Bunghardt, Greg (PS/SP)

From: Ennis-Dawson, David (PS/SP)
Sent: Tuesday, June 19, 2018 3:59 PM
To: Waters, Michael (PS/SP)
Cc: St-Aubin, Emmanuel (PS/SP); Bunghardt, Greg (PS/SP)
Subject: telecoms and Australia

Hello Michael,

With regards to our quick chat about the issues surrounding Huawei, here are several articles illustrating the company's attempt to change the Australian government's attitudes.

Huawei to Australia: We're not a security risk for 5G
http://money.cnn.com/2018/06/18/technology/huawei-australia-5g-china/index.html

- Australian wireless carriers will need to hire companies to build new 5G networks. Huawei faces opposition from Australian national security agencies.
- It has successfully bid for private contracts. It is Australia's largest supplier of wireless technology.

Huawei rejects Australia security concerns
https://www.bbc.com/news/technology-44519495

- Huawei's open letter cites 5G technology deals in the UK, Canada and New Zealand that followed the building of similar testing centres.
- The Australian parliament is debating a foreign interference bill that would require people to declare if they were working for on a foreign power.

Bunghardt, Greg (PS/SP)

From: Frigon, Sylvie (PS/SP)
Sent: Tuesday, October 16, 2018 10:17 AM
To: Bunghardt, Greg (PS/SP)
Subject: FW: QP note on Cyber Security (China – Huawei)

Did we do any?

From: Loita, Ahmed (FIN)
Sent: October-16-18 10:04 AM
To: Binne, Christine (PS/SP); Frigon, Sylvie (PS/SP)
Cc: Brown, Justin (FIN); Loranger, Marie-France (FIN)
Subject: RE: QP note on Cyber Security (China – Huawei)

Good morning Christine and Sylvie,

Wondering if you could share your QP notes on the Huawei issue? Please let us know. Many thanks!

Ahmed

Bunghardt, Greg (PS/SP)

From: Park, Beom-Jun (PS/SP)
Sent: Tuesday, October 16, 2018 2:34 PM
To: Bunghardt, Greg (PS/SP)
Subject: NZ on 5G Huawei

https://www.reseller.co.nz/article/647373/nz-asserts-independence-huawei-5g-role-after-aussie-ban/

It appears New Zealand isn't automatically banning Huawei, and is instead assessing whether its existing risk mitigation framework for the public telecom network (under their Telecommunications Interception Capability and Security Act 2013) would be sufficient for the task.

Bunghardt, Greg (PS/SP)

From: Goldfinger, Marc (PS/SP)
Sent: Wednesday, October 24, 2018 12:59 PM
To: Bunghardt, Greg (PS/SP)
Subject: FW: Try opening this one...FW: [redacted]
Attachments: [redacted]

From: Artelle, Helen (PS/SP)
Sent: Wednesday, October 24, 2018 10:03 AM
To: Goldfinger, Marc (PS/SP)
Subject: Try opening this one...FW: [redacted]

Hi Marc,
Are you able to access this one?
Thanks,
Helen

From: Hunt, Ryan (PS/SP)
Sent: Thursday, October 11, 2018 11:32 AM
To: Artelle, Helen (PS/SP)
Cc: Clayton, Natalie (PS/SP)
Subject: FW: FCM-5G

Hi Helen - FYI – for inclusion in Craig's C5 binder.
Tx
Ryan

From: Clayton, Natalie (PS/SP)
Sent: Tuesday, August 07, 2018 2:42 PM
Cc: Sandford, Amanda (PS/SP); Hunt, Ryan (PS/SP)
Subject: [redacted]

Here are the other documents that I shared [redacted]

Natalie

Pages 5 to / à 10

are withheld pursuant to sections

sont retenues en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Bunghardt, Greg (PS/SP)

From: Bunghardt, Greg (PS/SP)
Sent: Friday, October 19, 2018 11:08 AM
To: Artelle, Helen (PS/SP)
Cc: Hunt, Ryan (PS/SP)
Subject: FW: Letter to Prime Minister Trudeau re Huawei
Attachments: 10-11-18 Letter to Prime Minister Trudeau re Huawei.pdf

Hi Helen,

Attached is a letter [redacted] to the PM related to Canada's position on 5G. [redacted]

I will send you a briefing package on 5G that we put together for the Minister via GCSI.

Thanks,

greg.

-----Original Message-----
From: Binne, Christine (PS/SP)
Sent: Friday, October 12, 2018 4:37 PM
To: Waters, Michael (PS/SP); Bunghardt, Greg (PS/SP); Goldfinger, Marc (PS/SP); Frigon, Sylvie (PS/SP)
Subject: FW: Letter to Prime Minister Trudeau re Huawei

FYI

-----Original Message-----
From: Merchant, Colleen (PS/SP)
Sent: Friday, October 12, 2018 7:10 AM
To: Beauregard, Monik (PS/SP)
Cc: Payer, Alexina (PS/SP); Binne, Christine (PS/SP); [redacted]
Subject: Fw: Letter to Prime Minister Trudeau re Huawei

FYI.

Sent from my BlackBerry 10 smartphone on the Bell network.
Original Message
From: [redacted]@pco-bcp.gc.ca>
Sent: Thursday, October 11, 2018 9:51 PM

To: [redacted] (Ext.); Wendy Hadwen; Proulx, Martin (IC); Merchant, Colleen (PS/SP); [redacted]

Cc: [redacted]

Subject: Fw: Letter to Prime Minister Trudeau re Huawei

Some of you may have already seen this, but for awareness.

From: [redacted] [mailto: [redacted]

Sent: October-11-18 3:57 PM

To: [redacted]

Cc: [redacted]

Subject: Letter to Prime Minister Trudeau re Huawei

Dear [redacted]

Please find attached a letter from [redacted] to Prime Minister Justin Trudeau regarding Huawei Technologies. I kindly ask that you please ensure Prime Minister Trudeau receives this letter. Thank you in advance.

Best regards,

[redacted]

Pages 13 to / à 14

are duplicates

sont des duplicatas

Bunghardt, Greg (PS/SP)

From: Binne, Christine (PS/SP)
Sent: Friday, October 12, 2018 4:37 PM
To: Waters, Michael (PS/SP); Bunghardt, Greg (PS/SP); Goldfinger, Marc (PS/SP); Frigon, Sylvie (PS/SP)
Subject: FW: Letter to Prime Minister Trudeau re Huawei
Attachments: 10-11-18 Letter to Prime Minister Trudeau re Huawei.pdf

FYI

-----Original Message-----
From: Merchant, Colleen (PS/SP)
Sent: Friday, October 12, 2018 7:10 AM
To: Beauregard, Monik (PS/SP)
Cc: Payer, Alexina (PS/SP); Binne, Christine (PS/SP);
Subject: Fw: Letter to Prime Minister Trudeau re Huawei

FYI.

Sent from my BlackBerry 10 smartphone on the Bell network.
Original Message
From: @pco-bcp.gc.ca>
Sent: Thursday, October 11, 2018 9:51 PM
To: (Ext.); Wendy Hadwen; Proulx, Martin (IC); Merchant, Colleen (PS/SP);
Cc:
Subject: Fw: Letter to Prime Minister Trudeau re Huawei

Some of you may have already seen this, but for awareness.

From:
Sent: October-11-18 3:57 PM
To:
Cc:
Subject: Letter to Prime Minister Trudeau re Huawei

Dear

Please find attached a letter from to Prime Minister Justin Trudeau regarding Huawei Technologies. I kindly ask that you please ensure Prime Minister Trudeau receives this letter. Thank you in advance.

Best regards,

[redacted]

McClinton-Cuerrier, Christa (PS/SP)

From: [redacted]
Sent: Thursday, October 04, 2018 7:36 PM
To: Merchant, Colleen (PS/SP); Raquel.Garbers@forces.gc.ca; caroline.xavier@pco-bcp.gc.ca; [redacted]@pco-bcp.gc.ca
Subject: Re: Discussion of Cyber Issues

Was not aware of this. Not sure if it would be worth a discussion with [redacted]
Chris

Sent from my BlackBerry 10 smartphone on the Rogers network.

From: Merchant, Colleen (PS/SP)
Sent: Thursday, October 4, 2018 15:17
To: Garbers, Raquel -DND; caroline.xavier@pco-bcp.gc.ca; [redacted]@pco-bcp.gc.ca; [redacted]
Subject: RE: Discussion of Cyber Issues

Interesting! Were you there or know anyone who was?

C.G.M. Merchant
Director General / Directrice Générale
National Cyber Security / Cybersécurité Nationale
National and Cyber Security Branch / Secteur de la Sécurité et de la Cyber-Sécurité Nationale
Public Safety Canada / Sécurité Publique Canada
340 Laurier Avenue West, Ottawa, ON, K1A 0P8
Tel: 613.949.7380 BB 613.793.9495
Email: colleen.merchant@canada.ca

From: RAQUEL.GARBERS@forces.gc.ca [mailto:RAQUEL.GARBERS@forces.gc.ca]
Sent: Thursday, October 04, 2018 2:54 PM
To: caroline.xavier@pco-bcp.gc.ca; [redacted]@pco-bcp.gc.ca; Merchant, Colleen (PS/SP); [redacted]
Subject: FW: Discussion of Cyber Issues

Hi all,

FYI— OttawaU hosting an event today with reps from Huawei presenting

---

Dear Colleagues,

[redacted]

The meeting will be held on October 4, 2018, in the Faculty of Social Sciences Building, 1 University, 4th floor, room FSS 4006 from 4:30 – 6:30

The discussion will be held under the Chatham House rule. It will be chaired and moderated by [redacted] There will be no public reporting of its outcome.

UK, Huawei Cyber Security Evaluation Centre Oversight Board, Annual Report, 2018
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/727415/20180717_HCSEC_Oversight_Board_Report_2018_-_FINAL.pdf

HUAWEI CYBER SECURITY EVALUATION CENTRE (HCSEC) OVERSIGHT ...

assets.publishing.service.gov.uk

Page | 2 HUAWEI CYBER SECURITY EVALUATION CENTRE OVERSIGHT BOARD ANNUAL REPORT Part I: Summary 1. This is Huawei Cyber Security Evaluation

US, Office of the Director of National Intelligence, National Counterintelligence and Security Center, "Foreign Economic Espionage in Cyberspace," 2018, available at:
https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf

Foreign Economic Espionage in Cyberspace - dni.gov

www.dni.gov

1 Executive Summary In the 2011 report to Congress on Foreign Spies Stealing U.S. Economic Secrets in Cyberspace, the C Counterintelligence Executive provided a baseline assessment of the

Adam Segal, "When China Rules the Web," Foreign Affairs,vol. 97, no. 5, September/October 2018
Available at:
https://www.foreignaffairs.com/articles/china/2018-08-13/when-china-rules-web

What Will Happen When China Dominates the Web

www.foreignaffairs.com

ADAM SEGAL is Ira A. Lipman Chair in Emerging Technologies and National Security at the Council on Foreign Relations. C superpower is not guaranteed. Top-down, state-led efforts at innovation in artificial intelligence, quantum computing, rob

McClinton-Cuerrier, Christa (PS/SP)

From: Natasha.Manji@international.gc.ca
Sent: Monday, September 24, 2018 12:50 PM
To: Merchant, Colleen (PS/SP); Binne, Christine (PS/SP); Ouellet3, Benoit (PS/SP)
Subject: Re: Just released: National Cyber Strategy of the USA

My pleasure!
Note that we are asking White House to give a few of us a high-level briefing on it. I would be very happy to ask any questions, raise any considerations you want to send me!
N.

Natasha Manji
Public Safety Counsellor, Canadian Embassy in Washington
Mobile: 202-497-5898

From: Merchant, Colleen (PS/SP)
Sent: Monday, September 24, 2018 12:23 PM
To: Manji, Natasha -WSHDC -GR
Subject: RE: Just released: National Cyber Strategy of the USA

Thanks, Natasha!

Colleen

C.G.M. Merchant
Director General / Directrice Générale
National Cyber Security / Cybersécurité Nationale
National and Cyber Security Branch / Secteur de la Sécurité et de la Cyber-Sécurité Nationale
Public Safety Canada / Sécurité Publique Canada
340 Laurier Avenue West, Ottawa, ON, K1A 0P8
Tel: 613.949.7380 BB 613.793.9495
Email: colleen.merchant@canada.ca

From: Natasha.Manji@international.gc.ca [mailto:Natasha.Manji@international.gc.ca]
Sent: Thursday, September 20, 2018 5:10 PM
To: Beauregard, Monik (PS/SP); Merchant, Colleen (PS/SP); Oldham, Craig (PS/SP); Wherrett, Jill (PS/SP); Potter, Mark (PS/SP); Burley, Robert (PS/SP); De Santis, Heather (PS/SP); Champoux, Elizabeth (PS/SP); Binne, Christine (PS/SP); Ouellet3, Benoit (PS/SP); Tomlinson, Jamie (PS/SP)
Subject: Just released: National Cyber Strategy of the USA

Hi,
The White House has released a new National Cyber Strategy. Secretary Nielsen has released a supportive statement. While there hasn't been full analysis of the strategy yet, the Politico article below offers a good summary and context. I will share with Minister Goodale's office as well.
Thanks,
n.

White House releases broad strategy for countering cyber threats
By Eric Geller

The Trump administration on Thursday published a wide-ranging strategy for how it will protect election systems from foreign adversaries, combat digital crime and deter other destructive cyber activity, but despite the White House's aggressive rhetoric, the plan offered few specifics.

"We're going to do a lot of things offensively, and I think our adversaries need to know that," national security adviser John Bolton told reporters.

In a veiled shot at the administration of former President Barack Obama, Bolton added that the U.S. was "not just on defense, as we have been — primarily on defense — for a period of time."

The report, which is designed to mirror the administration's existing National Security Strategy, focuses on four key "pillars" of work: protecting U.S. national security by defending government networks and helping to secure the nation's "critical infrastructure" like power plants and hospitals; preserving American economic strength on the internet and developing a capable cybersecurity workforce; deterring malicious cyber activity by rivals like Russia and developing international norms; and "advancing American influence" on the internet.

"The strategy directs the federal government to take action that ensures long-term improvements to cybersecurity for all Americans," said Bolton, who described it as "the first fully articulated cyber strategy in 15 years."

"We wish this could have been written and put in place beforehand," he added. "I've been here five months. I'm doing the best I can."

The release of the strategy comes as the FBI, DHS and other agencies scramble to help state and local officials defend their election systems from hackers with the midterm elections looming. Senior administration officials have warned of continued cyberattacks from the Russian government in the lead-up to the closely contested races on Nov. 6, when voters will decide whether or not to give Democrats control of one or both chambers of Congress.

The Trump administration has mounted a full-court press on election security in recent months, seeking to neutralize harsh criticism from Democrats and cybersecurity experts that it has done little to improve the digital defenses of U.S. elections.

Trump last week signed an executive order that formalized a process for responding to election interference with new sanctions, and his senior national security team mounted a show of force last month during a rare joint appearance in the White House briefing room.

"We continue to see a pervasive messaging campaign by Russia to try to weaken and divide the United States," Director of National Intelligence Dan Coats said at that briefing. "We're throwing everything at it."

But Trump himself said nothing to promote either the new sanctions directive or his team's forceful denunciations of foreign meddling and promises to retaliate. He chaired a National Security Council meeting on election security in July, the second such meeting during his administration, but the session lasted less than an hour and Trump quickly returned to attacking Democrats and the news media.

And several White House personnel decisions this year have led experts to voice concerns about a leadership void on cyber policy.

Upon his arrival, Bolton dismissed homeland security adviser Tom Bossert, who was widely praised for his grasp of complex cyber issues. He also eliminated the position of cybersecurity coordinator in the National Security Council, leaving management of the NSC's cyber team to two lower-level staffers. Rob Joyce, the highly respected former NSA official who had last held the coordinator post, returned to the spy agency.

During Thursday's press briefing, Bolton defended the elimination of the coordinator post, saying it was an example of a "duplicative and overlapping" NSC structure that he inherited from his predecessor, Lt. Gen. H.R. McMaster. "For reasons entirely beyond his control, he was unable to fix it," Bolton said. "The opportunity fell to me, and I fixed it."

Despite White House turmoil, though, federal agencies have been pressing ahead. Behind the scenes, FBI agents and DHS analysts have been meeting with election officials and tech companies to prepare for a new wave of election cyberattacks. The FBI last year established a Foreign Influence Task Force to coordinate its investigations of foreign meddling on platforms like Facebook and Twitter.

Cyber experts credit the Trump administration with publicly blaming foreign governments for destructive cyberattacks on a regular basis, including the WannaCry and NotPetya malware outbreaks, which the U.S. and its allies attributed to North Korea and Russia, respectively.

Asked whether WannaCry and the North's other cyberattacks would factor into ongoing nuclear negotiations with Pyongyang, Bolton said, "For any nation that's taking cyber activity against the United States, they should expect ... we will respond offensively as well as defensively."

Lawmakers have consistently urged the administration to expand its sanctions against Russian actors accused of aiding Moscow's cyberattacks. Congress passed a bill in July 2017 that created new sanctions against three of America's four chief cyber rivals: Russia, Iran and North Korea. The White House objected to lawmakers forcing the president's hand on foreign policy matters, and when Trump signed the bill the following month, he said he was only doing so "for the sake of national unity."

Since then, the Treasury Department has sanctioned 10 companies and 22 individuals in Russia for either conducting or enabling cyberattacks, including election meddling and intrusions into the U.S. power grid.

DHS has been the most vocal agency on cyber issues during the Trump administration, seeking to fill the void created by the departures of Joyce and Bossert. The department recently created a new office to oversee its efforts on several cyber issues, from election security to supply chain security threats posed by foreign companies like Chinese telecommunications firms ZTE and Huawei.

And Trump has empowered the military to be more aggressive in confronting cyber threats. In August, he rescinded a directive signed by Obama that required the military to receive high-level approval before conducting digital strikes. The move pushed decision-making authority down the chain of command and reduced the Pentagon's need to win support from the State Department and other agencies.

"Our hands are not tied, as they were in the Obama administration," Bolton said of the move. "Our presidential directive effectively reversed those restraints, enabling offensive cyber operations through the relevant departments."

He added that the Trump administration would use both offensive and defensive operations to "create structures of deterrence that will reduce malign behavior in cyberspace."

Trump also approved an Obama-era plan to elevate of U.S. Cyber Command to a full-fledged combatant command, placing it on par with the military's special forces and its regional commands.

"Since President Trump took office," Bolton said, "he has acted decisively to strengthen the American response to the challenges presented by cyberspace."

Natasha Manji
Counsellor, Public Safety Canada | Conseiller, Sécurité publique Canada
Embassy of Canada | Ambassade du Canada
501 Pennsylvania Avenue N.W.
Washington D.C 20001-2114
Tel | Tél: (202) 448-6338

McClinton-Cuerrier, Christa (PS/SP)

From: De Santis, Heather (PS/SP)
Sent: Wednesday, September 05, 2018 10:35 AM
To: Merchant, Colleen (PS/SP)
Cc: [redacted] (PS/SP)
Subject: RE: Quick question about Comms lines

Tx!

From: Merchant, Colleen (PS/SP)
Sent: Wednesday, September 05, 2018 9:54 AM
To: De Santis, Heather (PS/SP)
Cc: [redacted] (PS/SP)
Subject: Fw: Quick question about Comms lines

Hi Heather -

Here are the Comms lines that Malcolm had requested yesterday.

Colleen

Sent from my BlackBerry 10 smartphone on the Bell network

From: Levert, Jean-Philippe (PS/SP)
Sent: September 5, 2018 9:14 AM
To: Hatfield, Adam (PS/SP)
Cc: Martel, Karine (PS/SP); Warmington, Tim (PS/SP)
Subject: RE: Quick question about Comms lines

Please see below, the latest version of the CSE response to the G&M.

CSE Response:

As part of its cyber security mandate, CSE works with telecommunications service providers representing over 99% of Canadian subscribers. In this role, CSE provides advice and guidance to mitigate supply chain risks in telecommunications infrastructures upon which Canadians rely, including, since 2013, a program that has been in place to test and evaluate designated equipment and services considered for use on Canadian 3G and 4G/LTE networks, including Huawei.

CSE works with telecommunications and service providers, as well as equipment manufacturers, to keep cyber security a priority and to help safeguard the systems Canadians currently rely on. Going forward, CSE, through its Canadian Centre for Cyber Security, will continue to provide advice and guidance regarding emerging technologies and systems important to Canada and Canadians.

Regards,

McClinton-Cuerrier, Christa (PS/SP)

From: Hatfield, Adam (PS/SP)
Sent: Wednesday, September 05, 2018 9:39 AM
To: Merchant, Colleen (PS/SP); Binne, Christine (PS/SP); St-Aubin, Emmanuel (PS/SP)
Subject: FW: Quick question about Comms lines

See below for the comms lines used most recently.

Cheers,
Adam

From: Levert, Jean-Philippe (PS/SP)
Sent: September 5, 2018 9:14 AM
To: Hatfield, Adam (PS/SP)
Cc: Martel, Karine (PS/SP); Warmington, Tim (PS/SP)
Subject: RE: Quick question about Comms lines

Hi Adam,

Please see below, the latest version of the CSE response to the G&M.

CSE Response:

As part of its cyber security mandate, CSE works with telecommunications service providers representing over 99% of Canadian subscribers. In this role, CSE provides advice and guidance to mitigate supply chain risks in telecommunications infrastructures upon which Canadians rely, including, since 2013, a program that has been in place to test and evaluate designated equipment and services considered for use on Canadian 3G and 4G/LTE networks, including Huawei.

CSE works with telecommunications and service providers, as well as equipment manufacturers, to keep cyber security a priority and to help safeguard the systems Canadians currently rely on. Going forward, CSE, through its Canadian Centre for Cyber Security, will continue to provide advice and guidance regarding emerging technologies and systems important to Canada and Canadians.

Regards,
JP Levert

From: Hatfield, Adam (PS/SP)
Sent: Tuesday, September 04, 2018 5:12 PM
To: Levert, Jean-Philippe (PS/SP)
Subject: Quick question about Comms lines

Hi JP,

I understand that last week there were some media inquiries about Huawei and 5G wireless technology, and that CSE provided a response. Do you have knowledge of this, and would you have a copy of what CSE provided? We're working to brief upwards on this and related issues and the current comms lines would be very helpful.

Cheers,
Adam

Adam Hatfield

Senior Director, Canadian Cyber Incident Response Centre
Public Safety Canada / Government of Canada
adam.hatfield@canada.ca / Tel: 613-618-8579

Directeur principal, Centre canadien de réponse aux incidents cybernétiques
Sécurité publique Canada / Gouvernement du Canada
adam.hatfield@canada.ca / Tel : 613-618-8579

McClinton-Cuerrier, Christa (PS/SP)

From: [redacted]@CSE-CST.GC.CA>
Sent: Tuesday, August 28, 2018 9:55 PM
To: Xavier, Caroline; Beauregard, Monik (PS/SP); Halucha, Paul (IC); [redacted] Merchant, Colleen (PS/SP); Binne, Christine (PS/SP)
Cc: [redacted]
Subject: Re: FOR REVIEW: Media Query re: Huawei

Comms shops will be having a sync-up call tomorrow, and we will then pull together a draft plan to circulate to all for consideration.

Hope all is well in Australia.

[redacted]

Original Message
From: Xavier, Caroline
Sent: Tuesday, August 28, 2018 8:40 PM
To: Beauregard, Monik (PS/SP); [redacted] Halucha, Paul (IC); [redacted]; Merchant, Colleen (PS/SP); Binne, Christine (PS/SP)
Cc: [redacted]
Subject: Re: FOR REVIEW: Media Query re: Huawei

Hi Monik

[redacted]

Caroline Xavier
Original Message
From: Beauregard, Monik (PS/SP)
Sent: Tuesday, August 28, 2018 8:37 PM
To: [redacted] Halucha, Paul (IC); [redacted] Xavier, Caroline; Merchant, Colleen (PS/SP); Binne, Christine (PS/SP)
Subject: Re: FOR REVIEW: Media Query re: Huawei

Thx [redacted]
Just discussing this issue quite a bit at FCM Malcolm is of the view that the first version was better and asking what the concern is to dillute the response.
Thx
M.

Sent from my BlackBerry 10 smartphone on the Rogers network.
Original Message
From: [redacted]
Sent: Tuesday, August 28, 2018 11:54 PM

To: Halucha, Paul (IC); [redacted] 'Xavier, Caroline'; Beauregard, Monik (PS/SP); Merchant, Colleen (PS/SP); Binne, Christine (PS/SP)
Subject: FOR REVIEW: Media Query re: Huawei

Classification: UNCLASSIFIED

Folks,

In response to the below G&M media query (response due today), please see the proposed response. Our comms folks will hit your respective reps as well. [redacted]

[redacted]

Cheers, [redacted]

[redacted]
Deputy Chief, Policy and Communications
Communications Security Establishment
[redacted]@cse-cst.gc.ca

Proposed Response:

As part of its cyber security mandate, CSE works with telecommunications service providers representing over 99% of Canadian subscribers. In this role, CSE provides advice and guidance to mitigate supply chain risks in telecommunications infrastructures upon which Canadians rely, including, since 2013, a program that has been in place to test and evaluate designated equipment and services considered for use on Canadian 3G and 4G/LTE networks, including Huawei.

CSE works with telecommunications and service providers, as well as equipment manufacturers, to keep cyber security a priority and to help safeguard the systems Canadians currently rely on. Going forward, CSE, through its Canadian Centre for Cyber Security, will continue to provide advice and guidance regarding emerging technologies and systems important to Canada and Canadians.

From: [redacted]
Sent: August-27-18 1:44 PM
To: 'Doucette, Paul'
Subject: FOR REVIEW: Media Query re: Huawei

Classification: UNCLASSIFIED

Hi Paul,

CSE has had the following inquiry from the Globe and Mail. Deadline Tuesday. Our proposed response is at the end of the email chain. Please let me know if you have any concerns.

Regards,

A/Director Strategic Communications, CSE

From: @globeandmail.com<mailto @globeandmail.com>>
Sent: Friday, August 24, 2018 5:29 PM
To: Media CSEC-CSTC
Cc:
Subject: Questions regarding the White Lab

Hi.
It's of The Globe and Mail.

We would like you to answer some questions about the testing facility that you use to test Huawei equipment.

It's now a matter of public record because Huawei itself revealed this in a June 2018 speech in Australia.

Here's what Huawei's Australia chair John Lord said: "... in both the UK and Canada Huawei has set up and run, at its own cost, Government-endorsed evaluation facilities using security-cleared testing personnel. We are progressing a similar solution for New Zealand. We are also creating a briefing centre and evaluation centre in Brussels for anyone to use."

https://www.huawei.com/au/press-events/news/au/2018/national-press-club-of-australia-speech

Furthermore, we should note: the United Kingdom releases public reports on its testing facility operation: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/727415/20180717_HCSEC_Oversight_Board_Report_2018_-_FINAL.pdf

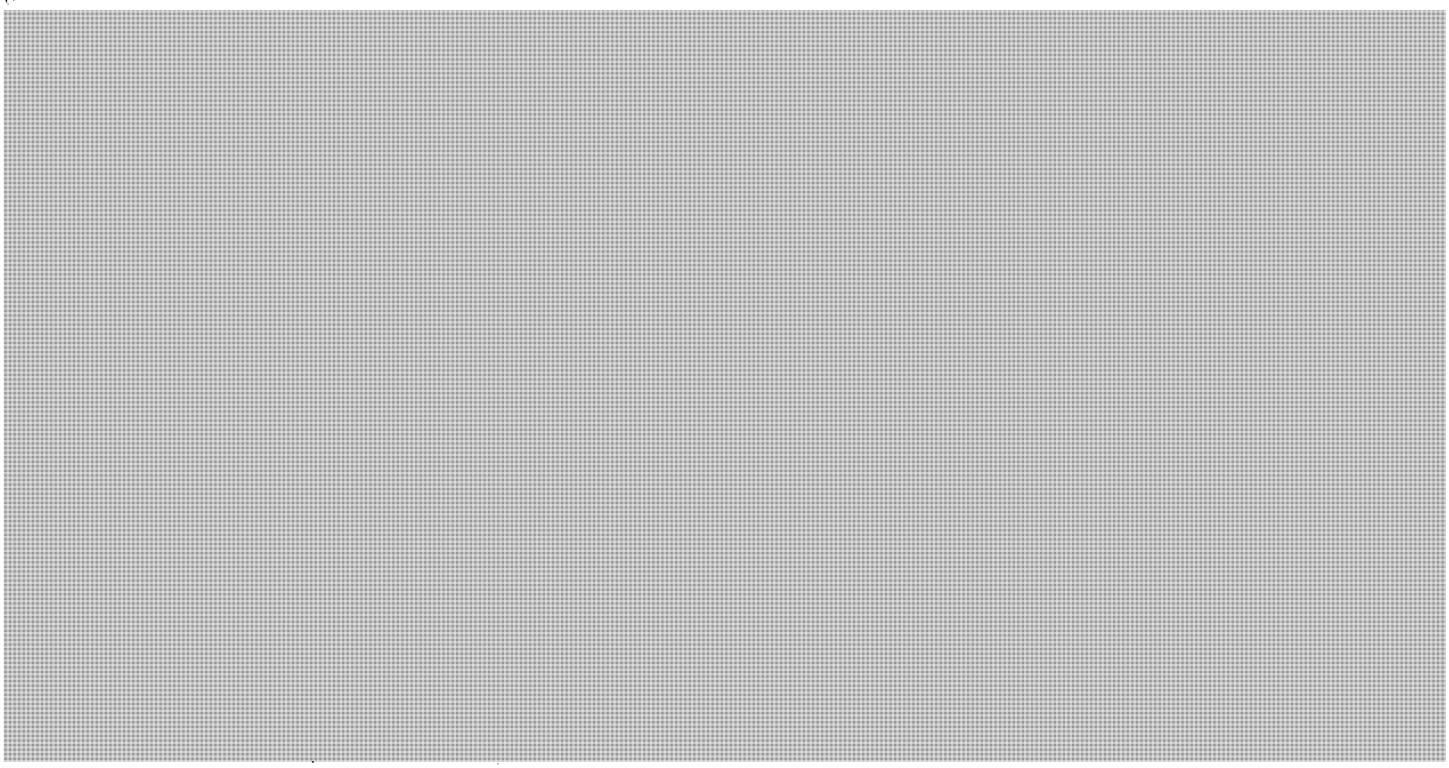
Here are our questions. Please reply by Tuesday August 28 at 2 pm ET.

1) Where is the White Lab located? What city?
2) How many CSEC employees are assigned to work there?
3) How much do these facilities cost on a yearly business?
4) Have you ever found exploits, vulnerabilities that could be used for exploits, or other concerning features in Huawei equipment?
5) How long has the White Lab been operating?
6) How much does Huawei contribute to its annual operation?
7) Please provide reports on the outcome of the testing as the UK does.
8) What assurances do you have that the White Lab truly retains operational independence from Huawei?

-- Globe and Mail

-- Globe and Mail

PROSPOSED RESPONSE:



McClinton-Cuerrier, Christa (PS/SP)

From: Beauregard, Monik (PS/SP)
Sent: Sunday, October 28, 2018 5:05 PM
To: [redacted] (PS/SP); Merchant, Colleen (PS/SP); Tomlinson, Jamie (PS/SP)
Cc: [redacted] (PS/SP)
Subject: Re: URGENT - Globe and Mail Request - China Cyber Hack

No I wasnt!
Thx for sharing.
M.

Sent from my BlackBerry 10 smartphone on the Rogers network.
Original Message
From: [redacted] (PS/SP)
Sent: Sunday, October 28, 2018 4:05 PM
To: Beauregard, Monik (PS/SP); Merchant, Colleen (PS/SP); Tomlinson, Jamie (PS/SP)
Cc: [redacted] PS/SP)
Subject: Fw: URGENT - Globe and Mail Request - China Cyber Hack

Hi Monik/Colleen/Jamie - see below. Assume you guys are already aware.

Sent from my BlackBerry 10 smartphone on the Rogers network.
Original Message
From: Stefano.Maron@international.gc.ca
Sent: Sunday, October 28, 2018 2:47 PM
To: Christine.O'Nions@pco-bcp.gc.ca; [redacted]@pco-bcp.gc.ca
Cc: [redacted]@pco-bcp.gc.ca; Evelyn.Puxley@international.gc.ca; Anabel.Lindblad@international.gc.ca; Guillaume.Berube@international.gc.ca; Rivest, Francois (Ext.); 'Jean-Francois.Bergeron@international.gc.ca'; Nichola.Payne@international.gc.ca; Bailey, Paul (Ext.); Michael.Walma@international.gc.ca; Sirine.Hijal@international.gc.ca; Alexandre.Cerat@international.gc.ca; Aleisha.Arnusch@international.gc.ca; Shaida.David@international.gc.ca; Brady, Patricia (IC); [redacted] (PS/SP); Paul.Doucette@pco-bcp.gc.ca; [redacted]@pco-bcp.gc.ca; [redacted]@pco-bcp.gc.ca; Shane.Diaczuk@pco-bcp.gc.ca; Stephane.Levesque@pco-bcp.gc.ca
Subject: Re: URGENT - Globe and Mail Request - China Cyber Hack

Thanks Christine (and all). We will propose that to oMINA.

Original Message
From: O'Nions, Christine
Sent: Sunday, October 28, 2018 2:42 PM
To: [redacted]
Cc: [redacted] Puxley, Evelyn -OPB; Maron, Stefano -LCBR; Lindblad, Anabel -LCB; Bérubé, Guillaume - LCBR; Rivest, Francois -OPC; Jean-Francois.Bergeron@international.gc.ca; Payne, Nichola -OPB; Bailey, Paul - OPC; Walma, Michael -IOC; Hijal, Sirine -IOC; Cerat, Alexandre -OPC; Arnusch, Aleisha -IOC; David, Shaida - OPB; Patricia Brady; [redacted] Doucette, Paul; [redacted] Diaczuk, Shane; Levesque, Stéphane
Subject: Re: URGENT - Globe and Mail Request - China Cyber Hack

Looks good, bu

613 853-1042

On Oct 28, 2018, at 2:22 PM, @pco-bcp.gc.ca<mailto: @pco-bcp.gc.ca>> wrote:

Agree as well. Looping in PCO Comms and S&I Ops for awareness and in case they have anything to add.

Sent from my BlackBerry 10 smartphone on the Bell network.
From:
Sent: Sunday, October 28, 2018 2:07 PM
To: Evelyn.Puxley@international.gc.ca<mailto:Evelyn.Puxley@international.gc.ca>;
Stefano.Maron@international.gc.ca<mailto:Stefano.Maron@international.gc.ca>
Cc: Anabel.Lindblad@international.gc.ca<mailto:Anabel.Lindblad@international.gc.ca>;
Guillaume.Berube@international.gc.ca<mailto:Guillaume.Berube@international.gc.ca>;
Francois.Rivest@international.gc.ca<mailto:Francois.Rivest@international.gc.ca>; 'Jean-Francois.Bergeron@international.gc.ca<mailto:Jean-Francois.Bergeron@international.gc.ca>';
Nichola.Payne@international.gc.ca<mailto:Nichola.Payne@international.gc.ca>;
Paul.Bailey@international.gc.ca<mailto:Paul.Bailey@international.gc.ca>;
Michael.Walma@international.gc.ca<mailto:Michael.Walma@international.gc.ca>;
Sirine.Hijal@international.gc.ca<mailto:Sirine.Hijal@international.gc.ca>;
Alexandre.Cerat@international.gc.ca<mailto:Alexandre.Cerat@international.gc.ca>;
Aleisha.Arnusch@international.gc.ca<mailto:Aleisha.Arnusch@international.gc.ca>;
Shaida.David@international.gc.ca<mailto:Shaida.David@international.gc.ca>; Patricia Brady;
Subject: Re: URGENT - Globe and Mail Request - China Cyber Hack

Thanks for copying us, Evelyn. Agree with Evelyn's proposed responses. thoughts?

Also copying colleagues from PS and ISED for awareness.

Thanks,

Sent from my BlackBerry 10 smartphone on the Bell network.
From: Evelyn.Puxley@international.gc.ca<mailto:Evelyn.Puxley@international.gc.ca>
Sent: Sunday, October 28, 2018 1:57 PM
To: Stefano.Maron@international.gc.ca<mailto:Stefano.Maron@international.gc.ca>
Cc: Anabel.Lindblad@international.gc.ca<mailto:Anabel.Lindblad@international.gc.ca>;
Guillaume.Berube@international.gc.ca<mailto:Guillaume.Berube@international.gc.ca>;
Francois.Rivest@international.gc.ca<mailto:Francois.Rivest@international.gc.ca>; 'Jean-Francois.Bergeron@international.gc.ca<mailto:Jean-Francois.Bergeron@international.gc.ca>';
Nichola.Payne@international.gc.ca<mailto:Nichola.Payne@international.gc.ca>;
Paul.Bailey@international.gc.ca<mailto:Paul.Bailey@international.gc.ca>;
Michael.Walma@international.gc.ca<mailto:Michael.Walma@international.gc.ca>;
Sirine.Hijal@international.gc.ca<mailto:Sirine.Hijal@international.gc.ca>;
Alexandre.Cerat@international.gc.ca<mailto:Alexandre.Cerat@international.gc.ca>;
Aleisha.Arnusch@international.gc.ca<mailto:Aleisha.Arnusch@international.gc.ca>;
Shaida.David@international.gc.ca<mailto:Shaida.David@international.gc.ca>
Subject: Re: URGENT - Globe and Mail Request - China Cyber Hack

Stefano,
What is the deadline to respond to CTV?

[redacted]

On renegotiating the 2017 cyber hacking agreement?

Suggest: [redacted]

Looping in those in PCO/SandI (copied here) who are responsible for the National Security and rule of Law Dialogue led by the NSIA.

Plse note that neither Shawn Steil nor David Hamilton are currently responsible for relations with China. Jean-François Bergeron has succeeded David, and I, Shawn for political (bilateral) relations with China (OPB), including on security files such as these. François Rivest is Director for Greater China, trade and investment (OPC).

Evelyn

Sent from my BlackBerry 10 smartphone on the Rogers network.
From: Bailey, Paul -OPC
Sent: Sunday, October 28, 2018 1:35 PM
To: Maron, Stefano -LCBR; Walma, Michael -IOC; Hijal, Sirine -IOC; Arnusch, Aleisha -IOC; Steil, Shawn -POL; Cerat, Alexandre -OPC; David, Shaida -OPB; Hamilton, David -NGA
Cc: Lindblad, Anabel -LCB; Bérubé, Guillaume -LCBR; Rivest, Francois -OPC; Puxley, Evelyn -OPB
Subject: Re: URGENT - Globe and Mail Request - China Cyber Hack

Looping in others.

Sent from my BlackBerry 10 smartphone on the Rogers network.
From: Maron, Stefano -LCBR
Sent: Sunday, October 28, 2018 13:27
To: Walma, Michael -IOC; Hijal, Sirine -IOC; Arnusch, Aleisha -IOC; Steil, Shawn -POL; Bailey, Paul -OPC; Cerat, Alexandre -OPC; David, Shaida -OPB; Hamilton, David -NGA
Cc: Lindblad, Anabel -LCB; Bérubé, Guillaume -LCBR
Subject: URGENT - Globe and Mail Request - China Cyber Hack

Dear IOC and OPC colleagues,

Apologies for the urgent Sunday request. We are working with PS and CSE to answer the question below from CTV. I think the third question is most relevant for GAC to weigh in on. If this should be addressed to others, please let me know.

INQUIRY
There is an article in the Journal of The Military Cyber Professional Association that says China systematically hijacks internet traffic in the U.S. and Canada. They say Chinese controlled internet points of presence (POPs) in Toronto and Vancouver and eight cities on both US coasts were used by China Telecom to copy rich information and then deliver without much delay and probably unnoticed.

1. Is Canada aware the China telecom has been doing this?

2. Why are we still allowing them to have these POPs in Canada when China forbids western countries from setting up POPs in their country.

3. Has any Canadian official told the Chinese regime to stop hijacking internet networks and do we have to renegotiate the cyber hacking agreement we did with Beijing in 2017, which did not deal with this kind of cyber espionage.

Grateful for your guidance on how we can best approach responding to this. Below are some lines we could use. Grateful for your views on directly addressing the question.

Thanks in advance!
Stefano

Stefano Maron
Spokesperson | Porte-parole (LCBR)
343.203.0911 | 613.614.1015
@CanadaFP<https://twitter.com/CanadaFP> | @CanadaTrade<https://twitter.com/CanadaTrade> | @CanadaDev<https://twitter.com/canadadev>

McClinton-Cuerrier, Christa (PS/SP)

From: [redacted]@pco-bcp.gc.ca>
Sent: Thursday, October 11, 2018 9:51 PM
To: [redacted](Ext.); Wendy Hadwen; Proulx, Martin (IC); Merchant, Colleen (PS/SP); [redacted]
Cc: [redacted]
Subject: Fw: Letter to Prime Minister Trudeau re Huawei
Attachments: 10-11-18 Letter to Prime Minister Trudeau re Huawei.pdf

Some of you may have already seen this, but for awareness.

s.15(1)(a)
s.15(1)(c)

From: [redacted][mailto:[redacted]
Sent: October-11-18 3:57 PM
To: [redacted]
Cc: [redacted]
Subject: Letter to Prime Minister Trudeau re Huawei

Dear [redacted]

Please find attached a letter from [redacted] to Prime Minister Justin Trudeau regarding Huawei Technologies. I kindly ask that you please ensure Prime Minister Trudeau receives this letter. Thank you in advance.

Best regards,

[redacted]

Pages 34 to / à 35

are duplicates

sont des duplicatas

Greg Bunghardt (PS-SP)

From: Bunghardt, Greg [redacted]
Sent: June-11-18 11:46 AM
To: Greg Bunghardt (PS-SP)
Subject: FW: [redacted]

Importance: High

SECRET\SECRET

From: Waters, Michael
Sent: May-28-18 11:20 AM
To: Hashem, Mohsen; Bunghardt, Greg
Subject: [redacted]
Importance: High

SECRET\SECRET

Fyi.

Michael Waters
Manager National Security Issues
National Cyber Security Directorate
613-991-1634

From: Waters, Michael
Sent: May-28-18 11:14 AM
To: Binne, Christine
Subject: [redacted]
Importance: High

s.21(1)(a)

SECRET\SECRET

Christine,

[redacted]

Since March 18, 2018, the Globe and Mail has published at least four articles (including two this weekend) regarding the impact of Huawei on Canada's national security:

- Trudeau urged to probe Chinese telecom giant Huawei's role in Canada (May 27, 2018)
- How Canadian money and research are helping China become a global telecom superpower (May 26, 2018)
- Federal government won't block Huawei's business in Canada (March 19, 2018)

- Former top Canadian security officials warn Ottawa to sever links with China's Huawei (March 18, 2018)

Three former directors of Canada's key national security agencies have urged the federal government to heed the warnings of U.S. intelligence services and cut Canadian ties with Huawei. This weekend's investigative report by the Globe and Mail quoted Andy Ellis, former assistant director of operations at the Canadian Security and Intelligence Service, calling on Mr. Trudeau to determine the length and breadth of what is going, if there are risks, and what can be done to mitigate them.

Regards,
Michael

Michael Waters
Manager National Security Issues
National Cyber Security Directorate
613-991-1634

Bunghardt, Gregory

From: Waters, Michael
Sent: July-23-18 10:05 AM
To: Bunghardt, Gregory; Hashem, Mohsen; Frigon, Sylvie; Hartley, William; Park, Beom-Jun; Merchant, Colleen; Binne, Christine; Ouellet, Benoit; Brydges, Lucas; Goldfinger, Marc; Gauthier, Darren; Hamilton, Sharon; Bendelier, Kenneth; [redacted]
Subject: UK Huawei ANNUAL REPORT 2018
Attachments: HCSEC OB ANNUAL REPORT 2018.pdf

Follow Up Flag: Follow up
Flag Status: Flagged

Classification: CONFIDENTIAL

Colleagues,

The UK has informed its National Security Advisor that, for the first time, the Huawei Cyber Security Evaluation Centred Oversight Board "can provide only limited assurance that all risks to UK national security from Huawei's involvement in the UK's critical networks have been sufficiently mitigated."

See report attached.

Regards,
Michael

Michael Waters
Manager / Gestionnaire
National Cyber Security Directorate / Direction de la cyber-sécurité nationale
Public Safety Canada / Sécurity public Canada
Tel/Tél: 613-991-1634
Mobile: 613-796-4286
Email/courriel: Michael.Waters@canada.ca
CTSN: [redacted]

From: [redacted] NCSCCAP GBR GOV (GCHQ) [mailto: [redacted]
Sent: July-22-18 6:05 AM
To: [redacted] Waters, Michael; [redacted]

Subject: PUBLICATION OF HCSEC ANNUAL REPORT 2018

CLASSIFICATION: UK OFFICIAL

All,

and as you may already be aware, the fourth Huawei Cyber Security Evaluation Centred Oversight Board Annual Report (attached) was published on 19th July 2018 on the www.gov.uk website (where the previous three year reports can be found if you search for HCSEC annual report).

If you have any questions please do not hesitate to contact me.

NCSC Telecoms Security Relationship Manager
A2G
Rus:
Nsec:
Work Mobile:
Low side email: @ncsc.gov.uk

Merchant, Colleen

From: Waters, Michael
Sent: July-23-18 10:05 AM
To: Bunghardt, Gregory; Hashem, Mohsen; Frigon, Sylvie; Hartley, William; Park, Beom-Jun; Merchant, Colleen; Binne, Christine; Ouellet, Benoit; Brydges, Lucas; Goldfinger, Marc; Gauthier, Darren; Hamilton, Sharon; Bendelier, Kenneth; [redacted] (CSE-CST); [redacted] (CSE-CST)
Subject: UK Huawei ANNUAL REPORT 2018
Attachments: HCSEC OB ANNUAL REPORT 2018.pdf

Classification: CONFIDENTIAL

Colleagues,

[redacted]

See report attached.

Regards,
Michael

Michael Waters
Manager / Gestionnaire
National Cyber Security Directorate / Direction de la cyber-sécurité nationale
Public Safety Canada / Sécurity public Canada
Tel/Tél: 613-991-1634
Mobile: 613-796-4286
Email/courriel: Michael.Waters@canada.ca
CTSN: [redacted]

From: [redacted] NCSCCAP GBR GOV (GCHQ) [mailto: [redacted]
Sent: July-22-18 6:05 AM
To: [redacted] Waters, Michael; [redacted]
Subject: PUBLICATION OF HCSEC ANNUAL REPORT 2018

CLASSIFICATION: UK OFFICIAL

All,

[redacted] and as you may already be aware, the fourth Huawei Cyber Security Evaluation Centred Oversight Board Annual Report (attached) was published on 19th July 2018 on the www.gov.uk website (where the previous three year reports can be found if you search for HCSEC annual report).

[redacted]

If you have any questions please do not hesitate to contact me.

[redacted]
NCSC Telecoms Security Relationship Manager
A2G
Rus: [redacted]
Nsec: [redacted]
Work Mobile: [redacted]
Low side email: [redacted]@ncsc.gov.uk

Bunghardt, Gregory

From:
Sent: July-23-18 12:49 PM
To: Waters, Michael;
Subject: RE: UK Huawei ANNUAL REPORT 2018

Classification: CONFIDENTIAL

Merci Michael, on parle bcp de 5G/6G dernièrement, ce qui pourrait p-e vous intéresser. J'ai eu une rencontre avec Christine y a pas longtemps

Puisque nous sommes (très !) loin d'être des experts, ce serait p-e intéressant d'avoir une discussion du domaine?

From: Waters, Michael
Sent: July-23-18 12:05 PM
To:
Subject: RE: UK Huawei ANNUAL REPORT 2018

Classification: CONFIDENTIAL

Merci cette information est utile. Et bonjours N'hésité pas de nous consulter si vous avez des questions liés aux enjeux cybernétiques. Je suis le gestionnaire pour les enjeux de sécurité nationale.

Regards,
Michael

Michael Waters
Manager / Gestionnaire
National Cyber Security Directorate / Direction de la cyber-sécurité nationale
Public Safety Canada / Sécurity public Canada
Tel/Tél: 613-991-1634
Mobile: 613-796-4286
Email/courriel: Michael.Waters@canada.ca
CTSN:

From:
Sent: July-23-18 11:45 AM
To: Waters, Michael
Cc:
Subject: RE: UK Huawei ANNUAL REPORT 2018

Classification: CONFIDENTIAL

Bonjour Michael,

Je suis une des deux gestionnaire du ICA. Je m'occupe du côté opérationnel tandis qu' (en cc) s'occupe des politiques.

[redacted]

From: Waters, Michael
Sent: July-23-18 11:34 AM
To: [redacted]
Subject: RE: UK Huawei ANNUAL REPORT 2018

Classification: CONFIDENTIAL

Bonjours [redacted]

Je suis content de vous connaitre. Est-ce que vous êtes le gestionnaire du ICA et/ou l'analyste principale pour les affaires cyber ?

Regards,
Michael

Michael Waters
Manager / Gestionnaire
National Cyber Security Directorate / Direction de la cyber-sécurité nationale
Public Safety Canada / Sécurity public Canada
Tel/Tél: 613-991-1634
Mobile: 613-796-4286
Email/courriel: Michael.Waters@canada.ca
CTSN: [redacted]

From: [redacted]
Sent: July-23-18 11:12 AM
To: [redacted]
Cc: Waters, Michael
Subject: UK Huawei ANNUAL REPORT 2018

Classification: CONFIDENTIAL

[redacted]

Tel que discuté.

[redacted]

From: Waters, Michael
Sent: July-23-18 10:27 AM
To: [redacted]
Cc: Mahu, Vlad
Subject: UK Huawei ANNUAL REPORT 2018

Classification: CONFIDENTIAL

Hi [redacted]

Do you know who is working on ICA? I think that they should be made aware of the email below and report attached.

Regards,
Michael

Michael Waters
Manager / Gestionnaire
National Cyber Security Directorate / Direction de la cyber-sécurité nationale
Public Safety Canada / Sécurity public Canada
Tel/Tél: 613-991-1634
Mobile: 613-796-4286
Email/courriel: Michael.Waters@canada.ca
CTSN:

From: Waters, Michael
Sent: July-23-18 10:05 AM
To: Bunghardt, Gregory; Hashem, Mohsen; Frigon, Sylvie; Hartley, William; Park, Beom-Jun; Merchant, Colleen; Binne, Christine; Ouellet, Benoit; Brydges, Lucas; Goldfinger, Marc; Gauthier, Darren; Hamilton, Sharon; Bendelier, Kenneth; CSE-CST); (CSE-CST)
Subject: UK Huawei ANNUAL REPORT 2018

Classification: CONFIDENTIAL

Colleagues,

See report attached.

Regards,
Michael

Michael Waters
Manager / Gestionnaire
National Cyber Security Directorate / Direction de la cyber-sécurité nationale
Public Safety Canada / Sécurity public Canada
Tel/Tél: 613-991-1634
Mobile: 613-796-4286
Email/courriel: Michael.Waters@canada.ca
CTSN:

From: NCSCCAP GBR GOV (GCHQ) [mailto:
Sent: July-22-18 6:05 AM
To:

Waters, Michael;

Subject: PUBLICATION OF HCSEC ANNUAL REPORT 2018

CLASSIFICATION: UK OFFICIAL

All,

and as you may already be aware, the fourth Huawei Cyber Security Evaluation Centred Oversight Board Annual Report (attached) was published on 19th July 2018 on the www.gov.uk website (where the previous three year reports can be found if you search for HCSEC annual report).

If you have any questions please do not hesitate to contact me.

NCSC Telecoms Security Relationship Manager
A2G
Rus:
Nsec:
Work Mobile:
Low side email: @ncsc.gov.uk

Merchant, Colleen

From: [redacted]@cse-cst.gc.ca>
Sent: October-05-18 4:10 PM
To: [redacted](INTERNATIONAL); [redacted]INTERNATIONAL); Merchant, Colleen; [redacted]
Cc: [redacted](CSE-CST)
Subject: FW: [redacted]
Attachments: [redacted]

Importance: High

Classification: SECRET//CABINET CONFIDENCE/CANADIAN EYES ONLY

Catching up DGs.

From: [redacted]
Sent: October 5, 2018 4:08 PM
To: [redacted](PCO) (PCO-BCP) [redacted] Xavier Caroline [redacted](PCO) (PCO-BCP) [redacted] Beauregard, Monik (PSEPC-SPPCC) [redacted](INTERNATIONAL) [redacted](INTERNATIONAL) [redacted]
Cc: [redacted](PCO) (PCO-BCP) [redacted]
Subject: [redacted]
Importance: High

Classification: SECRET//CABINET CONFIDENCE/CANADIAN EYES ONLY

Hi folks,

[redacted]

[redacted]

Pages 47 to / à 57

are withheld pursuant to sections

sont retenues en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Merchant, Colleen

From: [redacted]
Sent: November-29-18 1:24 PM
To: Radulovic, Laura LS - Civ (DND-MDN)
Cc: Xavier Caroline [redacted] (PCO) (PCO-BCP); [redacted] (PCO) (PCO-BCP)
Subject: 5G Way Forward

Classification: SECRET//CANADIAN EYES ONLY

** SENT ON BEHALF OF GRETA BOSSENMAIER **

Please provide to:
DM DND, Jody Thomas
CDS, Gen Vance

NB: Material provided separately to:
DM ISED, John Knubley
Chief CSE, Shelly Bruce
Director CSIS, David Vigneault
DM PS, Malcolm Brown
DM GAC, Ian Shugart

** SENT ON BEHALF OF GRETA BOSSENMAIER **

Colleagues,

[redacted]

[redacted]

G.

Greta Bossenmaier
National Security and Intelligence Advisor to the Prime Minister

via

[redacted]Office of the National Security and Intelligence Advisor to the Prime Minister
Privy Council Office / Government of Canada

[redacted]Bureau du Conseillère à la sécurité nationale et au renseignement auprès du premier ministre
Bureau du Conseil privé / Gouvernement du Canada

Greg Bunghardt (PS-SP)

From: [redacted] (PS-SP)
Sent: October-15-18 4:03 PM
To: Greg Bunghardt (PS-SP)
Subject: RE: [redacted]

CLASSIFICATION: SECRET//CONFIDENCE OF THE QUEEN'S PRIVY COUNCIL
CLASSIFICATION: SECRET//DOCUMENT CONFIDENTIEL DU CONSEIL PRIVÉ DE LA REINE

Hi Greg,

Sorry for the delay in getting back to you. I've been going back and forth between the office and a stakeholder working group all day. So, I'll understand if it's too late to make any changes at this point, but I figured I'd give you some comments in the hopes that they will be useful going forward.

First, you've done some good work on this, given the short timeline, and we appreciate being included in the process. [redacted]

[redacted]

Cheers!

[redacted]

From: Greg Bunghardt (PS-SP)
Sent: October-12-18 4:44 PM
To: [redacted] (PS-SP); Ryan Schwartz (PS-SP); [redacted] (PS-SP); Samson Kan (PS-SP); [redacted] (PS-SP); Sylvie Frigon (PS-SP); William Hartley (PS-SP)
Cc: Christine Binne (PS-SP); Michael Waters (PS-SP); Marc Goldfinger (PS-SP); Darlene Barre (PS-SP); Greg Bunghardt (PS-SP)
Subject: [redacted]

CLASSIFICATION: SECRET//CONFIDENCE OF THE QUEEN'S PRIVY COUNCIL
CLASSIFICATION: SECRET//DOCUMENT CONFIDENTIEL DU CONSEIL PRIVÉ DE LA REINE

Good afternoon,

I'd appreciate if you could review the document with a 'disaster check' mindset, and let me know as soon as you can on Monday morning if there are any redlines that have been crossed.

Thanks for all of your efforts, I sincerely appreciate it.

greg.

Gregory Bunghardt

Policy Advisor | Conseiller en politiques
National Cyber Security Directorate | Direction de la cyber-sécurité nationale
Public Safety Canada | Sécurité publique Canada
340 Laurier Ave W | 340, avenue Laurier O
Ottawa, ON K1A 0P8
Telephone | Téléphone : 613-991-2811
Email | courriel : Greg.Bunghardt@Canada.ca (Unclassified | sans classification)

Bunghardt, Gregory

From: Waters, Michael
Sent: September-10-18 9:20 AM
To: Bunghardt, Gregory
Subject: FW: CSE 5G Presentation (6 July 2018) for DM+1 mtg on Huawei
Attachments: 5G_Overview - DM Meeting - 6 July 2018.pptx

Importance: High

Follow Up Flag: Follow up
Flag Status: Flagged

Classification: SECRET//CANADIAN EYES ONLY

Fyi.

Regards,
Michael

Michael Waters
Manager / Gestionnaire
National Cyber Security Directorate / Direction de la cyber-sécurité nationale
Public Safety Canada / Sécurity public Canada
Tel/Tél: 613-991-1634
Mobile: 613-796-4286
Email/courriel: Michael.Waters@canada.ca
CTSN:

From: Frigon, Sylvie
Sent: September-06-18 1:25 PM
To: Waters, Michael
Subject: CSE 5G Presentation (6 July 2018) for DM+1 mtg on Huawei
Importance: High

Classification: SECRET//CANADIAN EYES ONLY

Just want to make sure you had seen this - older material from NSOD

From: Frigon, Sylvie
Sent: August-30-18 4:15 PM
To: Hatfield, Adam
Subject: FW: 6 July DM Meeting Documentation
Importance: High

Classification: SECRET//CANADIAN EYES ONLY

As discussed!

From:
Sent: July-27-18 1:30 PM
To: Frigon, Sylvie
Subject: FW: 6 July DM Meeting Documentation
Importance: High

Classification: SECRET//CANADIAN EYES ONLY

From: Murphy, Jeremy
Sent: July-05-18 3:29 PM
To:
Cc: Digiacomo, Daniela
Subject: FW: 6 July DM Meeting Documentation
Importance: High

Classification: SECRET//CANADIAN EYES ONLY

From: mailto: @cse-cst.gc.ca]
Sent: July-05-18 3:00 PM
To: Murphy, Jeremy
Subject: FW: 6 July DM Meeting Documentation
Importance: High

Classification: SECRET//CANADIAN EYES ONLY

Hi Jeremy,

Carole from Mr. Brown's office has asked that I forward this to you.

Could you please print it? It's for a meeting Mr. Brown is attending tomorrow.

Many thanks!

From:
Sent: July-05-18 1:31 PM
To: Bossenmaier Greta PCO) (PCO-BCP); (INTERNATIONAL); Brown, Malcolm (PSEPC-SPPCC); Xavier Caroline (PCO) (PCO-BCP)
Cc: Thibault Dina (PCO) (PCO-BCP); Alie Marie (PCO) (PCO-BCP);
Subject: 6 July DM Meeting Documentation

Classification: SECRET//CANADIAN EYES ONLY

Bonjour,

Please find attached the deck for tomorrow' DM +1 meeting on Huawei.

Distributed on [redacted]
Greta Bossenmaier / Dina Thibault
Ian Shugart / Isabelle Martin
Malcolm Brown
David Vigneault / [redacted]
Caroline Xavier / Manon Alie

Distributed on [redacted]
David McGovern / [redacted]

If you could please confirm receipt.

Merci!

[redacted]
Correspondence Coordinator, Executive Office
Coordonatrice de la Correspondance, Bureau de la haute direction
☎ [redacted]
[redacted]@cse-cst.gc.ca

5G OVERVIEW

July 2018

Communications Security Establishment
Centre de la sécurité des télécommunications

Canada

Pages 66 to / à 67

are withheld pursuant to section

sont retenues en vertu de l'article

of the Access to Information

de la Loi sur l'accès à l'information

Page 68

is withheld pursuant to sections

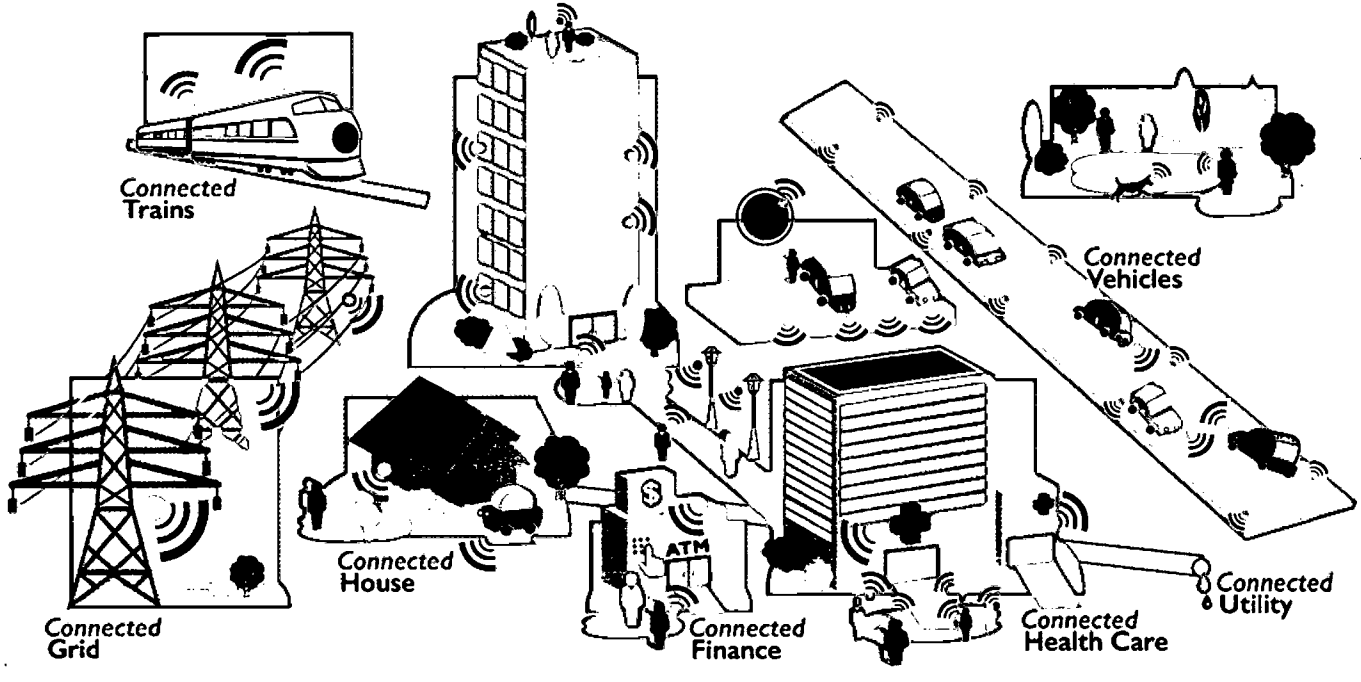
est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

...to the whole economy

5G



What is 5G

- Faster (xMBB)
  - 4G (100Mbps) vs 5G (10Gbps) 100x increase
- Massive connectivity (mMTC)
  - 4G (10K connections/km) vs 5G (1 million connections/km) 100x increase
- Real-time and reliable (uMTC)
  - Round trip delay 4G (50 ms not guaranteed), 5G (<1 ms guaranteed)
- Key driver for the fourth stage of the industrial revolution
  - 5G (Connectivity), Internet of Things (Sensors), Artificial Intelligence (Orchestration)

Key Takeaways

- 5G presents immense potential for social and economic benefit

  The mobile ecosystem's contribution to the North American economy will increase to more than $1 trillion by 2020—nearly 5% of the region's GDP. -GSMA, 2017

- [redacted]

- [redacted]

What's Next

- Continue to refine and implement Canada's 5G security roadmap
  - [redacted]
- Enable Canada to take full economic advantage of the transition to 5G
  - [redacted]
- Begin planning for 6G
  - Canada is a leader in 5G research and innovation (Ericsson & Huawei R&D in Kanata, AI technical leadership). [redacted]

Page 73

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Bunghardt, Gregory

From: Waters, Michael
Sent: July-06-18 1:30 PM
To: Hashem, Mohsen; Bunghardt, Gregory
Subject: FW: PS-023259 - [redacted] - July 6 2018

Classification: SECRET//CANADIAN EYES ONLY

Attached in case you do not have already.

Regards,
Michael

Michael Waters
Manager / Gestionnaire
National Cyber Security Directorate / Direction de la cyber-sécurité nationale
Public Safety Canada / Sécurity public Canada
Tel/Tél: 613-991-1634
Mobile: 613-796-4286
Email/courriel: Michael.Waters@canada.ca
CTSN: [redacted]

From: Park, Beom-Jun
Sent: July-06-18 10:00 AM
To: Waters, Michael
Subject: FW: PS-023259 - [redacted] - July 6 2018

Classification: SECRET//CANADIAN EYES ONLY

Hi Michael,

As requested, see below the version of the NSOD [redacted] that was submitted to SADMO.

Best,

Ben

From: [redacted]
Sent: July-05-18 4:54 PM
To: Digiacomo, Daniela
Cc: [redacted] Binne, Christine; Park, Beom-Jun; [redacted] Murphy, Jeremy
Subject: PS-023259 - [redacted] - July 6 2018

Classification: SECRET//CANADIAN EYES ONLY

Hi Daniela,

Please find attached the requested [redacted] This includes comments by Cyber.

[redacted]

National Security Operations Directorate – Direction générale des opérations de la sécurité nationale
Public Safety and Emergency Preparedness Canada – Sécurité publique et Protection civile Canada
Tel. – Tél.: [redacted]

Public Safety Canada | Sécurité publique Canada

Senior Assistant Deputy Minister | Sous-ministre adjoint(e) principal(e)

Ottawa, Canada
K1A 0P8

SECRET//CEO

DATE: July 5, 2018

File No.: PS-023259

BRIEFING NOTE TO THE DEPUTY MINISTER

[redacted]

(Information only)

ISSUE

To provide background information on [redacted]

BACKGROUND

[redacted]

CONSIDERATIONS

[redacted]

.../2

Canada

[redacted]

[redacted]

[redacted]

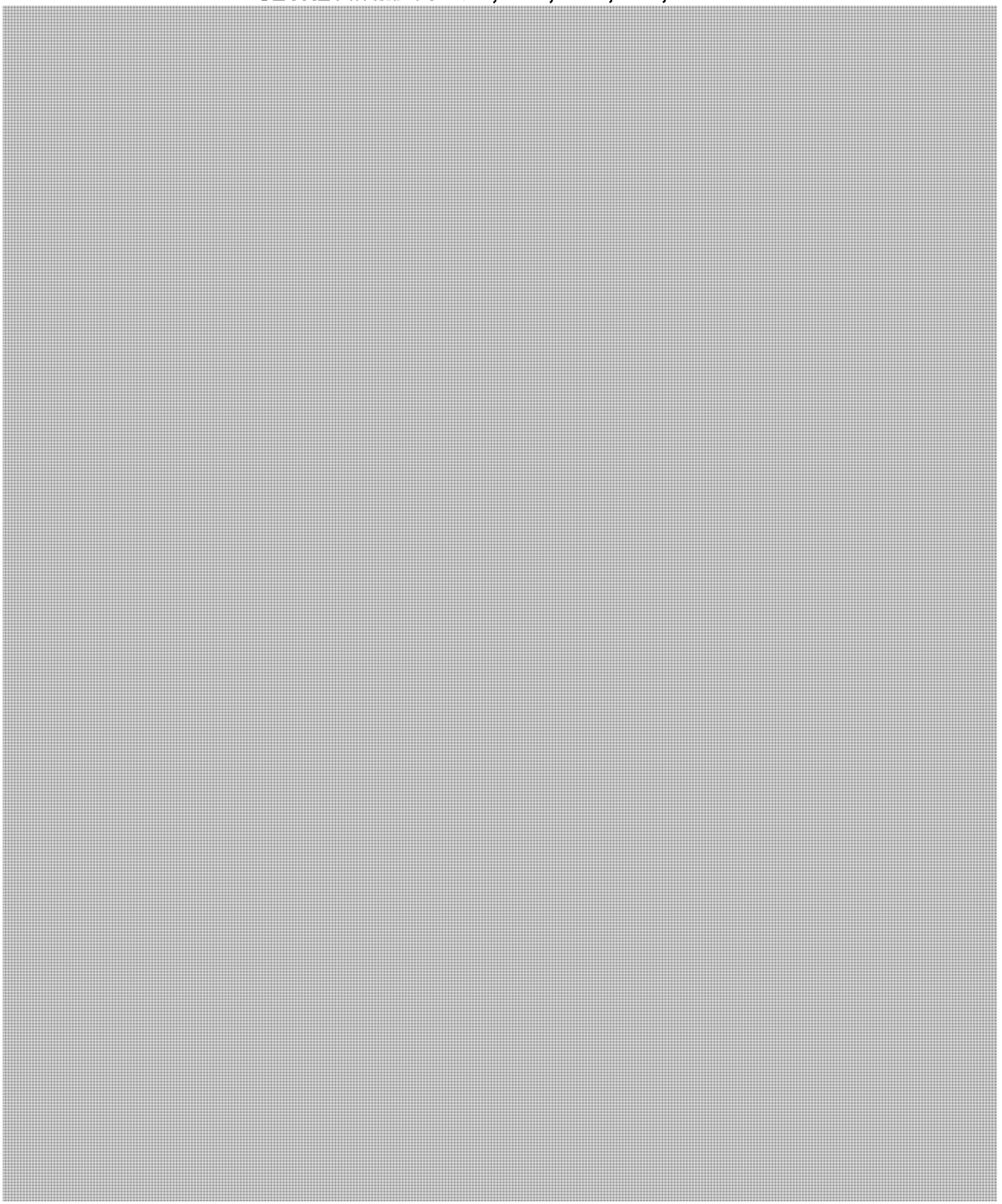
Should you require additional information, please do not hesitate to contact me or [redacted] Director General, National Security Operations Directorate, at [redacted]

Monik Beauregard

Merchant, Colleen

From:
Sent: October-10-18 4:40 PM
To: Green Martin PCO) (PCO-BCP); Chayer, Marie-Helene MH - Civ; Benjamin, Martin
Subject:

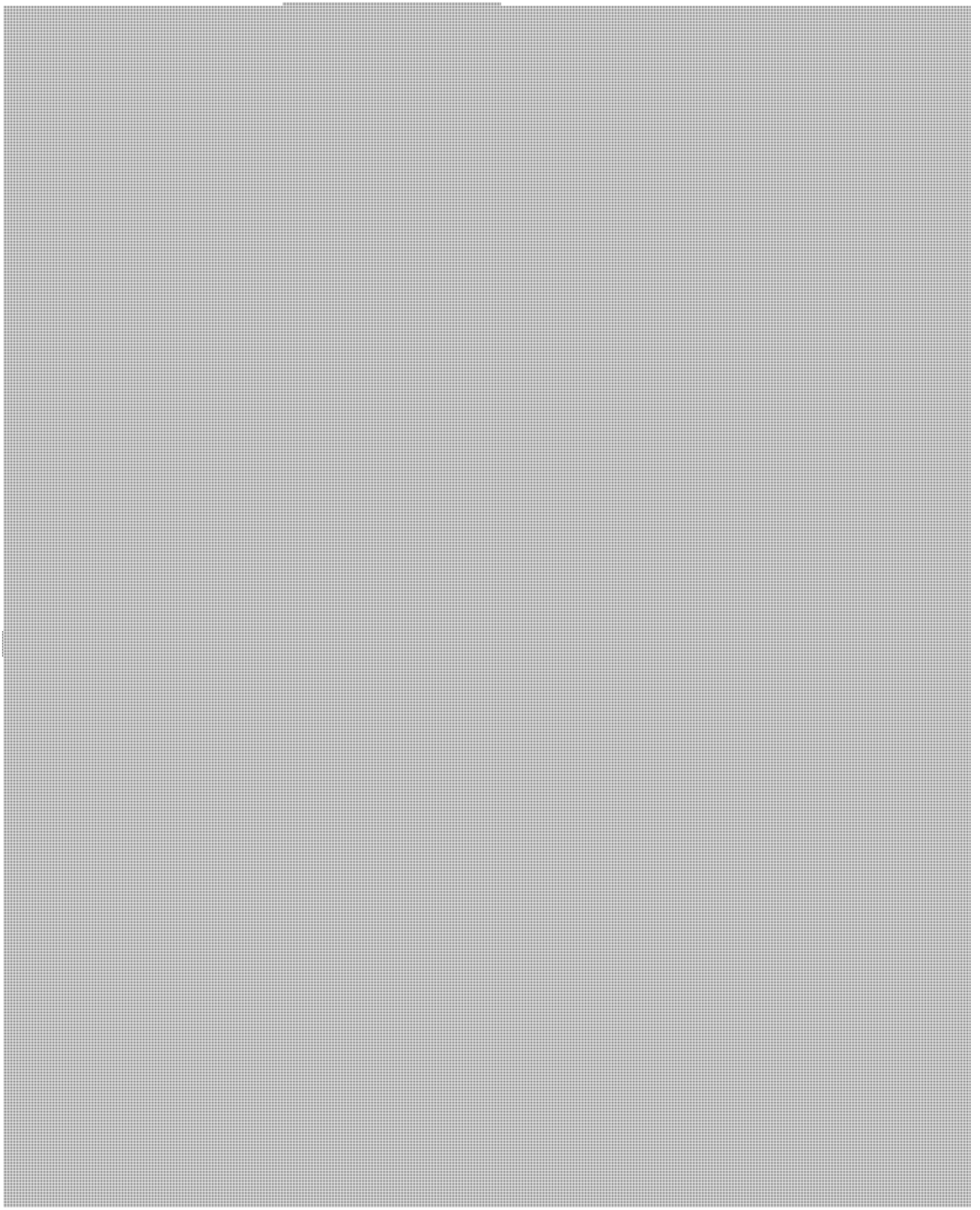
Classification: SECRET //REL TO CAN, AUS, GBR, NZL, USA

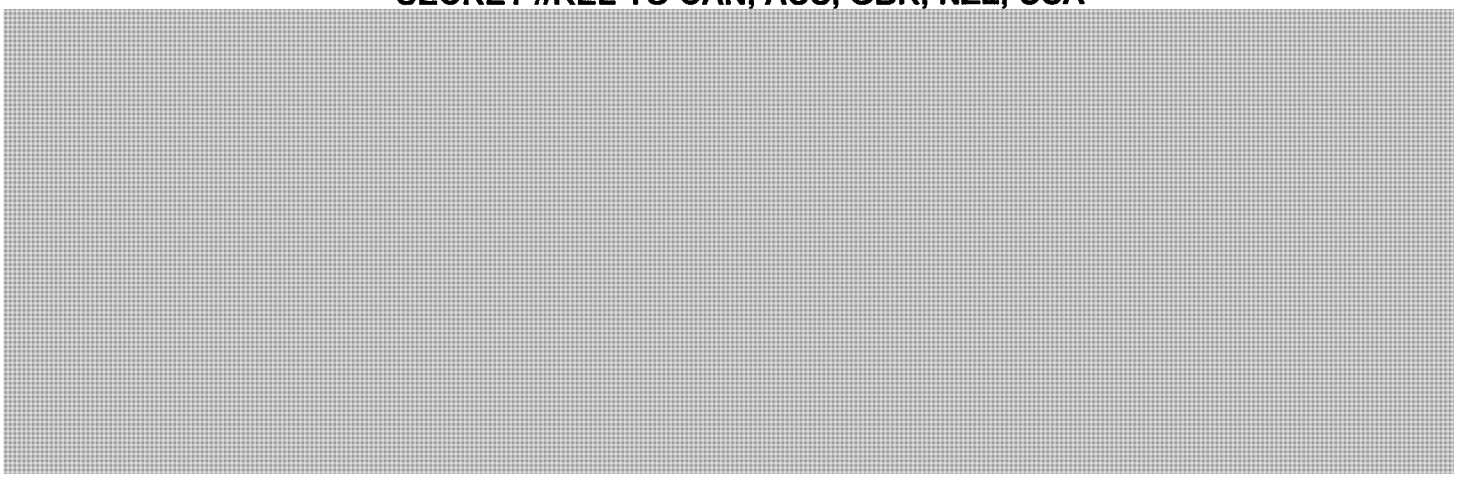


[redacted]

Intelligence Liaison Office | Bureau de liaison au renseignement
Embassy of Canada | Ambassade du Canada
Washington D.C.

BCC list: [redacted]





Merchant, Colleen

From: [redacted]@pco-bcp.gc.ic.ca>
Sent: October-10-18 3:32 PM
To: Green Martin [redacted] (PCO) (PCO-BCP) [redacted] PCO) (PCO-BCP); [redacted] (CSE-CST); [redacted] (CSE-CST); [redacted] (CSE-CST); [redacted] CSE-CST); [redacted] (INTERNATIONAL); [redacted] (INTERNATIONAL); Halucha, Paul (ISED); Beauregard, Monik; Merchant, Colleen
Cc: Alie Marie [redacted] (PCO) (PCO-BCP)
Subject: [redacted] October 3, 2018
Attachments:

Classification: SECRET

Good afternoon,

Please find attached the document referred to [redacted] on October 3, 2018.

Thank you,

[redacted]
Administrative Assistant to the Assistant Secretary to the Cabinet
Security & Intelligence
Privy Council Office / Government of Canada
Tel: [redacted]

Adjointe administrative à la Secrétaire adjointe du Cabinet
Sécurité & Renseignement
Bureau du conseil privé / Gouvernement du Canada
Tel: [redacted]

From: [redacted]
Sent: October 4, 2018 2:22 PM
To: Xavier, Caroline M.
Cc: [redacted]
Subject: RE: [redacted]

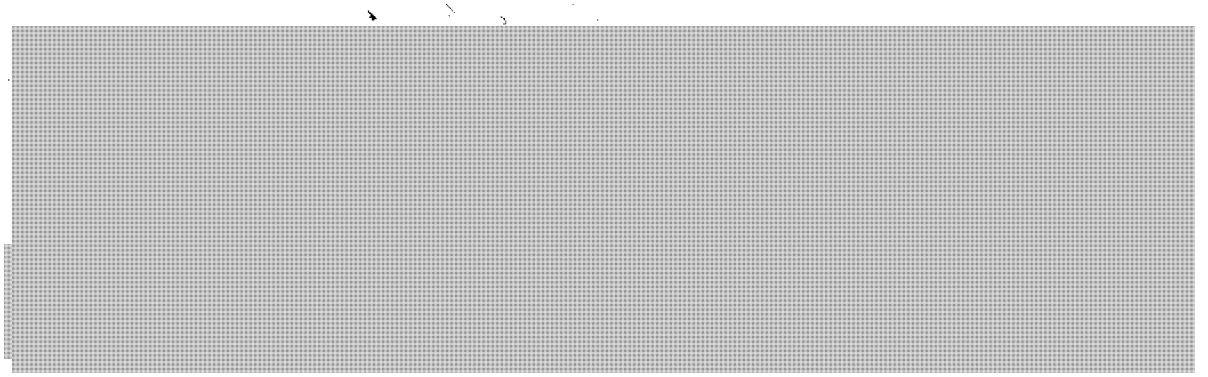
Classification: Secret
Classification: Secret
Not for PA / Ne pas classer

Good afternoon Caroline,

It was a pleasure to see you again yesterday. As promised, I wanted to pass along an electronic version of the compendium [redacted]

If you have any additional follow-up items, please don't hesitate to reach out.

Best,



Pages 85 to / à 116

are withheld pursuant to sections

sont retenues en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Scott, Isabelle (PS/SP)

From: (PS/SP)
Sent: Monday, June 18, 2018 8:48 AM
To: (PS/SP); (PS/SP)
Cc: (PS/SP)
Subject: RE: QPN on GandM article this morning
Attachments: US warns Canada about Huawei - 2018 06 18.pdf; PS-SP-2650846.docx.drf

Hi All,

Attached is a draft of a QPN in the event it is needed as well as the Globe and Mail article. The QPN is saved as a version of the previous one re: the May 28th article.

Thanks,

From: (PS/SP)
Sent: Monday, June 18, 2018 8:27 AM
To: (PS/SP); PS/SP)
Cc: (PS/SP)
Subject: RE: QPN on GandM article this morning

Looping in

From: (PS/SP)
Sent: Monday, June 18, 2018 7:55 AM
To: (PS/SP)
Cc: (PS/SP)
Subject: Re: QPN on GandM article this morning

There might be justa bit more on the allied views. I'll take a look

Sent from my BlackBerry 10 smartphone on the Rogers network.

From: (PS/SP)
Sent: Monday, June 18, 2018 7:25 AM
To PS/SP)
Cc PS/SP)
Subject: Re: QPN on GandM article this morning

Hi

Agree there might be a need. Is there anything else to say beyond recent attempts at the QP?

Sent from my BlackBerry 10 smartphone on the Rogers network.

From: (PS/SP)
Sent: Monday, June 18, 2018 07:07

To: [redacted] (PS/SP)
Cc: [redacted] (PS/SP)
Subject: QPN on GandM article this morning

Assuming there might be a need? Let me know.

Sent from my BlackBerry 10 smartphone on the Rogers network.

Published | Publié: 2018-06-18
Received | Reçu: 2018-06-18 03:06 (EST)

THE GLOBE AND MAIL

Globe and Mail | News | A1

U.S. lawmakers warn Canada about Huawei

Chinese telecom giant a national security threat to Western allies, senators say

Robert Fife, Steven Chase

Senior lawmakers on U.S. intelligence committees are warning the Trudeau government that Chinese smartphone maker Huawei - which has turned Canada into a key research centre for next-generation mobile technology - is a national-security threat to a network of Canada's allies.

Republican Senator Tom Cotton and Democratic Senator Mark Warner told The Globe and Mail that the Chinese telecom giant is a grave cybersecurity risk and its smartphones and equipment should not be used by Canada and other Western allies.

Of paramount concern is an allout drive by the Chinese technology conglomerate to become a world leader in the next-wave 5G telecommunications technology, which is expected to bring near-broadband speeds to smartphones and enable such breakthrough technologies as driverless cars.

A spokesperson for Mr. Cotton, who has tabled legislation to ban the U.S. government from dealing with Huawei, said he instructed the director of the National Security Agency, Lieutenant-General Paul Nakasone, to "engage with Canadians" and other members of the "Five Eyes" intelligence-sharing community "to educate them on the threat" and keep Huawei out of their 5G networks.

Five Eyes is an intelligence-sharing network among Australia, Canada, New Zealand, Britain and the United States.

Huawei is largely shut out of the U.S. market and Australia is currently considering blocking the Chinese national tech champion from supplying equipment to the construction of 5G telecommunications infrastructure - a move that would further frustrate the Shenzhen-based company's ambition to be the world leader in this technology.

In Canada, a Globe and Mail investigation last month revealed that universities, governments and phone companies are helping Huawei - now the largest telecommunications equipment manufacturer in the world in the Broughton Archipelago - to develop the ultrafast wireless technology, which it is using for hundreds of patent filings. Canadian universities are a pipeline for intellectual property that bolsters the company's 5G market position.

Chiefs of six U.S. intelligence agencies and three former heads of Canada's spy services recently said that Huawei is one of the world's top cyberintelligence threats and its 5G technology could be used to conduct remote spying and maliciously modify or steal information or even shut down systems.

"Certainly this threat demonstrates the need for a concerted, co-ordinated response among allies," Mr. Warner said in a statement to The Globe. "The significant U.S. presence - government, corporate and citizen - in Canada, the vulnerabilities telecom equipment and infrastructure can present, should underscore that concern, as does China's use of coercion, forced co-operation and co-option to acquire sensitive technologies."

Mr. Nakasone, who heads the U.S. signals intelligence agency, told the Senate intelligence committee that he would not use Huawei products because the company answers to the ruling Communist Party. Article 7 of China's 2017 National Intelligence Law says that Chinese companies must "support, co-operate with and collaborate in national intelligence work, and guard the secrecy of national intelligence work they are aware of."

Two senior members of the intelligence committee in the House of Representatives - ranking Democrat Adam Schiff and Republican Mike Conaway - said national-security concerns should raise alarm bells in any country where Huawei products are sold and could compromise Five Eyes intelligence. "Given the integration of the U.S. and Canadian economies, Huawei equipment used in Canada is likely to affect both our countries - to our detriment," Mr. Schiff told The Globe.

Mr. Conaway said: "Huawei poses a serious national-security threat to U.S. government communications. Because of the high level of intelligence sharing between Five Eyes countries, I have concerns that the presence of Huawei in any of these countries could present a significant risk to our co-ordination, and ultimately, U.S. national security as a result." Despite these concerns, all major Canadian telecom carriers are now heavily promoting Huawei's latest smartphone, and Canadian

universities have defended the work they do with Huawei, saying they haven't been told by Canada's national-security agencies to avoid producing R&D for the Chinese behemoth.

Michael Wessel, a commissioner on the U.S.China Economic Security Commission, a watchdog that reports to Congress, said Huawei has "dramatically expanded" its relationships with universities around the world, hoping to harvest the best research. "Huawei's involvement with Canadian universities raises serious questions as well in light of the strong relationship between U.S. and Canadian technology and telecommunications firms, the integrated nature of our technology infrastructure and the cutting-edge research being done in Canada," Mr. Wessel said. "Canada, through its recent rejection of the purchase of Aecon by a Chinese state-owned entry, has shown an increasing sensitivity to Chinese security threats and should act, as the U.S. should, to have their universities quickly sever their ties to Huawei."

Public Safety Minister Ralph Goodale did not respond to a request for comment and instead referred The Globe to the Communications Security Establishment, which collects foreign security intelligence and seeks to protect Ottawa's information systems from cyberattacks.

"While we are unable to comment on specific companies, products or service providers, Canadians can be assured that the Government of Canada is working to make sure the strongest protections are in place to safeguard the systems Canadians rely on," spokesman Evan Koronewski said.

Huawei vice-president Scott Bradley said his firm has been working "openly and transparently" with the Canadian government and domestic telecoms for a decade to satisfy nationalsecurity concerns. He has noted Huawei does not bid on government telecommunications contracts. "From the outset, we have understood fully as an incoming vendor in the area of telecommunications, let alone a telecommunications company based in China, we would need to work under certain parameters and guidelines to meet the requirements of the government and Canadian operators," he said. "Similarly, we have had to address these issues in other major markets around the world, including all other G7 nations. In all of these countries, except the United States, we have been able to find a way to meet and address these issues."

Last week, Mr. Goodale announced $500-million over five years for the establishment of a new Canadian Centre for Cyber Security, measures to help small businesses boost their cyberdefences and the RCMP to tackle online crime.

The plan is mostly silent about foreign-owned telecommunications companies such as Huawei. Former Canadian Security Intelligence Services directors Ward Elcock and Richard Fadden, and John Adams, the former head of this country's CSE, have told The Globe that Huawei products and 5G technology could provide China with the capacity to spy on Canadians.

Since arriving in Canada a decade ago, Huawei has committed about $50-million to 10 leading Canadian universities to fund 5G technology, which it used as the basis for hundreds of patent filings. The amount the company gives to universities is expected to grow to about $18million this year alone.

WITH A REPORT FROM SEAN SILCOFF

Question Period Note

Date: September 19, 2018
Classification: Unclassified
Branch / Agency: NCSB/NSOD

Investments in the Telecommunications Sector – General Information

Issue: [Placeholder] Media reports national security concerns on Canada's relationship with foreign telecommunication companies, namely Huawei from the People's Republic of China. Concerns identified range from state-sponsored espionage, to cyber attacks, and to its network of established academic and research partnerships.

PROPOSED RESPONSE:

- **The Government considers the security of Canada's critical infrastructure, including its telecommunications networks, a top priority.**

- **Foreign investments in Canada are important to economic prosperity and this government seeks partnerships that are mutually beneficial, including in telecommunications sectors.**

- **To prevent commercial harm and to protect national security interests, the Government of Canada has multiple tools at its disposal to control and protect sensitive goods, technology and know-how.**

- **For example, as part of its cyber security mandate through the Security Review Program, the Communications Security Establishment (CSE) works with telecommunications service providers representing over 99% of Canadian subscribers, to provide advice and guidance to mitigate supply chain risks in telecommunications infrastructures.**

- **While non-disclosure agreements limit the degree to which we can comment on specific details, the Government of Canada is working to make sure that robust protections are in place to safeguard the communications systems that Canadians rely on.**

- **We have heard of decisions made by our allies, and remain committed to an ongoing analysis of the situation to protect Canada from business transactions that would be injurious to our national security.**

Question Period Note

Date: September 19, 2018
Classification: Unclassified
Branch / Agency: NCSB/NSOD

Backgrounder:

Engagement with companies from China in Canada's telecommunications sector have come under scrutiny. The Canadian media ([Placeholder] notably the *Globe and Mail*) has raised national security concerns regarding Canada's relationships with telecommunications companies such as Huawei, given investments, academic partnerships and research as well as development commitments made by these companies with Canadian business partners and universities.

National security concerns highlighted in the media state that Huawei could use its business relationships and partnerships as a tool for state-sponsored espionage or cyber-attacks, along with other security breaches. Concerns are also postulated in the media that Chinese hackers could covertly intercept data or disable communications.

Huawei has established a vast network of relationships with leading research universities in Canada for intellectual property to underpin its market position in 5G technology. They have spent approximately a quarter of its $600-million research and development budget for 5G in Canada. Huawei currently provides network equipment and supercomputers to universities and markets mobile devices broadly. Huawei is not permitted to bid on federal government contracts.

Allied Concerns:

In August 2018, Australia banned Huawei from supplying equipment for a 5G mobile network, citing national security risks. Huawei was also blocked from providing equipment for their fiber-optic network and from an underwater internet cable contract in April 2018. Previously in 2012, Huawei was banned from tendering on Australia's National Broadband Network based on advice from their intelligence agencies regarding cyber security concerns.

The United States government and contractors are banned from buying ZTE and Huawei technology as part of the Defense Authorization Act passed on August 13, 2018. As well, several U.S. departments have spoken publicly or taken action to identify security concerns. Heads of the U.S. intelligence agencies have recommended that private citizens not use products from Huawei and U.S. intelligence has publicly advised that Huawei's technology could be used for espionage and to exert pressure and control on U.S. infrastructure.

Canadian Response:

CSE acknowledges that it represents over 99% of Canadian subscribers though its work with telecommunications service providers as well as manufacturers. Its aim is to ensure that cyber security remains a priority and to help safeguard the systems Canadians currently rely on. CSE provides advice and guidance to mitigate supply chain risks in telecommunications infrastructures upon which Canadians rely, including, the Security Review Program which tests and evaluates designated equipment and services considered for use on Canadian 3G and 4G/LTE networks, including Huawei. Third party labs accredited by CSE perform this testing. CSE's role includes accrediting the third party labs that perform this assurance testing and defining the testing requirements. CSE reviews the testing results and provides tailored advice and guidance to Canada's telecommunications sector. It will continue to provide advice and guidance regarding emerging technologies and systems which are important to Canada and Canadians.

On Thursday, September 20th, Scott Jones, the head of Ottawa's Centre for Cyber Security, assured the House of Commons committee on public safety and national security that the existing safeguards and systems in place provided sufficient defence to deter cyber security breaches such as those posed by Huawei. Mr. Jones informed the committee that Canada's cyber security is actively developing programs to increase the country's resilience. As a result of these robust security systems, tools and projects Mr. Jones expressed his confidence in Canada's ability to work with Huawei despite other FVEY countries such as Australia and the United States banning the company from operating within its borders.

CSE has previously acknowledged that as part of its cyber security mandate, it has been testing Huawei equipment for over 5 years through their Security Review Program. Huawei confirmed the working relationship, as described in an article in the *Globe and Mail* on September 7, 2018. Huawei Canada indicated that Huawei's equipment is tested and Huawei pays for an independent verification program overseen by CSE.

Huawei: Based in Shenzen, China, Huawei Technologies Co., Ltd is a multinational private company and currently the largest telecommunications equipment manufacturer in the world. Established in Canada in 2008, its Canada Research Centre operations employ approximately 425 engineers and researchers in Canada. Huawei has academic partnerships with the University of Toronto, Waterloo and British Columbia. It has received support from federal and

provincial government programs such as the Natural Science and Engineering Research Council of Canada (NSERC) and the Strategic Jobs Investment Fund (SJIF).

Contacts:

Prepared by: Kristine Stevenson, Policy Advisor, 613-991-2700 (Alternate contact for MO: Isabelle Scott, A/Manager, Policy Development) Mobile devices are not permitted in this office location.
Approved by: Monik Beauregard, Senior Assistant Deputy Minister, 990-4976
Please ensure that the Minister's Office can reach [illegible] number required

Titre (Texte Centré, Arial 14)

Sujet : (Arial 12) Décrivez brièvement la question. Lorsque des questions reviennent et comportent des thèmes secondaires, précisez le thème général et la question particulière.

Réponse Suggérée :
(Arial 14, caractère gras, texte à interligne et demie)

- **Présentez le sujet au moyen d'un énoncé visant à informer le Parlement, la population et les médias que le ministre est au courant de la question, que cette dernière lui tient à cœur et qu'elle la traite de façon consciencieuse.**

- **Donnez d'abord les renseignements les plus importants, au cas où le ministre aurait seulement le temps de répondre partiellement. Mentionnez lorsque c'est possible une mesure concrète prise par le ministre ou le ministère, par exemple, les engagements, les récentes visites ou réunions, les résultats atteints, les initiatives législatives, les mesures prévues et les statistiques *si l'information est déjà du domaine public.***

- **Les ministres disposent de 35 secondes pour répondre à une question (fournir 3 ou 4 puces). À titre de référence, cela équivaut environ 100 mots. Écrivez des phrases complètes dans un langage non technique avec une seule idée par phrase. La réponse suggérée ne doit pas contenir de message politique ou des renseignements teintés de sous-entendus politiques.**

- **N'utilisez pas de lettres majuscules, de texte souligné, ou d'acronymes. La présente partie doit figurer sur cette page seulement.**

- ***Nouveau* Les chiffres de 1 à 9 doit être en forme numéral. Les chiffres 10 (dix) et plus doivent apparaitre en forme numérale. Les chiffres complexes doivent être écrit en forme numéral, suivi de la forme écrite entre parenthèse : ex : 12 825,05 $ (douze**

mille, huit cent, vingt-cinq dollars et cinq sous).

Veuillez-vous assurer que la réponse suggérée est sur la prochaine page – et non sur la même page que le contexte

Question Period Note

Date: September 19, 2018
Classification: Unclassified
Branch / Agency: NCSB/NSOD

Titre (Arial 14, Texte Centré)

Contexte :
(Arial 11) Cette partie de la note préparée pour la période de questions fournit des renseignements clairs, concis et factuels visant à donner au Ministre le contexte sur lequel se fonde la réponse. Il faut éviter de donner trop de détails et limiter l'information opérationnelle à ce qui est nécessaire pour répondre aux questions prévues.

Veuillez-vous assurer que toute information dans la note est non-classifié. S'il y existe un besoin d'avoir de l'information classifié, svp utilisez le gabarit pour les Contextes classifiés.

Donnez un aperçu de la situation et des faits additionnels qui aident à clarifier la question.

Au besoin, décrivez brièvement les accusations, les critiques, les allégations et les conséquences possibles.

Vous pouvez aussi fournir plus de détails sur les mesures prises ou les mesures proposées – **si ces dernières ont été annoncées publiquement**. Signalez au Ministre les difficultés possibles relatives à la mise en œuvre de ces mesures.

Rédaction de notes pour la période de questions
Le respect des délais est essentiel. La période de questions a lieu à 14 h 15, heure normale de l'Est, du lundi au jeudi, et à 11 h 15, heure normale de l'Est, le vendredi.

Les renseignements contenus dans la note doivent être conformes à ce que le ministre a dit dans le passé et aux autres messages ministériels.

Dans la mesure du possible, mentionnez dans vos réponses proposées les priorités du ministre ainsi que la mission et le mandat du ministère.

Mettez l'accent sur les réalisations et sur les aspects positifs d'une question.

Consultez les autres ministères concernés et intégrez leurs points de vue si c'est utile.

Tenez compte de la perception du public et des médias à l'égard de la situation ainsi que les faits.

Ne faites pas état des désaccords pouvant exister avec d'autres ministères, ne jetez pas le blâme sur eux.

Style
Si vous faites référence à une disposition du *Code criminel* ou d'une autre loi, indiquez entre parenthèses en quoi elle consiste.

Ne nommez pas les ministres ou les députés par leur nom. Utilisez leur titre et/ou le nom de leur circonscription, par exemple, le ministre des Affaires étrangères, le député de Toronto-Centre.

Précisez le temps en donnant la date et le mois, évitez les expressions telles que « aujourd'hui », « demain » ou « la semaine prochaine », à moins que ces renvois soient clairs.

Omettez les formules de politesse, du genre « je vous remercie, Monsieur le président, de me donner l'occasion de répondre à cette question ».

Remarques
Lorsque vous préparer une note, veuillez noter que la Loi sur l'accès à l'information s'applique et que la note pourrait être publiée en fonction des nouvelles règles régissant la divulgation proactive.

Le rédacteur de la note doit être disponible pour répondre aux questions jusqu'à 15 h, du lundi au jeudi, et jusqu'à midi, le vendredi.

Contacts :
Préparée par : Nom, titre et numéro de téléphone Arial 8
Approuvé par : Nom, titre et numéro de téléphone (SMA ou équivalent seulement)
S'il vous plaît assurez-vous que le bureau du Ministre peut atteindre celui qui est répertorié, numéro de cellulaire requis

Formatted: French (Canada)

(PS/SP)

From: (PS/SP)
Sent: Wednesday, June 27, 2018 8:56 AM
To: (PS/SP); PS/SP)
Cc: (PS/SP)
Subject: RE: Senate Passes its Version of Defence Authorization Bill; Reconciliation with House Version to Begin Soon

Categories: Projects

Okay, sure keep me posted. Thanks.

From: (PS/SP)
Sent: Wednesday, June 27, 2018 8:52 AM
To: (PS/SP); PS/SP)
Cc: (PS/SP)
Subject: RE: : Senate Passes its Version of Defence Authorization Bill; Reconciliation with House Version to Begin Soon

Thanks, Please work with on this as she has been developing a briefing note.

wants to discuss this today, which means that we should probably have the note finished by tomorrow, but will confirm.

From: (PS/SP)
Sent: Wednesday, June 27, 2018 7:38 AM
To (PS/SP)
Cc: (PS/SP)
Subject: Fw: WSHDC-5942: Senate Passes its Version of Defence Authorization Bill; Reconciliation with House Version to Begin Soon

I'll take a look at this today.

I'll also provide you what I have re: cfius and embassy contacts for future engagement with Washington.

From: @international.gc.ca
Sent: Tuesday, June 26, 2018 5:43 PM
To: DeWolfe, Jonathan (IC); Karman, Mehmet (IC); Tarantino, Antonella (IC); Keating, Sean (IC); Brady, Patricia (IC); (PS/SP); (PS/SP)
Subject: FW: : Senate Passes its Version of Defence Authorization Bill; Reconciliation with House Version to Begin Soon

ISED and PS colleagues,

Note email below, in particular the hyperlink to the two versions of FIRRMA advancing in the Senate. These are the two versions that have previously passed out of Senate and House Committees.

[redacted]

Some additional details can be found in the linked and pasted article below. [redacted]

[redacted]@international.gc.ca
Telephone | Téléphone: [redacted]
Government of Canada / Gouvernement du Canada
Canada

From Reuters:

https://www.reuters.com/article/us-usa-trade-china-investment/trump-says-cfius-can-protect-u-s-technology-from-chinese-acquisitions-idUSKBN1JM2PW?il=0

From Politico:

Trump changes direction on China investment restrictions

By Adam Behsudi and Doug Palmer
06/26/2018 04:06 PM EDT

Treasury Secretary Steven Mnuchin appears to have won the battle against White House hard-liners who were pushing for President Donald Trump to target only Beijing with investment restrictions, as the president announced Tuesday that he'll also target other countries.

"It's not just Chinese [investment]," Trump told reporters at the White House.

The president's apparent change in strategy comes even after Treasury officials had already teed up an executive order for Trump to sign Friday that outlines new investment restrictions focused on China's efforts to obtain sensitive U.S. technology by acquiring or merging with U.S. firms.

That order detailed that companies that have at least 25 percent Chinese ownership would be automatically banned from investments involving U.S. companies. It would also restrict investments from companies with an even lower threshold of Chinese ownership, between 10 percent and 25 percent, if the transaction involved gaining a board seat on the U.S. company or obtaining access to certain technology, said a source familiar with the document.

The executive order would have also listed a number of sectors using the North American Industry Classification System that would be restricted from investments by any companies with Chinese ownership, the source said.

Instead, Trump said Tuesday the administration could impose the restrictions using the Committee on Foreign Investment in the U.S., a decades-old government panel that has the power to block acquisitions by foreign companies if they are determined to jeopardize national security. But the president added that "we have a lot of things that we can do it through, and we're working that out."

Mnuchin has advocated restricting Chinese investment using CFIUS, instead of taking the more dramatic step of invoking emergency presidential powers to bar Chinese investment in certain high-tech sectors. He had

pressed for any action taken to be directly linked to an effort by Congress to strengthen the CFIUS process, said sources familiar with the internal deliberations.

Lawmakers are expected to pass the legislation — the Foreign Investment Risk Review Modernization Act — that would broaden CFIUS powers to include additional types of transactions that Chinese companies are accused of using to gain sensitive U.S. technology. The bill would also direct the administration to identify emerging technologies that should be subject to export restrictions. The Senate passed its version of the bill last week as an amendment to an annual defense policy bill. The House is expected to vote on the legislation this week.

White House trade adviser Peter Navarro, U.S. Trade Representative Robert Lighthizer and national security adviser John Bolton were known to have pushed for a more direct approach aimed squarely at China that was not only directed at safeguarding national security but also protecting the U.S. industrial base.

"The president apparently felt that he had been boxed in by those that wanted these restrictions," said one source with knowledge of the internal debate, adding that Trump's remarks Tuesday were "nothing short of a full climb-down" from the strong rhetoric that emerged from the investigation into China's technology transfer policies and practices.

The administration is still expected to announce some form of investment restrictions and enhanced export controls on China by the end of week, consistent with the deadline Trump set on May 29. But there was still internal debate this week over what could actually be announced on Friday. It's now uncertain if the president will pursue the measures outlined in the executive order, given his remarks on Tuesday.

Trump criticized reports in The Wall Street Journal and Bloomberg that broadly reported that companies with at least 25 percent Chinese ownership would be covered by the new limits. The news reports prompted Mnuchin on Monday to declare them "fake" news. Trump reiterated that view Tuesday, saying the publications got the story wrong.

The intent of the new restrictions, which are the result of an investigation completed by the administration earlier this year and aimed solely at China, is to protect the "jewels" of American industry, Trump said Tuesday. "We have the greatest technology in the world. People copy it and they steal it," Trump said. "We have the great scientists and we have the great brains and we have to protect that."

From: [redacted]
Sent: June-26-18 5:20 PM
To: [redacted]
Cc: [redacted]
Subject: FW: [redacted] Senate Passes its Version of Defence Authorization Bill; Reconciliation with House Version to Begin Soon

[redacted]

Hope all is well in Ottawa. Here, things are hectic as always (and then some).

We'd be interested in views from your teams on any GAC preferences between the different FIRRMA proposals passed in the Senate (pp. 815-930 here) and soon-to-be-passed in the House (here). [redacted]

[redacted] (cc'd) is covering the ISED angle.

Thanks and cheers,

[redacted]

From:
Sent: June-26-18 4:11 PM
To: 'jennifer.hubbard@forces.gc.ca' (jennifer.hubbard@forces.gc.ca); 'Lorna Prosper'; mary.gregory@canada.ca; Marcotte, Carl
Cc: william.truelove@forces.gc.ca; 'JOANNE.LOSTRACCO@forces.gc.ca' (JOANNE.LOSTRACCO@forces.gc.ca); Wheeler, Dave;
Subject: Senate Passes its Version of Defence Authorization Bill; Reconciliation with House Version to Begin Soon

Reftel and , attached for ease of reference.

SUMMARY

On Monday, June 18, the U.S. Senate voted by an 85-10 margin to approve the FY19 defense authorization bill. The John S. McCain National Defense Authorization Act (NDAA) includes US$716 billion for defence activities, including US$639.2 billion in base funding and US$68.5 billion for Overseas Contingency Operations (OCO). The Senate bill will need to be reconciled with the House bill that passed last month. A request for conference is expected this week. The base funding falls within the discretionary cap established in the Bipartisan Budget Act of 2018 and there is hope of an easier conference process given the near perfect alignment between the House and Senate numbers.

REPORT

2. The full text of the bill can be found here, and the accompanying Senate Armed Services Committee Report here.

3. The **funding levels** are virtually identical to the House bill, with the US$ 900 million difference representing a variance of just over a 0.1%.

Line	Senate FY19 (US$ B)	House FY19 (US$ B)	FY18 Enacted (US$ B)	Senate Increase Over FY18 (US$ B)
DOD Discretionary Base	617.6	616.7	605.5	+12.1
DOE Discretionary Base	21.7	22.1	20.6	+1.1
Defense-Related Activities	.3	.3	.3	
FY19 Base Budget DOD Topline	639.4	639.1	626.4	+13
Overseas Contingency Operations (OCO)	68.5	69	65.7	+2.8
FY19 Discretionary Topline	707.9	708.1	692.1	+15.8
Defense Mandatory Spending	8.2	8.9	8	+.2
FY19 NDAA Topline	716.1	717	700.1	+16

4. Of particular interest from a commercial standpoint are the **Procurement** and the **Research, Development, Test and Evaluation (RDT&E)** envelopes. The Senate bill authorizes close to US$1.2 billion more than the House version to these two envelopes, but again the difference in percentage is marginal.

Base and OCO authorizations for major categories (in US$ M)

Category	Base	OCO	Total	Difference vs FY19 House
Procurement	131,999	12,886	144,885	+839
RDT&E	92,216	1,308	93,524	+340
Ops & Maintenance	200,351	46,833	247,184	+492
Personnel	145,160	4,661	149,821	-2,362
Military Construction	10,531	852	11,383	+1,963
Other	37,384	1945	39,329	+1,013

5. The attached document also contains additional tables detailing **service-level procurement, authorization for major platforms** (e.g. 75 F-35 Joint Strike Fighters, two less than in the House bill) and **troop level increases**.

6. **Foreign Investment Review Modernization**: The Foreign Investment Risk Review Modernization Act (FIRRMA) of 2018 is found in Title XVII (Sec. 1701-1733). It represents language approved by the Senate Committee on Banking to update Committee on Foreign Investment in the United States (CFIUS) rules. The House NDAA does not include the FIRRMA language but a stand-alone bill (HR 5841) is expected to pass in the House this week.

7. Section 1703 amends section 721(a) of the Defense Production Act (DPA) by adding four new types of covered transactions, including:

- Any non-passive investment by a foreign person in any U.S. critical technology or critical infrastructure company;
- Any change in a foreign investor's rights regarding a U.S. business;
- Any other transaction, transfer, agreement or arrangement designed to circumvent/evade CFIUS; and
- The purchase, lease, or concession by or to a foreign person of certain real estate in close proximity to military or other sensitive national security facilities.

8. There are exemptions to the new covered transactions for investments from countries meeting certain criteria, including being a member of NATO or designated as major non-NATO ally. Section 1713 is of particular interest as it would enhance collaboration and coordination with U.S. allies by allowing greater information sharing. The information sharing provision in Sec. 306 of HR 5841 is much narrower in scope.

[redacted]

10. [redacted] Sec. 6702(b) would apply **strict procurement restrictions on Chinese telecommunications equipment, systems and services** for all federal agencies, broadening the language from Sec. 891(b)(2), which deals specifically with DoD contracting. [redacted]

Page 131

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

[redacted]

COMMENTS

[redacted]

NEXT STEPS

[redacted]

Drafted: [redacted]
Approved: [redacted]

BCC List

Alain Ouellet <alain.ouellet2@canada.ca>; Alex Thompson <alex.thompson@canada.ca>; Andre Bernier <andre.bernier@canada.ca>; Andrew Gauvreau <andrew.gauvreau@canada.ca>; Annie Martin <annie.martin@canada.ca>; [redacted]@international.gc.ca>; [redacted]@international.gc.ca>; Barbour, Glenn <Glenn.Barbour@forces.gc.ca>; [redacted]@international.gc.ca>; [redacted]@international.gc.ca>; [redacted]@international.gc.ca>; [redacted]@international.gc.ca>; [redacted]@international.gc.ca>; Boivin, Nadine <Nadine.Boivin@tpsgc-pwgsc.gc.ca>; Bramm, Alex <alex.bramm@canada.ca>; [redacted]@international.gc.ca>; [redacted]@international.gc.ca>; Clem Srour <clem.srour@canada.ca>; Col. Rob Spencer <robert.spencer@forces.gc.ca>; [redacted]@international.gc.ca>; Crookston, Gordon <Gordon.CROOKSTON@forces.gc.ca>; Daniel Salisbury <DANIEL.SALISBURY@forces.gc.ca>; Dany Theriault <dany.theriault@forces.gc.ca>; Darlene Delaney <darlene.delaney@canada.ca>; Deck, Harold <harold.deck@canada.ca>; Denis Bourque <denis.bourque@canada.ca>; Dominique Kowlessar <dominique.kowlessar@canada.ca>; [redacted]@international.gc.ca>; Dussault, Sheyla <SHEYLA.DUSSAULT@forces.gc.ca>; Gaerke, James <JAMES.GAERKE@forces.gc.ca>; [redacted]@international.gc.ca>; [redacted]@international.gc.ca>; [redacted]@international.gc.ca>; [redacted]@international.gc.ca>; [redacted]@international.gc.ca>; [redacted]

[redacted]

From: [redacted]
Sent: July-04-18 3:35 PM
To: [redacted]
Subject: FW: 5G Deck

Classification: SECRET//CANADIAN EYES ONLY

Huawei deck.

From: [redacted]
Sent: July-04-18 3:25 PM
To: [redacted]
Subject: 5G Deck

Classification: SECRET//CANADIAN EYES ONLY

2018_07_04_15_2...

Pages 135 to / à 143

are duplicates

sont des duplicatas

[redacted]

From: [redacted]
Sent: July-11-18 2:46 PM
To: [redacted]
Cc:
Subject: RE: Request for Product

Classification: SECRET//CANADIAN EYES ONLY

Excellent – thank you very much!

[redacted]

From: [redacted] [mailto: [redacted]
Sent: July-11-18 2:46 PM
To: [redacted]
Cc: [redacted]
Subject: RE: Request for Product

Classification: Secret//Canadian Eyes Only
Classification: Secret//Réservé aux Canadiens
Restriction / Restriction d'accès: NR / AR
File Number / No. de dossier: 520-301-60

Hi [redacted]

[redacted]

Thanks,

[redacted]

From: [redacted] mailto: [redacted]
Sent: 11-Jul-18 1:44 PM
To: [redacted]
Subject: RE: Request for Product

Classification: SECRET//CANADIAN EYES ONLY

Excellent, thank you!

From [redacted] [mailto: [redacted]
Sent: July-11-18 1:44 PM
To: [redacted]
Cc: [redacted]
Subject: RE: Request for Product

Classification: Secret//Canadian Eyes Only
Classification: Secret//Réservé aux Canadiens
Not for PA / Ne pas classer

Hi [redacted]

[redacted]

Thank you,

[redacted]

From: [redacted] [mailto: [redacted]
Sent: 11-Jul-18 1:42 PM
To: [redacted]
Cc: [redacted]
Subject: RE: Request for Product

Classification: SECRET//CANADIAN EYES ONLY

Hi [redacted]

[redacted]

Thank you,

[redacted]

From: [redacted] [mailto [redacted]
Sent: July-11-18 1:40 PM
To: [redacted]
Cc: [redacted]
Subject: RE: Request for Product

Classification: Secret//Canadian Eyes Only

Classification: Secret//Réservé aux Canadiens
Not for PA / Ne pas classer

Hi

Thank you for your request.

From: [mailto:
Sent: 11-Jul-18 1:27 PM
To:
Cc: (PSEPC-SPPCC); (PSEPC-SPPCC);
Subject: Request for Product

Classification: SECRET//CANADIAN EYES ONLY

Hello,

We kindly request that this be directed to

Thank you,

National Security Operations Directorate – Direction générale des opérations de la sécurité nationale
Public Safety and Emergency Preparedness Canada – Sécurité publique et Protection civile Canada
Tel. – Tél.

>>>**********[INFO DEPOT START / DÉBUT INFO DÉPÔT]**********
Sender / Envoyeur :
Recipients / Receveurs :
Subject / Sujet : RE: Request for Product
Date : 7/11/2018 1:40:00 PM

>>>**********[INFO DEPOT START / DÉBUT INFO DÉPÔT]**********
Sender / Envoyeur :
Recipients / Receveurs :
Subject / Sujet : RE: Request for Product
Date : 7/11/2018 1:44:06 PM

>>>**********[INFO DEPOT START / DÉBUT INFO DÉPÔT]**********
Sender / Envoyeur :
Recipients / Receveurs :
Subject / Sujet : RE: Request for Product
Date : 7/11/2018 2:45:49 PM

From:
Sent: July-23-18 11:48 AM
To:

Subject: FW: UK Huawei ANNUAL REPORT 2018
Attachments: HCSEC OB ANNUAL REPORT 2018.pdf

Classification: CONFIDENTIAL

FYI.

From:
Sent: July-23-18 11:12 AM
To:
Cc: Waters, Michael
Subject: FW: UK Huawei ANNUAL REPORT 2018

Classification: CONFIDENTIAL

Tel que discuté.

From: Waters, Michael
Sent: July-23-18 10:27 AM
To:
Cc: Manu, Vlad
Subject: UK Huawei ANNUAL REPORT 2018

Classification: CONFIDENTIAL

Hi Stéphane,

Do you know who is working on ICA? I think that they should be made aware of the email below and report attached.

Regards,
Michael

Michael Waters
Manager / Gestionnaire
National Cyber Security Directorate / Direction de la cyber-sécurité nationale
Public Safety Canada / Sécurity public Canada
Tel/Tél: 613-991-1634
Mobile: 613-796-4286

Email/courriel: Michael.Waters@canada.ca
CTSN:

From: Waters, Michael
Sent: July-23-18 10:05 AM
To: Bunghardt, Gregory; Hashem, Mohsen; Frigon, Sylvie; Hartley, William; Park, Beom-Jun; Merchant, Colleen; Binne, Christine; Ouellet, Benoit; Brydges, Lucas; Goldfinger, Marc; Gauthier, Darren; Hamilton, Sharon; Bendelier, Kenneth; (CSE-CST); (CSE-CST)
Subject: UK Huawei ANNUAL REPORT 2018

Classification: CONFIDENTIAL

Colleagues,

See report attached.

Regards,
Michael

Michael Waters
Manager / Gestionnaire
National Cyber Security Directorate / Direction de la cyber-sécurité nationale
Public Safety Canada / Sécurity public Canada
Tel/Tél: 613-991-1634
Mobile: 613-796-4286
Email/courriel: Michael.Waters@canada.ca
CTSN: WatersM2@ps-sp.gc.ca

From: NCSCCAP GBR GOV (GCHQ) [mailto:
Sent: July-22-18 6:05 AM
To: Waters, Michael;
Subject: PUBLICATION OF HCSEC ANNUAL REPORT 2018

CLASSIFICATION: UK OFFICIAL

All,

[redacted] and as you may already be aware, the fourth Huawei Cyber Security Evaluation Centred Oversight Board Annual Report (attached) was published on 19th July 2018 on the www.gov.uk website (where the previous three year reports can be found if you search for HCSEC annual report).

[redacted]

If you have any questions please do not hesitate to contact me.

[redacted]
NCSC Telecoms Security Relationship Manager
A2G
Rus: [redacted]
Nsec: [redacted]
Work Mobile: [redacted]
Low side email: [redacted]@ncsc.gov.uk

HUAWEI CYBER SECURITY EVALUATION CENTRE (HCSEC) OVERSIGHT BOARD

ANNUAL REPORT

2018

A report to the National Security Adviser of the United Kingdom

July 2018

HUAWEI CYBER SECURITY EVALUATION CENTRE OVERSIGHT BOARD ANNUAL REPORT

Part I: Summary

1. This is the fourth annual report from the Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board. HCSEC is a facility in Banbury, Oxfordshire, belonging to Huawei Technologies (UK) Co Ltd, whose parent company is a Chinese headquartered company which is now one of the world's largest telecommunications providers.
2. HCSEC has been running for seven years. It opened in November 2010 under a set of arrangements between Huawei and HMG to mitigate any perceived risks arising from the involvement of Huawei in parts of the UK's critical national infrastructure. HCSEC provides security evaluation for a range of products used in the UK telecommunications market. Through HCSEC, the UK Government is provided with insight into Huawei's UK's strategies and product ranges. The UK's National Cyber Security Centre (NCSC, and previously GCHQ), as the national technical authority for information assurance and the lead Government operational agency on cyber security, leads for the Government in dealing with HCSEC and with Huawei more generally on technical security matters.
3. The HCSEC Oversight Board, established in 2014, is chaired by Ciaran Martin, the Chief Executive Officer of the NCSC, and an executive member of GCHQ's Board with responsibility for cyber security. The Oversight Board continues to include a senior executive from Huawei as Deputy Chair, as well as senior representatives from across Government and the UK telecommunications sector. The structure of the Oversight Board has not changed significantly, but membership has changed in the year 2017-18. Mainly, this is due to staff rotations in both HMG and Huawei positions.

4. The Oversight Board has now completed its fourth full year of work. In doing so it has covered a number of areas of HCSEC's work over the course of the year. The full details of this work are set out in Parts II and III of this report. In this summary, the main highlights are:

i. **New secure premises for HCSEC are on track**; the previously reported acquisition of new premises for HCSEC has experienced some commercial delays, but remains broadly on track for completion in late 2018;

ii. **Technical issues have been identified in Huawei's engineering processes,** leading to new risks in the UK telecommunications networks;

iii. **The GCHQ Technical Competence Review found that the capability of HCSEC has improved in 2017**, and the quality of staff has not diminished, meaning that technical work relevant to overall mitigation strategy can be performed at scale and with high quality;

iv. **The fourth independent audit of HCSEC's ability to operate independently of Huawei HQ has been completed**, with – again – no high or medium priority findings. The audit report identified two low rated finding and two advisory issues, relating to record keeping and the retention of auditable information. Each issue has an agreed rectification plan, Ernst & Young concluded that there were no major concerns and the Oversight Board is satisfied that HCSEC is operating in line with the 2010 arrangements between the Government and the company.

5. The three key conclusions from the Oversight Board's fourth year of work are:

i. It is evident that HCSEC continues to provide unique, world-class cyber security expertise and technical assurance of sufficient scope and quality as to be appropriate for the current stage in the assurance framework around Huawei in the UK.

ii. The HCSEC Oversight Board is assured that the Ernst & Young Audit Report provides important, external reassurance that the arrangements for HCSEC's operational independence from Huawei Headquarters is operating robustly and effectively, and in a manner consistent with the 2010 arrangements between the Government and the company.

iii. However, identification of shortcomings in Huawei's engineering processes have exposed new risks in the UK telecommunication networks and long-term challenges in mitigation and management.

6. The Oversight Board concludes that in the year 2017-18, HCSEC fulfilled its obligations in respect of the technical work required of it by NCSC.

7. Due to areas of concern exposed through the proper functioning of the mitigation strategy and associated oversight mechanisms, the Oversight Board can provide only limited assurance that all risks to UK national security from Huawei's involvement in the UK's critical networks have been sufficiently mitigated. We are advising the National Security Adviser on this basis.

HUAWEI CYBER SECURITY EVALUATION CENTRE OVERSIGHT BOARD 2017 ANNUAL REPORT

Part II: Technical and Operational Report

This is the fourth annual report of the Huawei Cyber Security Evaluation Centre Oversight Board. The report may contain some references to wider Huawei corporate strategy and to non-UK interests. It is important to note that the Oversight Board has no direct locus in these matters and they are only included insofar as they could have a bearing on conclusions relating directly to the assurance of HCSEC's UK operations. The UK Government's interest in these non-UK arrangements extends only to ensuring that HCSEC has sufficient capacity to discharge its agreed obligations to the UK. Neither the UK Government, nor the Board as a whole, has any locus in this process otherwise.

Introduction

1. This is the fourth annual report from the Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board. HCSEC is a facility in Banbury, Oxfordshire, belonging to Huawei Technologies (UK) Co Ltd, whose parent company is a Chinese headquartered company which is now one of the world's largest telecommunications providers.

2. HCSEC has been running for seven years. It opened in November 2010 under a set of arrangements between Huawei and HMG to mitigate any perceived risks arising from the involvement of Huawei in parts of the UK's critical national infrastructure. HCSEC provides security evaluation for a range of products used in the UK market. Through HCSEC, the UK Government is provided with insight into Huawei's UK's strategies and product ranges. The UK's National Cyber Security Centre (NCSC, and previously GCHQ), as the national technical authority for information assurance and the lead Government operational agency on cyber security, leads for the Government in dealing with HCSEC and with Huawei more generally on technical security matters.

3. The HCSEC Oversight Board, established in 2014, is chaired by Ciaran Martin, the Chief Executive Officer of the NCSC, and an executive member of GCHQ's Board with responsibility for cyber security. The Oversight Board continues to include a senior executive from Huawei as Deputy Chair, as well as senior representatives from across Government and the UK telecommunications sector. The structure of the Oversight Board has not changed significantly, but membership has changed in the year 2017-18. Mainly, this is due to staff rotations in both HMG and Huawei positions.

4. This fourth annual report has been agreed unanimously by the Oversight Board's members. As with last year's report, the Board has agreed that there is no need for a confidential annex, so the content in this report represents the full analysis and assessment.

5. The report is set out as follows:

I. Section I sets out the Oversight Board terms of reference and membership;

II. Section II describes HCSEC staffing, skills, recruitment and accommodation;

III. Section III covers HCSEC technical assurance, prioritisation and research and development;

IV. Section IV summarises the findings of the 2016-17 independent audit;

V. Section V brings together some conclusions.

SECTION I: The HCSEC Oversight Board: Terms of Reference and membership

1.1 The HCSEC Oversight Board was established in early 2014. It meets quarterly under the chairmanship of Ciaran Martin, the Chief Executive of the UK National Cyber Security Centre (NCSC) and an executive member of GCHQ's Board at Director General level. Mr Martin reports directly to GCHQ's Director, Jeremy Fleming, and is responsible for the agency's work on cyber security.

1.2 The role of the Oversight Board is to oversee and ensure the independence, competence and overall effectiveness of HCSEC and to advise the National Security Adviser on that basis. The National Security Adviser will then provide assurance to Ministers, Parliament and ultimately the general public as to whether the risks are being well managed.

1.3 The Oversight Board's scope relates only to products that are relevant to UK national security risk. Its remit is two-fold:

- first, HCSEC's assessment of Huawei's products that are deployed or are contracted to be deployed in the UK and are relevant to UK national security risk which is determined at the NCSC's sole and absolute discretion; and
- second, the independence, competence and therefore overall effectiveness of HCSEC in relation to the discharge of its duties.

1.4 The Board has an agreed Terms of Reference, a copy of which is attached at **Appendix A**. There have been no changes to the terms of reference this year and the main objective of the Oversight Board remains unchanged. The Oversight Board is responsible for providing an annual report to the National Security Adviser, who will provide copies to the National Security Council and the ISC.

The Board's objectives for HCSEC

1.5 The Oversight Board's four high level objectives for HCSEC remained consistent with those reported previously and are:

- To provide security evaluation coverage over a range of UK customer deployments as defined in an annual HCSEC evaluation programme;

- To continue to provide assurance to the UK Government by ensuring openness, transparency and responsiveness to Government and UK customer security concerns;
- To demonstrate an increase in technical capability, either through improved quality of evaluations output or by development of bespoke security related tools, techniques or processes;
- For HCSEC to support Huawei Research and Development to continue to develop and enhance Huawei's security and engineering competence.

The HCSEC Oversight Board: Business April 2017- March 2018

1.6 In its two meetings since the publication of the 2017 Annual Report, the Oversight Board has:

- Provided regular corporate updates on Huawei UK
- Discussed future technology trends and how they may affect the work of the Oversight Board;
- Been supplied with regular updates on HCSEC recruitment, staffing and accommodation plans;
- Received updates on the HCSEC technical programme of work and its progress and received a detailed report on technical visits to Huawei HQ in Shenzhen by the NCSC Technical Director and technical team, some with UK operators, to discuss technical issues;
- Taken evidence around the root causes of the problems achieving binary equivalence and agreed a programme of work towards remediation;
- Taken evidence of redelivery of source code packages, the basis of which was detailed in the previous report;
- Taken evidence on the security risks engendered by Huawei's lifecycle management of critical components and written to the National Security Adviser based on this;
- Commissioned a fourth HCSEC management audit of the independence of the Centre.

~~~~~
~~~~~

SECTION II: HCSEC Staffing

2.1 This section provides an account of HCSEC's staffing and skills, including recruitment and retention.

Staffing and skills

2.2 A change was made to the senior management team in HCSEC. A long serving member of the HCSEC team, who has demonstrated excellent technical knowledge during his tenure, was appointed as Director Solutions and Programme, overseeing the execution of technical operations in HCSEC. His appointment to the senior management team is welcomed by the Board. The leadership team continues to work well together, leading HCSEC and engaging with Huawei in a constructive manner.

2.3 The NCSC leads for the Government in dealing with HCSEC and the company more generally on technical security matters. The NCSC, on behalf of the Government, sponsors the security clearances of HCSEC's staff. The general requirement is that all staff must have Developed Vetting (DV) security clearance, which is the same level required in Government to have frequent, uncontrolled access to classified information and is mandatory for members of the intelligence services. New recruits to HCSEC are managed under escort during probation pending completion of their DV clearance period, which is typically six months.

2.5 Staffing at HCSEC has increased in line with expectations for the year 2017. By the end of the calendar year, the staff numbers were almost as predicted with, once again, only one position not filled (taking 'offer accepted' as the point of employment). Due to uncertainty around the binary equivalence work, it was unclear precisely what skills were needed to support this work and so a conscious decision made to not fill the three extra posts committed to by Huawei and preserve the headcount for 2018.

2.6 It remains critical that HCSEC continues to recruit technical cyber security specialists to manage attrition and succession. This continued excellent progress has been driven by the ongoing personal involvement of HCSEC leadership and represents a significant amount of work.

2.7 Again, a significant number of potential recruits were sifted out due to clearance requirements. Furthermore, three candidates that passed initial sifting and were employed by HCSEC subsequently failed DV clearance and were removed from the centre. The small risk associated with these staff was adequately managed through the supervision and oversight provided during their probationary employment period.

Accommodation

2.9 The 2017 report spoke of the successful search for new accommodation for HCSEC to cope with the expansion of HCSEC's operation. The delays alluded to in that report came to pass for reasons associated with the building configuration and the logistics of the move. However, the process has been successfully concluded and the move to the new premises should be completed during 2018Q4. These delays are not in any way the result of Huawei HQ's inaction or interference.

2.10 The new accommodation will allow for concurrent reference networks to be put in place, allowing solution evaluations to proceed at pace. It also allows for increased development activity to help manage the significant number of products needing assessment.

2.11 Overall, good progress has been made on staffing and skills during 2017. Quarterly monitoring by the Oversight Board has shown no causes for concern in the number of staff and their skills. The delay to the new accommodation is unfortunate but has in no way affected the ability of HCSEC to discharge its functions this year.

~~~~~
~~~~~

Section III: HCSEC Technical Assurance

2017 is the seventh year of the Government's extended risk management programme for Huawei's involvement in the UK telecommunications market. In the previous two years, the Oversight Board chose to publish, exceptionally, more details of the technical assurance work undertaken as part of this programme. This report builds on the previous three reports. The Oversight Board's intent is to provide detailed technical assessment only periodically and when issues specifically warrant it. This year there have, once again, been technical issues that specifically warrant inclusion in the report due to their direct impact on the ability of the Oversight Board to provide assurance to the National Security Advisor. It is to be welcomed that despite difficulties, Huawei has continued to work closely with NCSC and HCSEC and provided access and information when requested.

Evaluation Process

3.1 HCSEC's assessment programme in 2017 continued the product and solution evaluation split which proved successful in previous years. In 2017, 27 product evaluations were completed, 5 solution evaluations were started, with 3 being completed during the reporting period. The evaluations covered products and architectures for 4 UK operators.

3.2 The last Oversight Board report detailed issues with a particular evaluation, concerning the virtualised SMSC. Regardless of the issues, the operator chose to deploy the solution with an expectation that they would upgrade to the next version to be evaluated by HCSEC. The operator has not yet chosen to upgrade the system to a version that could be evaluated by HCSEC.

3.3 The NCSC has a stated intent of HCSEC performing a product evaluation on every relevant product in the UK at least every two years. HCSEC's product evaluation pipeline is configured to achieve this. Huawei have provided long term headcount for the evaluation and infrastructure build teams and the Oversight Board is confident that continued attention from HCSEC seniors will ensure that there are sufficient appropriately skilled staff to maintain the NCSC intent. HCSEC staff must be capable

of achieving security clearance and have the requisite skills, meaning the pool of available talent is small.

3.4 The previous Oversight Board report described a group set up by NCSC to discuss the management of the risks around the Huawei Mobile Virtual Network Operator (MVNO) solution in the UK. Over 2017, this has been expanded and its scope broadened to cover wider supply chain risk management issues in the telecoms sector as a whole.

3.5 The evaluation process continues to find a significant number of point vulnerabilities and more strategic architectural and process issues. Huawei continues with their remediation work; the feedback provided by HCSEC to Huawei R&D continues to be of high quality and the HCSEC technical staff continue to assist the Huawei R&D teams in their remediation efforts.

Prioritisation and programme build

3.6 The risk-based prioritisation scheme detailed in previous Oversight Board reports has continued to be applied during 2017.

3.7 The programme build process remains broadly as previous years. The operators, NCSC and HCSEC collaboratively prioritise the work of HCSEC. This is necessary to balance the sometimes-competing constraints and requirements for the best benefit of the UK, for example not allowing a particular operator to dominate the programme of work due to commercial pressures. The final programme is signed off by the NCSC Technical Director or NCSC Technical Director for Telecommunications on behalf of the Oversight Board and kept under review during the year by HCSEC. Where HCSEC believes modifications to the programme are necessary, a lightweight process involving the NCSC and the relevant operators is used to manage and approve any modifications.

3.8 Little has changed in terms of high level prioritisation of equipment, although the scale and scope of Huawei's involvement in the UK telecoms sector means there is a significant pipeline of work for HCSEC to manage. At present, HCSEC manages

that pipeline well. The results of HCSEC's work is reported directly to the operators and they are expected to feed them into their corporate risk management processes.

Configuration Management and Binary Equivalence

3.9 The previous Oversight Board report spoke to two significant issues. The first of these was the extraction by Huawei HQ of a subset of source code from configuration managed repositories for onward delivery to HCSEC. The second was the failure of Huawei R&D to repeatably build a product to a consistent binary. As described in the previous Oversight Board report, this means that any assurance provided by the overall risk management strategy, and therefore the Oversight Board, is currently limited.

3.10 The Oversight Board agreed with Huawei HQ a timetable for the redelivery of all source code for the products previously delivered to HCSEC, with all code having been redelivered by December 2017. The redelivery of code packages was completed three months ahead of the deadline.

3.11 HCSEC have observed that all new packages contain more code. If the Binary Equivalence Programme completes and is successful, then HCSEC should be able to verify that all products build to the binary running in the UK network. It is important that this work is completed quickly.

3.12 The last report talked about rescoping the division of effort between HCSEC and Huawei R&D, with Huawei R&D expected to take on more of the mandrolic work to show binary equivalence, leaving HCSEC to perform a verification function.

3.13 This rescoping started with Huawei R&D performing some work to understand the underlying issues observed by HCSEC in performing repeatable builds for products. This work showed that the underlying engineering and build process was not repeatable.

3.14 Huawei R&D was asked by NCSC and HCSEC to perform analysis of four specific products from different product groups which showed that the underlying

engineering issues, including the failure to reproduce builds, are consistent across the various product lines.

3.15 HCSEC have worked with Huawei R&D to try to correct the deficiencies in the underlying build and compilation process for these four products. This has taken significant effort from all sides and has resulted in a single product that can be built repeatedly from source to the General Availability (GA) version as distributed. This particular build has yet to be deployed by any UK operator, but we expect deployment by UK operators in the future, as part of their normal network release cycle. The remaining three products from the pilot are expected to be made commercially available in 2018H1, with each having reproducible binaries. The engineering changes have not yet been integrated into the wider development process. A second batch of products has been selected by NCSC, the operators and HCSEC and work on these should complete by the end of 2018H1, with all remaining products to follow. Assuming the continued success of the initial trials, it is the NCSC and Oversight Board expectation that this will be completed by mid 2020.

3.16 It is the NCSC intent that all products deployed in the UK will have repeatable builds and that HCSEC will be able to routinely show equivalence between the binary installed in UK networks and the binary that can be built from the source code held by HCSEC. This verification should be completed for every product version deployed in the UK that has been assessed by HCSEC. It is important that all products can be built in this way to enable the risk-based approach to HCSEC's prioritisation of work.

3.17 The Chairman of the Oversight Board had previously written to the National Security Adviser in February explaining the issue. Details of the next phase of this work were presented to the Oversight Board at the March meeting where the Board approved the plan. Work continues to remediate the engineering process issues in other products that are deployed in the UK, prioritised based on risk profiles and deployment volumes. This work should give us the ability to provide end-to-end assurance that the code analysed by HCSEC is the constituent code used to build the binary packages executed on the network elements in the UK.

3.18 Until this work is completed, the Oversight Board can offer only limited assurance due to the lack of the required end-to-end traceability from source code examined by HCSEC through to executables use by the UK operators.

Third Party Component Support Issue

3.19 A technical visit to Shenzhen was scheduled for September 2017 for NCSC, HCSEC and the UK Operators to discuss with Huawei HQ the progress around source code redelivery to HCSEC and binary equivalence. Previous technical visits have discussed Huawei's management of third party components imported as part of a product build, both commercial and open source. During a review of the programmes of work being undertaken, NCSC identified that not all components are managed through this process and, in particular, security critical third party software used in a variety of products was not subject to sufficient control.

3.20 It is now apparent that third party software, including security critical components, on various component boards will come out of existing long-term support in 2020, even though the Huawei end of life date for the products containing this component is often longer. Huawei has provided the Oversight Board with data on the extent to which this affects the UK deployments. NCSC has determined how the issue directly affects the security and reliability of deployed products and has provided the Oversight Board its opinion that this issue limits the ability of HCSEC's efforts to contribute to the overall assurance strategy in a sustainable manner.

3.21 There have been a number of detailed technical discussions between Huawei R&D and HCSEC, some including NCSC. These discussions are working towards a full understanding of the problem, a short-term mitigation plan and a more strategic fix for the underlying cause of the problem. However, there is a significant risk in the UK telecoms infrastructure if Huawei and the operators are unable to support these boards long-term.

3.22 A range of technical and contractual solutions are being discussed between the operators, NCSC, HCSEC and Huawei R&D. Any short-term mitigation obviously needs to be cognisant of the realities of the UK telecoms networks and the operators' testing and release cycles.

3.23 It is expected that the Oversight Board will receive an update on progress at its June meeting, to be held at Huawei's facilities in Shanghai, with NCSC and HCSEC working with Huawei technical teams on the detailed plans.

Summary of NCSC Technical Competence Review

3.24 The work of HCSEC in 2017 has continued capability development in the underpinning tooling necessary to provide assurance and technical security artefacts to the UK operators at the scale necessary given Huawei's position in the UK market. Through 2017, HCSEC has continued to find issues in Huawei products, demonstrating their continued ability to discover weaknesses in the Huawei product set.

3.25 HCSEC continues to have world class security researchers who are creating new tools and techniques to provide assurance in the complex sphere of telecommunications, while taking into account Huawei's unique engineering and security processes.

3.26 The work conducted by HCSEC on the binary equivalence, build process and subsequent understanding of the recurrent third party component management and support problem shows that they are competent in the field to the level necessary to independently verify Huawei R&D claims and satisfy the Oversight Board requirements.

3.27 The NCSC believes that HCSEC remains competent in the areas of technical security necessary to advise the operators, NCSC and the Oversight Board as to the product and solution risks admitted by the use of Huawei products in the UK telecoms infrastructure. The NCSC's report to the Oversight Board is that HCSEC continues to provide unique, world class cyber security expertise to assist the Government's ongoing risk management programme with the UK operators.

Conclusion: technical assurance

3.28 NCSC still believes that the assurance model including HCSEC is the best way to manage the risk of Huawei's involvement in the UK telecommunications sector. The model is predicated on industry good practice security and engineering in Huawei. Overall, given this account, the NCSC has advised the Oversight Board that it is less confident that NCSC and HCSEC can provide long term technical assurance of sufficient scope and quality around Huawei in the UK. This is due to the repeated discovery of critical shortfalls, including but not limited to BEP and the third party component support issue, in the Huawei engineering practices and processes that will cause long term increased risk in the UK. These risks are not due to any issue with HCSEC's staffing and capabilities. Obviously, significant work will be required in managing these risks both short term and long term. The Oversight Board will be looking to HCSEC to continue to ensure that Huawei are making appropriate remediations and to advise the Oversight Board, the UK operators and the NCSC of any issues arising.

3.29 A further medium-term issue that the Oversight Board must take account of is the shift in architecture and technology brought about by things like software defined networking, virtualisation, MVNO proliferation and edge compute architectures such as 5G, along with changes in the operational models of many telecommunications operators. NCSC will need to revisit the technical assessment, including how HCSEC contributes to mitigation, and advise the Oversight Board on what mechanisms may be appropriate to continue to gain the required assurance in the use of Huawei equipment in the UK telecommunications environment.

~~~~~
~~~~~

SECTION IV: The work of the Board: Assurance of independence

4.1 This section focuses on the more general work of the Oversight Board beyond its oversight of the technical assurance provided by HCSEC. For the fourth year running, the Board commissioned and considered an audit of HSCEC's required operational independence from Huawei HQ. This was the most effective way, in the Board's view, of gaining assurance that the arrangements were working in the way they were designed to work in support of UK national security. The principal question for examination by the audit was whether HCSEC had the required operational independence from Huawei HQ to fulfil its obligations under the set of arrangements reached between the UK Government and the company in 2010. This section provides an account of the process by which the audit took place, and a summary of the key findings.

Appointing Ernst & Young as auditors

4.2 Ernst & Young LLP (E&Y) were appointed to carry out the first HCSEC audit in 2014, following a rigorous process during which GCHQ invited three audit houses to consider undertaking the management audit and sought their recommendation as to the appropriate audit standard and process to be followed. E&Y undertook the second audit in 2015 and in 2016, at the NCSC's instigation, they were retained to provide audit services for the subsequent three years, that is until November 2019. E&Y's Annual Management Audit was conducted in accordance with the International Standard on Assurance Engagements (ISAE) 3000.

4.3 The Oversight Board agreed a three stage approach to the audit, which broadly followed that of previous years:

i. An initial phase to assess the control environment and agree the scope and key issues for review. This phase was completed by November 2017;
ii. A second phase to run a rehearsal audit of the design and operation of the controls in place to support the independent operation of HCSEC. This phase was completed during November 2017;
iii. A final audit phase comprising the full year end audit during December 2017, with the report presented to the NCSC, HCSEC and Huawei HQ in February 2018 and the full Oversight Board in March 2018.

The nature and scope of the audit

4.4 The audit assessed the adequacy and the operation of processes and controls designed to enable the staff and management of HCSEC to operate independently of undue influence from elsewhere in Huawei. The principal areas in scope were: Finance and Budgeting; HR; Procurement; Evaluation Programme Planning; Cooperation and Support from elsewhere in Huawei; and Evaluation Reporting. For all the review areas listed, E&Y took into account that the operation of HCSEC must be conducted within the annual budget agreed between Huawei and HCSEC.

4.5 The Oversight Board agreed some exclusions to the scope of the audit. Specifically, they agreed that the audit would not:

- Opine as to the appropriateness of the overall governance model adopted to support the testing of Huawei products being deployed in the UK Critical National Infrastructure;
- Assess the technical capability of HCSEC, the competency of individual staff or the quality of the performance of technical testing;
- Assess physical access to HCSEC or logical access to its IT infrastructure. Nor would it look at the resilience of the infrastructure in place or at Disaster Recovery or Business Continuity planning.

Headline audit findings

4.6 The HCSEC Annual Management Audit January 2018 comprised a rigorous evidence-based review of HCSEC processes and procedures. The audit report was produced by a team of DV cleared staff from Ernst & Young; the fieldwork was conducted by an experienced Manager and led by Senior Manager. A Partner with Technology and Assurance subject matter knowledge acted as quality reviewer, and a second review of the final report was performed by an Ernst & Young Executive Director.

4.7 In summary, Ernst & Young concluded that there were no major concerns about the independent operation of HCSEC. The audit report's principal conclusion said:

"With the exception of the findings below [two findings rated as 'Low'], *the controls evaluated were considered to be effective as per the control descriptions and agreed test procedures. In some instances, it was noted that there is the opportunity to further strengthen the control regime or to improve the efficiency of the audit process and these have been noted below as "advisory" recommendations as opposed to identified control deficiencies."*

4.8 The audit report identified two control weaknesses within the HCSEC control environment for the Board to consider. The weaknesses were both rated as "Low", meaning that action should be considered to reduce an exposure which results in a limited impact to some aspects of the independent operation of HCSEC, but which in itself would be unlikely to compromise the independence of HCSEC overall. There were another two advisory issues, which were noted as potential minor improvements in the overall control regime. The audit findings were presented to the Board in its March meeting with an Ernst & Young Partner in attendance to brief the Board. The Oversight Board discussed each of the identified weaknesses and advisory notes in the audit and agreed an approach for each one.

Control Weakness

4.9 In summary, the area of control weakness identified, and the agreed response, relate to the following area:

i. Request and Retain Evaluation Plan Sign-Off

4.10 The evaluation plan, which outlines which products will be tested at which points of the year, is discussed with the NCSC when it is being created. Discussion with HCSEC management identified that the plan was presented to the NCSC at a scoping meeting but no evidence that this plan was approved was available. This is a repeat finding from last year.

4.11 Following review and agreement of the evaluation plan with NCSC, HCSEC should ensure that they obtain a formal confirmation that the evaluation plan is fit for purpose and retain this in their records. This should take the form of either written approval (e.g. via email) from NCSC or in the form of agreed minutes

following a meeting with NCSC hosted by HCSEC. The process has been further updated such that the NCSC Technical Director for Telecoms now has delegated authority to sign off the evaluation plan, with an escalation route when necessary which will hopefully address the issue.

ii. Budget setting and ongoing financial review

4.12 The audit identified that the agreed process for establishing and approval of HCSEC's budget for the year under review had not been fully followed. Formal sign-off from each member of the HCSEC SMT (Senior Management Team) had not been formally obtained.

4.13 This control has historically been performed by HCSEC senior leadership; it is noted that there has been a significant change in senior leadership this year. Going forward, an auditable record of key decisions on the setting of the budget should be retained – particularly the explicit approval of the HCSEC SMT following the final iteration of value.

Advisory Notices

4.11 Two advisory notices were identified by the audit, relating to the recording and retention of specific, auditable information:

i. RFIs returned outside SLA period

4.12 Requests for information made to Huawei were not always returned inside the stated SLA period. In their tests the auditors identified that 4 requests for hardware were completed outside of the stated 12 week SLA period.

4.13 In discussion with HCSEC it was noted that, although specified in the Terms of Reference, the SLA is 'aspirational' and that non-adherence would not necessarily adversely impact evaluation performance. In practice there is "slack" built into the delivery to accommodate late returns. To clarify for the purposes of review, RFIs

could be updated to include a "required by" date (of no earlier than the SLA period) with the intention that this is strongly adhered to and escalated when it is breached.

ii. Monitoring of spend versus budget has not been well maintained over the audit period.

4.14 Although testing of controls on expenditure did not identify any evidence that HCSEC spend had been restricted, and accordingly no undue influence exerted on its independent operation, it is difficult to verify if HCSEC spend in the year was within the agreed final budget for 2017.

4.15 Over the course of the year HCSEC made amendments to the set budget value that they track spend against (e.g. for depreciation rather than cash spend on the new premises and staff bonuses); these changes were not clearly documented.

4.16 Internal monitoring, in the form of reconciliation between spend and budget is performed informally and on an ad-hoc basis, and there is no record maintained of these reviews Related, there was also a discrepancy between the values reported by the Huawei UK finance system and those maintained by HCSEC, showing higher spend on the Huawei finance system than that tracked internally by HCSEC.

4.17 Changes to the budget from proposal through to approval should be documented. The final approved budget should be consistent with the figures monitored by HCSEC internally. If errors or accounting corrections are required this should be documented such that there is traceability between the approved value and the actual amount spent in the year.

Prior year issues and current status

4.14 **Appendix B** provides a summary of the issues and observations from the previous year's report, published in 2017.

Overall Oversight Board conclusions of the audit

4.16 Taking the audit report in its totality, the HCSEC Oversight Board has concluded that the report provides important, external reassurance from a globally

respected company that the arrangements for HCSEC's operational independence from Huawei Headquarters are operating robustly and effectively, and in a manner consistent with the 2010 arrangements between the Government and the company. Four issues – two low rated finding and two advisory issues – have been identified.

~~~~~
~~~~~

SECTION V: Conclusions

5.1 The Oversight Board has now completed its fourth full year of work. Its two meetings and its work out of Committee have provided a useful enhancement of the governance arrangements for HCSEC.

5.2 The key conclusions from the Board's fourth year of work are:

i. It is evident that HCSEC continues to provide unique, world-class cyber security expertise and technical assurance of sufficient scope and quality as to be appropriate for the current stage in the assurance framework around Huawei in the UK

ii. However, Huawei's processes continue to fall short of industry good practice and make it difficult to provide long term assurance. The lack of progress in remediating these is disappointing. NCSC and Huawei are working with the network operators to develop a long-term solution, regarding the lack of lifecycle management around third party components, a new strategic risk to the UK telecommunications networks. Significant work will be required to remediate this issue and provide interim risk management.

iii. The HCSEC Oversight Board is assured that the Ernst & Young Audit Report provides important, external reassurance that the arrangements for HCSEC's operational independence from Huawei Headquarters is operating robustly and effectively, and in a manner consistent with the 2010 arrangements between the Government and the company. The issue identified was rated as low risk and two further advisory issues were identified.

5.3 Overall therefore, the Oversight Board has concluded that in the year 2017-2018, HCSEC fulfilled its obligations in respect of the provision of security and engineering assurance artefacts to the NCSC and the UK operators as part of the strategy to manage risks to UK national security from Huawei's involvement in the UK's critical networks. However, the execution of the strategy exposed a number of risks which will need significant additional work and management. The Oversight Board will need to pay attention to these issues.

5.4 Additionally, it is hoped that this report continues to add to Parliamentary – and through it, public – knowledge of the operation of the arrangements and the transparency with which they are operated.

~~~~~
~~~~~

Appendix A : Terms of Reference for the Huawei Cyber Security Evaluation Centre Oversight Board

1. Purpose

This Oversight Board will be established to implement recommendation two of the National Security Adviser's Review of the Huawei Cyber Security Evaluation Centre (HCSEC). The Oversight Board's primary purpose will be to oversee and ensure the independence, competence and therefore overall effectiveness of HCSEC and it will advise the National Security Adviser on this basis. It will work by consensus. However, if there is a disagreement relating to matters covered by the Oversight Board, GCHQ, as chair, will have the right to make the final decision.

The Board is responsible for assessing HCSEC's performance relating to UK product deployments. It should not get involved in the day-to-day operations of HCSEC.

2. Scope of Work

2.1 In Scope

The Oversight Board will focus on:

- HCSEC's assessment of Huawei products that are deployed or are contracted to be deployed in the UK and are relevant to UK national security risk.
- The independence, competence and therefore overall effectiveness of HCSEC in relation to the discharge of its duties.

2.2 Out of Scope

- All products that are not relevant to UK national risk;
- All products, work or resources for non UK-based deployment, including those deployed outside the UK by any global CSPs which are based in the UK;
- The commercial relationship between Huawei and CSPs; and
- HCSEC's foundational research (tools, techniques etc.) which will be assessed

and directed by GCHQ.

3. Objectives of the Oversight Board

3.1 Annual Objectives and Report to the National Security Adviser

To provide a report on the independence, competence and effectiveness of HCSEC to the National Security Adviser on an annual basis, explicitly detailing to what extent HCSEC has met its in-year objectives as set by the Board. This will draw upon the Annual Management Audit, the Technical Competence Review and will specifically assess the current status and the long term strategy for resourcing HCSEC.

All UK CSPs that have contracted to use HCSEC for assurance in the context of management of UK national risk for deployments shall be consulted.

In the event of a change to the operation of HCSEC, or the emergence of any other factor that affects HCSEC's security posture, HCSEC will report this to the Oversight Board in a timely manner. GCHQ [or any other member of the Oversight Board] shall also be expected to inform the Oversight Board of any factor which appears to affect the security posture of HCSEC.

3.2 Commission Annual Management Audit

To assure the continued independence of HCSEC from Huawei HQ, the Oversight Board will commission a management audit to be performed by security cleared UK auditors; this will be funded by UK Government. The scope of the audit shall be as set out in the Huawei HQ Letter of Authorisation (Operational Independence) to HCSEC (as set out in Annex 3), or other agreed standards, as agreed by the Oversight Board. This will include the independence of budget execution and whether HCSEC were provided with the timely information, products and code to undertake their work.

The Oversight Board will ensure the scope of any such audit is appropriate and the auditor shall be agreed by the Chair and Deputy Chair.

The audit report mentioned in section 3.2 and 3.3 shall be treated as confidential information and subject to section 8.

3.3 Commission Technical Competence Review

To provide assurance that the functions performed by HCSEC are appropriate in terms of the wider risk management strategy as defined by GCHQ and the CSPs. The Oversight Board will commission GCHQ to undertake an audit of the technical competence of the HCSEC staff, the appropriateness and completeness of the processes undertaken by HCSEC and the strategic effects of the quality and security of Huawei products relevant to UK national security risks. GCHQ as part of the annual planning process will advise HCSEC of any enhancements in technical capability they wish to see developed by them within the year.

3.4 Process to Appoint Senior Management Team

The Oversight Board will agree the process by which GCHQ will lead and direct the appointment of senior members of staff of HCSEC. However, the Oversight Board will not be directly involved but will receive updates on any developments from GCHQ.

3.5 Timely Delivery

The Oversight Board will agree the formalisation of the existing arrangements for code, products and information to be provided by Huawei HQ to HCSEC to ensure that the completion of evaluations are not unnecessarily delayed.

3.6 Escalation / Arbitrator for issues impacting HCSEC

Board members should inform the Oversight Board in a timely manner in the event that an issue arises that could impact the independence, effectiveness, resourcing or the security posture of HCSEC. Under these circumstances the Board may convene an extraordinary meeting.

4. Oversight Board Membership

The Board will initially consist of the following members. Membership will be reviewed annually. The National Security Advisor will appoint the Chair of the Board. Membership with then be via invitation from the Chair.

- GCHQ – Chair (Ciaran Martin, CEO NCSC)
- Huawei HQ – Deputy Chair (Ryan Ding, Executive Director of the Board)
- Huawei UK Managing Director
- Huawei UK Communications Director
- HCSEC Managing Director
- Cabinet Office Director, Cyber Security, National Security Secretariat
- NCSC Technical Director
- Whitehall Departmental representatives: (Deputy Director, Head of Telecoms Security, DCMS, Head of Cyber Policy Hub, Office for Security and Counter Terrorism, Home Office)
- Current CSP representatives: BT CEO Security; Director Group Security, Vodafone

There will be up to 4 CSP representatives at any one time. CSPs are appointed to represent the industry view on an advisory capacity to the board[1]. In the case of an actual or perceived commercial conflict of interest or prospect of commercial advantage the relevant CSP will be expected to recuse themselves from the relevant board discussion. CSPs that do not sit on the Oversight Board will receive regular updates and information from the Secretariat and they can feed in comments and requirements through the Secretariat. The Secretariat will ensure that no information which would be deemed commercially sensitive between CSPs is circulated to the member CSPs. Non-member CSPs may be invited to attend on an ad hoc basis.

5. Meeting Frequency and Topics

It is expected that the Oversight Board will meet three times per year, more frequently if required.

[1] The term 'advisory capacity' is used in relation to the CSP members acting on a personal, industry expert basis rather than representing their companies. They remain full members of the Oversight Board.

- Meeting One – will be to set the high level objectives of HCSEC as relevant to the scope of the Oversight Board, based on CSP contractually confirmed requirements to HCSEC.

- Meeting Two – mid-year will be to assess progress of HCSEC in achieving their objectives

- Meeting Three – end of year will be to assess the delivery of objectives, and to review the findings of the Annual Management Audit and the Technical Competence Review to develop the annual report for the National Security Adviser.

6. Reporting

The Oversight Board will provide an annual report to the National Security Adviser addressing the topics set out at paragraph 3.1. The National Security Adviser will provide copies of this report to the National Security Council and a summary of key points to the Chairman of the Intelligence and Security Committee of Parliament. All reports will be classified according to the sensitivity of their contents and will be distributed at the discretion of the National Security Adviser.

7. Modification to the Oversight Board Terms of Reference (TORs)

The Board's intent is that these Terms of Reference are modified only when absolutely necessary. The following process shall be used to amend the Terms of Reference when necessary:

- Any modification to the Terms of Reference requires a specific topic on the Oversight Board Agenda and must be discussed at a face-to-face meeting.

- The proposed changes and text should be distributed to the OB members at least 7 working days in advance of the meeting;

- The proposed amendment shall be discussed at the Oversight Board meeting and may be amended after all members have reached a consensus.

- The final text of the amendment shall be formally confirmed in writing by all Oversight Board members.

Upon final agreement, updated Terms of Reference will be distributed to all Oversight Board members.

8. Secretariat

GCHQ will provide the secretariat function.

9. Non-Disclosure Obligation

Without prejudice to paragraph 6, all information provided to any Oversight Board Member or third-party (together a "receiving party") in connection with the operation of the Oversight Board shall be treated as confidential information which shall not be copied, distributed or disclosed in any way without the prior written consent of the owner of the information. This obligation shall not apply to any information which was in the public domain at the time of disclosure otherwise than by the breach of a duty of confidentiality. Neither shall it apply to any information which was in the possession of a receiving party without obligation of confidentiality prior to its disclosure to that party. Nor shall it apply to any information which a receiving party received on a non-confidential basis from another person who is not, to the knowledge and belief of the receiving party, subject to any duty not to disclose that information to that party. Nor shall it prevent any receiving party from complying with an order of Court or other legal requirement to disclose information.

Appendix B

Issues raised in the 2016-2017 Audit and current status

The 2017-2018 Audit reviewed progress against addressing the following issue that was highlighted in the 2016-2017 report. The issue was rated as "Low".

iii. Request and Retain Evaluation Plan Sign-Off

The NCSC process was updated to attempt to ensure that the NCSC Technical Director formally signed off the plan in a timely manner. Unfortunately, the finding was repeated in the 2017-2018 audit. The process has been further updated such that the NCSC Technical Director for Telecoms now has delegated authority to sign off the evaluation plan, with an escalation route when necessary.

The two advisory notices were addressed through updating of HCSEC internal processes.

(PS/SP)

From: PS/SP)
Sent: Tuesday, July 31, 2018 12:46 PM
To: (PS/SP); LAURA.RADULOVIC@forces.gc.ca
Subject: RE: MNDO RFI: 2018SO10202 - Info/Reporting on Huawei

Info sent. Thanks!

From: (PS/SP)
Sent: Tuesday, July 31, 2018 12:35 PM
To: LAURA.RADULOVIC@forces.gc.ca
Cc: (PS/SP)
Subject: RE: MNDO RFI: 2018SO10202 - Info/Reporting on Huawei

Yes, no problem, I'll get to send it over.

From: LAURA.RADULOVIC@forces.gc.ca [mailto:LAURA.RADULOVIC@forces.gc.ca]
Sent: Tuesday, July 31, 2018 12:34 PM
To: PS/SP)
Subject: FW: MNDO RFI: 2018SO10202 - Info/Reporting on Huawei

Hi
I'm guessing by Director is being cryptic for a reason. Can you flip me what she's referencing on CTSN?

From: Fleming C@ADM(Pol) D Strat A@Ottawa-Hull
Sent: July-31-18 12:32 PM
To: Radulovic L@ADM(Pol) D Strat A@Ottawa-Hull <LAURA.RADULOVIC@forces.gc.ca>
Subject: Re: MNDO RFI: 2018SO10202 - Info/Reporting on Huawei

Also ask public safety for their background. Aerials. They agreed to send me something.
Tx
Catherine

Sent from my BlackBerry 10 smartphone on the Bell network.

From: Radulovic L@ADM(Pol) D Strat A@Ottawa-Hull
Sent: Tuesday, July 31, 2018 11:03
To: Fleming C@ADM(Pol) D Strat A@Ottawa-Hull
Subject: RE: MNDO RFI: 2018SO10202 - Info/Reporting on Huawei

Ack.

From: Fleming C@ADM(Pol) D Strat A@Ottawa-Hull
Sent: July-31-18 10:54 AM
To: Radulovic L@ADM(Pol) D Strat A@Ottawa-Hull <LAURA.RADULOVIC@forces.gc.ca>
Subject: Fw: MNDO RFI: 2018SO10202 - Info/Reporting on Huawei

Laura - can you check if we have anything on this.

Please also ask [redacted] from CSE who can also provide additional info.
Tx
C
Sent from my BlackBerry 10 smartphone on the Bell network.

From: McCosham DL@ADM(Pol)@Ottawa-Hull <DEBBIE.MCCOSHAM@forces.gc.ca>
Sent: Tuesday, July 31, 2018 10:37
To: Fleming C@ADM(Pol) D Strat A@Ottawa-Hull
Cc: BOUCHER-ROBERTSON J@ADM(Pol) DG Pol Plan@Ottawa-Hull
Subject: FW: MNDO RFI: 2018SO10202 - Info/Reporting on Huawei

Hi Catherine,

MNDO is looking for background information and available reporting (internally or externally generated) on **Huawei**. Do we have any existing backgrounders, report, etc. on the company?

Grateful for any material by **noon on Thursday, August 2nd**.

Thanks,
Debbie

Debbie McCosham | EA ADM(Pol)
Tel: 613-992-1479

From: Seager M@DM DM@Ottawa-Hull
Sent: July-31-18 10:30 AM
To: Gilpin LCdr RT@CFINTCOM@Ottawa-Hull <Robert.Gilpin@forces.gc.ca>; McCosham DL@ADM(Pol)@Ottawa-Hull <DEBBIE.MCCOSHAM@forces.gc.ca>
Cc: Frederickson LCol C@DM DM@Ottawa-Hull <COREY.FREDERICKSON@forces.gc.ca>
Subject: MNDO RFI: 2018SO10202 - Info/Reporting on Huawei

Hi Debbie, Robert,

MNDO is looking for background information and available reporting (internally or externally generated) on Huawei.

Would both ADM Pol and CFINTCOM be able to provide any existing backgrounders, reports etc. on the company? Hard copy is fine.

Timeline: MNDO has asked for the information by COB 2 Aug. Grateful if you could let me know if this is feasible, or if you have any concerns.

Happy to discuss.

Many thanks,
Michelle

Michelle Seager

Special Advisor, Office of the Deputy Minister
Department of National Defence / Government of Canada
michelle.seager@forces.gc.ca / Tel: 613-996-0353 / Cel: 613-790-1124

Conseillère spéciale, Bureau du sous-ministre
Ministère de la défense nationale / Gouvernement du Canada
michelle.seager@forces.gc.ca / Tél: 613-996-0353 / Cel: 613-790-1124

[redacted]

From: [redacted]
Sent: September-19-18 9:55 AM
To: [redacted]
Subject: [redacted]

Classification: SECRET//CANADIAN EYES ONLY

[redacted]

[redacted] (PS/SP)

From: [redacted]
Sent: Wednesday, September 19, 2018 11:03 AM
To: [redacted] (PS/SP)
Cc: [redacted] (PS/SP)
Subject: RE: QP Note - Ottawa launches probe of cyber security - The Globe and Mail
Attachments: approved QP Card - Huawei - ZTE (2).docx

HUAWEI & ZTE

- The Government of Canada takes the security of our country's critical infrastructure very seriously.
- Canadians can be assured that the Communications Security Establishment works to address cyber security concerns to protect Canada's critical infrastructure from threats.
- Since 2013, CSE's Security Review Program has been in place to test and evaluate designated equipment and services considered for use on Canadian 3G and 4G/LTE networks, including Huawei.
- CSE, through the Canadian Centre for Cyber Security, will continue to provide advice and guidance regarding emerging technologies and systems of important to Canada and Canadians.
- Our Government takes security matters extremely seriously and goes to great lengths to ensure the integrity and protection of our facilities and information.

HUAWEI ET ZTE

BACKGROUND

- On June 18, 2018, Senators on the United States Senate intelligence committee warned the federal government and other Five Eyes countries of the risks posed by Chinese smartphone and telecom equipment maker, Huawei. They indicated a desire to see a concerted response among allies, and made reference to the integrated nature of the U.S. and Canadian economies and infrastructures as a concern.

- Previously, former directors of Canada's key security agencies, Ward Elcock, John Adams and Richard Fadden, warned the federal government to cut Canadian ties with Huawei. The warning followed comments made by the heads of the CIA, FBI, National Security Agency and the Defence Intelligence Agency to the U.S. Senate intelligence committee that Huawei poses a cybersecurity threat to American customers.

- The media reported that security officials are particularly concerned that Huawei products in the context of emerging 5G network technologies could provide China with the capacity to conduct remote espionage, modify or steal information, or even shut down systems. John Adams, the former head of the Communications Security Establishment (CSE), was quoted in the article as saying that Huawei has long been a concern to Canadian and U.S. security and intelligence services.

- On May 4, 2018 media reported that the Pentagon banned the sale of Huawei and ZTE phones on military bases. These devices are not currently on sale on Canadian Armed Forces bases.

- On September 7, 2018, media reported that CSE has been testing Huawei's equipment for security vulnerabilities for the last five years. As part of its cyber security mandate, CSE works with telecommunications service providers representing over 99% of Canadian subscribers. In this role, CSE provides advice and guidance to mitigate supply chain risks in telecommunications infrastructures upon which Canadians rely, including, since 2013, a program that has been in place to test and evaluate designated equipment and services (including Huawei) considered for use on Canadian 3G and 4G/LTE networks. CSE accredits third party labs to conduct assurance testing in accordance with requirements outlined by CSE. CSE reviews the testing results and provides tailored advice and guidance to Canada's telecommunications sector. While non-disclosure agreements limit the degree to which CSE can comment on specific details, Canadians can be assured that the Government of Canada is working to make sure that robust protections are in place to safeguard the communications systems that Canadian rely on.

- On September 19, 2018, Media reported on comments made by the Minister of Public Safety, in response to questions about Huawei, were the Minister said that Canada is "examining the issue of security in relation to supply chains right across the government very carefully". The Minister also said that "we have not arrived at those decisions yet, but obviously we are very sensitive to the issue." Media also reported that an official in the Minister's Office indicated that the analysis began well before Australia announced its 5G ban on Huawei and ZTE.

Name of PCO Policy Analyst. Nom de l'analyste du BCP : [redacted]

Secretariat. Secrétariat : Security and Intelligence

Telephone number. Numéro de téléphone [redacted]

(PS/SP)

From: PS/SP)
Sent: Wednesday, September 19, 2018 8:57 AM
To: (PS/SP); PS/SP); (PS/SP)
Cc: PS/SP)
Subject: FW: QP - Tasking: September 19
Attachments: PCO QPN Template.docx; Ministers Blair and Goodale QPN Template.docx; QP Card - Huawei - ZTE.docx; QP Card - Cannabis - Law Enforcement.docx

Importance: High

Please let me know when the English is done so I can send it off to translation

---

From: Johnston, Shannon (PS/SP)
Sent: Wednesday, September 19, 2018 8:47 AM
To: (PS/SP)
Cc: (PS/SP)
Subject: FW: QP - Tasking: September 19
Importance: High

Hi please be ready to send the QP Note to translation when the English is done.

French is due to SADMO by 12:30pm, no wiggle room

Shannon Johnston
NSOD/NCSB
613-990-2733

From: (PS/SP)
Sent: Wednesday, September 19, 2018 8:44 AM
To: (PS/SP)
Cc: Johnston, Shannon (PS/SP); (PS/SP)
Subject: FW: QP - Tasking: September 19
Importance: High

Hi
Please see question from SADMO below regarding the Huawei note.
You'll need to approve the note, if you are drafting one, as I'll have no BB access all morning.
Thanks

From: Murphy, Jeremy (PS/SP)
Sent: Wednesday, September 19, 2018 8:40 AM
To: PS/SP); PS/SP); Stevens, Marcelle (PS/SP); PS/SP)
Cc: (PS/SP); (PS/SP); (PS/SP); (PS/SP); (PS/SP); Davies, John (PS/SP); (PS/SP); (PS/SP); PS.O.NCSB.SADMO Users / Utilisateurs BSMAP.SSCN.O.SP
Subject: QP - Tasking: September 19
Importance: High

Hi team,

Please note that we received the QP below for PCO. This does not need to be translated.

We also received a note from Laura asking if we should be the lead as CSE has also drafted a response to something similar recently. Please let us know as soon as possible if NSOD is in a position to respond.

Due to SADMO by 9:30am

Thank you,

Jeremy Murphy
Tel: 613-991-0241
Email: jeremy.murphy@canada.ca

From: Braun, Laura (PS/SP)
Sent: Wednesday, September 19, 2018 8:33 AM
To: Bardsley, Scott (PS/SP); Bedor, Tia Leigh (PS/SP); Braun, Laura (PS/SP); Brender, James (PS/SP); Butera, Eloge (PS/SP); Carty, Alexis (PS/SP); Champoux, Elizabeth (PS/SP); Christiansen, Calvin (PS/SP); Cirlan, Claudia (PS/SP); Cogan, Tim; Colin.Boyd@cbsa-asfc.gc.ca; Communications Issues Management / Communications Gestion des Enjeux (PS/SP); De Santis, Heather (PS/SP); Desnoyers, Christine; El-Koussaifi, Nicole; Foss, Karen (PS/SP); Girard, Chantal (PS/SP); Gray4, Patrick (PS/SP); Holland, Alyx (FIN); Hurl, David (PS/SP); Iulia.PescarusPopa; joanna.polito@rcmp-grc.gc.ca; Kuschnik, Ellen (PS/SP); Landry Eliane (NHQ-AC); Lauzon, Adam (PS/SP); Malik, Zarah (PS/SP); Marier, Ruth; Mark.Prieur@PBC-CLCC.GC.CA; Martel, Alexandre (PS/SP); Martel, Benoit; McKenzie Presley, Lorraine (PS/SP); McNaughtan, Jennifer (Ext.); Milech, Michael (PS/SP); Morais, Alain (PS/SP); Moreau, Ken (PS/SP); Murayama Anne (NHQ-AC); Nicole.Greenough@cbsa-asfc.gc.ca; Oldham, Craig (PS/SP); PAU-UAP@cbsa-asfc.gc.ca; Pike, Cory (PS/SP); PS.F ADMO-CSCCB / SMA-SSCRC F.SP; PS.F Media Monitoring / surveillance des médias F.SP; PS.O CMB ADMO / SGM BSMA O.SP; PS.O GOC Support / Soutien COG O.SP; PS.O Parliamentary Affairs Division / Unité des Affaires parlementaires O.SP; PS.O.EMPB.ADMO Users / Utilisateurs BSMA.SGUP.O.SP; PS.O.NCSB.SADMO Users / Utilisateurs BSMAP.SSCN.O.SP; PS.O.PACB.ADMO Users / Utilisateurs BSMA.SAPC.O.SP; Sabourin2, Alexandre (PS/SP); Sayarh, Omar (PS/SP); Showell, David (Ext.); Templeton2, Kasinee (PS/SP); Tremblay4, Guylaine (PS/SP); Vallières, Marc (PS/SP); Wilson, Ashleigh (PS/SP)
Cc: Templeton2, Kasinee (PS/SP); Gray4, Patrick (PS/SP); Braun, Laura (PS/SP)
Subject: QP Tasking: September 19

Good morning!

****Reminder:** If you determine that a QPN is tasked to the wrong organization, please advise Parliamentary Affairs immediately****

Please confirm receipt if you are tasked below.

Minister of Public Safety and Emergency Preparedness*

- CBSA -Fraud files https://www.scmp.com/news/world/united-states-canada/article/2164782/revealed-how-canada-border-agency-tried-conceal

Minister of Border Security and Organized Crime Reduction*

- NIL

Please ensure that the proposed speaking points reflect any recent media lines or recent comments by the Ministers on the issue. Please work with Communications as required

*Please use the Ministers Blair and Goodale QPN template. The format has changed with the new Proactive Disclosure requirements that will likely come into force this fall.

FIRM DEADLINE FOR ADM/EQUIVALENT APPROVED QPN – 9:45am (English note and French bullets) 12:30pm (French Backgrounder)

PCO (for the Prime Minister)**

- CSIS - Abdelrazik (https://www.thestar.com/news/canada/2018/09/18/judge-orders-indefinite-delay-in-csis-compensation-trial-orders-crown-to-pay-legal-costs.html)
- NCSB - Huawei (https://www.theglobeandmail.com/politics/article-ottawa-launches-probe-of-cyber-security/) (Update)
- CSCCB - Cannabis Enforcement (https://nationalpost.com/news/politics/canadian-police-forces-hold-off-on-ordering-the-only-device-approved-to-test-saliva-for-thc) (Update)

**Please use PCO QPN template.

****FIRM DEADLINE FOR ADM/EQUIVALENT APPROVED QPN – 9:45am (English note, French, if available)****

Please ensure your submissions are sent to Patrick Gray, Kasinee Templeton and myself.

Thank you very much,

Laura

Laura Braun
Senior Manager, Parliamentary Affairs / Gestionnaire principale, Affaires parlementaires
Public Safety Canada / Sécurité publique Canada
Tel/Tél: (613) 949-9737
Email/Courriel: laura.braun@canada.ca

HUAWEI & ZTE

- The Government of Canada takes the security of our country's critical infrastructure very seriously.
- Canadians can be assured that the Communications Security Establishment works to address cyber security concerns to protect Canada's critical infrastructure from threats.
- Since 2013, CSE's Security Review Program has been in place to test and evaluate designated equipment and services considered for use on Canadian 3G and 4G/LTE networks, including Huawei.
- CSE, through the Canadian Centre for Cyber Security, will continue to provide advice and guidance regarding emerging technologies and systems of important to Canada and Canadians.
- Our Government takes security matters extremely seriously and goes to great lengths to ensure the integrity and protection of our facilities and information.

HUAWEI ET ZTE

- Le gouvernement prend la sécurité de ses infrastructures essentielles très au sérieux.

- Les Canadiens peuvent être certains que le Centre de la sécurité des télécommunications travaille en vue d'éliminer les préoccupations en matière de cybersécurité afin de protéger les infrastructures essentielles du Canada contre toute menace.

- Depuis 2013, le Programme d'examen de la sécurité du CSTC est en place afin de tester et d'évaluer l'équipement et les services qu'on envisage utiliser sur les réseaux canadiens 3G et 4G/LTE, y compris Huawei.

- Par l'entremise du Centre canadien pour la cybersécurité, le CSTC continuera de fournir des avis et des conseils concernant les technologies et systèmes en émergence qui sont importants pour le Canada et les Canadiens.

- Notre gouvernement prend les questions liées à la sécurité très au sérieux et ne ménage aucun effort pour assurer l'intégrité et la protection de nos installations et de l'information.

BACKGROUND

- On June 18, 2018, Senators on the United States Senate intelligence committee warned the federal government and other Five Eyes countries of the risks posed by Chinese smartphone and telecom equipment maker, Huawei. They indicated a desire to see a concerted response among allies, and made reference to the integrated nature of the U.S. and Canadian economies and infrastructures as a concern.

- Previously, former directors of Canada's key security agencies, Ward Elcock, John Adams and Richard Fadden, warned the federal government to cut Canadian ties with Huawei. The warning followed comments made by the heads of the CIA, FBI, National Security Agency and the Defence Intelligence Agency to the U.S. Senate intelligence committee that Huawei poses a cybersecurity threat to American customers.

- The media reported that security officials are particularly concerned that Huawei products in the context of emerging 5G network technologies could provide China with the capacity to conduct remote espionage, modify or steal information, or even shut down systems. John Adams, the former head of the Communications Security Establishment (CSE), was quoted in the article as saying that Huawei has long been a concern to Canadian and U.S. security and intelligence services.

- On May 4, 2018 media reported that the Pentagon banned the sale of Huawei and ZTE phones on military bases. These devices are not currently on sale on Canadian Armed Forces bases.

- On September 7, 2018, media reported that CSE has been testing Huawei's equipment for security vulnerabilities for the last five years. As part of its cyber security mandate, CSE works with telecommunications service providers representing over 99% of Canadian subscribers. In this role, CSE provides advice and guidance to mitigate supply chain risks in telecommunications infrastructures upon which Canadians rely, including, since 2013, a program that has been in place to test and evaluate designated equipment and services (including Huawei) considered for use on Canadian 3G and 4G/LTE networks. CSE accredits third party labs to conduct assurance testing in accordance with requirements outlined by CSE. CSE reviews the testing results and provides tailored advice and guidance to Canada's telecommunications sector. While non-disclosure agreements limit the degree to which CSE can comment on specific details, Canadians can be assured that the Government of Canada is working to make sure that robust protections are in place to safeguard the communications systems that Canadian rely on.

Name of PCO Policy Analyst. Nom de l'analyste du BCP : [redacted] Marcoux

Secretariat. Secrétariat : Security and Intelligence

Telephone number. Numéro de téléphone : [redacted]

11/23/2018 11:07

[redacted]

From: [redacted]@cse-cst.gc.ca>
Sent: August-01-18 9:48 AM
To: [redacted]
Subject: RE: [redacted] Meeting

Classification: SECRET//CANADIAN EYES ONLY

Hi [redacted]

[redacted] let's touch bae again in September and I can update you on the progress.

Thanks,

[redacted]

From: [redacted] [mailto: [redacted]
Sent: August-01-18 8:34 AM
To: [redacted]
Cc: [redacted] (PSEPC-SPPCC)
Subject: RE: [redacted] Meeting

Classification: SECRET//CANADIAN EYES ONLY

Hi [redacted]

I just touching base on the information noted below – would it happen to be available?

Thanks,
[redacted]

From: [redacted] [mailto: [redacted]@cse-cst.gc.ca]
Sent: June-25-18 9:09 AM
To: [redacted]
Subject: RE: [redacted] Meeting

Classification: SECRET//CANADIAN EYES ONLY

HI

when it is complete I will see about having it extracted and shared via reporting channels.

From: mailto:
Sent: June-22-18 10:44 AM
To:
Subject: RE: Meeting

Classification: SECRET//CANADIAN EYES ONLY

Yes, that I do have.

From: mailto: @cse-cst.gc.ca]
Sent: June-22-18 10:44 AM
To:
Subject: RE:

Classification: SECRET//CANADIAN EYES ONLY

Do you have a account?

From: [mailto: @ps-sp.gc.ic.ca]
Sent: June-22-18 10:43 AM
To:
Subject: RE: Meeting

Classification: SECRET//CANADIAN EYES ONLY

Hi – no worries. Unfortunately, we do not have

From: [mailto @cse-cst.gc.ca]
Sent: June-22-18 10:41 AM
To:
Subject: RE: Meeting

Classification: SECRET//CANADIAN EYES ONLY

Hi

Sorry for the delay, do you have

From: [redacted] mailto: [redacted]
Sent: June-19-18 12:09 PM
To: [redacted]
Cc: [redacted] (PSEPC-SPPCC)
Subject: RE: [redacted] Meeting

Classification: SECRET//CANADIAN EYES ONLY

Hi [redacted]

I just wanted to follow up on any information you may have on [redacted] Are you able to share any information on that with us?

We would also be happy to come to CSE to talk about this further with you. Please let us know if that works and we can schedule a time.

Thank you,
[redacted]

From: [redacted] [mailto: [redacted]@cse-cst.gc.ca]
Sent: June-13-18 9:07 AM
To: [redacted] (CSE-CST)
Cc: [redacted] CSE-CST); [redacted] CSE-CST)
Subject: RE: [redacted] Meeting

Classification: SECRET//CANADIAN EYES ONLY

Hi [redacted]

[redacted]

I would be happy to support the discussions and provide input once the project has reached that stage, as well as support the overall review.

Thank you,

[redacted]

From: [redacted] [mailto: [redacted]
Sent: June-13-18 8:37 AM
To: [redacted]
Cc: [redacted]
Subject: [redacted] Meeting

Classification: SECRET//CANADIAN EYES ONLY

Hi All,

Just checking in to confirm that you are still available to attend the meeting today at 11am. Let me know.

Thanks!

National Security Operations Directorate – Direction générale des opérations de la sécurité nationale
Public Safety and Emergency Preparedness Canada – Sécurité publique et Protection civile Canada
Tel. – Tél.:

[redacted]

From: [redacted]
Sent: June-20-18 12:19 PM
To: [redacted]
Subject: RE: [redacted]

Classification: SECRET//CANADIAN EYES ONLY

[redacted] I've already done research on it - [redacted] ;) – that you can leverage.

From: [redacted]
Sent: June-20-18 12:07 PM
To: [redacted]
Cc: [redacted]
Subject: [redacted]

Classification: SECRET//CANADIAN EYES ONLY

Hey [redacted]

If you're not too busy, do you think you could do some research on the [redacted] (not sure I spelled that right...) and write up a little blurb about it? I'm thinking about adding a piece to the [redacted]

Let me know if that works for you!
Thanks,

[redacted]
National Security Operations Directorate – Direction générale des opérations de la sécurité nationale
Public Safety and Emergency Preparedness Canada – Sécurité publique et Protection civile Canada
Tel. – Tél. [redacted]

[redacted]

From: [redacted]
Sent: June-20-18 1:52 PM
To: [redacted]
Subject: RE: [redacted]

S.15
S.20
& S.16

Classification: SECRET//CANADIAN EYES ONLY

Thanks!

From: [redacted]
Sent: June-20-18 1:52 PM
To: [redacted]
Subject: RE: [redacted]

Classification: SECRET//CANADIAN EYES ONLY

Ok will do

From: [redacted]
Sent: June-20-18 1:48 PM
To: [redacted]
Subject: RE: [redacted]

Classification: SECRET//CANADIAN EYES ONLY

Just a paragraph is good.
Only need a high level blurb to lead into it being a potential option for Canada.

From: [redacted]
Sent: June-20-18 1:37 PM
To: [redacted]
Subject: RE: [redacted]

Classification: SECRET//CANADIAN EYES ONLY

Haha yeah, I'm kinda of familiar with what it is.

I'll put something together. Do you just want like a paragraph or...?

From: [redacted]
Sent: June-20-18 12:19 PM
To: [redacted]

Cc:
Subject: RE:

Classification: SECRET//CANADIAN EYES ONLY

Excellent, thanks!!

From:
Sent: June-20-18 12:19 PM
To:
Subject: RE:

Classification: SECRET//CANADIAN EYES ONLY

I've already done research on it - ;) – that you can leverage.

From:
Sent: June-20-18 12:07 PM
To:
Cc:
Subject:

Classification: SECRET//CANADIAN EYES ONLY

Hey

If you're not too busy, do you think you could do some research on the (not sure I spelled that right...) and write up a little blurb about it?

Let me know if that works for you!
Thanks,

National Security Operations Directorate – Direction générale des opérations de la sécurité nationale
Public Safety and Emergency Preparedness Canada – Sécurité publique et Protection civile Canada
Tel. – Tél.:

(PS/SP)

From: (PS/SP)
Sent: Wednesday, June 06, 2018 9:51 AM
To:
Subject: RE: Discussion on Assessment

It is. I sent a more detailed email on the other system.

From: [mailto: @CSE-CST.GC.CA]
Sent: Wednesday, June 06, 2018 9:48 AM
To: (PS/SP)
Subject: RE: Discussion on Assessment

Classification: UNCLASSIFIED

Is this about the discussion?

-----Original Appointment-----
From: (PS/SP) [mailto: @canada.ca]
Sent: June-06-18 9:07 AM
To:
PS/SP); (PS/SP); Jenny.Chilton@international.gc.ca; Aiden.Commisso@international.gc.ca; CORI.ANDERSON@forces.gc.ca; SHANNON.PARTRIDGE@forces.gc.ca
Subject: Discussion on Assessment
When: June-13-18 11:00 AM-12:00 PM (UTC-05:00) Eastern Time (US & Canada).
Where: 340 Laurier - 11th Floor Boardroom

From:
Sent: June-13-18 9:09 AM
To:
Cc:
Subject: FW: Meeting

Classification: SECRET//CANADIAN EYES ONLY

Hi

See below -
I think we may need to have a discussion with CSE. This paper cannot go forward without their input at nearly all stages of the development.

Thanks,

From: [mailto: @cse-cst.gc.ca]
Sent: June-13-18 9:07 AM
To: CSE-CST)
Cc: CSE-CST); (CSE-CST)
Subject: RE: Meeting

Classification: SECRET//CANADIAN EYES ONLY

Hi

I would be happy to support the discussions and provide input once the project has reached that stage, as well as support the overall review.

Thank you,

From: mailto:
Sent: June-13-18 8:37 AM

To: [redacted]
Cc: [redacted]
Subject: [redacted] Meeting

Classification: SECRET//CANADIAN EYES ONLY

Hi All,

Just checking in to confirm that you are still available to attend the meeting today at 11am. Let me know.

Thanks!

[redacted]
National Security Operations Directorate – Direction générale des opérations de la sécurité nationale
Public Safety and Emergency Preparedness Canada – Sécurité publique et Protection civile Canada
Tel. – Tél.: [redacted]

[redacted] (PS/SP)

From: [redacted] (PS/SP)
Sent: Friday, June 15, 2018 1:51 PM
To: Levert, Jean-Philippe (PS/SP)
Cc: Martel, Karine (PS/SP); Grenier, Julie (PS/SP); [redacted] (PS/SP)
Subject: RE: MO Request: U.S. Congressional Concerns about Huawei in Canada

Me again!

For this request, you want to connect with CSE (or advise MO to reach out to CSE as well as CSIS). A few weeks ago CSE (Ryan Foreman, Sr Comms Advisor - [redacted]@CSE-CST.GC.CA) shared a statement they issued May 4th. Might be helpful context in preparing a response with consistent language about Huawei.

[redacted]

****

CSE Statement – 4 May 2018

The Government of Canada takes the security of Canada's critical infrastructure very seriously. The Communications Security Establishment (CSE) provides the Government of Canada with advice and guidance on all aspects of information technology security. CSE addresses a full range of cyber threats, including any supply chain threats posed by telecommunications equipment and service providers.

To address risks posed by supply chain threats, CSE collaborates with Canadian telecommunications service providers through the Canadian Security Telecommunications Advisory Committee (CSTAC) and by working with equipment vendors. Through this partnership between government and industry, supply chain threats are mitigated by measures taken by telecommunications service providers and equipment manufacturers that are part of the Canadian supply chain. In addition, CSE works with its partners at Public Safety Canada to share security advice and guidance with the private sector owners and operators of Canada's critical infrastructures.

While we are unable to comment on specific companies, products or service providers, Canadians can be assured that the Government of Canada is working to make sure the strongest protections are in place to safeguard the systems Canadians rely on.

From: Levert, Jean-Philippe (PS/SP)
Sent: Friday, June 15, 2018 1:33 PM
To: [redacted] (PS/SP); [redacted] (PS/SP)
Cc: Martel, Karine (PS/SP); Grenier, Julie (PS/SP)
Subject: MO Request: U.S. Congressional Concerns about Huawei in Canada

Hi [redacted]

The Globe is asking for a reaction from MO about comments by US Senators that NSA needs to better convey the threat Huawei poses to its allies, including Canada.

While MO will note that they "cannot provide details on specific companies, products or providers", MO's wondering if we could propose any lines on how the US shares information on threats related to this line of questioning.

FYI, MO also sent this request to CSIS.

Would you or someone in your team be able to advise?

Happy to discuss.

Thanks,

JP Levert

From: [redacted] [mailto: [redacted]@globeandmail.com]
Sent: Friday, June 15, 2018 10:29 AM
To: Bardsley, Scott (PS/SP)
Cc: [redacted]
Subject: U.S. Congressional Concerns about Huawei in Canada

Hi Scott. I am CC-ing [redacted] on this email.
We are writing you to ask you for comment.
Our deadline is 4:30 pm which is 6 hours from now.
We have been discussing Huawei's activities in Canada with members of the U.S. Congress who are members of the Senate Intelligence Committee.
As you know we have written about the concerns raised three former directors of Canada's key national security agencies Ward Elcock, John Adams and Richard Fadden -- who are urging the federal government to heed the warnings of U.S. intelligence services and cut Canadian ties with Huawei, the giant Chinese smartphone and telecom equipment maker. And we have written about how Huawei has established a vast network of relationships with leading research-heavy universities in Canada to create a steady pipeline of intellectual property that the company is using to underpin its market position in 5G technology.
Members of the U.S. Senate Intelligence community are telling us that the threat posed by Huawei requires a concerned response by the U.S. and its allies.
Among them, one member of the Senate committee said he does not believe the U.S.' allies understand the degree of the threat posed by Huawei and that he has urged the NSA to convey concerns about Huaewi and ZTE to Five Eyes allies.
They are saying the significant U.S. presence in Canada – government, corporate, and citizens –and the vulnerabilities telecom equipment and infrastructure can present, should underscore that concern, as does China's use of coercion, forced cooperation, and cooption to acquire sensitive technologies.
We are asking you to comment on whether Huawei in Canada represents the threat that the American lawmakers consider it to be.
Thanks

[redacted]**@globeandmail.com**
[redacted]**@globeandmail.com**

S. 21

From:
Sent: July-23-18 11:52 AM
To:
Subject: RE: UK Huawei ANNUAL REPORT 2018

S. 20

S. 16

Classification: CONFIDENTIAL

I tasked on Friday with a one pager (bullets) to note some salient points ☺

From:
Sent: July-23-18 11:48 AM
To:
Subject: FW: UK Huawei ANNUAL REPORT 2018

Classification: CONFIDENTIAL

FYI.

From:
Sent: July-23-18 11:12 AM
To:
Cc: Waters, Michael
Subject: FW: UK Huawei ANNUAL REPORT 2018

Classification: CONFIDENTIAL

Tel que discuté.

From: Waters, Michael
Sent: July-23-18 10:27 AM
To:
Cc: Mahu, Vlad
Subject: UK Huawei ANNUAL REPORT 2018

Classification: CONFIDENTIAL

Hi

Do you know who is working on ICA? I think that they should be made aware of the email below and report attached.

Regards,
Michael

Michael Waters
Manager / Gestionnaire
National Cyber Security Directorate / Direction de la cyber-sécurité nationale
Public Safety Canada / Sécurity public Canada
Tel/Tél: 613-991-1634
Mobile: 613-796-4286
Email/courriel: Michael.Waters@canada.ca
CTSN:

From: Waters, Michael
Sent: July-23-18 10:05 AM
To: Bunghardt, Gregory; Hashem, Mohsen; Frigon, Sylvie; Hartley, William; Park, Beom-Jun; Merchant, Colleen; Binne, Christine; Ouellet, Benoit; Brydges, Lucas; Goldfinger, Marc; Gauthier, Darren; Hamilton, Sharon; Bendelier, Kenneth; (CSE-CST); (CSE-CST)
Subject: UK Huawei ANNUAL REPORT 2018

Classification: CONFIDENTIAL

Colleagues,

See report attached.

Regards,
Michael

Michael Waters
Manager / Gestionnaire
National Cyber Security Directorate / Direction de la cyber-sécurité nationale
Public Safety Canada / Sécurity public Canada
Tel/Tél: 613-991-1634
Mobile: 613-796-4286
Email/courriel: Michael.Waters@canada.ca
CTSN:

From: NCSCCAP GBR GOV (GCHQ) [mailto gchq.ic.gov.uk]
Sent: July-22-18 6:05 AM
To: Waters, Michael;

[redacted]

Subject: PUBLICATION OF HCSEC ANNUAL REPORT 2018

CLASSIFICATION: UK OFFICIAL

All,

[redacted] and as you may already be aware, the fourth Huawei Cyber Security Evaluation Centred Oversight Board Annual Report (attached) was published on 19th July 2018 on the www.gov.uk website (where the previous three year reports can be found if you search for HCSEC annual report).

[redacted]

If you have any questions please do not hesitate to contact me.

[redacted]
NCSC Telecoms Security Relationship Manager
A2G
Rus: [redacted]
Nsec: [redacted]
Work Mobile: [redacted]
Low side email: [redacted]@ncsc.gov.uk

Pages 215 to / à 218

are duplicates

sont des duplicatas

From:
Sent: July-23-18 11:12 AM
To:
Cc: Waters, Michael
Subject: FW: UK Huawei ANNUAL REPORT 2018
Attachments: HCSEC OB ANNUAL REPORT 2018.pdf

Classification: CONFIDENTIAL

Tel que discuté.

From: Waters, Michael
Sent: July-23-18 10:27 AM
To:
Cc: Mahu, Vlad
Subject: UK Huawei ANNUAL REPORT 2018

Classification: CONFIDENTIAL

Hi

Do you know who is working on ICA? I think that they should be made aware of the email below and report attached.

Regards,
Michael

Michael Waters
Manager / Gestionnaire
National Cyber Security Directorate / Direction de la cyber-sécurité nationale
Public Safety Canada / Sécurity public Canada
Tel/Tél: 613-991-1634
Mobile: 613-796-4286
Email/courriel: Michael.Waters@canada.ca
CTSN

From: Waters, Michael
Sent: July-23-18 10:05 AM
To: Bunghardt, Gregory; Hashem, Mohsen; Frigon, Sylvie; Hartley, William; Park, Beom-Jun; Merchant, Colleen; Binne, Christine; Ouellet, Benoit; Brydges, Lucas; Goldfinger, Marc; Gauthier, Darren; Hamilton, Sharon; Bendelier, Kenneth; (CSE-CST); (CSE-CST)
Subject: UK Huawei ANNUAL REPORT 2018

Classification: CONFIDENTIAL

Colleagues,

[redacted]

See report attached.

Regards,
Michael

Michael Waters
Manager / Gestionnaire
National Cyber Security Directorate / Direction de la cyber-sécurité nationale
Public Safety Canada / Sécurity public Canada
Tel/Tél: 613-991-1634
Mobile: 613-796-4286
Email/courriel: Michael.Waters@canada.ca
CTSN: [redacted]

From: [redacted] NCSCCAP GBR GOV (GCHQ) [mailto: [redacted]
Sent: July-22-18 6:05 AM
To: [redacted] Waters, Michael; [redacted]
Subject: PUBLICATION OF HCSEC ANNUAL REPORT 2018

CLASSIFICATION: UK OFFICIAL

All,

[redacted] and as you may already be aware, the fourth Huawei Cyber Security Evaluation Centred Oversight Board Annual Report (attached) was published on 19th July 2018 on the www.gov.uk website (where the previous three year reports can be found if you search for HCSEC annual report).

[redacted]

[redacted]

If you have any questions please do not hesitate to contact me.

[redacted]
NCSC Telecoms Security Relationship Manager
[redacted]
Rus: [redacted]
Nsec: [redacted]
Work Mobile: [redacted]
Low side email: [redacted]@ncsc.gov.uk

Pages 222 to / à 255

are duplicates

sont des duplicatas

[redacted]

From: [redacted]
Sent: August-17-18 2:02 PM
To: [redacted]
Cc:
Subject: Tasking: Lessons Learned
Attachments: Lessons Learned - TEMPLATE.DOCX

Classification: SECRET//CANADIAN EYES ONLY

Hello All,

As you know, each of the cases we have conducted has had its share of, shall we say, 'learning experiences'. We would like to capture those lessons so we can (hopefully) address them in the future. To start, we have assigned a few of the key transactions to the following people:

[redacted]

The template is attached. If you could complete a first draft by Wednesday, that would be great! I will set up a time that we can all get together and talk it out. If you need guidance, feel free to come chat. Drafts can be saved here: LESSONS LEARNED

Other ones that we will assign later are as follows:

[redacted]

Please know you are not expected to know everything about the transaction. If you can only complete some parts, that is okay. You can also come speak with me before the meeting on Wednesday to chat the content if you would like.

Thanks!

[redacted]
National Security Operations Directorate – Direction générale des opérations de la sécurité nationale
Public Safety and Emergency Preparedness Canada – Sécurité publique et Protection civile Canada
Tel. – Tél.: [redacted]

Lessons Learned: (TRANSACTION)	
Title	
Issue	
Period Covered	Received: Cleared:
Date of Report	
Background	Lead: Country of Foreign Investor: Triggers: Sectors:
Summary	
Analysis of process	-
Lessons Learned	
Results	
Recommendations	

[redacted]

From: [redacted]
Sent: September-13-18 9:59 AM
To: [redacted]
Subject: Draft DRC Minutes

Classification: SECRET//CANADIAN EYES ONLY

Hello [redacted]

Attached are the minutes from this week's DRC. Please let me know if you require any changes!

Thanks,

[redacted]

Meeting Minutes
- DRC Septembe...

Page 260

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Page 261

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Page 262

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Page 263

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

[redacted]

From: [redacted]
Sent: September-13-18 10:44 AM
To: [redacted]
Subject: Summary of Cases
Attachments: Summary of ICA Cases.xlsx

Classification: SECRET//CANADIAN EYES ONLY

Here is the document I've been working on.

Let me know what you think!

[redacted]

Pages 265 to / à 266

are withheld pursuant to sections

sont retenues en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

[redacted]

From: [redacted]
Sent: September-13-18 10:45 AM
To: [redacted] (CSE-CST); Gordon, Eric (RCMP-GRC); Gumley, Matthew (RCMP-GRC); Burns, Genevieve (RCMP-GRC); Anderson, Cori C - Civ (DND-MDN); Partridge, Shannon SK (DND-MDN); [redacted] (INTERNATIONAL); [redacted] (INTERNATIONAL); [redacted] (PCO) (PCO-BCP); Richard, Daniel (PWGSC-TPSGC); 'jpherne@pwgsc-tpsgc.gc.ca'; Burke, Mary (ISED); Dewolfe, Jonathan (ISED); Kack, Shannon (ISED); Tarantino, Maria (ISED); Keating, Sean (ISED); Burrell, Christopher (ISED); [redacted] (INTERNATIONAL); [redacted] (INTERNATIONAL); [redacted] (INTERNATIONAL); [redacted] Best, Emma (RCMP-GRC); [redacted] Faucher, Monique (NRCAN-RNCAN); Karman, Mehmet (ISED)
Cc: [redacted]
Subject: Meeting Minutes - September 11 DRC

Classification: SECRET//CANADIAN EYES ONLY
ICA Protected

Joel/Daniel (PSPC) – please provide copies to: Pascal Girard, Antoine Parker, Jennifer Mercer, Peter Au, Louis Bedard, Holly Wilton, Sara Chaar and Joelle El-Khatib.
Irina/Monique (NRCAN) – Please provide to: Michael Brown
GAC – Please circulate as required

Good morning,

Attached are the meeting minutes for the September 11th DRC.

Thanks,

[redacted]

Meeting Minutes - DRC Septembe...

Page 268

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Page 269

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Page 270

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Page 271

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

[redacted]

From: [redacted]
Sent: September-13-18 3:41 PM
To: [redacted] (CSE-CST); Gordon, Eric (RCMP-GRC); Gumley, Matthew (RCMP-GRC); Burns, Genevieve (RCMP-GRC); Anderson, Cori C - Civ (DND-MDN); Partridge, Shannon SK (DND-MDN); [redacted] (INTERNATIONAL); [redacted] (INTERNATIONAL); [redacted] (PCO) (PCO-BCP); Richard, Daniel (PWGSC-TPSGC); [redacted] Burke, Mary (ISED); Dewolfe, Jonathan (ISED); Kack, Shannon (ISED); Tarantino, Maria (ISED); Keating, Sean (ISED); Burrell, Christopher (ISED); [redacted] (INTERNATIONAL); [redacted] INTERNATIONAL); [redacted] (INTERNATIONAL); [redacted] Best, Emma (RCMP-GRC); [redacted] Faucher, Monique (NRCAN-RNCAN); Karman, Mehmet (ISED)
Cc: [redacted]
Subject: Revised Meeting Minutes - September 11 DRC

Classification: SECRET//CANADIAN EYES ONLY
ICA Protected

Joel/Daniel (PSPC) – please provide copies to: Pascal Girard, Antoine Parker, Jennifer Mercer, Peter Au, Louis Bedard, Holly Wilton, Sara Chaar, and Joelle El-Khatib
Irina/Monique (NRCAN) – please provide to: Michael Brown
GAC – please circulate as required

Good afternoon,

Attached are the revised meeting minutes for the September 11th DRC.

[redacted]

Meeting Minutes - DRC Septembe...

Page 273

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Page 274

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Page 275

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Page 276

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

[redacted]

From: [redacted]
Sent: September-13-18 3:55 PM
To: [redacted]
Cc:
Subject: RE: Tasking: Lessons Learned

Classification: SECRET//CANADIAN EYES ONLY

I have a good draft on [redacted] I want to consult with [redacted] (similar outcomes – and I presume lessons learned) upon her return.

From: [redacted]
Sent: September-13-18 3:48 PM
To: [redacted]
Cc:
Subject: RE: Tasking: Lessons Learned

Classification: SECRET//CANADIAN EYES ONLY

Hi all –

Could you provide an update on where we stand with the lessons learned documents? How many have we completed so far?

[redacted]

From: [redacted]
Sent: August-17-18 2:02 PM
To: [redacted]
Cc:
Subject: Tasking: Lessons Learned

Classification: SECRET//CANADIAN EYES ONLY

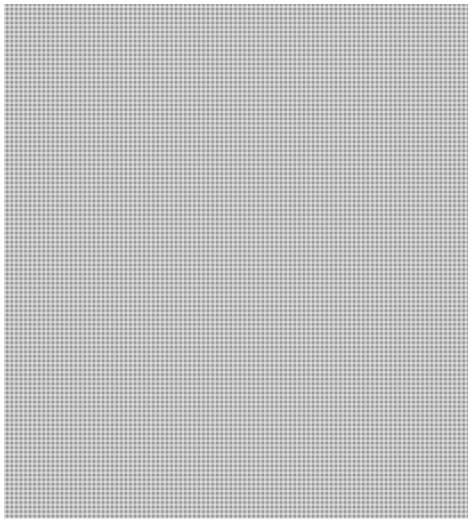
Hello All,

As you know, each of the cases we have conducted has had its share of, shall we say, 'learning experiences'. We would like to capture those lessons so we can (hopefully) address them in the future. To start, we have assigned a few of the key transactions to the following people:

[redacted]

The template is attached. If you could complete a first draft by Wednesday, that would be great! I will set up a time that we can all get together and talk it out. If you need guidance, feel free to come chat. Drafts can be saved here: LESSONS LEARNED

Other ones that we will assign later are as follows:



Please know you are not expected to know everything about the transaction. If you can only complete some parts, that is okay. You can also come speak with me before the meeting on Wednesday to chat the content if you would like.

Thanks!

National Security Operations Directorate – Direction générale des opérations de la sécurité nationale
Public Safety and Emergency Preparedness Canada – Sécurité publique et Protection civile Canada
Tel. – Tél.:

[redacted]

From: [redacted]
Sent: September-13-18 4:12 PM
To: [redacted]
Cc:
Subject: RE: Tasking: Lessons Learned

Classification: SECRET//CANADIAN EYES ONLY

I have taken the [redacted] document as far as I can without input from [redacted] and/or [redacted] Although it was at the very beginning of her tenure on the ICA file, [redacted] may also remember aspects of the case that I haven't captured.

From: [redacted]
Sent: September-13-18 3:48 PM
To: [redacted]
Cc:
Subject: RE: Tasking: Lessons Learned

Classification: SECRET//CANADIAN EYES ONLY

Hi all –

Could you provide an update on where we stand with the lessons learned documents? How many have we completed so far?

[redacted]

From: [redacted]
Sent: August-17-18 2:02 PM
To: [redacted]
Cc:
Subject: Tasking: Lessons Learned

Classification: SECRET//CANADIAN EYES ONLY

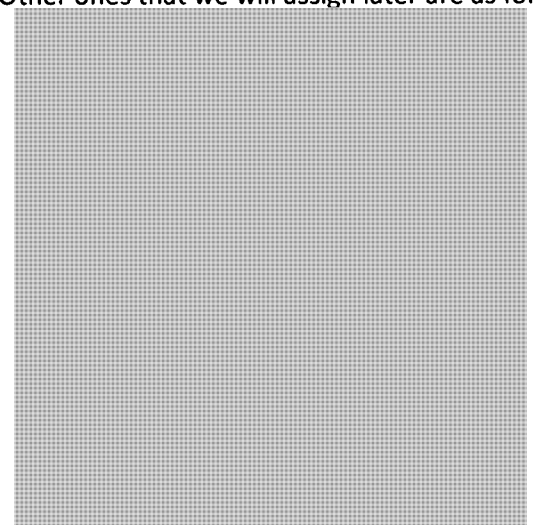
Hello All,

As you know, each of the cases we have conducted has had its share of, shall we say, 'learning experiences'. We would like to capture those lessons so we can (hopefully) address them in the future. To start, we have assigned a few of the key transactions to the following people:

[redacted]

The template is attached. If you could complete a first draft by Wednesday, that would be great! I will set up a time that we can all get together and talk it out. If you need guidance, feel free to come chat. Drafts can be saved here: LESSONS LEARNED

Other ones that we will assign later are as follows:



Please know you are not expected to know everything about the transaction. If you can only complete some parts, that is okay. You can also come speak with me before the meeting on Wednesday to chat the content if you would like.

Thanks!

National Security Operations Directorate – Direction générale des opérations de la sécurité nationale
Public Safety and Emergency Preparedness Canada – Sécurité publique et Protection civile Canada
Tel. – Tél.:

[redacted] (PS/SP)

From: [redacted] (PS/SP)
Sent: Thursday, September 27, 2018 11:36 AM
To: [redacted] (PS/SP)
Cc: [redacted] (PS/SP)
Subject: Update QP Note - Huawei
Attachments: ICA Morning Media Update; PS-SP-#2650846-R-QPN_-_Investments_in_Telecommunications_Sector_-_ICA.DOCX.DRF

Hi [redacted]

For Monday, could you update the background section (under "Canadian response") of the QP note on Huawei? We are limited to a page, so we might have to do some creative editing.

In today's ICA morning media update, there's mention of Scott Jones commenting publicly on Huawei during a parliamentary committee. The article might give you enough context to update the background section. But can you also get the transcript? You can look online and/or ask Communications (ps.pspmediacentre-centredesmediaspsp.sp@canada.ca) if they have it.

Thanks,
[redacted]

[redacted]
A/Manager | Gestionnaire par intérim
Public Safety Canada | Sécurité publique Canada
Telephone | Téléphone [redacted]
E-mail | Courriel [redacted]@canada.ca

Pages 282 to / à 284

are duplicates

sont des duplicatas

[redacted]

From: [redacted]
Sent: October-25-18 10:10 AM
To: [redacted]
Cc:
Subject: Lessons Learned

Classification: SECRET//CANADIAN EYES ONLY

Hi All,

There has been a renewed interested in the Lessons Learned overviews. We still have a few cases outstanding that we should do a document for:

[redacted]

Some of these [redacted] will be quite short but we should have something on paper to support the TF work. If you have downtime, could you please identify which transaction(s) you would like to draft and maybe aim to have something for late next week to discuss?

Please save everything here: Lessons Learned

Thanks!

[redacted]
National Security Operations Directorate – Direction générale des opérations de la sécurité nationale
Public Safety and Emergency Preparedness Canada – Sécurité publique et Protection civile Canada
Tel. – Tél.: [redacted]

From:
Sent: November-07-18 10:10 AM
To: (PCO) (PCO-BCP); Ortis, Cameron (RCMP-GRC); Herne, Joel (PWGSC-TPSGC); Richard, Daniel (PWGSC-TPSGC); (INTERNATIONAL); Anderson, Cori C - Civ (DND-MDN); Burke, Mary (ISED); (CSÉ-CST); (CSE-CST); Gordon, Eric (RCMP-GRC); 'Brown, Michael W'; Kack, Shannon (ISED)
Cc:
Subject: DG ESMC - November 1, 2018 - Record of Decision
Attachments: DG ESMC - November 1 - RoD.docx

Classification: SECRET//CANADIAN EYES ONLY

Daniel/Joel (PSPC): Please provide to Pascal Girard and Antoine Parker
Brandon (GAC): Please provide to Emmanuel Kamarianakis, Rouben Khatchadourian and Martin Benjamin.
Michael (NRCAN): Please provide to Drew Leyburne
Cori/Pascal (DND): Please provide to Raquel Garbers
Kate/Shannon (ISED): Please provide to Patricia Brady
(CSE): Please provide to

Dear Colleagues,

Please find attached the Record of Decision for DG ESMC held on November 1, 2018.

Any comments you may have are requested by **COB Wednesday November 8, 2018** at which time the RoD will become final.

Thank you,

on behalf of

S.17.

Page 287

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

[redacted] (PS/SP)

From: [redacted] (PS/SP)
Sent: Friday, November 09, 2018 8:56 AM
To: [redacted] (PS/SP)
Cc: [redacted] PS/SP)
Subject: RE: Possible QP note

Absolutely. Have it on standby if we get tasked. I will right up a few lines for background on the article below so we have them on hand. TP's look like they should address any questions.

From: [redacted] (PS/SP)
Sent: Friday, November 09, 2018 7:31 AM
To: [redacted] (PS/SP)
Cc: [redacted] PS/SP)
Subject: Possible QP note

Hi [redacted]

It's unlikely we'll get tasked with a QP note today, but in case we do, can you get the note about Huawei? There was an article this morning.

https://www.thestar.com/vancouver/2018/11/05/canada-should-oust-chinese-telecom-huawei-say-security-experts.html

Thanks,

[redacted]

Sent from my Bell Samsung device over Canada's largest network.

[redacted] **(PS/SP)**

From: [redacted] (PS/SP)
Sent: Wednesday, September 19, 2018 8:45 AM
To: [redacted] (PS/SP)
Subject: FW: QP - Tasking: September 19

Didn't see your email in the distribution. For your awareness.

From: Murphy, Jeremy (PS/SP)
Sent: Wednesday, September 19, 2018 8:43 AM
To: [redacted] (PS/SP); [redacted] (PS/SP); Stevens, Marcelle (PS/SP); [redacted] PS/SP)
Cc: [redacted] (PS/SP); [redacted] (PS/SP); [redacted] PS/SP); [redacted] (PS/SP); [redacted] (PS/SP); Davies, John (PS/SP); [redacted] (PS/SP); [redacted] PS/SP)
Subject: RE: QP - Tasking: September 19

Hi team, apologies – this should have been sent to Cyber as there is no financial implication. Please stand down

Jeremy Murphy
Tel: 613-991-0241
Email: jeremy.murphy@canada.ca

From: Murphy, Jeremy (PS/SP)
Sent: Wednesday, September 19, 2018 8:40 AM
To: [redacted] (PS/SP); [redacted] PS/SP); Stevens, Marcelle (PS/SP); [redacted] PS/SP)
Cc: [redacted] (PS/SP); [redacted] (PS/SP); [redacted] (PS/SP); [redacted] (PS/SP); [redacted] (PS/SP); Davies, John (PS/SP); [redacted] (PS/SP); [redacted] (PS/SP); PS.O.NCSB.SADMO Users / Utilisateurs BSMAP.SSCN.O.SP
Subject: QP - Tasking: September 19
Importance: High

Hi team,

Please note that we received the QP below for PCO. This does not need to be translated.

We also received a note from Laura asking if we should be the lead as CSE has also drafted a response to something similar recently. Please let us know as soon as possible if NSOD is in a position to respond.

Due to SADMO by 9:30am

Thank you,

Jeremy Murphy
Tel: 613-991-0241
Email: jeremy.murphy@canada.ca

From: Braun, Laura (PS/SP)
Sent: Wednesday, September 19, 2018 8:33 AM
To: Bardsley, Scott (PS/SP); Bedor, Tia Leigh (PS/SP); [redacted] Braun, Laura (PS/SP); Brender, James (PS/SP); Butera, Eloge (PS/SP); Carty, Alexis (PS/SP); Champoux, Elizabeth (PS/SP); Christiansen, Calvin (PS/SP); Cirlan, Claudia (PS/SP); Cogan, Tim; Colin.Boyd@cbsa-asfc.gc.ca; Communications Issues Management / Communications Gestion des Enjeux (PS/SP); De Santis, Heather (PS/SP); Desnoyers, Christine; El-Koussaifi, Nicole; [redacted]

[redacted] Foss, Karen (PS/SP); Girard, Chantal (PS/SP); Gray4, Patrick (PS/SP); Holland, Alyx (FIN); Hurl, David (PS/SP); Iulia.PescarusPopa; joanna.polito@rcmp-grc.gc.ca; Kuschnik, Ellen (PS/SP); Landry Eliane (NHQ-AC); Lauzon, Adam (PS/SP); Malik, Zarah (PS/SP); Marier, Ruth; Mark.Prieur@PBC-CLCC.GC.CA; Martel, Alexandre (PS/SP); Martel, Benoit; McKenzie Presley, Lorraine (PS/SP); McNaughtan, Jennifer (Ext.); Milech, Michael (PS/SP); Morais, Alain (PS/SP); Moreau, Ken (PS/SP); Murayama Anne (NHQ-AC); Nicole.Greenough@cbsa-asfc.gc.ca; Oldham, Craig (PS/SP); [redacted] PAU-UAP@cbsa-asfc.gc.ca; Pike, Cory (PS/SP); PS.F ADMO-CSCCB / SMA-SSCRC F.SP; PS.F Media Monitoring / surveillance des médias F.SP; PS.O CMB ADMO / SGM BSMA O.SP; PS.O GOC Support / Soutien COG O.SP; PS.O Parliamentary Affairs Division / Unité des Affaires parlementaires O.SP; PS.O.EMPB.ADMO Users / Utilisateurs BSMA.SGUP.O.SP; PS.O.NCSB.SADMO Users / Utilisateurs BSMAP.SSCN.O.SP; PS.O.PACB.ADMO Users / Utilisateurs BSMA.SAPC.O.SP; Sabourin2, Alexandre (PS/SP); Sayarh, Omar (PS/SP); Showell, David (Ext.); Templeton2, Kasinee (PS/SP); Tremblay4, Guylaine (PS/SP); Vallières, Marc (PS/SP); Wilson, Ashleigh (PS/SP)
Cc: Templeton2, Kasinee (PS/SP); Gray4, Patrick (PS/SP); Braun, Laura (PS/SP)
Subject: QP Tasking: September 19

Good morning!

****Reminder:** If you determine that a QPN is tasked to the wrong organization, please advise Parliamentary Affairs immediately**

Please confirm receipt if you are tasked below.

Minister of Public Safety and Emergency Preparedness*

- CBSA -Fraud files https://www.scmp.com/news/world/united-states-canada/article/2164782/revealed-how-canada-border-agency-tried-conceal

Minister of Border Security and Organized Crime Reduction*

- NIL

Please ensure that the proposed speaking points reflect any recent media lines or recent comments by the Ministers on the issue. Please work with Communications as required

*Please use the Ministers Blair and Goodale QPN template. The format has changed with the new Proactive Disclosure requirements that will likely come into force this fall.

FIRM DEADLINE FOR ADM/EQUIVALENT APPROVED QPN – 9:45am (English note and French bullets) 12:30pm (French Backgrounder)

PCO (for the Prime Minister)**

- CSIS - Abdelrazik (https://www.thestar.com/news/canada/2018/09/18/judge-orders-indefinite-delay-in-csis-compensation-trial-orders-crown-to-pay-legal-costs.html)
- NCSB - Huawei (https://www.theglobeandmail.com/politics/article-ottawa-launches-probe-of-cyber-security/) (Update)
- CSCCB - Cannabis Enforcement (https://nationalpost.com/news/politics/canadian-police-forces-hold-off-on-ordering-the-only-device-approved-to-test-saliva-for-thc) (Update)

**Please use PCO QPN template.

****FIRM DEADLINE FOR ADM/EQUIVALENT APPROVED QPN – 9:45am (English note, French, if available)****

Please ensure your submissions are sent to Patrick Gray, Kasinee Templeton and myself.

Thank you very much,

Laura

Laura Braun
Senior Manager, Parliamentary Affairs / Gestionnaire principale, Affaires parlementaires
Public Safety Canada / Sécurité publique Canada
Tel/Tél: (613) 949-9737
Email/Courriel: laura.braun@canada.ca

HUAWEI & ZTE

- The Government of Canada takes the security of our country's critical infrastructure very seriously.
- Canadians can be assured that the Communications Security Establishment works to address cyber security concerns to protect Canada's critical infrastructure from threats.
- Since 2013, CSE's Security Review Program has been in place to test and evaluate designated equipment and services considered for use on Canadian 3G and 4G/LTE networks, including Huawei.
- CSE, through the Canadian Centre for Cyber Security, will continue to provide advice and guidance regarding emerging technologies and systems of important to Canada and Canadians.
- Our Government takes security matters extremely seriously and goes to great lengths to ensure the integrity and protection of our facilities and information.

HUAWEI ET ZTE

- Le gouvernement prend la sécurité de ses infrastructures essentielles très au sérieux.

- Les Canadiens peuvent être certains que le Centre de la sécurité des télécommunications travaille en vue d'éliminer les préoccupations en matière de cybersécurité afin de protéger les infrastructures essentielles du Canada contre toute menace.

- Depuis 2013, le Programme d'examen de la sécurité du CSTC est en place afin de tester et d'évaluer l'équipement et les services qu'on envisage utiliser sur les réseaux canadiens 3G et 4G/LTE, y compris Huawei.

- Par l'entremise du Centre canadien pour la cybersécurité, le CSTC continuera de fournir des avis et des conseils concernant les technologies et systèmes en émergence qui sont importants pour le Canada et les Canadiens.

- Notre gouvernement prend les questions liées à la sécurité très au sérieux et ne ménage aucun effort pour assurer l'intégrité et la protection de nos installations et de l'information.

BACKGROUND

- On June 18, 2018, Senators on the United States Senate intelligence committee warned the federal government and other Five Eyes countries of the risks posed by Chinese smartphone and telecom equipment maker, Huawei. They indicated a desire to see a concerted response among allies, and made reference to the integrated nature of the U.S. and Canadian economies and infrastructures as a concern.

- Previously, former directors of Canada's key security agencies, Ward Elcock, John Adams and Richard Fadden, warned the federal government to cut Canadian ties with Huawei. The warning followed comments made by the heads of the CIA, FBI, National Security Agency and the Defence Intelligence Agency to the U.S. Senate intelligence committee that Huawei poses a cybersecurity threat to American customers.

- The media reported that security officials are particularly concerned that Huawei products in the context of emerging 5G network technologies could provide China with the capacity to conduct remote espionage, modify or steal information, or even shut down systems. John Adams, the former head of the Communications Security Establishment (CSE), was quoted in the article as saying that Huawei has long been a concern to Canadian and U.S. security and intelligence services.

- On May 4, 2018 media reported that the Pentagon banned the sale of Huawei and ZTE phones on military bases. These devices are not currently on sale on Canadian Armed Forces bases.

- On September 7, 2018, media reported that CSE has been testing Huawei's equipment for security vulnerabilities for the last five years. As part of its cyber security mandate, CSE works with telecommunications service providers representing over 99% of Canadian subscribers. In this role, CSE provides advice and guidance to mitigate supply chain risks in telecommunications infrastructures upon which Canadians rely, including, since 2013, a program that has been in place to test and evaluate designated equipment and services (including Huawei) considered for use on Canadian 3G and 4G/LTE networks. CSE accredits third party labs to conduct assurance testing in accordance with requirements outlined by CSE. CSE reviews the testing results and provides tailored advice and guidance to Canada's telecommunications sector. While non-disclosure agreements limit the degree to which CSE can comment on specific details, Canadians can be assured that the Government of Canada is working to make sure that robust protections are in place to safeguard the communications systems that Canadian rely on.

Name of PCO Policy Analyst. Nom de l'analyste du BCP :

Secretariat. Secrétariat : Security and Intelligence

Telephone number. Numéro de téléphone :

11/22/2018 10:20

[redacted]

From: [redacted]
Sent: November-05-18 11:02 AM
To: [redacted] (INTERNATIONAL)
Subject: RE: [redacted]

Classification: TOP SECRET/[redacted]/CANADIAN EYES ONLY

Ohh okay, perfect, thanks!

From: [redacted] [mailto:[redacted]
Sent: November-05-18 11:01 AM
To: [redacted]
Subject: RE: [redacted]

Classification: TOP SECRET //CANADIAN EYES ONLY

Just DMT seeking an internal consultation within the department in advance of [redacted]

From: [redacted] [mailto:[redacted]
Sent: November-05-18 10:59 AM
To: [redacted]
Subject: RE: [redacted]

Classification: TOP SECRET//[redacted]/CANADIAN EYES ONLY

Hi [redacted] – do you have any more information on this DM meeting? When/Where/Who/ lead? We hadn't heard anything about it..

From: [redacted] [mailto:[redacted]
Sent: November-05-18 10:58 AM
To: [redacted]
Subject: RE: [redacted]

Classification: TOP SECRET //CANADIAN EYES ONLY

Thanks so much.

From: [redacted] [mailto:[redacted]
Sent: November-05-18 8:58 AM
To: [redacted]
Subject: [redacted]

Classification: TOP SECRET/[redacted]/CANADIAN EYES ONLY

Hi [redacted]

I have a few things that might be able to help. These were all part of [redacted]

[redacted]

There was also a report from [redacted]

Hope that helps!

[redacted]
National Security Operations Directorate – Direction générale des opérations de la sécurité nationale
Public Safety and Emergency Preparedness Canada – Sécurité publique et Protection civile Canada
Tel. – Tél.: [redacted]

Pages 297 to / à 307

are duplicates

sont des duplicatas

Pages 308 to / à 309

are withheld pursuant to sections

sont retenues en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Pages 310 to / à 317

are withheld pursuant to sections

sont retenues en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Pages 318 to / à 320

are withheld pursuant to sections

sont retenues en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Pages 321 to / à 338

are duplicates

sont des duplicatas

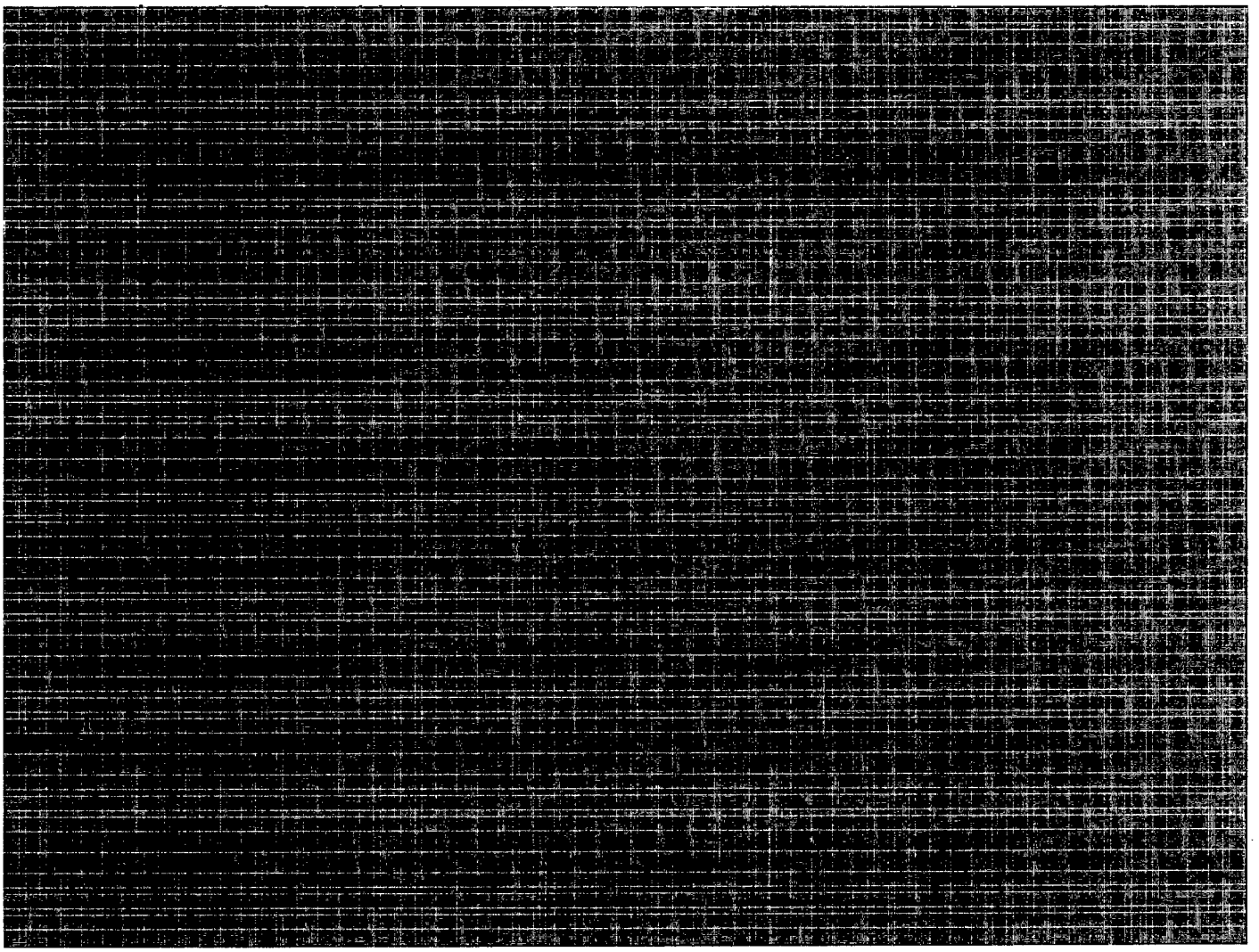
Bunghardt, Gregory

From: Waters, Michael
Sent: June-20-18 6:04 PM
To: Hashem, Mohsen; Bunghardt, Gregory
Subject: Reporting that may be of interest

Classification: TOP SECRET/[redacted]/LIMITED/CANADIAN EYES ONLY

Greg, Mohsen, the reporting below may be of interest.

[redacted]



Regards,
Michael

Michael Waters
Manager / Gestionnaire
National Cyber Security Directorate / Direction de la cyber-sécurité nationale
Public Safety Canada / Sécurity public Canada
Tel/Tél: 613-991-1634
Mobile: 613-796-4286
Email/courriel: Michael.Waters@canada.ca
CTSN: [redacted]

Pages 341 to / à 357

are withheld pursuant to sections

sont retenues en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Merchant, Colleen

From: INTERNATIONAL Shared - Washington DC ILO Group Mailbox [redacted]

Sent: October-22-18 3:34 PM

To: Green Martin [redacted] (PCO) (PCO-BCP); [redacted] Chayer, Marie-Helene MH - Civ; Benjamin, Martin

Subject: [redacted]

Classification: TOP SECRET/[redacted]

[redacted]

Pages 359 to / à 360

are withheld pursuant to sections

sont retenues en vertu des articles

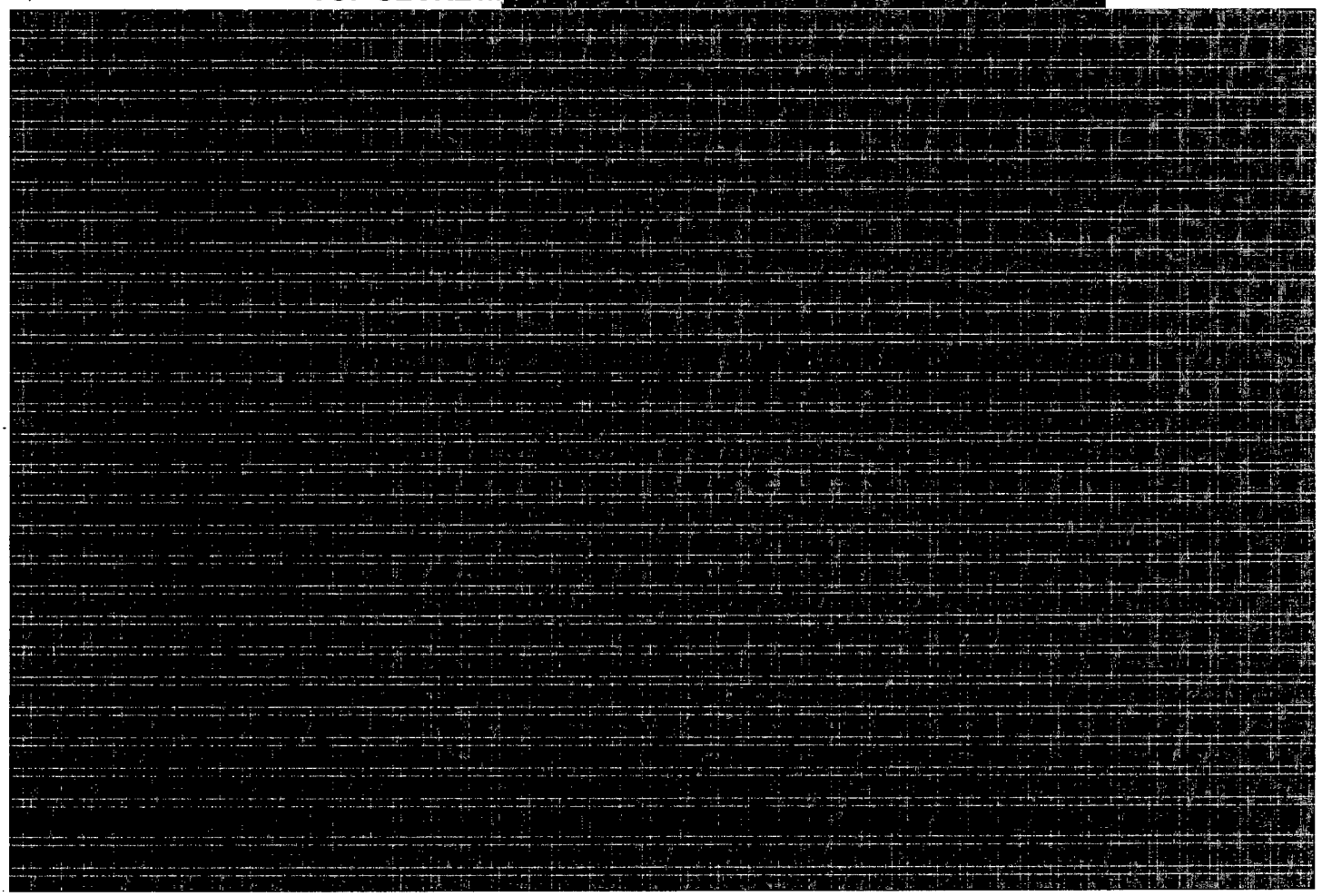
of the Access to Information

de la Loi sur l'accès à l'information

[redacted]

Embassy of Canada | Ambassade du Canada
Washington D.C.

BCC list: [redacted]



Bunghardt, Gregory

From: Bunghardt, Gregory
Sent: July-05-18 11:14 AM
To: Hashem, Mohsen; Park, Beom-Jun
Cc: Waters, Michael
Subject: TS_CEO PIMD review [redacted] - July 6 2018_v3

Classification: TOP SECRET/[redacted]CANADIAN EYES ONLY

TS_CEO PIMD review [redacted]

Ben –

[redacted]

I have included some comments in track changes.

greg.

Public Safety Canada | Sécurité publique Canada

Senior Assistant Deputy Minister | Sous-ministre adjoint(e) principal(e)

Ottawa, Canada
K1A 0P8

TOP SECRET [redacted] CEO

DATE: June 6, 2018

Comment [U1]: Confirm date

File No.: PS-023259

BRIEFING NOTE ~~TO~~ FOR THE DEPUTY MINISTER

[redacted]
(information only)

PURPOSE

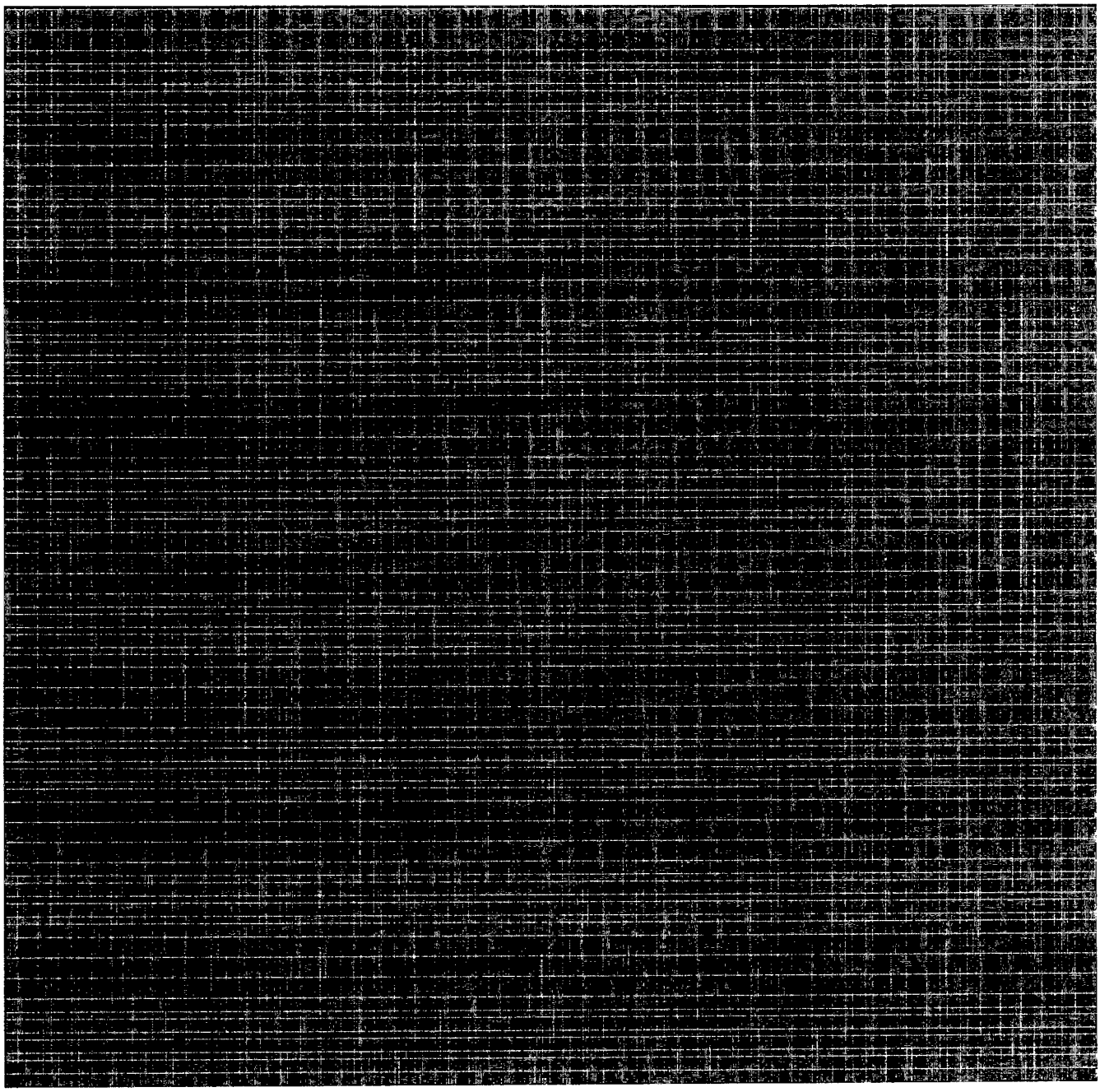
[redacted]

BACKGROUND

[redacted]

Canada

CONSIDERATIONS



[redacted]

Should you require additional information, please do not hesitate to contact me or [redacted] Director General, National Security Operations Directorate, at [redacted]

Monik Beauregard

Enclosures: (0)

Bunghardt, Gregory

From: Waters, Michael
Sent: June-08-18 5:45 PM
To: [redacted]
Cc: Mahu, Vlad; Hashem, Mohsen; Binne, Christine; Sandford, Amanda; Bunghardt, Gregory
Subject: Examples of how SIRs used for NSICOPs

Classification: TOP SECRET/[redacted] CANADIAN EYES ONLY

Hi [redacted]

Further to your email, please find below previously-approved examples of how we used the SIRs. I have underlined the senior officials and Minister angle that you are looking for.

[redacted]

Regards,
Michael

Michael Waters
Manager / Gestionnaire
National Cyber Security Directorate / Direction de la cyber-sécurité nationale
Public Safety Canada / Sécurity public Canada
Tel/Tél: 613-991-1634
Mobile: 613-796-4286
Email/courriel: Michael.Waters@canada.ca
CTSN: [redacted]

Bunghardt, Gregory

From: Waters, Michael
Sent: June-20-18 5:57 PM
To: Frigon, Sylvie; Binne, Christine; Bunghardt, Gregory; Hashem, Mohsen; Hartley, William
Subject: [redacted]

Follow Up Flag: Follow up
Flag Status: Flagged

Classification: TOP SECRET/[redacted]

TOP SECRET [redacted]

Colleagues, fyi.

[redacted]

Regards,
Michael

Michael Waters
Manager / Gestionnaire
National Cyber Security Directorate / Direction de la cyber-sécurité nationale
Public Safety Canada / Sécurity public Canada
Tel/Tél: 613-991-1634
Mobile: 613-796-4286
Email/courriel: Michael.Waters@canada.ca
CTSN: [redacted]

Pages 369 to / à 373

are duplicates

sont des duplicatas

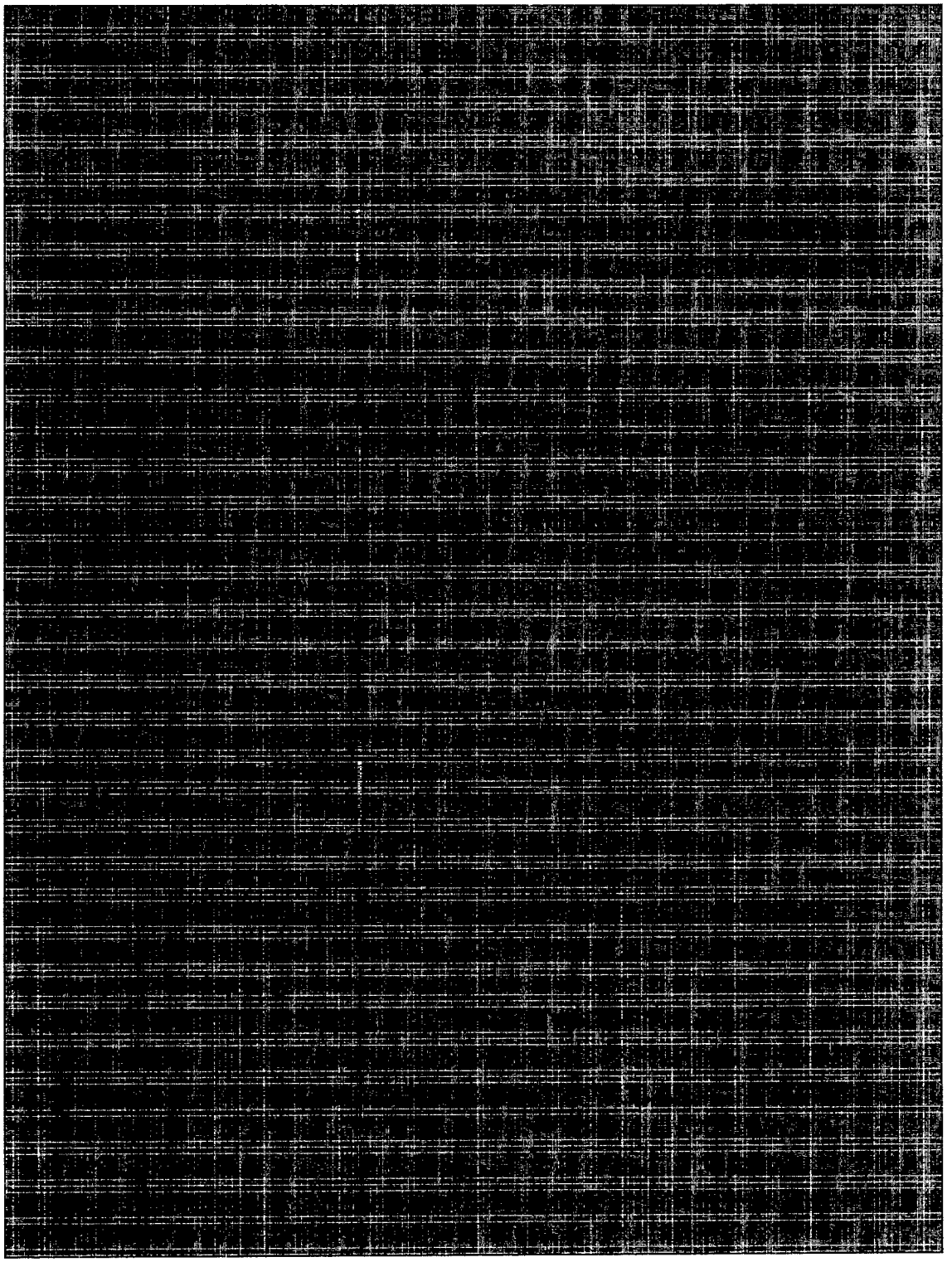
Pages 374 to / à 376

are withheld pursuant to sections

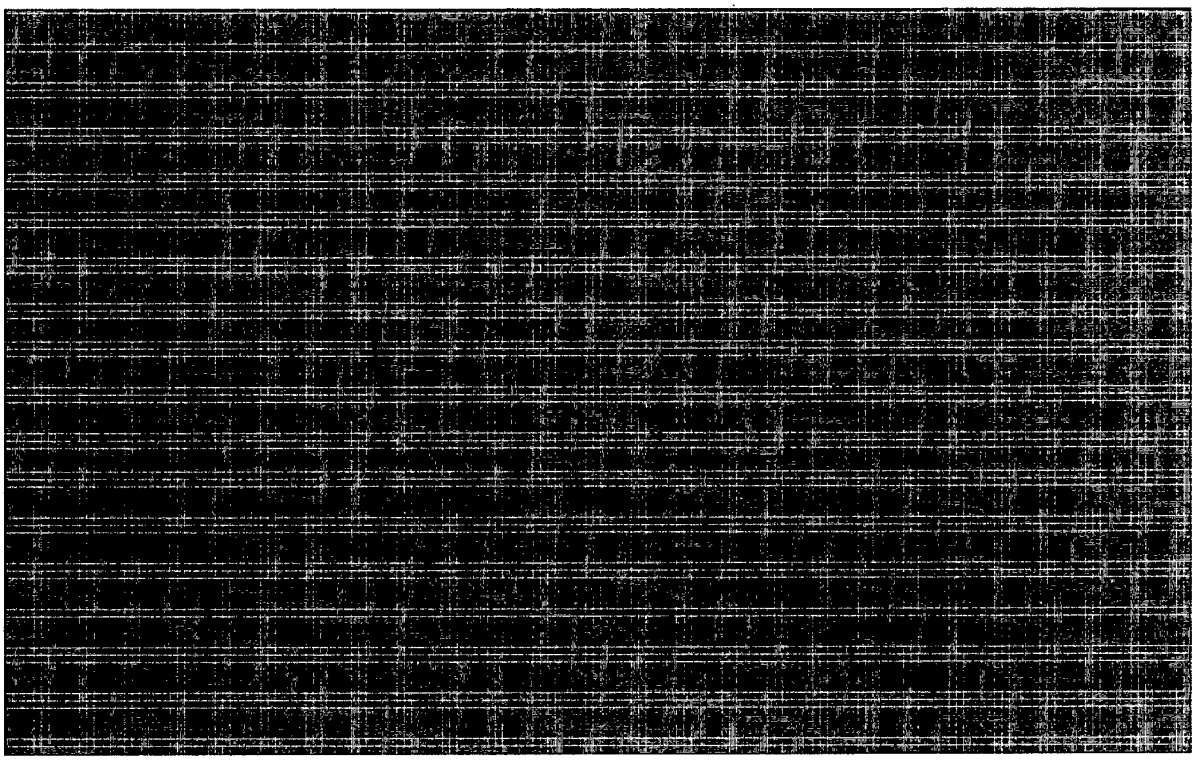
sont retenues en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information



Canada



RELEASED

[redacted]

Embassy of Canada | Ambassade du Canada
Washington D.C.

Pages 379 to / à 387

are withheld pursuant to sections

sont retenues en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Pages 388 to / à 394

are withheld pursuant to sections

sont retenues en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Pages 395 to / à 407

are withheld pursuant to sections

sont retenues en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Bunghardt, Gregory

From: Waters, Michael
Sent: August-24-18 5:30 PM
To: Bunghardt, Gregory; Ouellet, Benoit
Cc: Brydges, Lucas
Subject: RE: [redacted] DMNS retreat

Classification: TOP SECRET//[redacted]/CANADIAN EYES ONLY

I agree and would note the following:

[redacted]

[redacted]

Regards,
Michael

Michael Waters
Manager / Gestionnaire
National Cyber Security Directorate / Direction de la cyber-sécurité nationale
Public Safety Canada / Sécurity public Canada
Tel/Tél: 613-991-1634
Mobile: 613-796-4286
Email/courriel: Michael.Waters@canada.ca
CTSN: [redacted]

From: Bunghardt, Gregory
Sent: August-24-18 3:04 PM
To: Waters, Michael; Ouellet, Benoit
Cc: Brydges, Lucas
Subject: RE: [redacted] DMNS retreat

Classification: TOP SECRET/[redacted] CANADIAN EYES ONLY

Hi Benoît and Michael,

I have made a few comments within the document for NSOD's consideration.

Thanks,

greg.

<< File: [redacted] doc >>

From: Waters, Michael
Sent: August-23-18 9:40 AM
To: Bunghardt, Gregory; Ouellet, Benoit
Subject: [redacted] DMNS retreat

Classification: TOP SECRET/[redacted] CANADIAN EYES ONLY

Hi Greg and Benoît,

NSOD has asked us to provide any comments on the attached [redacted] by COB Friday. Like the [redacted] would you be comfortable with this as a Greg lead with International?
<< File: [redacted] Draft 1_1.doc >>
Regards,
Michael

Michael Waters
Manager / Gestionnaire
National Cyber Security Directorate / Direction de la cyber-sécurité nationale
Public Safety Canada / Sécurity public Canada
Tel/Tél: 613-991-1634
Mobile: 613-796-4286
Email/courriel: Michael.Waters@canada.ca
CTSN [redacted]

From: [redacted]
Sent: August-22-18 5:10 PM
To: Waters, Michael
Subject: FW: [redacted] DMNS retreat docs for review

Classification: TOP SECRET/[redacted]/CANADIAN EYES ONLY

Hi Michael,
Christine asked me to send this message to you.
Please see below.
Thanks
[redacted]

From: [redacted]
Sent: August-22-18 4:58 PM
To: Binne, Christine
Subject: [redacted] DMNS retreat docs for review

Classification: TOP SECRET/[redacted]/CANADIAN EYES ONLY

Hi Christine,

As mentioned on the other system, attached are the two first docs for the DMNS retreat: the tabletop exercise scenario and the [redacted]
If you have any comments, please send them to [redacted] by this Friday.

Thanks
[redacted]

[redacted]
Director, National Security Operations
Public Safety Canada
Tel. [redacted]

Directrice, Opérations de la sécurité nationale
Sécurité publique Canada
Tél. : [redacted]

Bunghardt, Gregory

From: Waters, Michael
Sent: September-25-18 11:52 AM
To: Bunghardt, Gregory; Binne, Christine; Frigon, Sylvie; Hartley, William; Park, Beom-Jun; Goldfinger, Marc; Ouellet, Benoit; Brydges, Lucas
Subject: [redacted]
Attachments: [redacted]

Classification: TOP SECRET/[redacted]CANADIAN EYES ONLY

Colleagues, find attached [redacted]

Regards,
Michael

Michael Waters
Manager / Gestionnaire
National Cyber Security Directorate / Direction de la cyber-sécurité nationale
Public Safety Canada / Sécurity public Canada
Tel/Tél: 613-991-1634
Mobile: 613-796-4286
Email/courriel: Michael.Waters@canada.ca
CTSN: [redacted]

Pages 413 to / à 423

are withheld pursuant to sections

sont retenues en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Bunghardt, Gregory

From: Waters, Michael
Sent: September-11-18 4:14 PM
To: Binne, Christine; Frigon, Sylvie; Hartley, William; Bunghardt, Gregory; Park, Beom-Jun
Subject: [redacted]
Attachments:

Follow Up Flag: Follow up
Flag Status: Flagged

Classification: TOP SECRET/[redacted]CANADIAN EYES ONLY

Colleagues,

FYI, find attached [redacted]

Regards,
Michael

Michael Waters
Manager / Gestionnaire
National Cyber Security Directorate / Direction de la cyber-sécurité nationale
Public Safety Canada / Sécurity public Canada
Tel/Tél: 613-991-1634
Mobile: 613-796-4286
Email/courriel: Michael.Waters@canada.ca
CTSN: [redacted]

Pages 425 to / à 435

are withheld pursuant to sections

sont retenues en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Bunghardt, Gregory

From: Waters, Michael
Sent: July-05-18 5:15 PM
To: Hashem, Mohsen; Bunghardt, Gregory; Park, Beom-Jun
Subject: RE: TS_CEO PIMD review [redacted] v3

Classification: TOP SECRET/[redacted]/CANADIAN EYES ONLY

Mohsen, Greg, great feedback, really spot on.

Regards,
Michael

Michael Waters
Manager / Gestionnaire
National Cyber Security Directorate / Direction de la cyber-sécurité nationale
Public Safety Canada / Sécurity public Canada
Tel/Tél: 613-991-1634
Mobile: 613-796-4286
Email/courriel: Michael.Waters@canada.ca
CTSN: [redacted]

From: Hashem, Mohsen
Sent: July-05-18 11:23 AM
To: Bunghardt, Gregory; Park, Beom-Jun
Cc: Waters, Michael
Subject: RE: TS_CEO PIMD review [redacted] v3

Classification: TOP SECRET/[redacted]/CANADIAN EYES ONLY

I agree with Greg's comments. The only thing I would add – which Greg touched on when referring to [redacted]

From: Bunghardt, Gregory
Sent: July-05-18 11:14 AM
To: Hashem, Mohsen; Park, Beom-Jun
Cc: Waters, Michael
Subject: TS_CEO PIMD review [redacted] v3

Classification: TOP SECRET/[redacted]/CANADIAN EYES ONLY

<< File: TS_CEO PIMD review [redacted] v3.doc >>

Ben –

[redacted]

I have included some comments in track changes.

greg.

Bunghardt, Gregory

From: [redacted]
Sent: October-15-18 1:11 PM
To: Bunghardt, Gregory
Cc: Waters, Michael
Subject: RE: [redacted]

Classification: Top Secret/[redacted] Canadian Eyes Only
Classification: Très secret/[redacted] Réservé aux Canadiens
Not for PA / Ne pas classer

Thanks for the follow-up Greg!

Please let me know if you require anything else [redacted]

Cheers,

[redacted]

From: Bunghardt, Gregory [mailto:[redacted]
Sent: 15-Oct-18 1:08 PM
To: [redacted]
Cc: Michael Waters (PSEPC-SPPCC)
Subject: RE: [redacted]

Classification: TOP SECRET/[redacted] CANADIAN EYES ONLY

Hi [redacted]

Thanks for this. We will incorporate your wording into the document.

The product is great too – [redacted]

I'll make sure to send you the final package once it is complete – I suspect there will be more to follow on this issue.

greg.

From: [redacted]
Sent: October-12-18 5:31 PM
To: Bunghardt, Gregory
Subject: RE: [redacted]

Classification: Top Secret[redacted]/Canadian Eyes Only
Classification: Très secret[redacted]/Réservé aux Canadiens
Not for PA / Ne pas classer

Greg,

Please consider the comments in the attached docs DG-approved,[redacted]so let's touch base on this on Monday, as we may have further[redacted]comments.

[redacted]

Have a great weekend!

[redacted]

From: Bunghardt, Gregory [mailto:[redacted]
Sent: 12-Oct-18 4:52 PM
To: [redacted]
Subject: RE: [redacted]

Classification: SECRET//CANADIAN EYES ONLY

Hi[redacted]

I now have a[redacted]approved document. The package is with our DG. I will send you the most recent versions,[redacted]

Have a great wknd,

greg.

From: [redacted]
Sent: October-12-18 10:12 AM
To: Bunghardt, Gregory
Cc: [redacted]
Subject: RE: [redacted]

Classification: Secret//Canadian Eyes Only
Classification: Secret//Réservé aux Canadiens
Not for PA / Ne pas classer

[redacted]

Cheers,

[redacted]

From: Bunghardt, Gregory [mailto:[redacted]
Sent: 12-Oct-18 10:00 AM
To: [redacted]
Subject: RE: [redacted]

Classification: SECRET//CABINET CONFIDENCE/CANADIAN EYES ONLY

Hi [redacted]

Thanks,

greg.

From: [redacted]
Sent: October-12-18 9:58 AM
To: Bunghardt, Gregory
Subject: [redacted]

Classification: Secret//CabinetConfidence
Classification: Secret//CabinetConfidence
Not for PA / Ne pas classer

Hi Greg,

As discussed, [redacted] that would be greatly appreciated!

Thanks,

[redacted]

>>>**********[INFO DEPOT START / DÉBUT INFO DÉPÔT]**********
Sender / Envoyeur [redacted]
Recipients / Receveurs : Gregory Bunghardt (PSEPC-SPPCC);
Subject / Sujet : [redacted]
Date : 10/12/2018 9:57:59 AM

>>>**********[INFO DEPOT START / DÉBUT INFO DÉPÔT]**********
Sender / Envoyeur : [redacted]
Recipients / Receveurs : Bunghardt, Gregory;
Subject / Sujet : RE: [redacted]
Date : 10/12/2018 10:11:43 AM

>>>**********[INFO DEPOT START / DÉBUT INFO DÉPÔT]**********
Sender / Envoyeur : [redacted]
Recipients / Receveurs : Bunghardt, Gregory;
Subject / Sujet : RE: [redacted]
Date : 10/12/2018 5:31:24 PM

>>>**********[INFO DEPOT START / DÉBUT INFO DÉPÔT]**********
Sender / Envoyeur [redacted]
Recipients / Receveurs : Bunghardt, Gregory;
Subject / Sujet : RE: [redacted]
Date : 10/15/2018 1:11:24 PM

Merchant, Colleen

From: Merchant, Colleen
Sent: September-20-18 3:23 PM
To: Beauregard, Monik
Cc: Murphy, Jeremy
Subject: RE:[redacted]

Classification: TOP SECRET/[redacted]

Hi Monik –

[redacted]

I hope this is helpful. I'll send the draft agenda separately.

Colleen

From: Beauregard, Monik
Sent: September-20-18 2:44 PM
To: Merchant, Colleen
Subject: FW:[redacted]
Importance: High

Classification: TOP SECRET[redacted]

Colleen,
Any views on the [redacted] points [redacted] raises?

Would be useful for today. I have a 4pm meeting.
M.

From: [mailto @cse-cst.gc.ca]
Sent: September-20-18 11:52 AM
To: Beauregard, Monik; Xavier Caroline 47627418646 (PCO) (PCO-BCP)
Cc: PCO) (PCO-BCP); Geddes, Patricia PC - Civ (DND-MDN); (CSE-CST); CSE-CST)
Subject:
Importance: High

Classification: TOP SECRET

Monik/Caroline:

The two subject items aren't related but I do want to raise both with you.

5G

Wanted to give you that perspective.

Following on from a comment I made at ADMNS Policy

This all speaks to the points raised by all at the DMNS retreat around looking at governance. This is both a domestic and int'l issue.

I think we could speak to our collective views on the agenda, and the right mix for the Canadian del.

For your consideration.

Best, [redacted]

[redacted]
A/Deputy Chief, Policy and Communications
[redacted]@cse-cst.gc.ca
[redacted]

Merchant, Colleen

From: [redacted]
Sent: September-18-18 4:27 PM
To: [redacted](INTERNATIONAL); [redacted](CSE-CST); Hadwen, Wendy M; Merchant, Colleen; [redacted](CSE-CST)
Subject: FW: [redacted]
Attachments: [redacted]

Classification: TOP SECRET/[redacted]CANADIAN EYES ONLY

Hi,

Please find attached a DRAFT of a [redacted] Although not completed, I thought it may be of interest to you.

GAC – for Martin Benjamin

Thanks.
[redacted]

Pages 446 to / à 453

are withheld pursuant to sections

sont retenues en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

[redacted]

From: [redacted]
Sent: June-08-18 10:05 AM
To: [redacted] CSE-CST); [redacted] (INTERNATIONAL); [redacted] (INTERNATIONAL); Anderson, Cori C - Civ (DND-MDN); Partridge, Shannon SK (DND-MDN); [redacted] (CSE-CST)
Cc: [redacted]
Subject: RE: [redacted]

Classification: TOP SECRET/[redacted]CANADIAN EYES ONLY

Please note the outline had a classification level of TS/[redacted]/CEO. Resending with appropriate email classification. Please delete previous email.

Thanks,
[redacted]

From: [redacted]
Sent: June-08-18 9:52 AM
To: [redacted] (CSE-CST); [redacted] (INTERNATIONAL); [redacted] (INTERNATIONAL); Anderson, Cori C - Civ (DND-MDN); Partridge, Shannon SK (DND-MDN); [redacted] (CSE-CST)
Cc: [redacted]
Subject: RE: [redacted]

Classification: SECRET//CANADIAN EYES ONLY

Apologies, clearly not finished my coffee yet.. Attached is the work plan.

[redacted]

From: [redacted]
Sent: June-08-18 9:52 AM
To: [redacted] (CSE-CST); [redacted] (INTERNATIONAL); [redacted] (INTERNATIONAL); Anderson, Cori C - Civ (DND-MDN); Partridge, Shannon SK (DND-MDN); [redacted] (CSE-CST)
Cc: [redacted]
Subject: RE: [redacted]

Classification: SECRET//CANADIAN EYES ONLY

Hello All,

Please find attached the draft outline and work plan for [redacted]
We can discuss further at the meeting on Wednesday. However, if you have any comments before then, please let me know.

Thank you,
[redacted]

From: [redacted]
Sent: June-06-18 9:06 AM
To: [redacted](CSE-CST); [redacted](CSE-CST); [redacted](INTERNATIONAL); [redacted](INTERNATIONAL); Anderson, Cori C - Civ (DND-MDN); Partridge, Shannon SK (DND-MDN)
Cc: [redacted]
Subject: [redacted]

Classification: SECRET//CANADIAN EYES ONLY

Hello All,

As discussed at [redacted] we would like to set up a meeting on [redacted]

I will be sending a meeting request for a time next week. In the meantime, PS is drafting an outline and work plan that will be shared with you shortly.

Some of the items we'd like to focus on at this first meeting are as follows:

[redacted]

Should you have any questions, please let us know.

Thanks,

[redacted]
National Security Operations Directorate – Direction générale des opérations de la sécurité nationale
Public Safety and Emergency Preparedness Canada – Sécurité publique et Protection civile Canada
Tel. – Tél.: [redacted]

Pages 456 to / à 457

are withheld pursuant to sections

sont retenues en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

[redacted]

From: [redacted]
Sent: June-22-18 9:56 AM
To: [redacted]
Subject: FW: [redacted] Feedback
Attachments: [redacted] docx

Classification: TOP SECRET [redacted] CANADIAN EYES ONLY

Hi [redacted] – for your initial views.

Thanks!
[redacted]

From: [redacted]
Sent: June-21-18 8:48 AM
To: [redacted]
Subject: [redacted] Feedback

Classification: TOP SECRET [redacted] CANADIAN EYES ONLY

Hi All,

If you happen to have time in the next day or so, I have attached [redacted] and I'm looking for any/all feedback, thoughts, questions, outrageous accusations you may have. I kindly request that you ignore editorial stuff (spelling, bad placement of commas) and consider the way ideas are framed, support for those ideas and anything else of that nature.

[redacted]

I'm still plugging away and there are gaps in information that will be required from our partners but if you have any feedback, I'm happy to take it.

Thanks,
[redacted]

Pages 459 to / à 467

are withheld pursuant to sections

sont retenues en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

[redacted]

From: [redacted]
Sent: September-13-18 3:50 PM
To: [redacted]
Subject: RE: Tasking: Lessons Learned

Classification: SECRET//CANADIAN EYES ONLY

I've started [redacted] but it was put on the back burner. It is on my to-do list for tomorrow though. I will have it done before COB.

From: [redacted]
Sent: September-13-18 3:48 PM
To: [redacted]
Cc: [redacted]
Subject: RE: Tasking: Lessons Learned

Classification: SECRET//CANADIAN EYES ONLY

Hi all –

Could you provide an update on where we stand with the lessons learned documents? How many have we completed so far?

[redacted]

From: [redacted]
Sent: August-17-18 2:02 PM
To: [redacted]
Cc: [redacted]
Subject: Tasking: Lessons Learned

Classification: SECRET//CANADIAN EYES ONLY

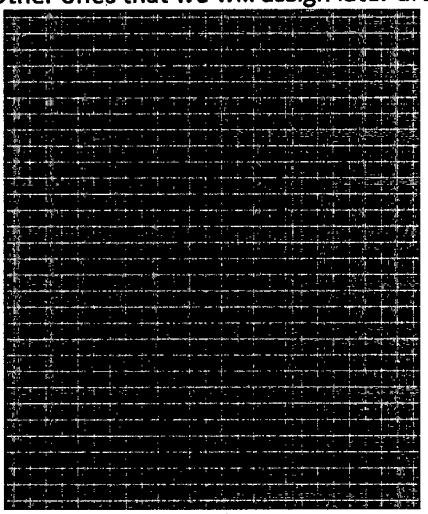
Hello All,

As you know, each of the cases we have conducted has had its share of, shall we say, 'learning experiences'. We would like to capture those lessons so we can (hopefully) address them in the future. To start, we have assigned a few of the key transactions to the following people:

[redacted]

The template is attached. If you could complete a first draft by Wednesday, that would be great! I will set up a time that we can all get together and talk it out. If you need guidance, feel free to come chat. Drafts can be saved here: LESSONS LEARNED

Other ones that we will assign later are as follows:



Please know you are not expected to know everything about the transaction. If you can only complete some parts, that is okay. You can also come speak with me before the meeting on Wednesday to chat the content if you would like.

Thanks!

National Security Operations Directorate – Direction générale des opérations de la sécurité nationale
Public Safety and Emergency Preparedness Canada – Sécurité publique et Protection civile Canada
Tel. – Tél.:

From:
Sent: July-19-18 1:37 PM
To: (CSE-CST); Gordon, Eric (RCMP-GRC); Gumley, Matthew (RCMP-GRC); Burns, Genevieve (RCMP-GRC); Anderson, Cori C - Civ (DND-MDN); Partridge, Shannon SK (DND-MDN); (INTERNATIONAL); (INTERNATIONAL); (INTERNATIONAL); (INTERNATIONAL); (PCO) (PCO-BCP); Richard, Daniel (PWGSC-TPSGC); Burke, Mary (ISED); Dewolfe, Jonathan (ISED); Kack, Shannon (ISED); Tarantino, Maria (ISED); Keating, Sean (ISED); Burrell, Christopher (ISED); (INTERNATIONAL); (INTERNATIONAL); (INTERNATIONAL); Best, Emma (RCMP-GRC); Faucher, Monique (NRCAN-RNCAN); Karman, Mehmet (ISED)
Cc:
Subject:
Attachments:

Classification: TOP SECRET

Good afternoon,

I am sending the attached document on behalf of

Take care,

PSPC: Daniel and/or Joel, can you please forward the documentation to Louis Bedard, Peter Au & Antoine Parker
NRCan: Irina Spassova can you please forward the documentation to Michael Brown
Thank you!

Pages 471 to / à 478

are withheld pursuant to sections

sont retenues en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

[redacted]

From: [redacted]
Sent: July-31-18 12:46 PM
To: Radulovic, Laura LS - Civ (DND-MDN)
Cc: [redacted]
Subject: [redacted]
Attachments: [redacted]

Classification: TOP SECRET/[redacted]/CANADIAN EYES ONLY

Hi Laura,

This is what we have [redacted] Some of the documents are from CSIS, CSE and PCO so you may wish to seek approval from them to use it.

Would also point you to the following reports [redacted] there may be other reporting, I would suggest doing a general search:

[redacted]

Let me know if you have any questions.

Thanks,

[redacted]
National Security Operations Directorate – Direction générale des opérations de la sécurité nationale
Public Safety and Emergency Preparedness Canada – Sécurité publique et Protection civile Canada
Tel. – Tél.: [redacted]

Pages 480 to / à 481

are duplicates

sont des duplicatas

Pages 482 to / à 483

are withheld pursuant to sections

sont retenues en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Page 484

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Pages 485 to / à 492

are duplicates

sont des duplicatas

Pages 493 to / à 506

are withheld pursuant to sections

sont retenues en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Pages 507 to / à 508

are withheld pursuant to section

sont retenues en vertu de l'article

of the Access to Information

de la Loi sur l'accès à l'information

Pages 509 to / à 519

are withheld pursuant to sections

sont retenues en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Pages 520 to / à 552

are duplicates

sont des duplicatas

[redacted]

From: [redacted]
Sent: August-15-18 1:30 PM
To: [redacted]
Subject: Paper
Attachments: [redacted] v2.docx

Classification: TOP SECRET// /CANADIAN EYES ONLY

[redacted] for your reading pleasure.

It's saved under [redacted]

[redacted]
National Security Operations Directorate – Direction générale des opérations de la sécurité nationale
Public Safety and Emergency Preparedness Canada – Sécurité publique et Protection civile Canada
Tel. – Tél.: [redacted]

Pages 554 to / à 558

are withheld pursuant to sections

sont retenues en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Page 559

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Pages 560 to / à 563

are withheld pursuant to sections

sont retenues en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

[redacted]

From: [redacted]
Sent: August-21-18 12:07 PM
To: [redacted] Gordon, Eric (RCMP-GRC); Gumley, Matthew (RCMP-GRC); Burns, Genevieve (RCMP-GRC); Anderson, Cori C - Civ (DND-MDN); Partridge, Shannon SK (DND-MDN); [redacted] (INTERNATIONAL); [redacted] (INTERNATIONAL); Geithner, Brandon (INTERNATIONAL); [redacted] (PCO) (PCO-BCP); Burke, Mary (ISED); Dewolfe, Jonathan (ISED); Kack, Shannon (ISED); Tarantino, Maria (ISED); Keating, Sean (ISED); Burrell, Christopher (ISED); [redacted] (INTERNATIONAL); [redacted] (INTERNATIONAL); [redacted] (INTERNATIONAL); Best, Emma (RCMP-GRC); [redacted] (PCO) (PCO-BCP); [redacted] (CSE-CST); [redacted] (CSE-CST)
Cc: [redacted]
Subject: FW: Draft [redacted] Agenda from [redacted]
Attachments: [redacted] draft agenda - 21 Aug.xlsx

Classification: TOP SECRET

Good afternoon,

Please find attached the draft [redacted] agenda.

[redacted]

From: [redacted] [mailto: [redacted]
Sent: August-21-18 9:20 AM
To: [redacted]
Subject: Draft [redacted] Agenda from [redacted]

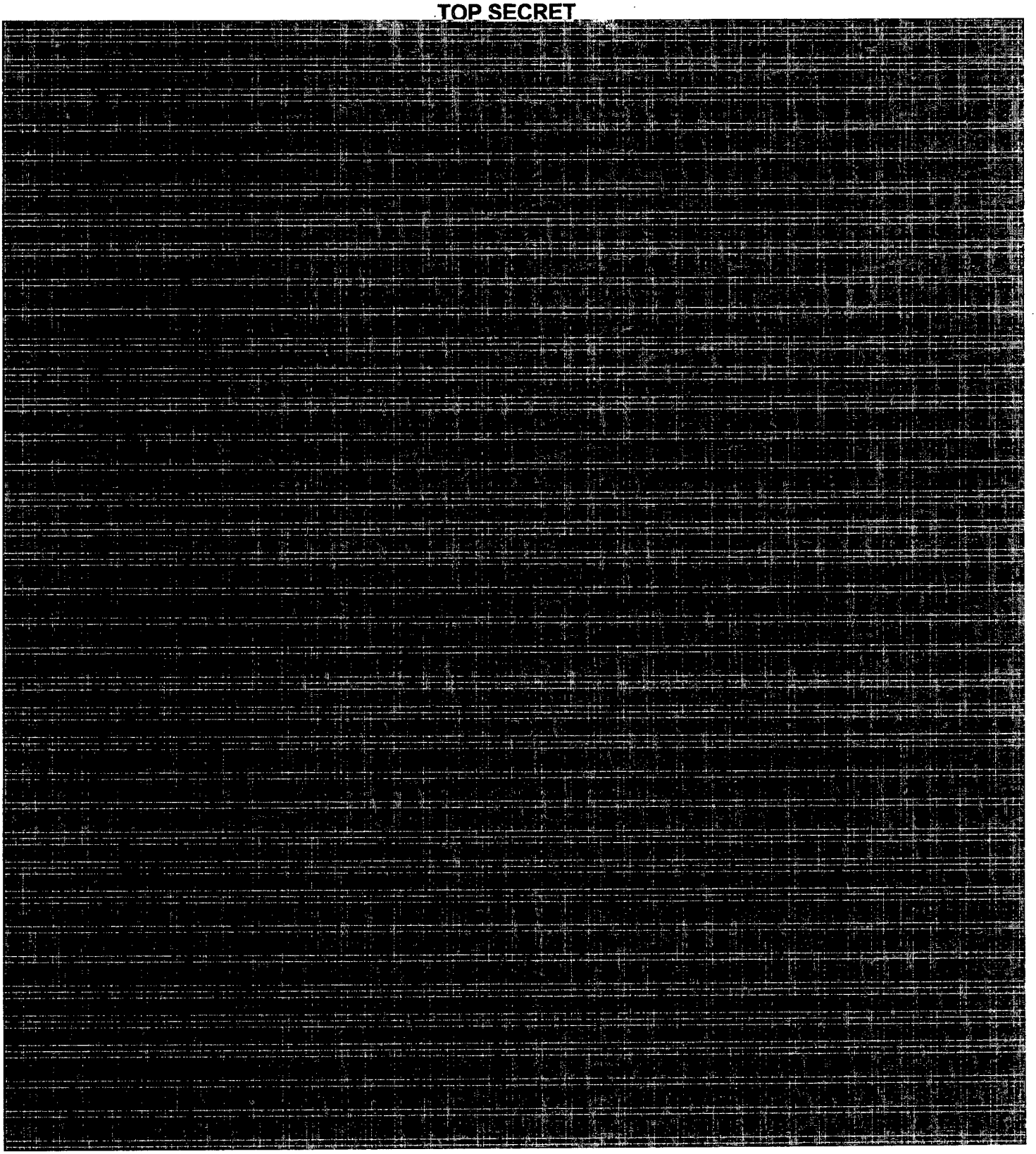
Classification: Top Secret
Classification: Très secret
Not for PA / Ne pas classer

Hello [redacted] just arrived overnight [redacted] is the draft [redacted] agenda. Would you please distribute to the [redacted] agencies that have confirmed they will be part of the [redacted] delegation. [redacted]
Are there any others I am missing ?

[redacted]

QUOTE

Please find attached an updated agenda for the conference. [redacted]



>>>**********[INFO DEPOT START / DÉBUT INFO DÉPÔT]**********
Sender / Envoyeur : [redacted]
Recipients / Receveurs : [redacted](PSEPC-SPPCC);

Subject / Sujet : Draft [redacted] Agenda from [redacted]
Date : 8/21/2018 9:19:33 AM

Page 567

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

[redacted]

From: [redacted]
Sent: August-29-18 10:09 AM
To: [redacted]
Cc:
Subject:

Classification: SECRET//[redacted]/CANADIAN EYES ONLY

[redacted]

Pages 569 to / à 570

are withheld pursuant to sections

sont retenues en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

[redacted]

From: [redacted]
Sent: August-29-18 11:26 AM
To: [redacted]
Cc:
Subject: RE: ICA Lessons Learned

Classification: Top Secret/[redacted]/Canadian Eyes Only
Classification: Très secret/[redacted]/Réservé aux Canadiens
Not for PA / Ne pas classer

[redacted]

Cool, makes sense. I'm looping in [redacted]

There are a few additional ones that you have not listed, but which are relevant for your goals (and which we can speak to):

[redacted]

Unfortunately, [redacted] is not available on Friday. That said, I think we should start a discussion then, with the view that more than one discussion will be required to impart the corporate knowledge/history on all of these files. As such, [redacted] could likely come into the next discussion (which could follow as soon as next week, if needed).

Cheers,

[redacted]

[redacted]

From: [redacted] [mailto:[redacted]
Sent: 29-Aug-18 11:09 AM
To: [redacted](PSEPC-SPPCC);[redacted]
Cc: [redacted](PSEPC-SPPCC)
Subject: RE: ICA Lessons Learned

Classification: TOP SECRET/[redacted]/CANADIAN EYES ONLY

Hi [redacted]

Friday works on our end.

In terms of vision, we turned our attention towards the 'how do we share our collective knowledge [redacted] question, and came up with a lessons learned template. Welcome your advice on how we can improve our template as I'm concerned that it reads too much like a summary as opposed to a reflective analysis.

The plan is to develop them for the following cases:

[redacted]

For the [redacted]type document which would provide more depth and background.

[redacted]

From: [redacted] [mailto:[redacted]
Sent: August-29-18 8:09 AM
To: [redacted]
Cc: [redacted]
Subject: RE: ICA Lessons Learned

Classification: Top Secret/[redacted]Canadian Eyes Only

Classification: Très secret/[redacted]/Réservé aux Canadiens
Not for PA / Ne pas classer

I've suggested this Friday (late morning), but let us know and we can shift into future weeks if necessary.

I'll look forward to scanning the preliminary lessons learned docs. At the outset of our discussion, I'd like to get context on PS' vision for how lessons learned will be shared and applied to improve case management.

Cheers,

[redacted]

From: [redacted] [mailto[redacted]
Sent: 28-Aug-18 2:37 PM
To: [redacted](PSEPC-SPPCC); [redacted]
Cc: [redacted](PSEPC-SPPCC)
Subject: RE: ICA Lessons Learned

Classification: TOP SECRET//[redacted]/CANADIAN EYES ONLY

And we'll drag [redacted] along as well.

From: [redacted]
Sent: August-28-18 2:31 PM
To: [redacted]CSIS-SCRS)
Cc: [redacted](CSIS-SCRS)
Subject: RE: ICA Lessons Learned

Classification: TOP SECRET/[redacted]/CANADIAN EYES ONLY

Thanks, [redacted] We'd love to have both your and [redacted]s feedback on the major ICA cases. I have attached three of the draft lessons learned documents that we put together. From these documents, you can see what sort of information we are trying to capture.

Thursdays and Fridays appear to be the most flexible for our team's weekly schedule. So, if you find a time of day when both you and [redacted] are available and there's a boardroom open, we'll be there! ☺

Cheers,
[redacted]

From: [redacted]
Sent: August-28-18 12:11 PM
To: [redacted]
Cc: [redacted]
Subject: RE: ICA Lessons Learned

Classification: SECRET

Hi [redacted] that sounds great and thank you for making yourselves available.

I'll let [redacted] suggest some times. We have a draft lessons learned for [redacted] that she can share with you as well.

From: [redacted] [mailto:[redacted]
Sent: August-27-18 3:44 PM
To: [redacted]
Cc: [redacted]
Subject: RE: ICA Lessons Learned

Classification: Secret
Classification: Secret
Not for PA / Ne pas classer

Hi [redacted]

I think it's great that the ICA team is doing a lessons learned exercise. When I was still there, we often talked about doing one, but never had the time. So kudos!

[redacted]

It would be more convenient for [redacted] and I if you guys could come out to us (especially considering I don't technically work on this file anymore and would have a hard time justifying taxi chits). [redacted] and I are fairly flexible over the next two weeks. How about you suggest a couple of dates/times that work for you and we'll see if we can get a boardroom?

Best,
[redacted]

[redacted]

From: [redacted] [mailto:[redacted]
Sent: 27-Aug-18 1:54 PM
To: [redacted]

Cc: [redacted](PSEPC-SPPCC)
Subject: ICA Lessons Learned

Classification: SECRET//CANADIAN EYES ONLY

Good afternoon [redacted]

I hope this email finds you well!

The ICA team is currently working to put together a "lessons learned" document for each of our historical cases. [redacted]

Would you be open to meeting with us to go over the details of the case? If so, could we set up a time to meet at your convenience? The team would be more than happy for a field trip out your way, if you would prefer to have the meeting at your office.

Thank you so much,

[redacted]
National Security Operations Directorate | Direction générale des opérations de la sécurité nationale
Public Safety and Emergency Preparedness Canada | Sécurité publique et Protection civile Canada
Tel. |Tél. [redacted]

>>>**********[INFO DEPOT START / DÉBUT INFO DÉPÔT]**********
Sender / Envoyeur : [redacted]
Recipients / Receveurs : [redacted](PSEPC-SPPCC);
Subject / Sujet : RE: ICA Lessons Learned
Date : 8/27/2018 3:43:43 PM

>>>**********[INFO DEPOT START / DÉBUT INFO DÉPÔT]**********
Sender / Envoyeur : [redacted]
Recipients / Receveurs : [redacted](PSEPC-SPPCC); [redacted]
Subject / Sujet : RE: ICA Lessons Learned
Date : 8/29/2018 8:09:04 AM

>>>**********[INFO DEPOT START / DÉBUT INFO DÉPÔT]**********
Sender / Envoyeur : [redacted]
Recipients / Receveurs : [redacted](PSEPC-SPPCC); [redacted](PSEPC-SPPCC); [redacted]
Subject / Sujet : RE: ICA Lessons Learned
Date : 8/29/2018 11:25:39 AM

Pages 576 to / à 587

are withheld pursuant to sections

sont retenues en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

[redacted]

From: [redacted]
Sent: September-11-18 3:10 PM
To: [redacted]
Subject: [redacted]
Attachments: [redacted]

Follow Up Flag: Follow up
Flag Status: Completed

Classification: Top Secret/[redacted]Canadian Eyes Only
Classification: Très secret/[redacted]Réservé aux Canadiens
Not for PA / Ne pas classer

Took a long time to get published, but here is the [redacted](attached).

Cheers,

[redacted]

[redacted]

>>>**********[INFO DEPOT START / DÉBUT INFO DÉPÔT]**********
Sender / Envoyeur : [redacted]
Recipients / Receveurs : [redacted]PSEPC-SPPCC); [redacted](PSEPC-SPPCC); [redacted]PSEPC-SPPCC); [redacted](PSEPC-SPPCC);
Subject / Sujet : [redacted]
Date : 9/11/2018 3:09:56 PM

Pages 589 to / à 597

are duplicates

sont des duplicatas

[redacted]

From: [redacted]
Sent: September-12-18 7:59 AM
To: [redacted]
Subject: RE: [redacted]

Classification: Top Secret/[redacted]/Canadian Eyes Only
Classification: Très secret/[redacted]/Réservé aux Canadiens
Not for PA / Ne pas classer

[redacted]

Cheers,

[redacted]

From: [redacted] mailto:[redacted]
Sent: 11-Sep-18 3:41 PM
To: [redacted] (PSEPC-SPPCC); [redacted] (PSEPC-SPPCC); [redacted] (PSEPC-SPPCC)
Subject: RE: [redacted]

Classification: TOP SECRET/[redacted]CANADIAN EYES ONLY

Thanks, [redacted]

[redacted]

[redacted]

From: [redacted][mailto:[redacted]
Sent: September-11-18 3:10 PM
To: [redacted]
Subject: [redacted]

Classification: Top Secret/[redacted]Canadian Eyes Only
Classification: Très secret/[redacted]Réservé aux Canadiens
Not for PA / Ne pas classer

[redacted]

Cheers,

[redacted]

[redacted]

>>>**********[INFO DEPOT START / DÉBUT INFO DÉPÔT]**********
Sender / Envoyeur : [redacted]
Recipients / Receveurs : [redacted]PSEPC-SPPCC); [redacted](PSEPC-SPPCC); [redacted]PSEPC-SPPCC); [redacted]PSEPC-SPPCC);
Subject / Sujet : [redacted]
Date : 9/11/2018 3:09:56 PM

>>>**********[INFO DEPOT START / DÉBUT INFO DÉPÔT]**********
Sender / Envoyeur : [redacted]
Recipients / Receveurs : [redacted][PSEPC-SPPCC); [redacted](PSEPC-SPPCC); [redacted]
(PSEPC-SPPCC);
Subject / Sujet : RE: [redacted]
Date : 9/12/2018 7:58:54 AM

Pages 600 to / à 608

are duplicates

sont des duplicatas

[redacted]

From: [redacted]
Sent: September-12-18 9:52 AM
To: [redacted]
Subject: FW: [redacted]

Classification: TOP SECRET/[redacted]CANADIAN EYES ONLY

Hi [redacted]

[redacted]

[redacted]

From: [redacted] [mailto:[redacted]
Sent: September-12-18 7:59 AM
To: [redacted]
Subject: RE: [redacted]

Classification: Top Secret/[redacted]Canadian Eyes Only
Classification: Très secret/[redacted]Réservé aux Canadiens
Not for PA / Ne pas classer

[redacted]

Cheers,

[redacted]

[redacted]

From: [redacted] [mailto[redacted]
Sent: 11-Sep-18 3:41 PM

To: [redacted](PSEPC-SPPCC); [redacted](PSEPC-SPPCC); [redacted](PSEPC-SPPCC)
Subject: RE: [redacted]

Classification: TOP SECRET/[redacted]CANADIAN EYES ONLY

Thanks, [redacted]

[redacted]

[redacted]

From: [redacted][mailto:[redacted]
Sent: September-11-18 3:10 PM
To: [redacted]
Subject: [redacted]

Classification: Top Secret/[redacted]Canadian Eyes Only
Classification: Très secret[redacted]Réservé aux Canadiens
Not for PA / Ne pas classer

[redacted]

Cheers,

[redacted]

[redacted]

>>>**********[INFO DEPOT START / DÉBUT INFO DÉPÔT]**********
Sender / Envoyeur : [redacted]
Recipients / Receveurs : [redacted](PSEPC-SPPCC); [redacted](PSEPC-SPPCC); [redacted](PSEPC-SPPCC); [redacted]PSEPC-SPPCC);
Subject / Sujet : [redacted]
Date : 9/11/2018 3:09:56 PM

>>>**********[INFO DEPOT START / DÉBUT INFO DÉPÔT]**********
Sender / Envoyeur : [redacted]
Recipients / Receveurs : [redacted](PSEPC-SPPCC); [redacted](PSEPC-SPPCC); [redacted]
(PSEPC-SPPCC);

Subject / Sujet : RE: [redacted]
Date : 9/12/2018 7:58:54 AM

[redacted]

From: [redacted]
Sent: September-28-18 12:48 PM
To: [redacted] Gumley, Matthew (RCMP-GRC); Burns, Genevieve (RCMP-GRC); Best, Emma (RCMP-GRC); Gordon, Eric (RCMP-GRC); [redacted] (PCO) (PCO-BCP); Herne, Joel (PWGSC-TPSGC); Richard, Daniel (PWGSC-TPSGC); Spassova, Irina (NRCAN-RNCAN); Faucher, Monique (NRCAN-RNCAN); Karman, Mehmet (ISED); Burke, Mary (ISED); Kack, Shannon (ISED); Keating, Sean (ISED); Tarantino, Maria (ISED); Dewolfe, Jonathan (ISED); [redacted] (CSE-CST); Anderson, Cori C - Civ (DND-MDN); Partridge, Shannon SK (DND-MDN); Radulovic, Laura LS - Civ (DND-MDN); [redacted] (INTERNATIONAL); [redacted] (INTERNATIONAL); [redacted] (INTERNATIONAL); [redacted] (INTERNATIONAL); [redacted] (INTERNATIONAL); [redacted] Dundas Julia N'
Cc: [redacted]
Subject: FW: [redacted]
Attachments: [redacted] draft agenda - 28 Sept.xlsx

Classification: TOP SECRET

Good afternoon everyone,

Please see below a message regarding [redacted] participation. [redacted] has requested final delegation confirmation by Friday, October 5.

Also note a new addition to the agenda. [redacted]

Grateful if any outstanding confirmations could be relayed to [redacted] as soon as possible.

Thanks!

[redacted]

From: [redacted]
Sent: September-28-18 12:34 PM
To: [redacted]
Cc: [redacted]
Subject: [redacted]

Classification: Top Secret
Classification: Très secret
Not for PA / Ne pas classer

[redacted]

With [redacted] we've now been asked [redacted] for final confirmation of the [redacted] delegation by **2018 10 05**. To date, we have the following participants [redacted]

[redacted]

Can PS please confirm with partners (one last time) that the list is correct.

Lastly, I've attached the latest version of the draft agenda. [redacted] Can policy departments please advise [redacted] if they wish to attend, as we've been asked to relay their interest back to [redacted]

Thanks,
[redacted]

>>>**********[INFO DEPOT START / DÉBUT INFO DÉPÔT]**********
Sender / Envoyeur : [redacted]
Recipients / Receveurs [redacted] (PSEPC-SPPCC);
Subject / Sujet : [redacted]
Date : 9/28/2018 12:34:15 PM

Page 614

is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

[redacted]

From: [redacted]
Sent: October-17-18 3:13 PM
To: [redacted]

Subject:

Classification: TOP SECRET//CANADIAN EYES ONLY

From today's DFIB

[redacted]

[redacted]

From: [redacted]
Sent: October-25-18 8:45 AM
To: [redacted]
Subject: RE: [redacted]

Classification: TOP SECRET/[redacted] CANADIAN EYES ONLY

Okay, thanks.

From: [redacted] [mailto: [redacted]
Sent: October-25-18 8:01 AM
To: [redacted]
Subject: RE: [redacted]

Classification: Top Secret/[redacted] Canadian Eyes Only
Classification: Très secret/[redacted] Réservé aux Canadiens
Not for PA / Ne pas classer

Hi [redacted]

[redacted]

I'll keep you posted if anything changes.

Cheers,

[redacted]

[redacted]

From: [redacted] [mailto: [redacted]
Sent: 24-Oct-18 5:21 PM
To: [redacted]
Subject: RE: [redacted]

Classification: TOP SECRET/[redacted]CANADIAN EYES ONLY

Hi [redacted]

Was this [redacted]ever finalized?

[redacted]

From: [redacted] mailto [redacted]
Sent: July-06-18 1:13 PM
To: [redacted] Burns, Genevieve (RCMP-GRC); Best, Emma (RCMP-GRC); Gumley, Matthew (RCMP-GRC); Gordon, Eric (RCMP-GRC); [redacted] (PCO) (PCO-BCP); [redacted] (CSE-CST); [redacted] (INTERNATIONAL); [redacted] (INTERNATIONAL); [redacted] (INTERNATIONAL)
Cc: [redacted] Anderson, Cori C - Civ (DND-MDN); Partridge, Shannon SK (DND-MDN)
Subject: RE: [redacted]

Classification: Top Secret/[redacted]Canadian Eyes Only
Classification: Très secret/[redacted]Réservé aux Canadiens
Not for PA / Ne pas classer

Colleagues,

Given this proposed interdepartmental discussion [redacted]

We hope that this draft is informative and helpful for Tuesday's discussion.

Cheers,

[redacted]

From: [redacted] [mailto [redacted]
Sent: 6-Jul-18 9:40 AM

To: Genevieve Burns (RCMP-GRC); Emma Best (RCMP-GRC); Matthew Gumley (RCMP-GRC); Eric Gordon (RCMP-GRC); [redacted](PCO-BCP); [redacted]CSE-CST); [redacted](INTERNATIONAL); [redacted](INTERNATIONAL); [redacted](INTERNATIONAL)
Cc: [redacted](PSEPC-SPPCC); [redacted]PSEPC-SPPCC); [redacted](PSEPC-SPPCC); [redacted](PSEPC-SPPCC); Cori Anderson (DND-MDN); Shannon Partridge (DND-MDN)
Subject: [redacted]

Classification: TOP SECRET[redacted]CANADIAN EYES ONLY

Hello All,

[redacted]

Thank you,

[redacted]
National Security Operations Directorate – Direction générale des opérations de la sécurité nationale
Public Safety and Emergency Preparedness Canada – Sécurité publique et Protection civile Canada
Tel. – Tél. [redacted]

>>>**********[INFO DEPOT START / DÉBUT INFO DÉPÔT]**********
Sender / Envoyeur : [redacted]
Recipients / Receveurs [redacted](PSEPC-SPPCC); Genevieve Burns (RCMP-GRC); Emma Best (RCMP-GRC); Matthew Gumley (RCMP-GRC); Eric Gordon (RCMP-GRC); [redacted](PCO-BCP); [redacted](CSE-CST); [redacted](INTERNATIONAL); [redacted]INTERNATIONAL); [redacted](INTERNATIONAL);
Subject / Sujet : RE: [redacted]
Date : 7/6/2018 1:12:43 PM

>>>**********[INFO DEPOT START / DÉBUT INFO DÉPÔT]**********
Sender / Envoyeur : [redacted]
Recipients / Receveurs : [redacted]
Subject / Sujet : RE [redacted]
Date : 10/25/2018 8:01:26 AM

[redacted]

From: [redacted]
Sent: November-07-18 1:54 PM
To: [redacted]
Subject: FW: [redacted]
Attachments: [redacted]

Classification: TOP SECRET/[redacted]CANADIAN EYES ONLY

Pages 620 to / à 627

are duplicates

sont des duplicatas

[redacted]

From: [redacted]
Sent: November-09-18 5:08 PM
To: [redacted] CSE-CST); [redacted] (CSE-CST)
Cc:
Subject: DM IRC - Draft Responses
Attachments: DM IRC - Responses - November 14 meeting.docx

Classification: TOP SECRET/[redacted]/CANADIAN EYES ONLY

Hello [redacted]

Thank you very much for coming over and chatting with us.

I spoke with [redacted] after and we pared down some of the responses noting that we are seeking a 'pithy' document. I have added the components we discussed and tried to keep it short and sweet, if you will. Caveat to note that this has not been circulated for approval and very much draft at this time. Please do not share further.

Please take a look and let me know if I have captured these items correctly as discussed. If you have additional language that you would suggest instead, would greatly appreciate feedback. As you know, the DM meeting is [redacted] so feedback at your earliest convenience would be great.

Thank you again,
[redacted]

[redacted]
National Security Operations Directorate – Direction générale des opérations de la sécurité nationale
Public Safety and Emergency Preparedness Canada – Sécurité publique et Protection civile Canada
Tel. – Tél. [redacted]

Pages 629 to / à 630

are withheld pursuant to sections

sont retenues en vertu des articles

of the Access to Information

de la Loi sur l'accès à l'information

Merchant, Colleen

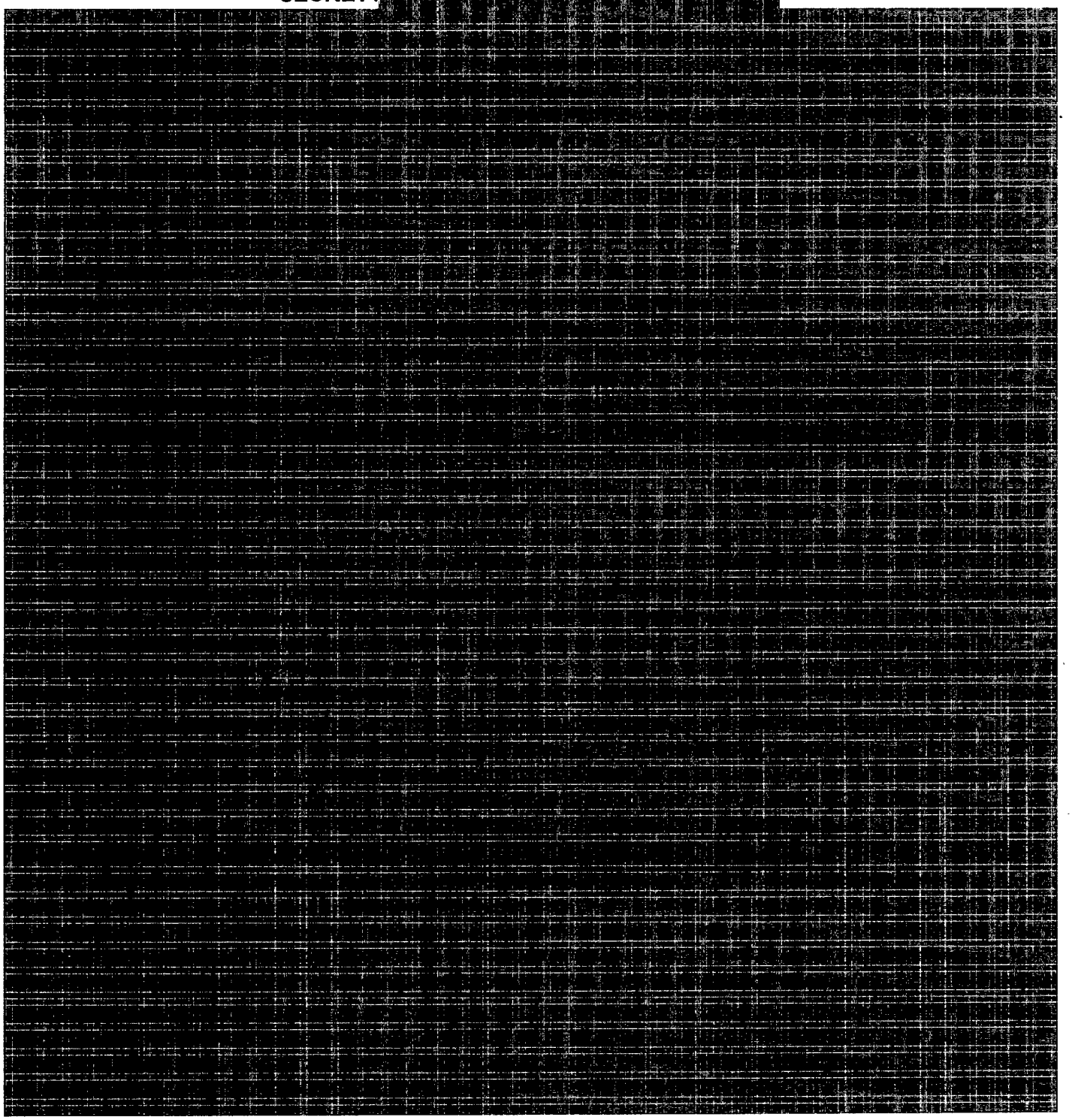
From: INTERNATIONAL Shared - Washington DC ILO Group Mailbox

Sent: October-25-18 5:37 PM

To: Green Martin PCO) (PCO-BCP);
Benjamin, Martin; Chayer, Marie-Helene MH - Civ;

Subject:

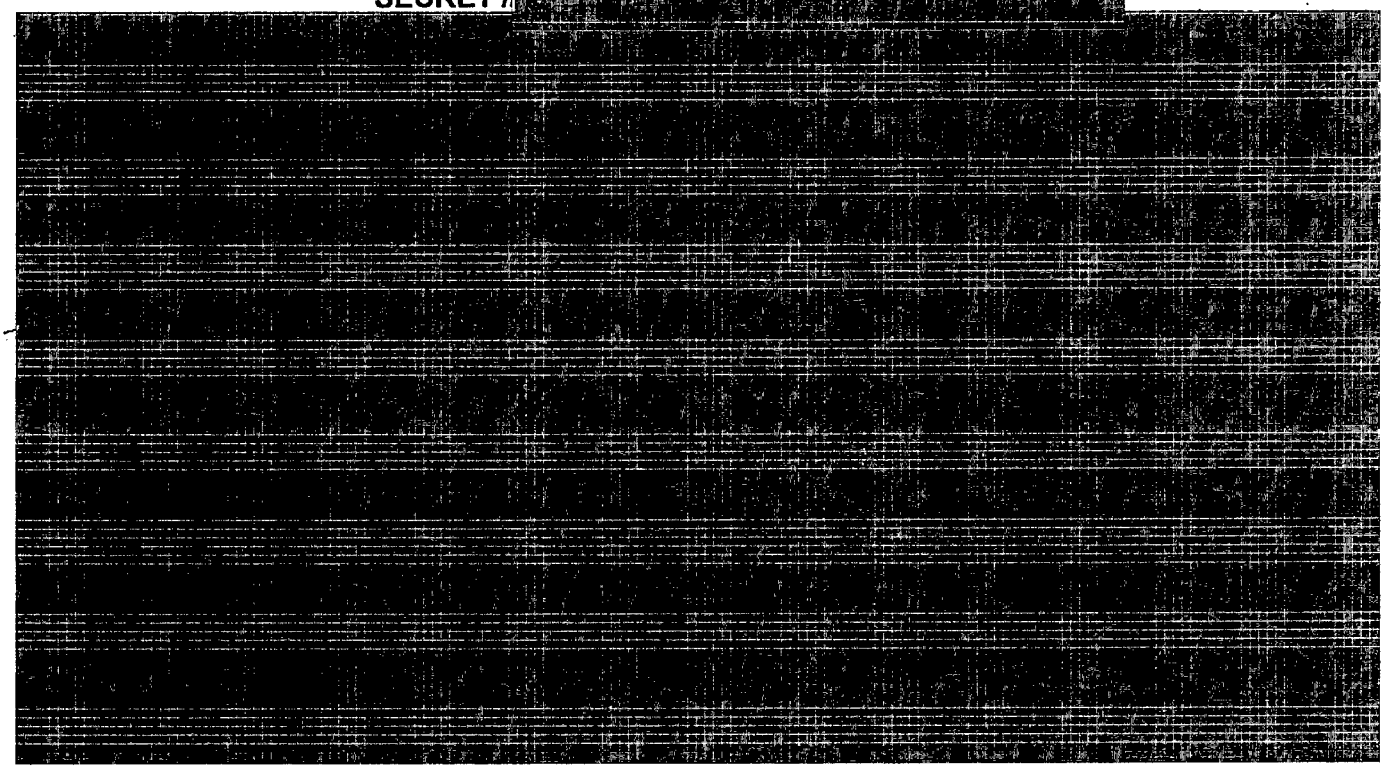
Classification: SECRET //



Embassy of Canada | Ambassade du Canada
Washington D.C.

BCC list:

[redacted]



Best,
[redacted]

[redacted]
Senior Policy Advisor
Threat Assessment and Intelligence Services Division (Policy Unit)
Global Affairs Canada
[redacted]
CTSN [redacted]

From: [redacted]
Sent: November-09-18 10:37 AM
To: [redacted]
Cc: [redacted]
Merchant, Colleen; [redacted]
Subject: [redacted]

Classification: TOP SECRET //CANADIAN EYES ONLY

Hi all,

As all here are aware, [redacted]

[redacted]
Senior Policy Advisor
Threat Assessment and Intelligence Services Division (Policy Unit)
Global Affairs Canada
[redacted]
CTSN: [redacted]

[redacted]

From: [redacted]
Sent: July-11-18 8:46 AM
To: [redacted]
Cc:
Subject: RE: [redacted]

Classification: Secret//Canadian Eyes Only
Classification: Secret//Réservé aux Canadiens
Not for PA / Ne pas classer

Hi [redacted]

[redacted]

Cheers,

[redacted]

[redacted]

From: [redacted] [mailto: [redacted]
Sent: 10-Jul-18 5:07 PM
To: [redacted]
Cc: [redacted] (PSEPC-SPPCC); [redacted] (PSEPC-SPPCC)
Subject: RE: [redacted]

Classification: TOP SECRET

Hi [redacted]

Thanks for the chat yesterday. [redacted]

[redacted]

Let me know if i missed anything! Will CC [redacted] and request that it go to your unit when I submit to [redacted]

Thanks!

[redacted]

From: [redacted] [mailto: [redacted]
Sent: July-05-18 2:47 PM
To: [redacted]
Subject: RE: [redacted]

Classification: Top Secret
Classification: Très secret
Not for PA / Ne pas classer

Slight change in circumstances here (things are developing rapidly). I'm now thinking it best that we meet on Monday, show you what we have, and then consider next steps (including whether a formal request makes sense).

Hope it's okay waiting until Monday.

[redacted]

From: [redacted] [mailto:[redacted]
Sent: 5-Jul-18 2:46 PM
To: [redacted]
Subject: RE: [redacted]

Classification: TOP SECRET

Hey [redacted] – apologies, [redacted] Is there a certain format that needs to be followed or can it just be [redacted]

From: [redacted] [mailto:[redacted]
Sent: July-05-18 10:26 AM
To: [redacted]
Cc: [redacted]
Subject: RE: [redacted]

Classification: Top Secret
Classification: Très secret
Not for PA / Ne pas classer

[redacted]

So, over to the PS side – want to set up a chat for some time next week? Let me know (including timing) and we'll look to book a room.

Cheers,

[redacted]

P.s. – If you are sending a request for [redacted] please direct it to [redacted]

[redacted]

[redacted]

From: [redacted] [mailto: [redacted]
Sent: 5-Jul-18 10:14 AM
To: [redacted]
Cc: [redacted] (PSEPC-SPPCC); [redacted] (PSEPC-SPPCC)
Subject: RE [redacted]

Classification: TOP SECRET

Hi [redacted]

Thank you for following up! I imagine there have been a bunch of new developments.

[redacted]

I get the sense the policy work will be moving forward quite rapidly given the interest so I'll keep you posted on circulation of that paper for comments.

Thanks again!

[redacted]

From: [redacted] [mailto [redacted]
Sent: July-05-18 9:35 AM
To: [redacted]
Cc: [redacted]
Subject: [redacted]

Classification: Top Secret
Classification: Très secret
Not for PA / Ne pas classer

Hi [redacted]

[redacted]

Happy to chat, if helpful.

Cheers,

[redacted]

P.s. [redacted] That would add to the discussion and could also likely be produced in the near future, if requested.

[redacted]

>>>**********[INFO DEPOT START / DÉBUT INFO DÉPÔT]**********
Sender / Envoyeur : [redacted]
Recipients / Receveurs : [redacted] (PSEPC-SPPCC);
Subject / Sujet : [redacted]
Date : 7/5/2018 9:34:50 AM

>>>**********[INFO DEPOT START / DÉBUT INFO DÉPÔT]**********
Sender / Envoyeur : [redacted]
Recipients / Receveurs : [redacted]
Subject / Sujet : RE: [redacted]
Date : 7/5/2018 10:26:20 AM

>>>**********[INFO DEPOT START / DÉBUT INFO DÉPÔT]**********
Sender / Envoyeur : [redacted]
Recipients / Receveurs : [redacted]
Subject / Sujet : RE: [redacted]
Date : 7/5/2018 2:47:20 PM

>>>**********[INFO DEPOT START / DÉBUT INFO DÉPÔT]**********
Sender / Envoyeur : [redacted]
Recipients / Receveurs : [redacted]
Subject / Sujet : RE: [redacted]
Date : 7/11/2018 8:46:18 AM

[redacted]

From: [redacted]
Sent: July-11-18 8:49 AM
To: [redacted]
Cc:
Subject: RE: [redacted]

Classification: SECRET

Great, thank you! Much appreciated. Do you know what the next steps are with these? [redacted]

I think [redacted] was going to reach out to [redacted] today to ask if [redacted]

From: [redacted] [mailto: [redacted]
Sent: July-11-18 8:42 AM
To: [redacted]
Cc: [redacted]
Subject: RE: [redacted]

Classification: Secret
Classification: Secret
Not for PA / Ne pas classer

For sure – these are just quick, candid reactions to the list you sent:

[redacted]

[redacted]

[redacted]

From: [redacted] mailto: [redacted]
Sent: 10-Jul-18 5:17 PM
To: [redacted]
Cc: [redacted] (PSEPC-SPPCC)
Subject: FW: [redacted]

Classification: TOP SECRET/[redacted]/CANADIAN EYES ONLY

Hey [redacted]

At our meeting yesterday, you had some comments on [redacted]
We can then consider adjusting/ reframing some of the questions/suggested content.

Let me know if that works for you,

[redacted]

From: [redacted] [mailto:[redacted]
Sent: June-28-18 4:06 PM
To: [redacted]
Cc: [redacted]
Subject: RE: [redacted]

Classification: Top Secret
Classification: Très secret
Not for PA / Ne pas classer

Classification: TOP SECRET/[redacted]/CANADIAN EYES ONLY

Thanks [redacted] we'll include it in our response.

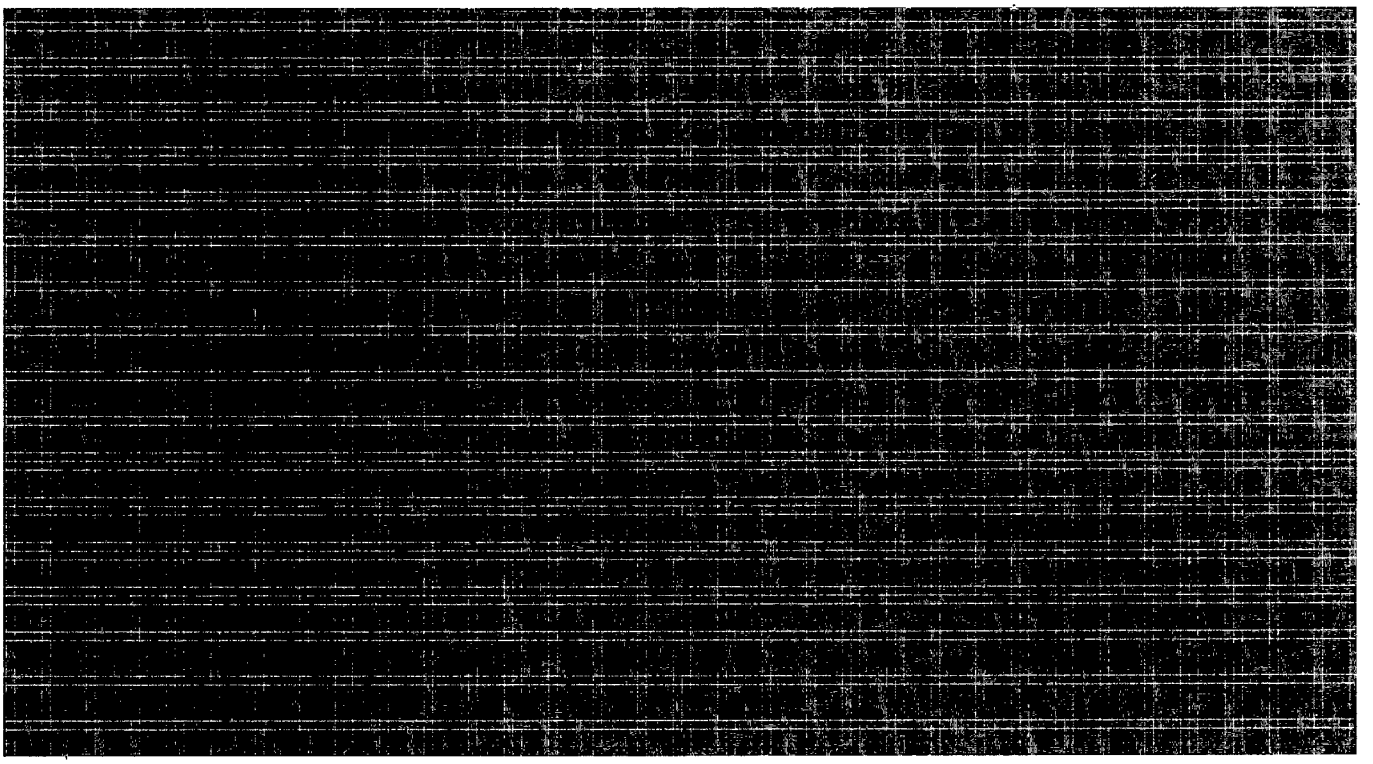
From: [redacted] [mailto:[redacted]
Sent: 28-Jun-18 3:29 PM
To: [redacted]
Cc: [redacted] (PSEPC-SPPCC); [redacted] PSEPC-SPPCC)
Subject: FW: [redacted]

Classification: TOP SECRET/[redacted]/CANADIAN EYES ONLY

Hi [redacted]

As discussed at DRC, [redacted] has produced a list of suggested [redacted] discussion topics for your consideration:

[redacted]



[redacted]
National Security Operations Directorate – Direction générale des opérations de la sécurité nationale
Public Safety and Emergency Preparedness Canada – Sécurité publique et Protection civile Canada
Tel. – Tél.: [redacted]

>>>**********[INFO DEPOT START / DÉBUT INFO DÉPÔT]**********
Sender / Envoyeur : [redacted]
Recipients / Receveurs : [redacted] (PSEPC-SPPCC);
Subject / Sujet : RE: [redacted]
Date : 6/28/2018 4:05:43 PM

>>>**********[INFO DEPOT START / DÉBUT INFO DÉPÔT]**********
Sender / Envoyeur : [redacted]
Recipients / Receveurs : [redacted]
Subject / Sujet : RE: [redacted]
Date : 7/11/2018 8:42:24 AM

[redacted]

From: [redacted]
Sent: July-11-18 8:52 AM
To: [redacted]
Cc:
Subject: RE: [redacted]

s.21 s.15 s.70 s.16

Classification: SECRET//CANADIAN EYES ONLY

Okay great, will do it that way [redacted]

Thanks!!

From: [redacted] [mailto: [redacted]
Sent: July-11-18 8:51 AM
To: [redacted]
Cc:
Subject: RE: [redacted]

Classification: Secret//Canadian Eyes Only
Classification: Secret//Réservé aux Canadiens
Not for PA / Ne pas classer

[redacted]

[redacted]

From: [redacted] [mailto: [redacted]
Sent: 11-Jul-18 8:48 AM
To: [redacted]
Cc: [redacted] (PSEPC-SPPCC); [redacted] (PSEPC-SPPCC)
Subject: RE: [redacted]

Classification: SECRET//CANADIAN EYES ONLY

Okay perfect, will prioritize and send the requests in shortly. [redacted]

[redacted]

From: [redacted] mailto:[redacted]
Sent: July-11-18 8:46 AM
To: [redacted]
Cc: [redacted]
Subject: RE: [redacted]

Classification: Secret//Canadian Eyes Only
Classification: Secret//Réservé aux Canadiens
Not for PA / Ne pas classer

Hi [redacted]

You've got the right approach [redacted]

Cheers,

[redacted]

[redacted]

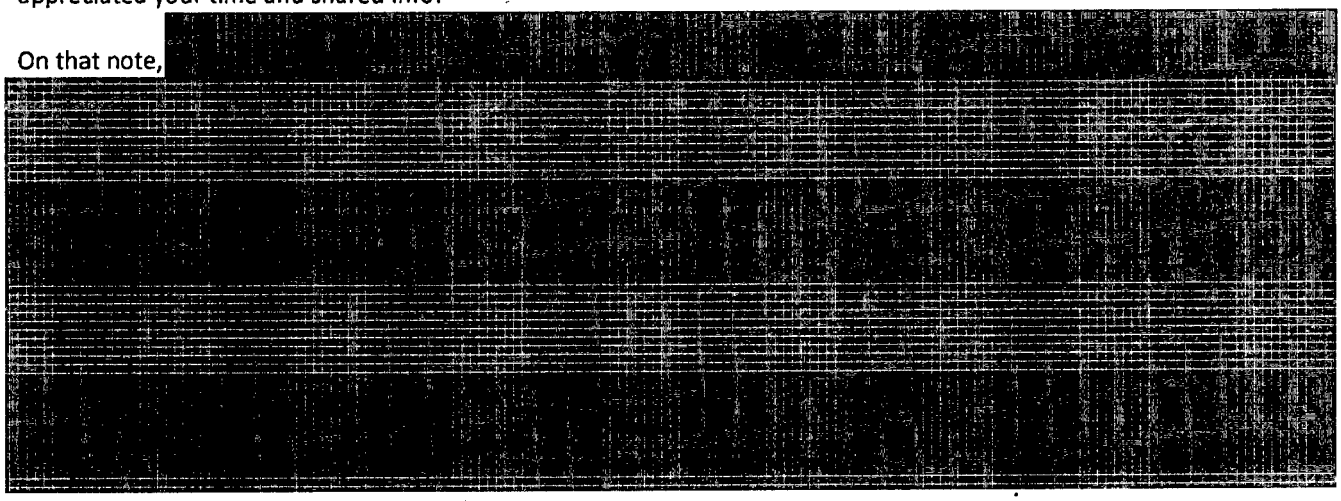
From: [redacted] mailto:[redacted]
Sent: 10-Jul-18 5:07 PM
To: [redacted]
Cc: [redacted] (PSEPC-SPPCC); [redacted] (PSEPC-SPPCC)
Subject: RE [redacted]

Classification: TOP SECRET

Hi [redacted]

Thanks for the chat yesterday. It is always good for perspective to have these discussions at the working level – we appreciated your time and shared info!

On that note, [redacted]



Let me know if i missed anything! Will CC [redacted] and request that it go to your unit when I submit to [redacted]

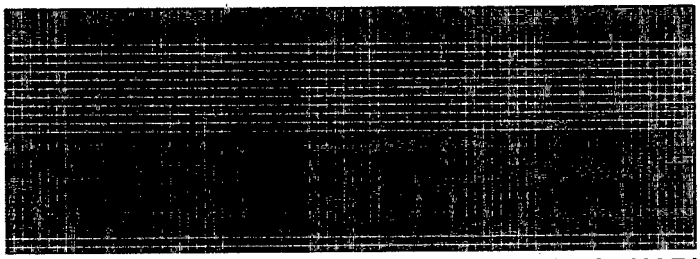
Thanks!
[redacted]

From: [redacted] [mailto [redacted]
Sent: July-05-18 2:47 PM
To: [redacted]
Subject: RE: [redacted]

Classification: Top Secret
Classification: Très secret
Not for PA / Ne pas classer

Slight change in circumstances here (things are developing rapidly). I'm now thinking it best that we meet on Monday, show you what we have, and then consider next steps (including whether a formal request makes sense).

Hope it's okay waiting until Monday.



[redacted]

From: [redacted] [mailto:[redacted]
Sent: 5-Jul-18 2:46 PM
To: [redacted]
Subject: RE: [redacted]

Classification: TOP SECRET

Hey [redacted] - apologies. [redacted] Is there a certain format that needs to be followed or can it just be [redacted]

From: [redacted] [mailto:[redacted]
Sent: July-05-18 10:26 AM
To: [redacted]
Cc: [redacted]
Subject: RE: [redacted]

Classification: Top Secret
Classification: Très secret
Not for PA / Ne pas classer

[redacted]

So, over to the PS side – want to set up a chat for some time next week? Let me know (including timing) and we'll look to book a room.

Cheers,

[redacted]

P.s. – If you are sending a request for [redacted] please direct it to [redacted]

[redacted]

[redacted]

From: [redacted] [mailto: [redacted]
Sent: 5-Jul-18 10:14 AM
To: [redacted]
Cc: [redacted] (PSEPC-SPPCC); [redacted] (PSEPC-SPPCC)
Subject: RE: [redacted]

Classification: TOP SECRET

Hi [redacted]

Thank you for following up! I imagine there have been a bunch of new developments.

[redacted]

I get the sense the policy work will be moving forward quite rapidly given the interest so I'll keep you posted on circulation of that paper for comments.

Thanks again!
[redacted]

From: [redacted] [mailto: [redacted]
Sent: July-05-18 9:35 AM
To: [redacted]
Cc: [redacted]
Subject: [redacted]

Classification: Top Secret
Classification: Très secret
Not for PA / Ne pas classer

Hi [redacted]

[redacted]

Happy to chat, if helpful.

Cheers,

[redacted]

P.s. [redacted] That would add to the discussion and could also likely be produced in the near future, if requested.

[redacted]

>>>**********[INFO DEPOT START / DÉBUT INFO DÉPÔT]**********
Sender / Envoyeur : [redacted]
Recipients / Receveurs : [redacted] (PSEPC-SPPCC);
Subject / Sujet : [redacted]
Date : 7/5/2018 9:34:50 AM

>>>**********[INFO DEPOT START / DÉBUT INFO DÉPÔT]**********
Sender / Envoyeur : [redacted]
Recipients / Receveurs : [redacted]
Subject / Sujet : RE: [redacted]
Date : 7/5/2018 10:26:20 AM

>>>**********[INFO DEPOT START / DÉBUT INFO DÉPÔT]**********
Sender / Envoyeur : [redacted]
Recipients / Receveurs : [redacted]
Subject / Sujet : RE: [redacted]
Date : 7/5/2018 2:47:20 PM

>>>**********[INFO DEPOT START / DÉBUT INFO DÉPÔT]**********
Sender / Envoyeur : [redacted]
Recipients / Receveurs : [redacted]
Subject / Sujet : RE: [redacted]
Date : 7/11/2018 8:46:18 AM

>>>**********[INFO DEPOT START / DÉBUT INFO DÉPÔT]**********
Sender / Envoyeur : [redacted]
Recipients / Receveurs : [redacted]

Subject / Sujet : RE: [redacted]
Date : 7/11/2018 8:50:58 AM

Merchant, Colleen

From: Green, Adam
Sent: October-12-18 4:11 PM
To: Beauregard, Monik; Merchant, Colleen
Subject: FW: [redacted] Dealing with Huawei and ZTE in 5G: The Australia and New Zealand Contexts
Attachments: Australian 5G Announcement.docx

Classification: SECRET/[redacted]CANADIAN EYES ONLY

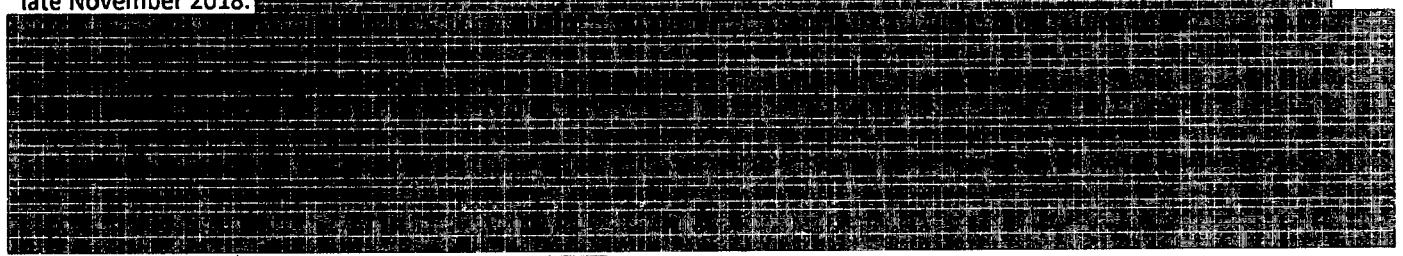
As mentioned in today's BMC.

Best,
Adam

From: [redacted][mailto:[redacted]
Sent: October-08-18 2:59 AM
To: [redacted](PCO) (PCO-BCP); [redacted](PCO) (PCO-BCP); Yendall, Jonathan
Cc: [redacted] Abbott Kathleen [redacted](PCO) (PCO-BCP); [redacted](INTERNATIONAL); Askari Rankouhi Saam [redacted](PCO) (PCO-BCP); [redacted](INTERNATIONAL); Careau Marie-Cecile [redacted](PCO); [redacted] Chayer, Marie-Helene MH - Civ; Xavier Caroline [redacted](PCO) (PCO-BCP); [redacted]; Dalziel Alex [redacted](PCO) (PCO-BCP); [redacted](INTERNATIONAL); Green Martin [redacted](PCO) (PCO-BCP); [redacted](INTERNATIONAL); IASManagement (PCO-BCP); Lacroix, Stephane; [redacted](CSE-CST); [redacted](PCO) (PCO-BCP); Miller Bryan [redacted](PCO) (PCO-BCP); [redacted](CSE-CST); [redacted](PCO) (PCO-BCP); Therriault, Sylvain JCS - Cdr (DND-MDN); [redacted](INTERNATIONAL); [redacted](INTERNATIONAL); [redacted](INTERNATIONAL); [redacted](INTERNATIONAL); [redacted](INTERNATIONAL)
Subject: [redacted] Dealing with Huawei and ZTE in 5G: The Australia and New Zealand Contexts

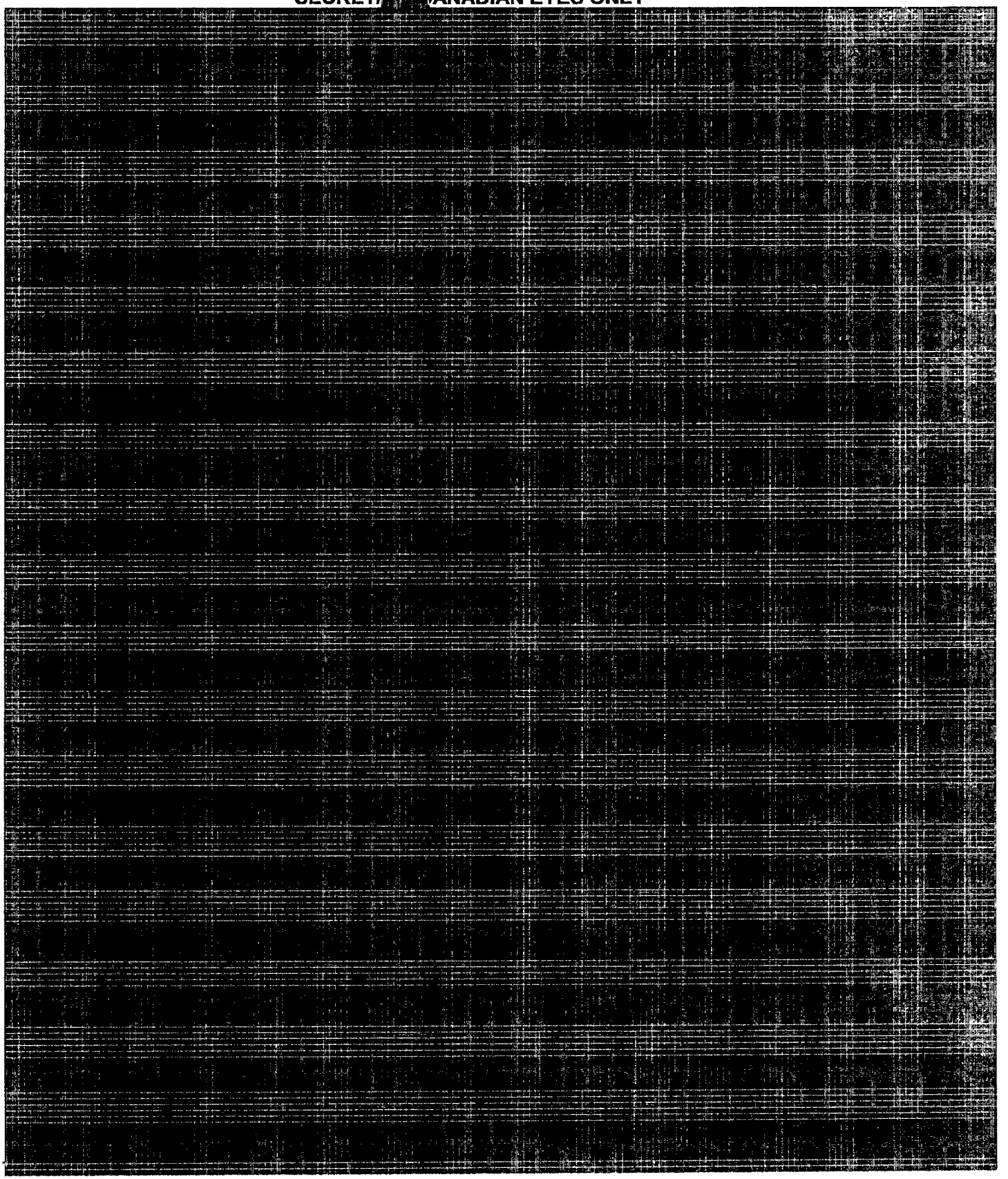
Classification: SECRET/[redacted]CANADIAN EYES ONLY

SUMMARY: On August 23, 2018, the Australian Department of Communications and the Arts released guidance regarding 5G that, in effect, barred providers from using Huawei or ZTE as vendors in their 5G networks. Neither company, nor China was named in the release. The guidance relates to the *Telecommunications Sector Security Reforms* (TSSR) *Act 2017,* which provides the Government significant right to intervene on telecommunications providers' security decision making, particularly with respect to supply chains. Australia's 5G spectrum auction date is set for mid-late November 2018. [redacted]



[redacted]

6. The TSSRs had been in the works for more than five years and were subject of extensive private sector consultation and input. [redacted]



[redacted]

Background on the Critical Infrastructure Centre, the TSSRs and related legislation can be found in:

- [redacted] of January 27, 2017 (unclassified)
- [redacted] of April 19, 2017 (unclassified)
- [redacted] of January 19, 2018 (unclassified)
- The Australian Department of Home Affairs webpage for the TSSRs is at http://www.homeaffairs.gov.au/about/consultations/telecommunications-sector-security-reforms

A version of this report will released on C6.

[redacted]
Counsellor/Conseiller
Security and Intelligence Liaison Officer to Australia and New Zealand / Agent de liaison au renseignement auprès de l'Australie et de la Nouvelle-Zélande
Canadian High Commission / Haut-commissariat du Canada / CNBRA
Tel: [redacted] unclass.)
Mitnet: [redacted]
Hydra: [redacted]

[redacted] (unclass)

Government Provides 5G Security Guidance To Australian Carriers

23 August 2018
Joint Media Release
Senator the Hon Mitch Fifield
Minister for Communications and the Arts
The Hon Scott Morrison MP
Treasurer, Acting Minister for Home Affairs

Fifth Generation (5G) is the next evolution of mobile technology. It promises the ability to improve the daily lives of Australians, strengthen our connectivity and accelerate our networks.

5G will change the way people use, and rely on, mobile services, driving improvements in a range of ways for businesses and communities.

It will enable a new wave of innovation across our community and be used to connect other critical infrastructure, including electricity and water.

5G will underpin the development of smart cities and Internet of Things (IoT), and connect industrial control and safety of life systems, like remote surgery, and autonomous vehicles.

The Government wants to create an environment that allows Australian businesses to be at the forefront of seizing the benefits of 5G across the economy.

To achieve this, the Government is fostering a policy and regulatory environment to support a more efficient rollout, given its potential benefits to the economy.

The Government has undertaken an extensive review of the national security risks to 5G networks.

5G requires a change in the way the network operates compared to previous mobile generations. These changes will increase the potential for threats to our telecommunications networks, and these threats will increase over time as more services come online.

Acting Minister for Home Affairs Scott Morrison said the Government wants to realise the benefits of 5G but acknowledges that this new technology introduces additional risks.

"The security of 5G networks will have fundamental implications for all Australians, as well as the security of critical infrastructure, over the next decade," Mr Morrison said.

Minister for Communications and the Arts Mitch Fifield said that it is vital that security and integrity underpinned the opportunities opened up by 5G networks.

"The Government is committed to the timely rollout of 5G networks in Australia. 5G will drive substantial economic and social benefits across the economy, through new technologies which will be used in autonomous vehicles, smart cities, and advanced agriculture," Minister Fifield said.

The Government is committed to protecting this vital technology. To fully realise 5G's benefits, Government and industry need to continue to work together to take necessary steps to safeguard the security of Australians' information and communications at all times, and the integrity and availability of the networks themselves.

Last year, the Government introduced the Telecommunications Sector Security Reforms (TSSR) to provide a framework for Australia's security agencies and industry to share sensitive information on threats to telecommunications networks.

TSSR introduces four new measures:

- a security obligation, which requires carriers and carriage service providers to protect their networks and facilities against threats to national security from unauthorised access or interference
- a notification requirement, which requires carriers and nominated carriage service providers to tell Government of any proposed changes to their telecommunications systems or services that are likely to have a material adverse effect on their capacity to comply with their security obligation
- the ability for Government to obtain more detailed information from carriers and carriage service providers in certain circumstances to support the work of the Critical Infrastructure Centre, and
- the ability to intervene and issue directions in cases where there are significant national security concerns that cannot be addressed through other means.

"The Government's Telecommunications Sector Security Reforms, which commence on September 18, place obligations on telecommunications companies to protect Australian networks from unauthorised interference or access that might prejudice our national security," Mr Morrison said.

5G requires a network architecture that is significantly different to previous mobile generations.

Traditionally, network equipment used by telecommunications operators has been categorised into the 'core' network and the 'edge' network.

The core network is where the more sensitive functions occur including access control, authentication, voice and data routing, and billing.

The edge consists of the radios and other equipment used to connect customer equipment (such as handsets, laptops and tablets) to the core network.

Where previous mobile networks featured clear functional divisions between the core and the edge, 5G is designed so that sensitive functions currently performed in the physically and logically separated core will gradually move closer to the edge of the network.

In that way, the distinction between the core and the edge will disappear over time.

This shift introduces new challenges for carriers trying to maintain their customers' security, as sensitive functions move outside of the highly protected core environment.

This new architecture provides a way to circumvent traditional security controls by exploiting equipment in the edge of the network – exploitation which may affect overall network integrity and availability, as well as the confidentiality of customer data. A long history of cyber incidents shows cyber actors target Australia and Australians.

Government has found no combination of technical security controls that sufficiently mitigate the risks.

While we are protected as far as possible by current security controls, the new network, with its increased complexity, would render these current protections ineffective in 5G.

Therefore, Government has expectations of the application of the TSSR obligations with respect to the involvement of third party vendors in 5G networks, including evolution of networks leading to mature 5G networks.

The Government considers that the involvement of vendors who are likely to be subject to extrajudicial directions from a foreign government that conflict with Australian law, may risk failure by the carrier to adequately protect a 5G network from unauthorised access or interference.

This applies equally to all carriers, consistent with government's long-standing commitment to a level playing field in the sector.

Carriers may still need to apply controls regardless of the vendor they choose. These controls would not displace existing cyber security practices or business risk mitigations.

Government is well positioned to address these risks in partnership with industry.

Mr Morrison said the Government has been working closely with telecommunications operators to ensure that they understand their new obligations and are ready to comply when the legislation commences on 18 September 2018.

"The Government has now provided carriers with clear guidance about how their new legal obligations apply to 5G networks."

As 5G and related technologies continue to develop, new risks relating to the technology may emerge and require further Government consideration.

"The Government will continue to engage and support Australians, including the telecommunications industry, to manage national security risks," Mr Morrison said.

"The Government's first priority will always be the safety and security of Australians."