(1)(b)
- s.20(1)(c)

•

•

•

•

Canada

OVERALL CLASSIFICATION IS TOP SECRET//



Communications Security
Establishment Canada

Centre de la sécurité
des télécommunications Canada



Huawei

- s.15(1) - Def
- s.15(1) - Int
- s.15(1) - Subv
- s.20(1)(b)
- s.20(1)(c)



Canada

OVERALL CLASSIFICATION IS TOP SECRET/



Communications Security
Establishment Canada

Centre de la sécurité
des télécommunications Canada



- s.13(1)(a)
- s.13(1)(b)
- s.15(1) - Def
- s.15(1) - Int
- s.15(1) - Subv
- s.21(1)(a)

•

•

•

Canada

OVERALL CLASSIFICATION IS TOP SECRET//



Communications Security
Establishment Canada

Centre de la sécurité
des télécommunications Canada



- s.15(1) - Def
- s.15(1) - Int
- s.15(1) - Subv
- s.20(1)(b)
- s.20(1)(c)
- s.21(1)(a)

'Huawei'

[The main body of the document is heavily redacted with a dense, grainy pattern, obscuring the text.]

Canada

OVERALL CLASSIFICATION IS TOP SECRET//:



Communications Security Establishment Canada

Centre de la sécurité des télécommunications Canada



- s.15(1) - Def
- s.15(1) - Int
- s.15(1) - Subv
- s.20(1)(b)
- s.20(1)(c)
- s.21(1)(a)

Next Steps

-
-

Canada

Maille, Marie Anick

From: Plunkett, Shawn
Sent: Friday, June 15, 2012 12:32 PM
To: MacDonald, Michael
Cc: Kingsley, Michèle; Maille, Marie Anick
Subject: Report - CSEC Supply Chain Interdepartmental Meeting (June 15, 2012)

s.15(1) - Def
s.15(1) - Int
s.15(1) - Subv
s.16(2)(c)
s.21(1)(a)

Classification: TOP SECRET//

Mike,

As mentioned by Michele, I attended a meeting today at CSEC regarding [redacted] in Canada's supply chain, Huawei. CSEC/ [redacted] head of Strategic Relationships at CSEC, presented a deck to representatives from [redacted]

E-copy of deck is to be provided shortly.

CSEC appeared to have three messages/objectives at the meeting:

1) CSEC wants to ensure [redacted] with respect to Huawei. This is especially important given the impending visit to Canada of high ranking [redacted] Huawei officials, expected in July, 2012.

2) CSEC underscored the fact [redacted]

3)

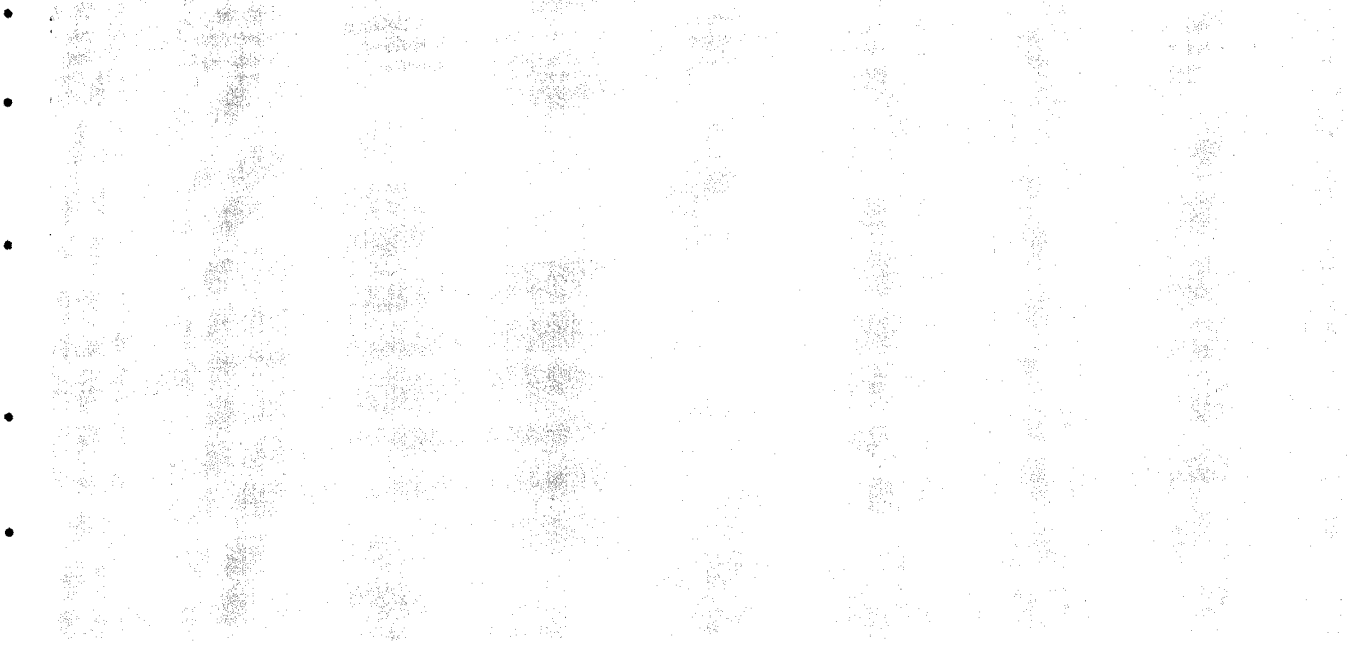
NEXT STEPS

- CSEC is requesting that organizations brief up on this issue to ensure [redacted]
- Also raised was the notion of [redacted]
- [redacted] that [redacted] should expect a call. [redacted] indicated to CSEC/ [redacted]

BACKGROUND

•

•



Shawn

s.15(1) - Def
s.15(1) - Int
s.15(1) - Subv
s.16(2)(c)
s.20(1)(b)
s.20(1)(c)
s.21(1)(a)

**Pages 586 to / à 589
are withheld pursuant to sections
sont retenues en vertu des articles**

13(1)(a), 15(1) - Subv, 16(1)(a)(iii), 16(1)(c), 24(1)

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