

Vinodrai, Arjun

From: Hawrylak, Maciek
Sent: March-06-13 1:10 PM
To: Vinodrai, Arjun
Cc: Chayer, Marie-Helene; Johnston, Shannon; Bizai-Levesque, N; Bedor, Tia Leigh; Dupuis, Chantal; Gélinas, Emilie
Subject: TASKING: DM meetings with Deputy Attorney General (March 14)
Attachments: PS-SP-SEC-#5678-1-Notes - Lawful Access - DM meeting with US Deputy Attorney General - 2013-03-14.DOC

Arjun,

Please find attached NSOD's input regarding "Lawful Access (withdrawal of C-30)" for the Deputy's meeting with US counterparts. It is DG approved.

Best,
Maciek

Senior Policy Advisor | Conseiller principal
National Security Operations Directorate | Direction-générale des opérations de la sécurité nationale
Public Safety Canada | Sécurité publique Canada
Maciek_hawrylak@dragon.ps.gc.ca
613-991-6036

s.13(1)(a)

s.15(1) - Int'l

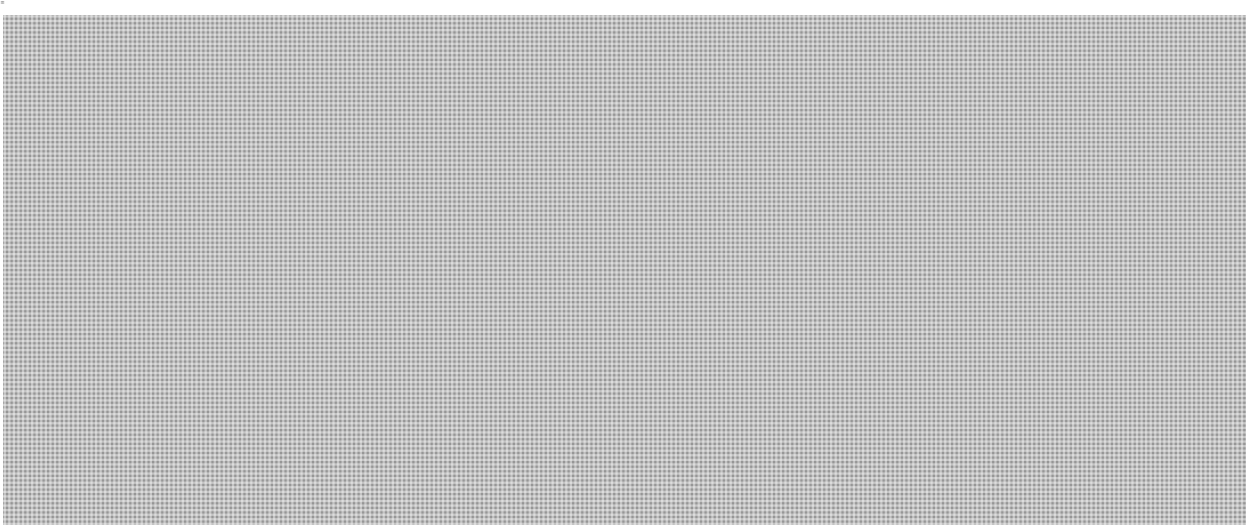
CONFIDENTIAL

s.15(1)(i) and 21(1)(a) of ATI Act apply

**Deputy Minister's meeting with James Cole, US Deputy Attorney General
Background Information and Talking Points
for a Potential Lawful Access Discussion
March 14, 2013**

BACKGROUND

Under the 1994 *Communications Assistance for Law Enforcement Act* (CALEA), telecommunications service providers (TSPs) in the United States (US) must maintain the capability to intercept communications. While CALEA was originally drafted to cover managed wireline voice technologies (i.e. the public telephone system) that were prevalent in the early 1990s, the scope of the law was extended in 2004 to cover new types of telecommunications developed since the law's introduction, including some high speed internet services.



Canada does not have legislation similar to CALEA. An attempt in 2012 to introduce lawful access legislation was met with much criticism, and the Government of Canada has since announced that it will not be pursuing current Bill C-30. This Bill included a suite of legislative measures aimed at:

1. compelling TSPs to build and maintain intercept capable systems;
2. requiring TSPs to provide limited basic subscriber information (such as a subscriber's name, address, telephone number, and e-mail address) to designated authorities and to police officers in certain circumstances;
3. streamlining the warrant application process for multiple investigative techniques involving an interception;
4. modernizing some investigative powers; and
5. introducing safeguards for the use of warrantless interceptions conducted in exceptional circumstances (in response to a 2012 Supreme Court decision, which ruled that the current *Criminal Code* provisions on emergency wiretapping are unconstitutional).

CONFIDENTIAL

s.15(1)(i) and 21(1)(a) of ATI Act apply

On February 11, 2013, the Minister of Justice introduced Bill C-55, the *Response to the Supreme Court of Canada Decision in R. v. Tse Act*, which mainly consists of C-30's provisions to introduce safeguards for the use of warrantless interceptions conducted in exceptional circumstances (number 5 above). The Government publicly indicated that the provisions in Bill C-30 pertaining to interception capability and access to basic subscriber information (numbers 1 and 2 above) would not go forward.

TALKING POINTS

- Technological changes in the telecommunications sector are affecting how law enforcement and national security agencies around the world do their job. We must all adapt to these changes.
- We are following with interest your discussions [REDACTED] If we can provide any assistance, please do not hesitate to contact my officials.

(If pressed on Bill C-30)

- The Government recently introduced legislation to increase the safeguards related to the conduct of warrantless interceptions in exceptional circumstances.
- Specifically, the proposed amendments would include notification and reporting requirements, and would limit the authority to use emergency wiretapping to police officers for specific offences.
- Providing law enforcement and national security agencies with the tools they need to do their job remains a priority, and we continue to look at ways to more effectively fight crime in the digital age.
- Our aim is to strike the right balance between investigative needs and privacy protection.

s.15(1) - Int'l

s.21(1)(a)

16/09/2013



Public Safety / Sécurité publique
Canada

s.15(1) - Int'l

Deputy Minister / Sous-ministre

s.21(1)(a)

Ottawa, Canada
K1A 0P8

CONFIDENTIAL

DATE:

File No.: NS 6950-O1 / 397962
RDIMS: Dragon 18825

MEMORANDUM FOR THE MINISTER

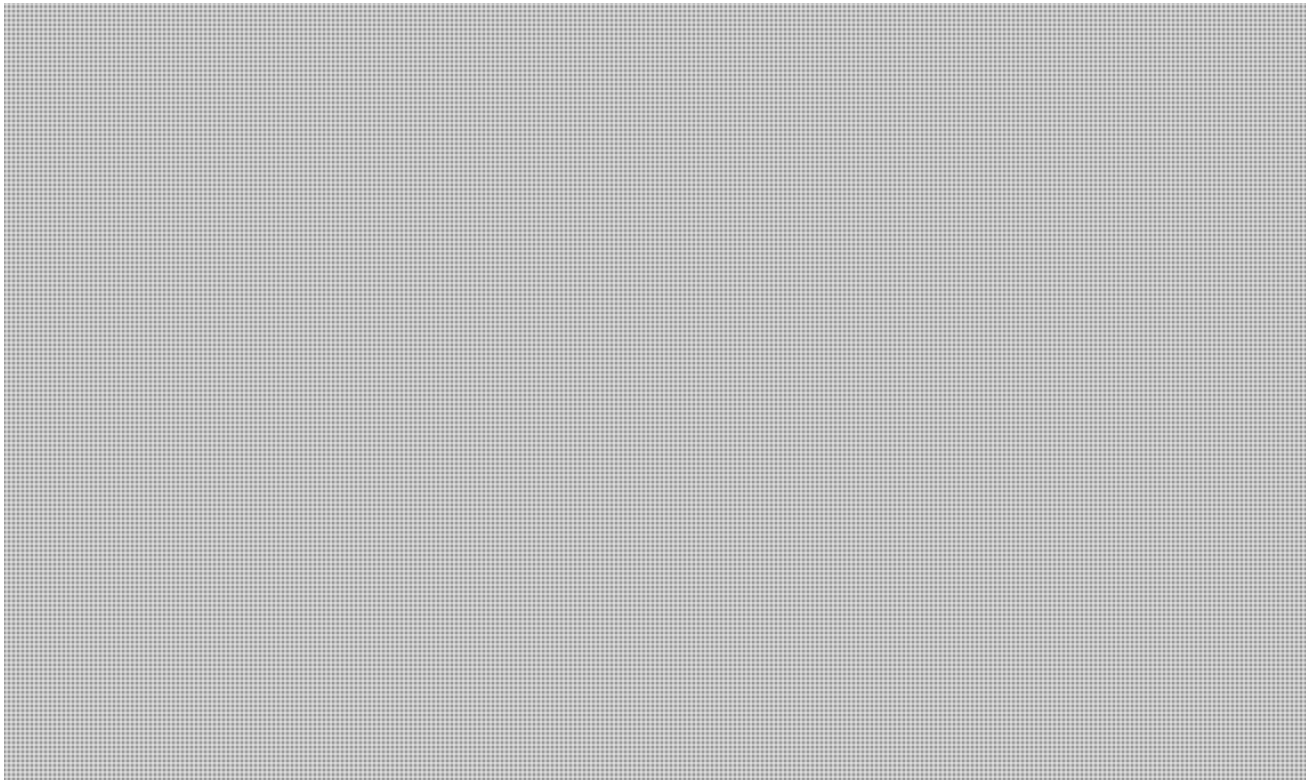


(Signature required)

ISSUE



BACKGROUND



.../2

Page 32

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

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

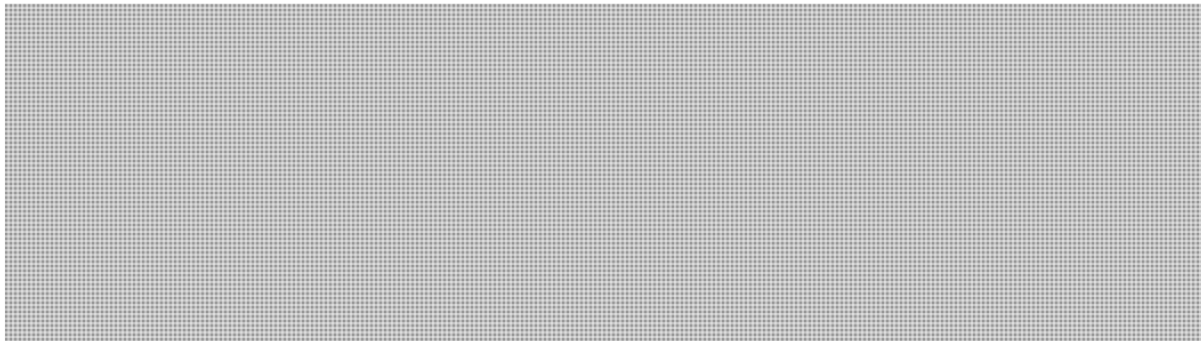
**of the Access to Information
de la Loi sur l'accès à l'information**

s.21(1)(a)

- 3 -

CONFIDENTIAL

NEXT STEPS



RECOMMENDATION



Should you require additional information, please do not hesitate to contact me or Lynda Clairmont, Senior Assistant Deputy Minister, National and Cyber Security, at 613-990-4976.

François Guimont

I approve:

I do not approve:

Steven Blaney, P.C., M.P.

Date

Prepared by: Maciek Hawrylak

Emmett, Jamie

From: Hawrylak, Maciek
Sent: September-06-13 4:06 PM
To: Plunkett, Shawn
Subject: Report - Lawful Access - Report on the Use of Electronic Surveillance
(Federal/Provincial)
Attachments: PS-SP-#756252-R-
Report_-_Lawful_Access_-_Report_on_the_Use_of_Electronic_Surveillance_(Federal_Provi
ncial)_.DOCX.DRF

As discussed.

Maciek

s.13(1)(c)

s.14(a)

UNCLASSIFIED

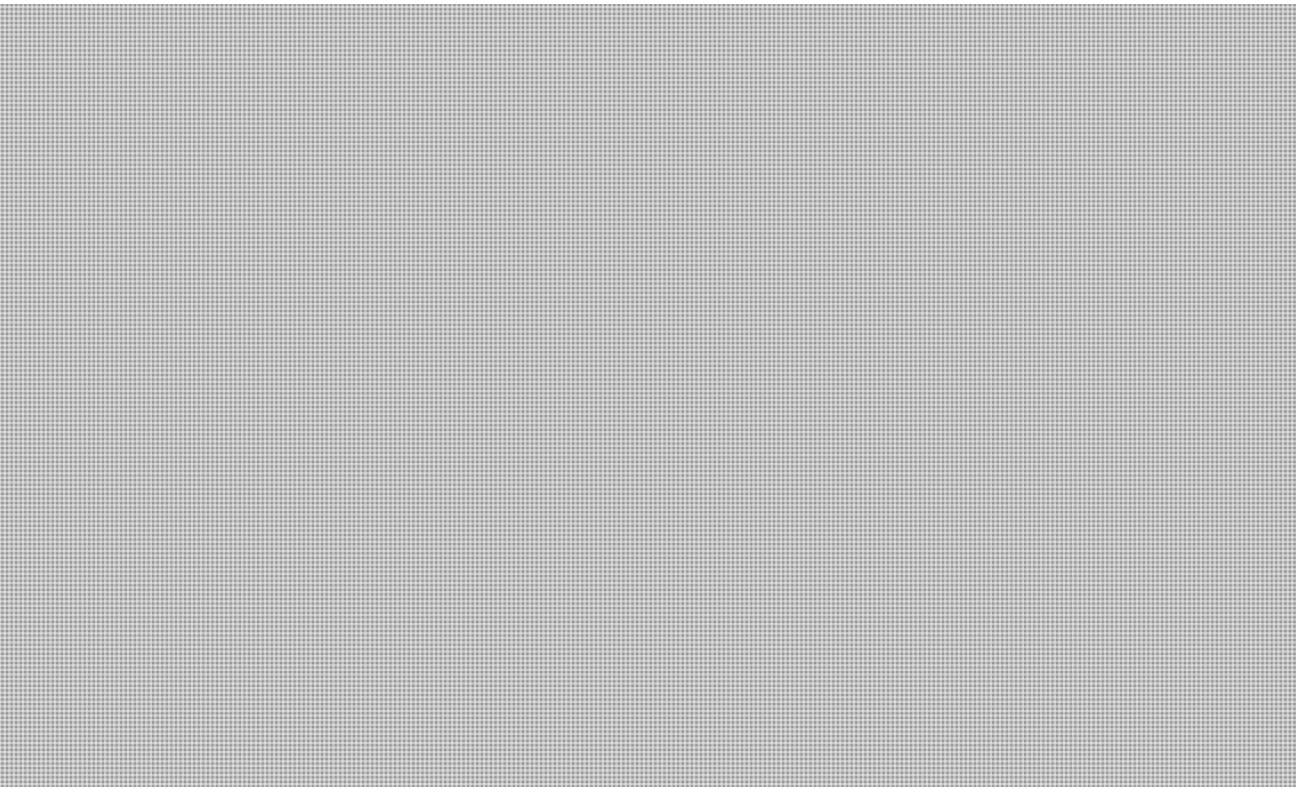
Issue:

Reporting on the total number of court authorizations for interceptions, as well as the total number of interceptions, pursuant to the *Criminal Code*, in Canada.

Number of Authorizations and Interceptions at the Federal Level

According to the federal annual reports on the use of electronic surveillance, on average, 131 authorizations were granted each year from 2000 to 2011. For the same period, only 4 applications or renewals were refused, and 14 authorizations were granted for interceptions under exceptional circumstances (s.188 of the *Criminal Code*). Of the 131 authorizations granted per year,¹ an average of 110 (84%) were granted under audio surveillance (s.185) and nearly all the remaining authorizations were granted for video surveillance (s.487).

For the 131 authorizations granted per year, an average of 945 interceptions (79% of the total) were conducted by means of telecommunications, with the remaining 255 interceptions conducted by microphone, video and other means. This gives a grand total of 1,200 interceptions per year, and an average of 9 interceptions per authorization.



¹ It should be noted that the number of total investigations involving interceptions in a given year may be fewer than the total number of authorizations. This can occur when police seek a new authorization for an ongoing case instead of a renewal, usually due to changing targets, interception locations, or other details.




s.13(1)(c)

s.14(a)


Types of Offences for which Authorizations were Granted – Federal and Provincial Level –

Most granted authorizations are for electronic surveillance in relation to more than one offence (e.g. conspiracy and drug trafficking). At the federal level, most authorizations are related to drug trafficking and organized crime offences. For 2000-2011, the most frequently stated offenses in authorizations were conspiracy and possession of property obtained by the commission of an offense under the *Criminal Code*, and trafficking, possession for the purpose of trafficking, and importing and exporting under the *Controlled Drugs and Substances Act* (CDSA).



Dual Reporting and Duplications of Reported Interceptions

Joint investigations (e.g. regarding a drug offence with both provincial and federal implications) often result in both levels of government applying for authorizations for the same offence. As a result, both sides report on the authorization in their reports. Thus, the possible duplication of authorizations for the same investigations means that aggregating the number of interceptions at the federal and provincial levels may overestimate the total number of interceptions for the country.



Total Number of Authorizations and Interceptions



**Pages 42 to / à 45
are withheld pursuant to sections
sont retenues en vertu des articles**

13(1)(c), 14(a)

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

Dyer, Lara

From: Hawrylak, Maciek
Sent: September-05-13 12:21 PM
To: Dyer, Lara
Subject: FW: Lawful Access - compensation for "Hook-up"

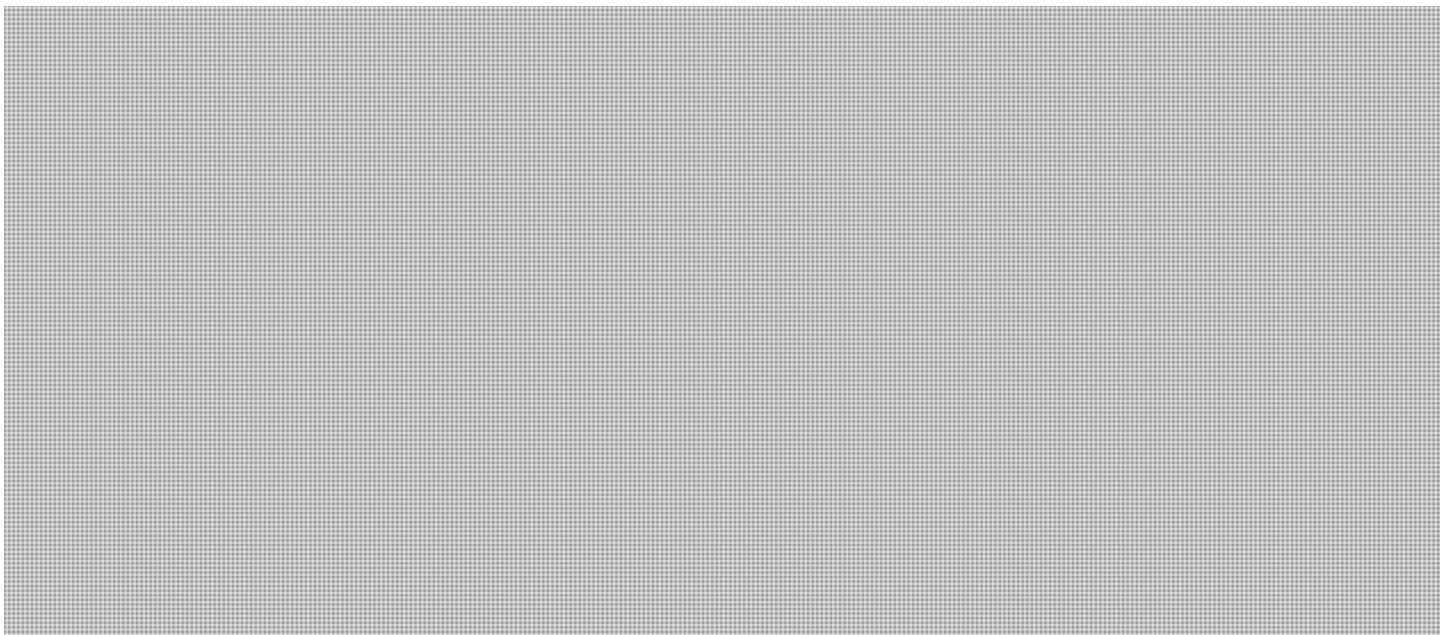
Success!

Maciek

From: Dewar, David [<mailto:Dewar.David@fin.gc.ca>]
Sent: August-04-05 4:56 PM
To: Sitka, Darryl
Cc: Damico, Chris
Subject: RE: Lawful Access - compensation for "Hook-up"

s.21(1)(b)

Hi Darryl,



Hope things are going well with the policy paper. Happy to discuss. Cheers

Dave Dewar
Senior Policy Analyst | *Analyste principal de la politique*
Social Policy | *Politique sociale*
Finance Canada | *Finances Canada*
Ottawa, Canada K1A 0G5
613-943-9408 | Dewar.David@fin.gc.ca | facsimile/télécopieur 613-943-2919



Department of Finance
Canada

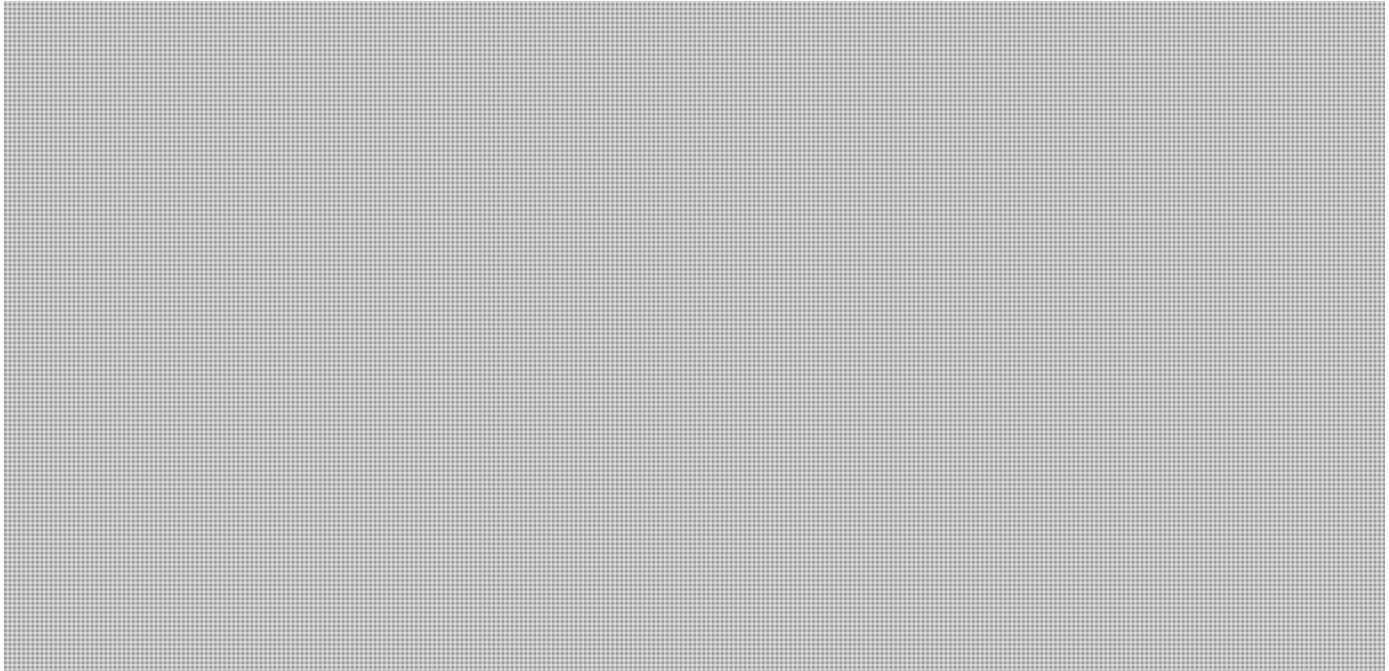
Ministère des Finances
Canada

Canada

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

From: Sitka, Darryl
Sent: July 21, 2005 4:34 PM
To: Dewar, David
Cc: Damico, Chris
Subject: FW: Lawful Access - compensation for "Hook-up"

Hello David.



Thanks very much for your assistance with this matter. s.21(1)(b)

Please contact me if you have any questions.

Cheers

Darryl Sitka
Investigative and Telecommunication Technologies/Politiques des technologies d'investigation et de télécommunication
National Security Policy Division/Direction générale des politiques de la sécurité nationale
Public Safety and Emergency Preparedness Canada/Sécurité publique et Protection civile Canada
340 Laurier Avenue West/340 avenue Laurier Ouest
Ottawa (Ontario) K1A 0P8
Tel/Tél: (613) 949-0643
Fax/Télécopieur: (613) 991-4669/(613) 990-2632 (S)
E-mail/Courriel: darryl.sitka@psepc.gc.ca

Page 48

**is withheld pursuant to section
est retenue en vertu de l'article**

21(1)(b)

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

06/08/2013



Public Safety
Canada

Sécurité publique
Canada

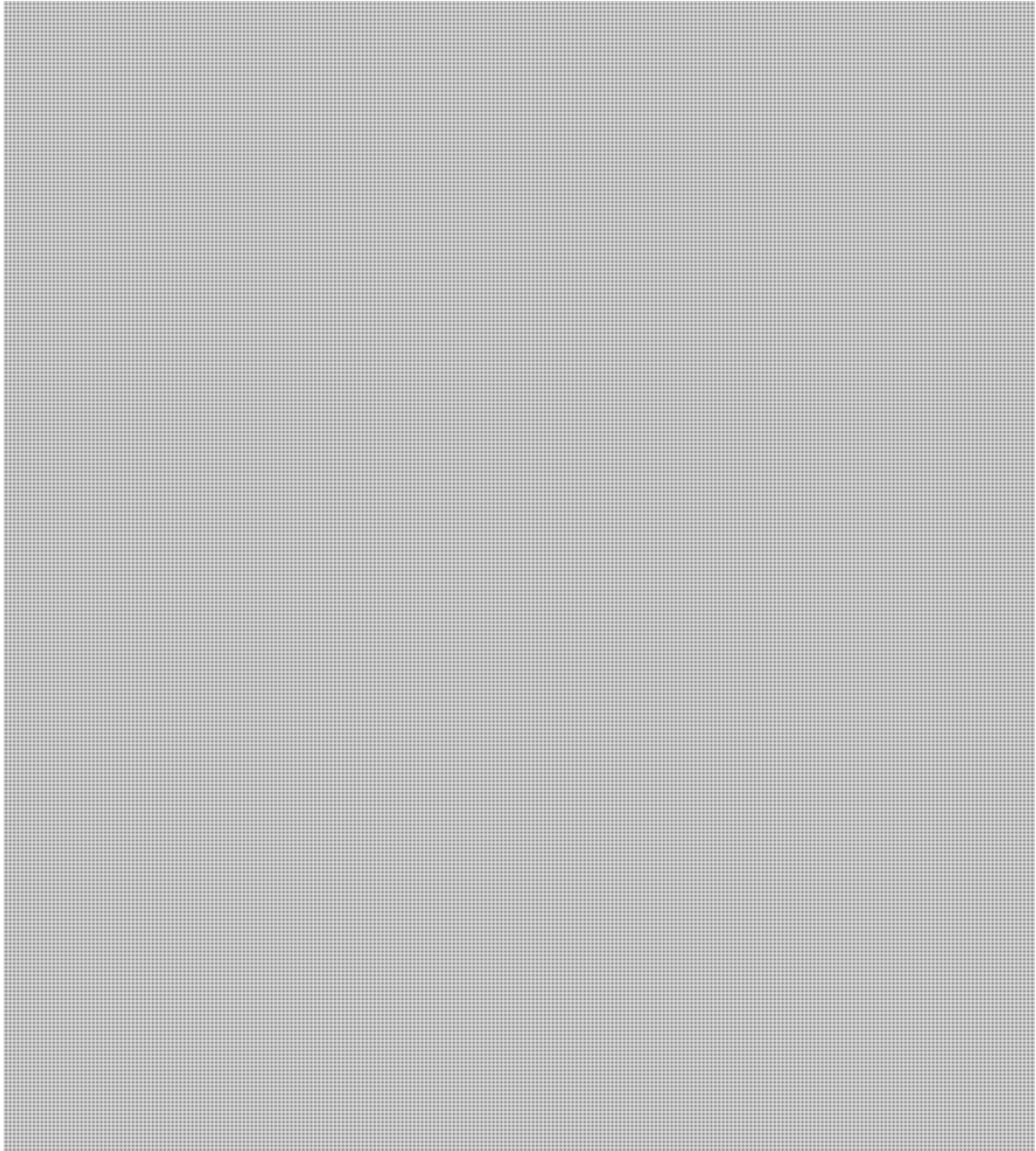
s.15(1) - Int'l
s.21(1)(a)

CONFIDENTIAL

DATE:

File No.: NS 6950-O1 / 397013
RDIMS: Dragon 18379

MEMORANDUM FOR THE SENIOR ASSISTANT DEPUTY MINISTER



Page 90

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

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

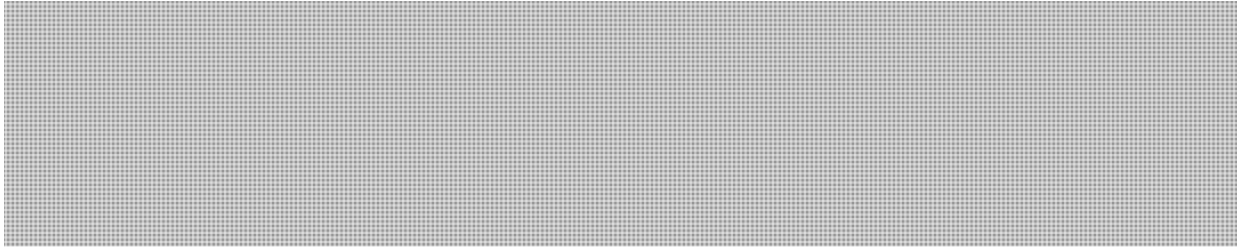
**of the Access to Information
de la Loi sur l'accès à l'information**

s.15(1) - Int'l

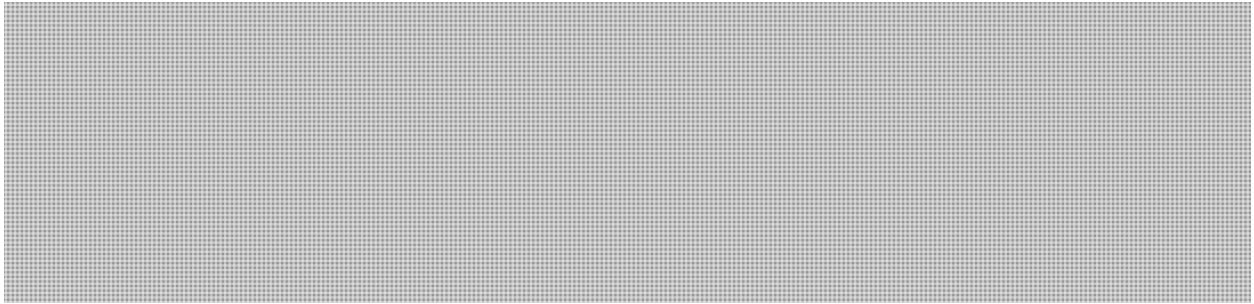
s.21(1)(a)

CONFIDENTIAL

- 3 -



NEXT STEPS



RECOMMENDATION



Should you require additional information, please do not hesitate to contact me or Marie-Hélène Chayer, Director, Investigative Technologies and Telecommunications Policy, at 613-949-3181.

Michael MacDonald

I approve:

Lynda Clairmont
Senior Assistant Deputy Minister
National and Cyber Security Branch

Prepared by: Maciek Hawrylak

CONFIDENTIAL

For Internal Use Only

Subject to ATI exemptions 21(1)(a)(b)

s.21(1)(a)

**DISCUSSION PAPER – SOLICITOR GENERAL'S ENFORCEMENT
STANDARDS FOR LAWFUL INTERCEPTION
OF TELECOMMUNICATIONS**

PURPOSE

To agree on a common interpretation of the [REDACTED] telecommunications service providers (TSPs) under [REDACTED] the *Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications* (SGES).

BACKGROUND

[REDACTED]

Following the initial inclusion of the SGES in the lawful interception condition of licence, an annotated version of the standards was drafted to provide additional clarity for each requirement.

[REDACTED]

While the SGES annotations serve as a guide to TSPs to assist with delivering lawful interception requirements,

[REDACTED]

CONSIDERATIONS

[REDACTED]

Page 201

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

21(1)(a), 21(1)(b)

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

Page 202

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

20(1)(b), 21(1)(b)

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

Page 203

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

20(1)(b), 21(1)(a), 21(1)(b)

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

July 12, 2013



Public Safety
Canada

Sécurité publique
Canada

SECRET

Jolie/Shawn.

• good work
• pls see my comments.

merci

DATE:

File No.: NS 6652-O3 / CCM 396403
RDIMS No.: DRAGON 11635

s.16(1)(c)
s.16(2)
s.21(1)(a)
s.21(1)(b)

MEMORANDUM FOR THE DIRECTOR GENERAL

FORBEARANCE QUARTERLY REPORT, FY 2013-2014, Q1

(Information only)

ISSUE

To provide an update on the forbearance program for the first quarter of FY 2013-2014, from April 1, 2013, to June 30, 2013. The next report is due September 13, 2013. Last quarter's report is included as ANNEX A.

STATUS OF FORBEARANCE REQUESTS

[Redacted content]

Status:

[Redacted content]

Report:

/ Good practice

SECRET

s.16(1)(c)
s.16(2)
s.21(1)(a)
s.21(1)(b)

[Redacted]

Next Steps:

[Redacted]

✓
*proceed
asap.*

Status:

[Redacted]

Status:

[Redacted]

Report:

[Redacted]

[Redacted]

Next Steps:

[Redacted]

Status:

[Redacted]

Report:

[Redacted]

s.16(1)(c)
s.16(2)
s.21(1)(a)
s.21(1)(b)

SECRET

-3-

Next Steps:

Status:

Report:

Next Steps:

LOOK AHEAD

- July 2013
 - [REDACTED]
 - Consultation with partners of forbearance enhancement implementation tools ✓
- August 2013
 - Bi-monthly Forbearance Working Group
- September 2013
 - [REDACTED] forbearance expiration (September 30, 2013)

Should you require additional information, please do not hesitate to contact me at 613-949-3181 or Shawn Plunkett, Senior Policy Advisor, Investigative Technologies and Telecommunications Policy at 613-990-7066.


Marie-Hélène Chayer
Director, Investigative Technologies and Telecommunications Policy
National Security Operations

Prepared by: Julie Thompson and Shawn Plunkett



SECRET

s.16(1)(c)
s.16(2)
s.21(1)(a)
s.21(1)(b)

DATE:

**File No.: NS 6652-O3 /394413
RDIMS No.: DRAGON 6411**

MEMORANDUM FOR THE DIRECTOR GENERAL

FORBEARANCE QUARTERLY REPORT, FY 2012-2013, Q4

(Information only)

ISSUE

To provide an update on forbearance requests for the fourth quarter of FY 2012-2013; from January 1, 2013, to March 31, 2013. The next report is due July 12, 2013.

STATUS OF FORBEARANCE REQUESTS

[Redacted]

Status:

[Redacted]

Report:

[Redacted]

Next Steps:

[Redacted]

Status:

[Redacted]

should/can we clarify better?

s.16(1)(c)
s.16(2)
s.21(1)(a)
s.21(1)(b)

Report:

[Redacted]

Next Steps:

[Redacted] } why n go + all med

Status:

[Redacted]

Report:

[Redacted] }

Next Steps:

[Redacted]

Status:

[Redacted]

Report:

[Redacted]

Next Steps:

[Redacted]

Status:

[Redacted]

CBCF
topic.
PS/DAT
stand-alone
topic?

SECRET

s.16(1)(c)
s.16(2)
s.21(1)(a)
s.21(1)(b)

- 3 -

Report: [Redacted]

Next Steps: [Redacted]

FORBEARANCE PROGRAM ENHANCEMENT

*Good stuff.
Should we
do a 2pg
memo to
SADM?*

In February 2013, PS met again with the RCMP, CSIS and IC to further discuss a strategy to enhance the forbearance program. [Redacted]

LOOK AHEAD

- April 2013
 - Bi-monthly Forbearance Working Group (April, 29, 2013- TBC)
- May 2013
 - Conference call with [Redacted] (Forbearance expires June 30, 2013)
- June 2013
 - Conference call with [Redacted] for progress update (Forbearance expires September 30, 2013)
 - Conference call with [Redacted] (Forbearance expires June 28, 2013)

Should you require additional information, please do not hesitate to contact me at 613-949-3181 or Shawn Plunkett, Senior Policy Advisor, Investigative Technologies and Telecommunications Policy at 613-990-7066.

Marie-Hélène Chayer
Director, Investigative Technologies and Telecommunications Policy
National Security Operations

Prepared by: Julie Thompson

s.23

Hawrylak, Maciek

From: Pilon, Claude
Sent: June-07-13 3:56 PM
To: Hawrylak, Maciek
Subject: Interception Center

Maciek,

I have chosen the dragon email format for delivering this advice, should you wish to have a formal opinion, please let me know.

Solicitor-client privilege - Secret

If more detail are required, please let me know.

Regards

Claude

Claude Pilon
Counsel / Avocat
Public Safety Canada Legal Services / Services juridiques de Sécurité publique Canada
(613) 991-4364 / claudio.pilon@ps-sp.gc.ca

**Pages 220 to / à 223
are withheld pursuant to sections
sont retenues en vertu des articles**

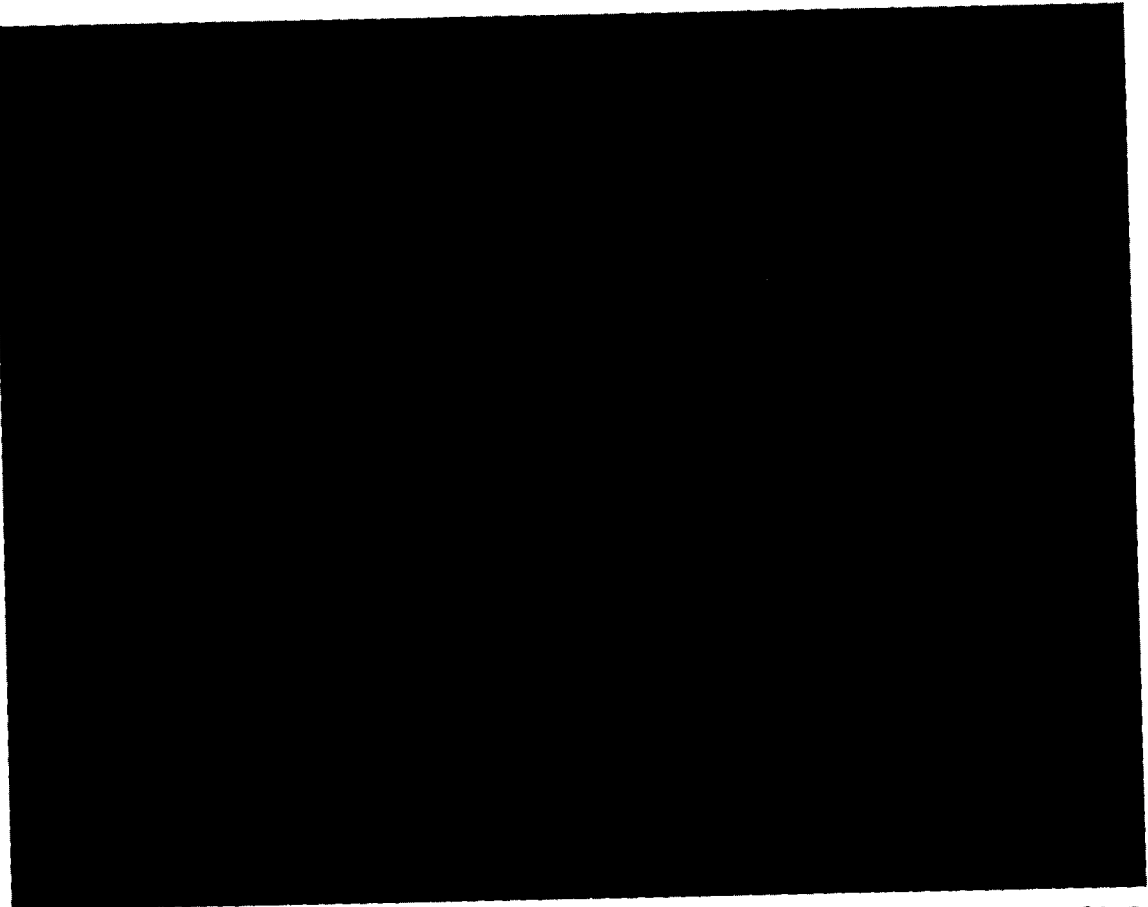
13(1)(c), 14(a)

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

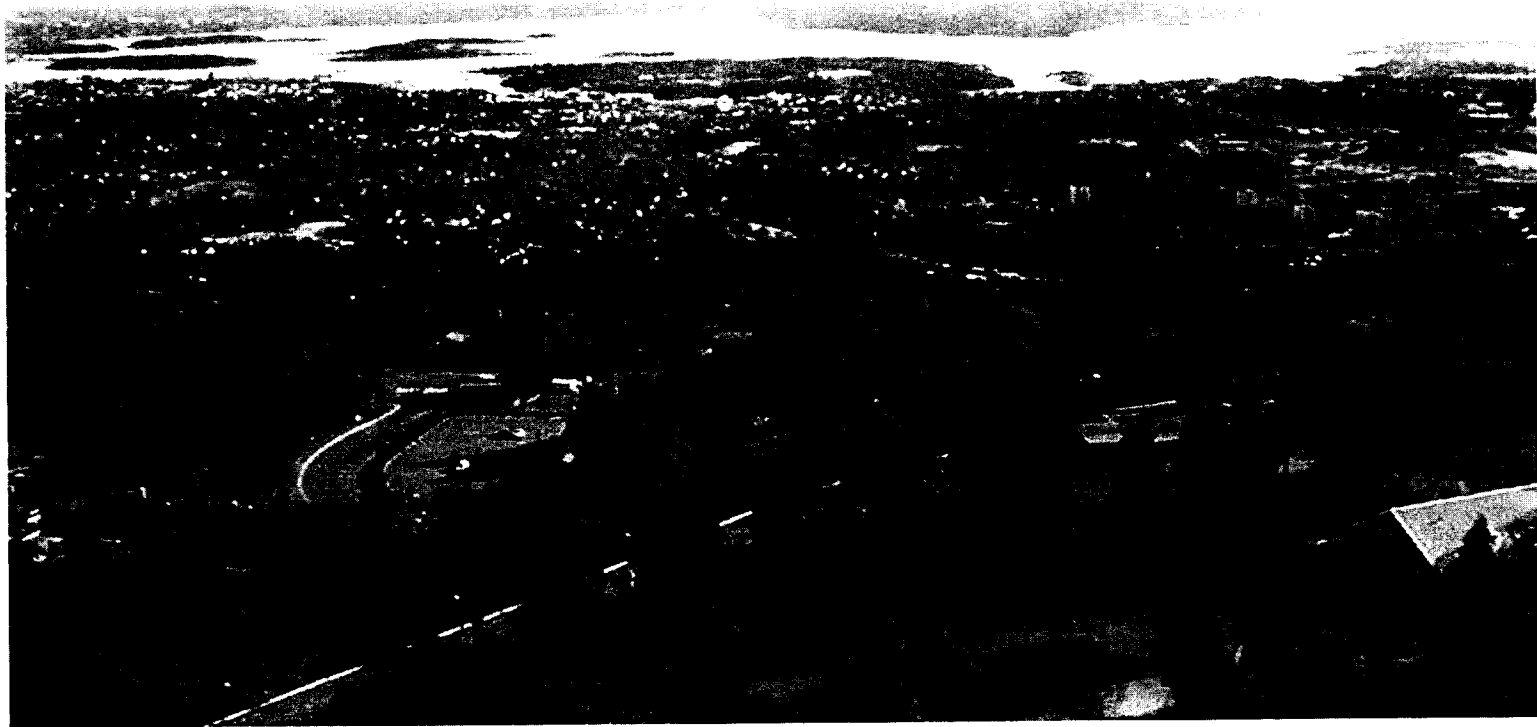


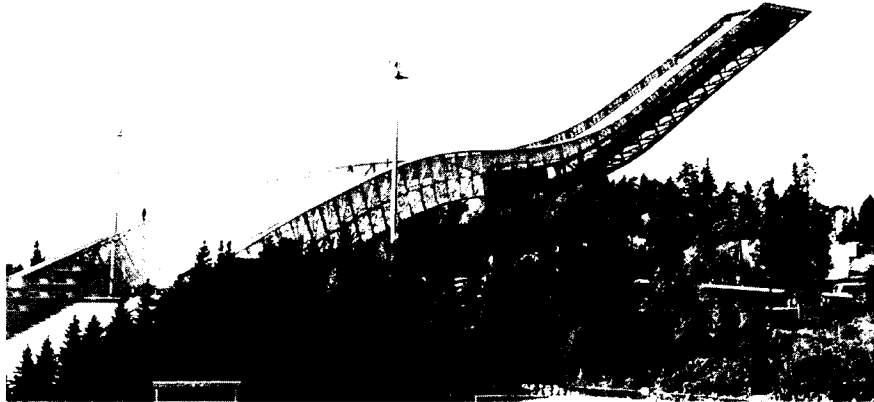
Public Safety
Canada

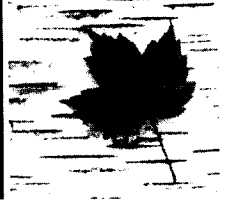
Sécurité publique
Canada



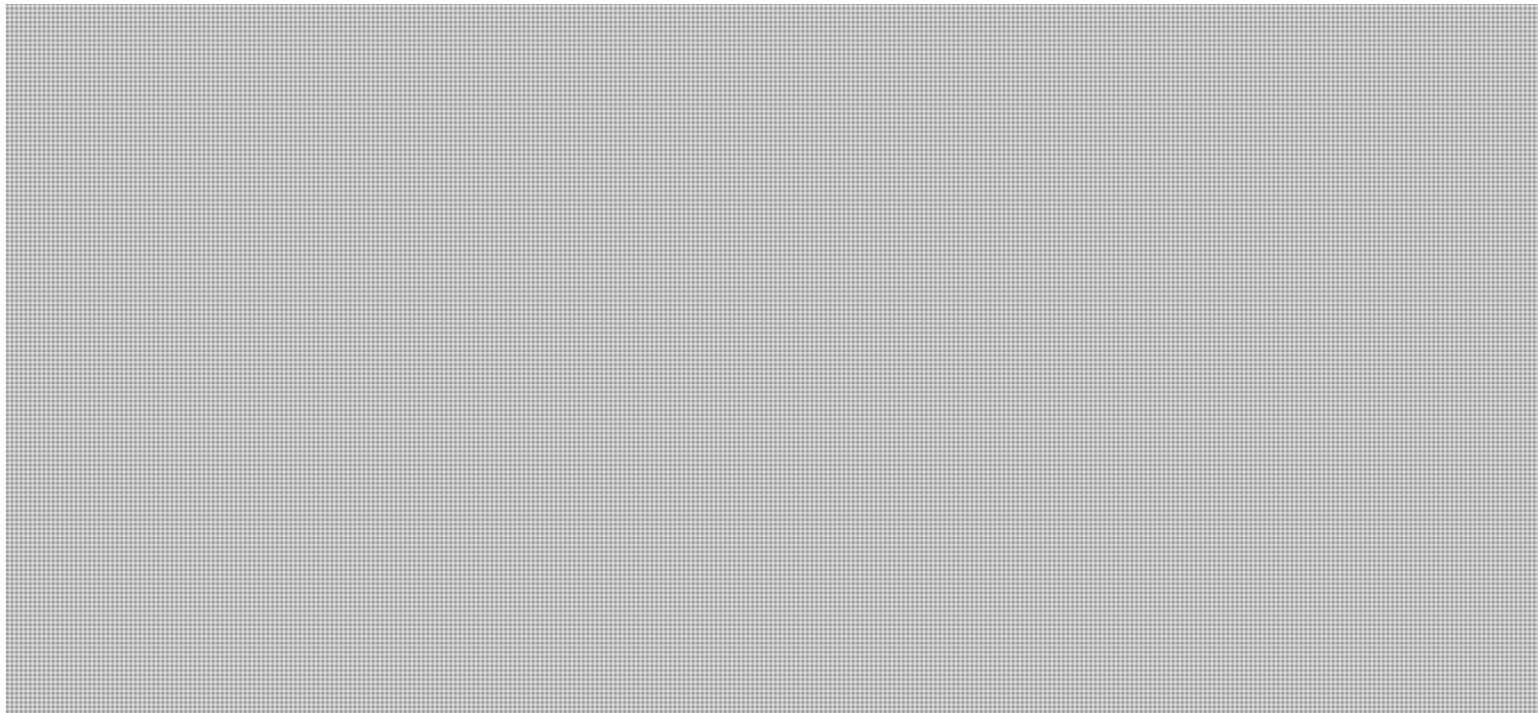
Canada







- Presentations/Panel Discussions



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



Page 228

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

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

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

Page 229

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

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

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

**Pages 230 to / à 237
are withheld pursuant to sections
sont retenues en vertu des articles**

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

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



Thank you

Questions?



Public Safety
Canada

Sécurité publique
Canada

Hawrylak, Maciek

From: [REDACTED]
Sent: May-23-13 2:07 PM
To: Chayer, Marie-Helene
Cc: Hawrylak, Maciek
Subject: NOT PROTECTIVELY MARKED RE: UK IP lawful access information gathering

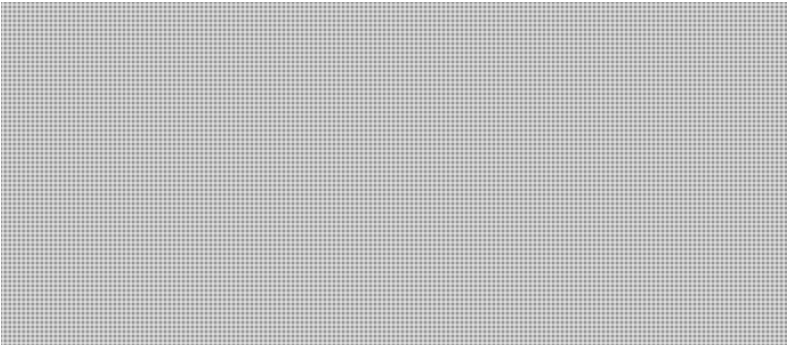
NOT PROTECTIVELY MARKED

Dear Marie-Helene

Sorry for the slow reply on this. Thanks very much indeed for your very comprehensive answers. We are still drafting our report on the results of our questions to 5 Eyes colleagues. Once this is done we will definitely be looking to share the results. It's not yet clear what the overall protective marking of this document will be so, if it does go above unclassified, we will need to work out how to get it to you – presumably via the High Commission, but we will cross that bridge when we get to it, hopefully in the next couple of weeks.

Thanks again

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

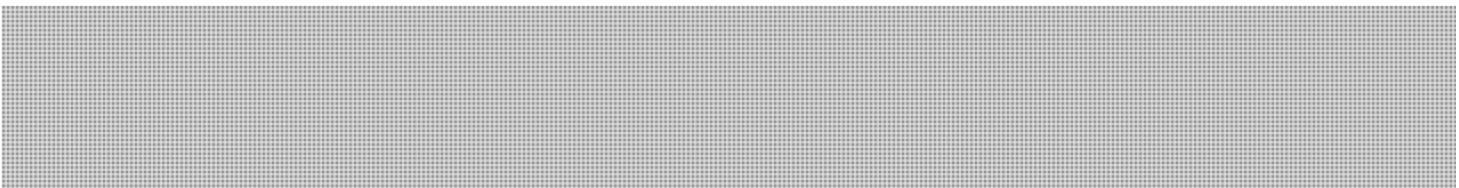


T: [REDACTED]
E: [REDACTED]
www.gov.uk/home-office

From: Chayer, Marie-Helene [mailto:Marie-Helene.Chayer@ps-sp.gc.ca]
Sent: 16 May 2013 21:35
To: [REDACTED]
Cc: Hawrylak, Maciek
Subject: RE: UK IP lawful access information gathering

Hi [REDACTED]

Below are responses to your questions.



Please do not hesitate to contact me if you have further questions.

Regards,

Marie-Hélène

Marie-Hélène Chayer
Director – Investigative Technology and Telecommunications Policy /
Directrice – Politique sur les technologies d'enquête et les télécommunications
National Security Operations Division / Division des Opérations de sécurité nationale
Public Safety Canada / Sécurité Publique Canada
(613)949-3181

s.13(1)(a)
s.15(1) - Int'l
s.19(1)

From: [REDACTED]
Sent: May-16-13 12:31 PM
To: Chayer, Marie-Helene; MacDonald, Michael
Cc: [REDACTED]
Robert.Sinclair@international.gc.ca
Subject: NOT PROTECTIVELY MARKED UK IP lawful access information gathering

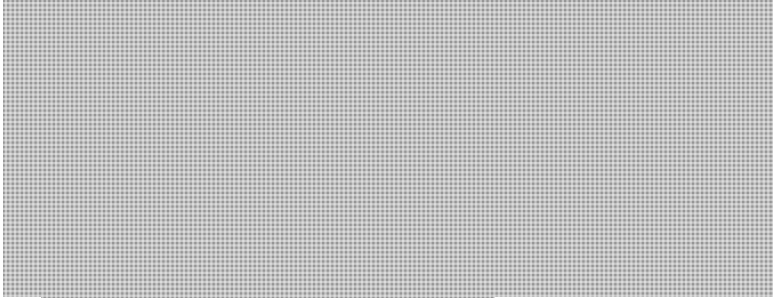
NOT PROTECTIVELY MARKED
NOT PROTECTIVELY MARKED

Dear Marie-Helene, Michael,

Thanks for your kind offer to assist with our information gathering exercise which we received via [REDACTED] at the High Commission. We have now received the response to our specific questions (attached) and these have provided us with a very comprehensive understanding.

Thanks again for your continued assistance and we will of course keep you posted on the progress of our efforts.

Kind regards



s.19(1)

T:

E:

www.gov.uk/home-office

This email and any files transmitted with it are private and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please return it to the address it came from telling them it is not for you and then delete it from your system.

This email message has been swept for computer viruses.

The original of this email was scanned for viruses by the Government Secure Intranet virus scanning service supplied by Vodafone in partnership with Symantec. (CCTM Certificate Number 2009/09/0052.) On leaving the GSi this email was certified virus free.

Communications via the GSi may be automatically logged, monitored and/or recorded for legal purposes.

This email was received from the INTERNET and scanned by the Government Secure Intranet anti-virus service supplied by Vodafone in partnership with Symantec. (CCTM Certificate Number 2009/09/0052.) In case of problems, please call your organisation's IT Helpdesk.

Communications via the GSi may be automatically logged, monitored and/or recorded for legal purposes.

This email and any files transmitted with it are private and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please return it to the address it came from telling them it is not for you and then delete it from your system.

This email message has been swept for computer viruses.

The original of this email was scanned for viruses by the Government Secure Intranet virus scanning service supplied by Vodafone in partnership with Symantec. (CCTM Certificate Number 2009/09/0052.) On leaving the GSi this email was certified virus free.

Communications via the GSi may be automatically logged, monitored and/or recorded for legal purposes.

Hawrylak, Maciek

From: Chayer, Marie-Helene
Sent: May-21-13 12:27 PM
To: Plunkett, Shawn; Hawrylak, Maciek
Subject: Re: Canadian Lawful Intercept Follow up

Hi,
Yes, the policy remains unchanged.

s.19(1)
s.21(1)(a)
s.21(1)(b)

Thanks [REDACTED]

Marie

From: Plunkett, Shawn
Sent: Tuesday, May 21, 2013 12:17 PM
To: Chayer, Marie-Helene; Hawrylak, Maciek
Subject: Fw: Canadian Lawful Intercept Follow up

[REDACTED]

Shawn Plunkett
[REDACTED]
PS/SP Canada

From: [REDACTED]
Sent: Monday, May 20, 2013 04:01 PM
To: Plunkett, Shawn
Subject: Canadian Lawful Intercept Follow up


Shawn,
[REDACTED]

Your input would be greatly appreciated.


Thank you,

[REDACTED]
Regional Sales Manager, North America

M [REDACTED]
E [REDACTED]



Notice to Recipient: Privileged/Confidential information may be contained in this message and may be subject to legal privilege. Access to this e-mail by anyone other than the intended is unauthorized. This e-mail is meant only for the intended recipient(s) of the transmission; any unauthorized use, copying, distribution, or dissemination is prohibited. If you are not the intended recipient, please contact the sender by reply e-mail and please delete this e-mail from your system and destroy any copies. All rights to this information is reserved by



s.19(1)

Emmett, Jamie

From: Plunkett, Shawn s.13(1)(a)
Sent: May-28-13 12:16 PM s.13(1)(b)
To: Grigsby, Alexandre s.15(1) - Int'l
Subject: RE: Paper on lawful access
Attachments: Australian presentation - [REDACTED] - For Group Use.pptx

Thanks Alex.

Was at a meeting last week [REDACTED]

From: Grigsby, Alexandre
Sent: May-28-13 11:33 AM
To: Plunkett, Shawn; Hamilton, Sharon; Cameron, Bud; Bonvie, Jeff; Dvorkin, Corey; Bradley, Kees
Cc: Hatfield, Adam
Subject: Paper on lawful access

Hi all,

Came across this paper that might be of interest. It's authored by some engineers concerned that mandating backdoors in software for lawful intercept purposes introduces new vulnerabilities into software that will be exploited by non-authorized purposes. Their solution seems to be: "all software has vulnerabilities – just have law enforcement exploit existing vulnerabilities as opposed to creating new ones"

<https://www.cs.columbia.edu/~smb/papers/GoingBright.pdf>

alex

Alexandre Grigsby
Analyst | Analyste
National Cyber Security Directorate | Direction générale de la cybersécurité nationale
Public Safety Canada | Sécurité publique Canada
tel. 613.949.4243
www.publicsafety.gc.ca | www.securitepublique.gc.ca

**Pages 303 to / à 312
are withheld pursuant to section
sont retenues en vertu de l'article**

13(1)(a)

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

Emmett, Jamie

From: Plunkett, Shawn
Sent: May-16-13 10:57 AM
To: Dyer, Lara
Subject: FW: [REDACTED] - NSOD Comments

s.14(a)
s.21(1)(a)
s.21(1)(b)

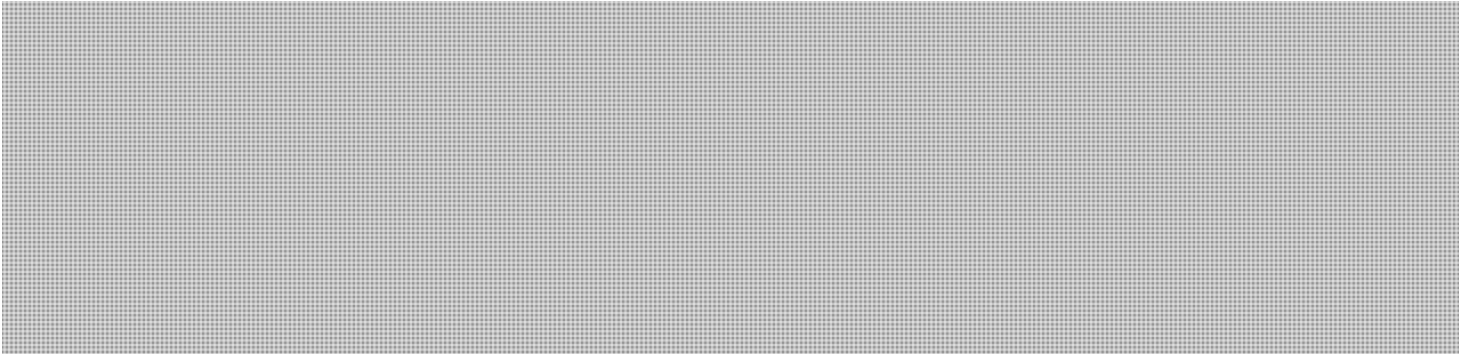
As discussed. Our comments to DoJ on the [REDACTED]

From: Plunkett, Shawn
Sent: March-18-13 3:11 PM
To: Nguyen, Trang Dai <Trang-Dai.Nguyen@justice.gc.ca> (Trang-Dai.Nguyen@justice.gc.ca); Audcent, Karen (Karen.Audcent@justice.gc.ca)
Cc: Chayer, Marie-Helene
Subject: [REDACTED] NSOD Comments

Trang, Karen,

We would like to first recognize the significant effort you have put into developing this comprehensive report. [REDACTED]

[REDACTED]



Please do not hesitate to contact me should you have any questions or comments. We would be happy to discuss this further with you either at the upcoming meeting or at a separate meeting.

Thank you.

Shawn Plunkett
Senior Policy Advisor / Conseiller principal en politiques
Investigative Technologies and Telecommunications Policy (ITTP) /
Technologies d'enquêtes et politiques des télécommunications (TEPT)
National Security Operations Directorate / Direction des opérations de sécurité nationale
Public Safety Canada / Sécurité Publique Canada
Tel: (613) 990-7066
Email: shawn.plunkett@ps.gc.ca

s.21(1)(a)

s.21(1)(b)

**Pages 315 to / à 359
are withheld pursuant to sections
sont retenues en vertu des articles**

13(1)(c), 14(a), 21(1)(a), 21(1)(b)

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

Hawrylak, Maciek

From: Maurice, Marie-Elise <Marie-Elise.Maurice@tbs-sct.gc.ca>
Sent: May-15-13 1:39 PM
To: Hawrylak, Maciek
Cc: Nordenstrom, Joanna; Chénier, Jean-Philippe
Subject: RE: Lawful Access PMR Mock-up

Good afternoon!

I apologize for the misunderstanding. The condensing is not responsible for the report being below the "performance measurement threshold". This comment could apply for your previous PMR, which led to a comment in the letter from my ADM encouraging you to continue your work to develop performance measures.

The comments regarding Pillar 1 that asked for information not featured in previous versions of the PMR were suggestions to help you develop more robust performance measurement. I believe that such measures should be incorporated in this year's report, given that this was formally requested last August after your draft report, and restated in the ADM letter.

Joanna and I remain available to support you in the development of these performance measures. I would also be happy to discuss at any time.

Many thanks!
Marie-Élise

From: Hawrylak, Maciek [mailto:Maciek.Hawrylak@ps-sp.gc.ca]
Sent: May 15, 2013 1:17 PM
To: Maurice, Marie-Elise
Cc: Nordenstrom, Joanna; Chenier, Jean-Philippe: PS-SP
Subject: Re: Lawful Access PMR Mock-up

s.21(1)(b)

Marie-Elise,

Thanks for this. I'm sure many of the items you list in your email can be retained without difficulty.



I will phone you tomorrow to discuss these in more detail and see if we can arrive at a solution that meets your needs.

Maciek

From: Maurice, Marie-Elise [<mailto:Marie-Elise.Maurice@tbs-sct.gc.ca>]
Sent: Wednesday, May 15, 2013 10:37 AM
To: Hawrylak, Maciek
Cc: Nordenstrom, Joanna <Joanna.Nordenstrom@tbs-sct.gc.ca>; Chénier, Jean-Philippe
Subject: Lawful Access PMR Mock-up

s.21(1)(a)

Hi Maciek,



Let me know if you wish to discuss further.

Many thanks!
Marie-Élise

Marie-Élise Maurice
Senior Advisor | Conseillère principale
Security and Justice Division | Division de la sécurité et de la justice
International Affairs, Security and Justice Sector | Secteur des affaires internationales, de la sécurité et de la justice
Treasury Board of Canada Secretariat | Secrétariat du Conseil du Trésor du Canada
Ottawa, Canada K1A 0R5
Marie-Elise.Maurice@tbs-sct.gc.ca
Telephone | Téléphone 613-952-7037 / Facsimile | Télécopieur 613-957-0525 / Teletypewriter | Téléimprimeur 613-957-9090
Government of Canada | Gouvernement du Canada



Treasury Board of Canada
Secrétariat

Secrétariat du Conseil du Trésor
du Canada

Canada

Better government: with partners, for Canadians | Un meilleur gouvernement : avec nos partenaires, pour les Canadiens

Emmett, Jamie

From: Plunkett, Shawn
Sent: May-14-13 2:39 PM
To: Thompson, Julie
Subject: RE: Update on [REDACTED] Lawful Interception Solution

Did you ever get a response from [REDACTED] on this?

s.19(1)

s.16(1)(c)

s.16(2)

From: Thompson, Julie
Sent: April-05-13 2:04 PM
To: [REDACTED]
Cc: Plunkett, Shawn
Subject: Update on [REDACTED] Lawful Interception Solution

Good afternoon,

As I understand, [REDACTED] have been working closely with PS's agencies in testing equipment. The latest update from the agencies was that further detailed test configuration information and test data was required.

Would it be possible to obtain an update on [REDACTED] testing progress and potential launch plans?

Many thanks,

Julie

Julie Thompson
Policy Analyst/Analyste en politiques
Investigative Technologies and Telecommunications Policy/Politiques sur les technologies d'enquête et les télécommunications
National Security Operations Directorate/Direction des Operations de Sécurité Nationale
Public Safety Canada/Sécurité Publique Canada
Tel: 613.998.7893
Email/Courriel : julie.thompson@ps-sp.gc.ca

s.19(1)

Emmett, Jamie

From: Plunkett, Shawn s.16(1)(c)
Sent: May-16-13 10:53 AM s.16(2)
To: [REDACTED]
Cc: Thompson, Julie
Subject: Update on [REDACTED] Lawful Interception Solution

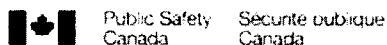
Hi [REDACTED]
 Hope things are well and you are enjoying Ottawa's rush into summer.
 I understand that you had tried to touch base with Julie earlier as [REDACTED] forbearance expires at the end of June, 2013.

As per our usual protocol, we would like to arrange a conference call or meeting with [REDACTED] during the week of May 27th. I would suggest the afternoon of May 28th as a proposed starting point. Grateful if you could let me know if this time works for your side and who would be participating in the call/meeting.

Please feel free to give me a call either today or tomorrow and we can discuss. (I will be on official travel next week, but Julie (613.998.7893) will be available).

Thanks.

Shawn Plunkett
 Senior Policy Advisor / Conseiller principal en politiques
 National Security Operations Directorate / Direction des opérations de sécurité nationale
 Public Safety Canada / Sécurité Publique Canada
 340 Ave Laurier W, Ottawa,
 Ontario, Canada, K1A 0P9
 Telephone | Téléphone: (613) 990-7066
 Facsimile | Télécopieur: (613) 991-4669
 Email | Courriel: shawn.plunkett@ps.gc.ca



From: Thompson, Julie
Sent: April-05-13 2:04 PM
To: [REDACTED]
Cc: Plunkett, Shawn
Subject: Update on [REDACTED] Lawful Interception Solution

Good afternoon,
 As I understand, [REDACTED] have been working closely with PS's agencies in testing equipment. The latest update from the agencies was that further detailed test configuration information and test data was required.

Would it be possible to obtain an update on [REDACTED] testing progress and potential launch plans?

Many thanks,

Julie

Julie Thompson
Policy Analyst/Analyste en politiques
Investigative Technologies and Telecommunications Policy/Politiques sur les technologies d'enquête et les
télécommunications
National Security Operations Directorate/Direction des Operations de Sécurité Nationale
Public Safety Canada/Sécurité Publique Canada
Tel: 613.998.7893
Email/Courriel : julie.thompson@ps-sp.gc.ca

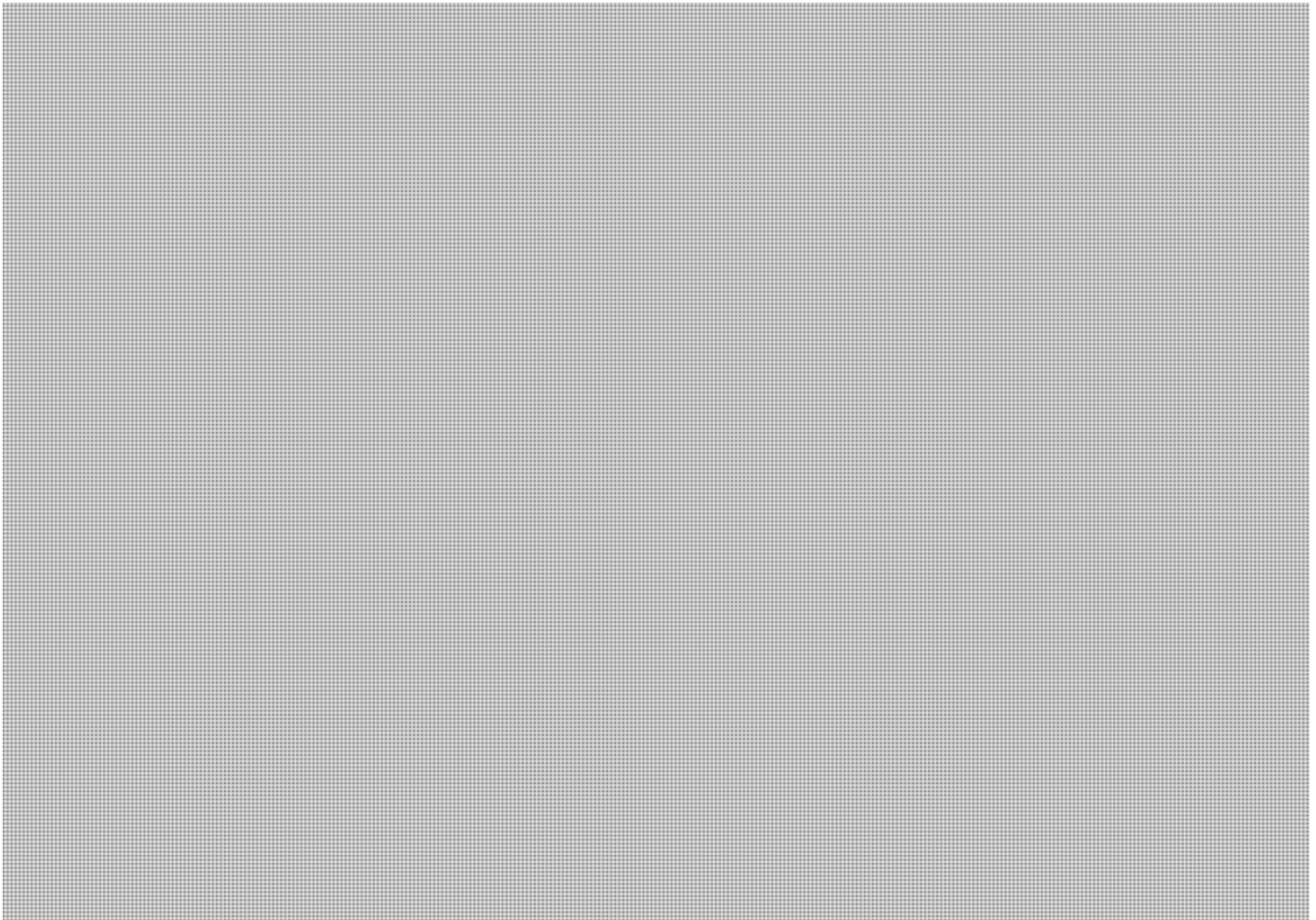
s.21(1)(a)

Hawrylak, Maciek

From: Cameron, Frank
Sent: May-14-13 12:35 PM
To: Hawrylak, Maciek
Cc: Lajeunesse, Elizabeth; Larose, Nathalie
Subject: RE: THC Event Estimates - Lawful Access

Maciek,

I do recall parts of our conversation from several weeks ago. Firstly, PS does not have the authority to recover fees from other foreign governments.



At this point, I would suggest that you have a conversation(s) with Nathalie and Elizabeth to determine if there is THC Cap available to undertake the event and then go from there.

I hope this helps. Please feel free to contact me should you wish to discuss further.

Frank Cameron

Senior Financial Management Advisor / Conseiller principal en gestion financière
(613) 990-9366

From: Hawrylak, Maciek
Sent: May-14-13 10:56 AM
To: Cameron, Frank
Cc: Lajeunesse, Elizabeth; Larose, Nathalie
Subject: RE: Estimates

Frank,

The delegates would be foreign government representatives who work on lawful access issues. Canada would also have a contingent. The total size would be around 50 people (5 Canadian, roughly speaking).

Maciek

From: Cameron, Frank
Sent: May-14-13 10:54 AM
To: Hawrylak, Maciek
Cc: Lajeunesse, Elizabeth; Larose, Nathalie
Subject: RE: Estimates

Maciek,

Again, to provide greater clarity....please identify specifically what "delegates" are. Ie., Canadian or Foreign government departments, private corporations, etc.

Thank you.

Frank Cameron

Senior Financial Management Advisor / Conseiller principal en gestion financière
(613) 990-9366

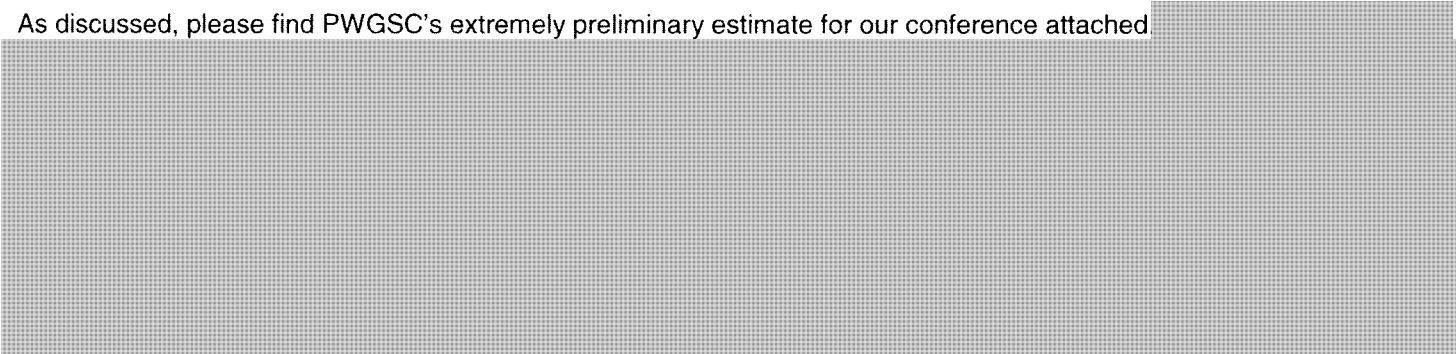
s.21(1)(a)

From: Hawrylak, Maciek
Sent: May-14-13 9:55 AM
To: Cameron, Frank
Subject: FW: Estimates

s.21(1)(b)

Frank,

As discussed, please find PWGSC's extremely preliminary estimate for our conference attached.



Thanks,
Maciek

Maciek Hawrylak
National Security Operations Directorate | Direction des Operations de Sécurité Nationale
Public Safety Canada | Sécurité Publique Canada
Tel | Tél : 613-991-6036

Fax | Téléc : 613-991-4669
Maciek.Hawrylak@ps-sp.gc.ca


From: Tyler Zettel [<mailto:Tyler.Zettel@tpsgc-pwgsc.gc.ca>]
Sent: May-09-13 4:08 PM
To: Hawrylak, Maciek; Paul Schafer
Subject: Estimates

Hi Maciek,

Please see the attached spreadsheet. Although we are still waiting on prices from a few venues, this should give you a good idea of prices. Note that hospitality has been quoted at the very high end. Also, in speaking with the hotels today, it looks as though we could possibly avoid guaranteeing guest rooms.

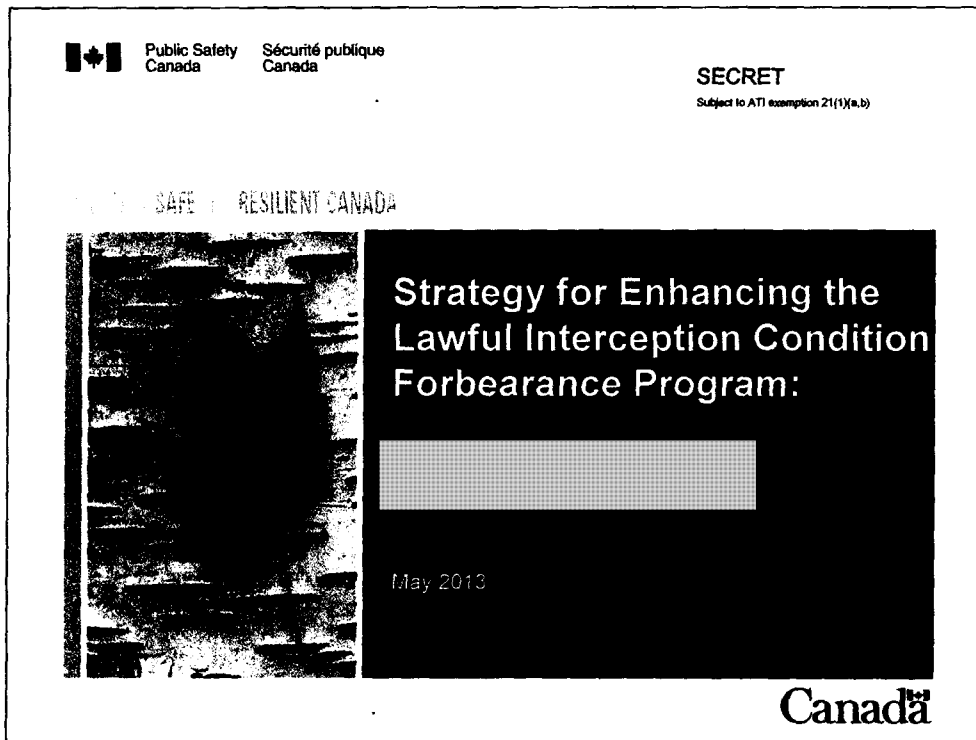
Let me know if you have any questions.

Tyler

From: Tyler Zettel [<mailto:> 
Sent: Thursday, May 09, 2013 04:00 PM
To: Tyler Zettel

s.19(1)

s.21(1)(a)



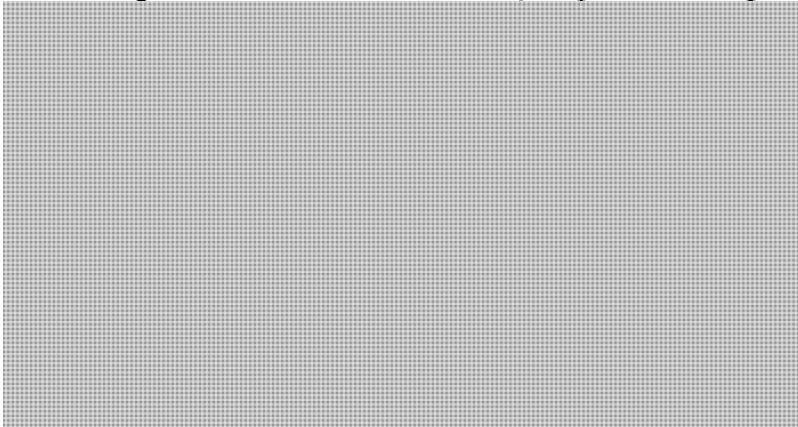
- Apologies we were not able to provide beforehand.
- We will send along e-copies to you after the meeting
- Not a finished document, your input is important for this process.
- We will also provide you in the coming days some of the companion documents for your review.

s.21(1)(a)

Overview

SAFE AND RESILIENT CANADA

- Strengthen the forbearance program along



Public Safety Canada / Sécurité publique Canada

1

eg. FBI

- At our last meeting, I had briefly walked you through a strategy we were considering to enhance the forbearance regime.
- After some further discussions with IC, we have put together a strategy to work towards strengthening the program.

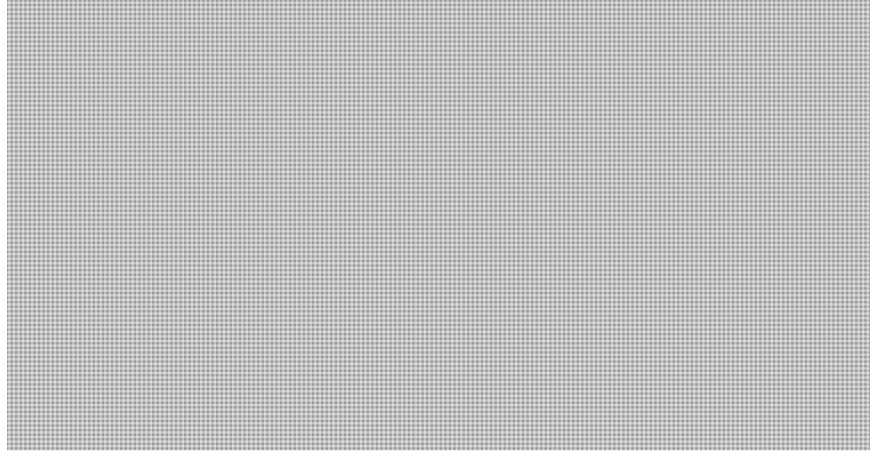


- Essential what we are trying to achieve is this...



Rationale

- Problem Definition:



s.21(1)(a)

- Some of the reasons for why there is a need to strengthen the program

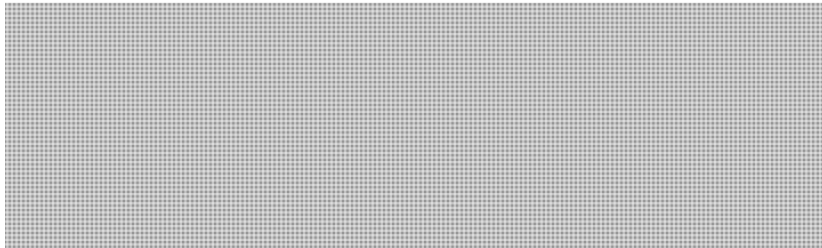
s.21(1)(a)

Opportunity

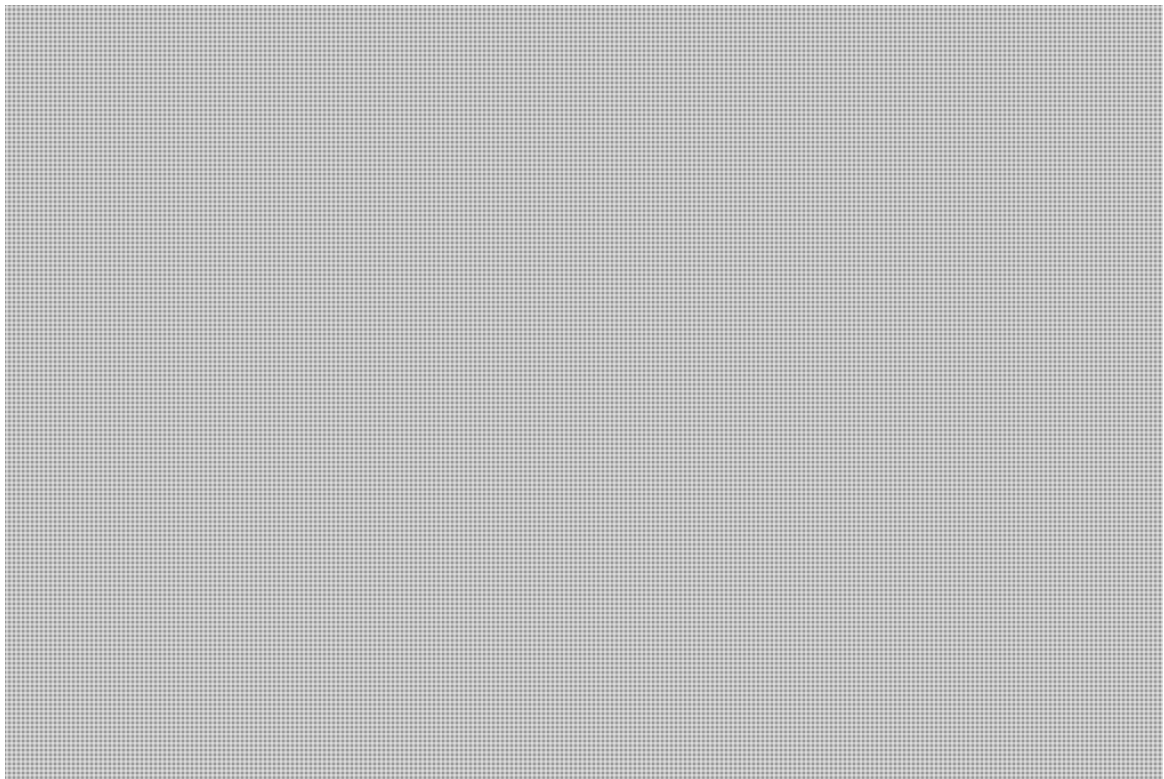


SAFE RESILIENT CANADA

- We need to make the most of all existing regulatory measures related to lawful interception
- PS will continue to process forbearance requests, but also will identify opportunities to improve the program



Public Safety Canada / Sécurité publique Canada

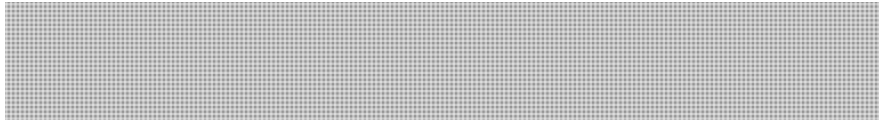


Engaging Licence Holders

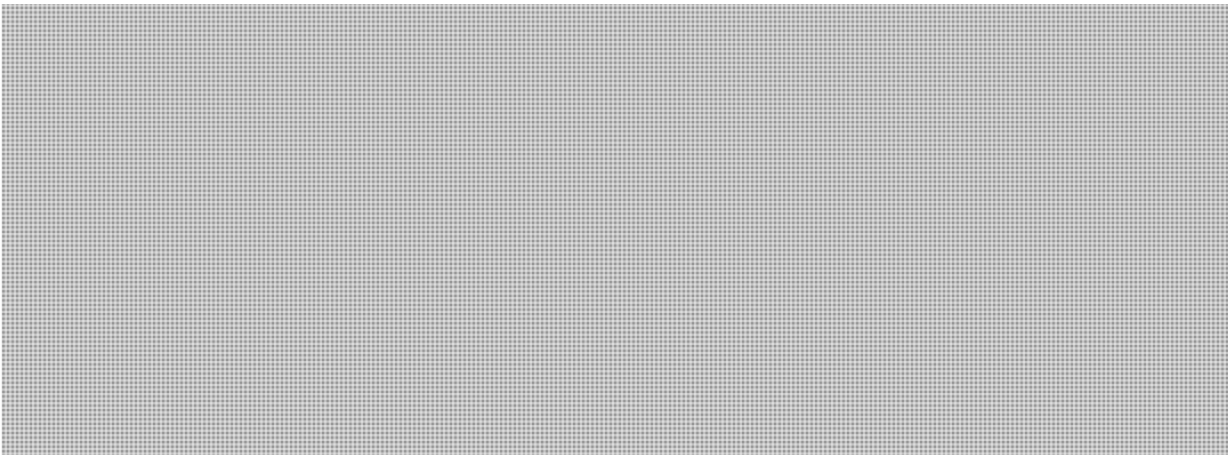
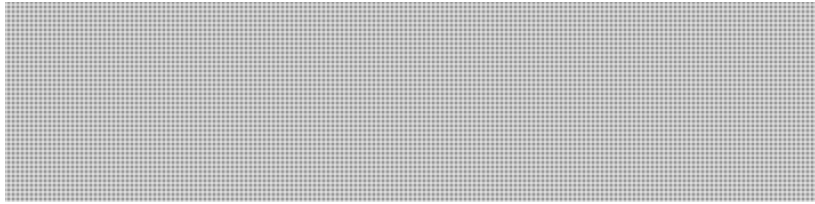
SAFETY AND RESILIENT CANADA

s.21(1)(a)

- Industry Canada (IC) is responsible for administering and ensuring compliance with the lawful interception condition of licence



- The preferred approach that emerged involves:



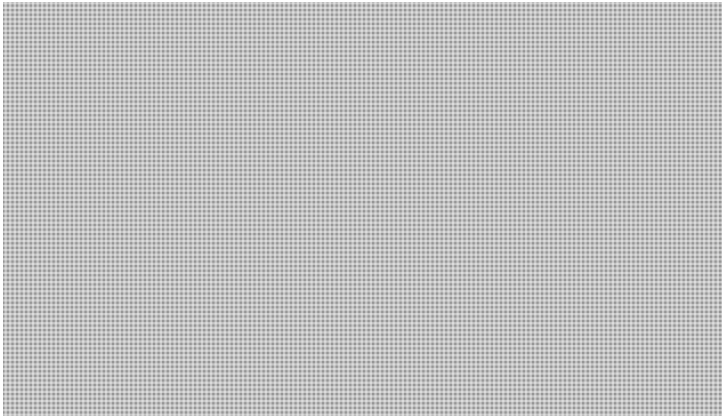
optics

s.21(1)(a)

Proposed Approach

SAFETY OF RESIDENT CANADA

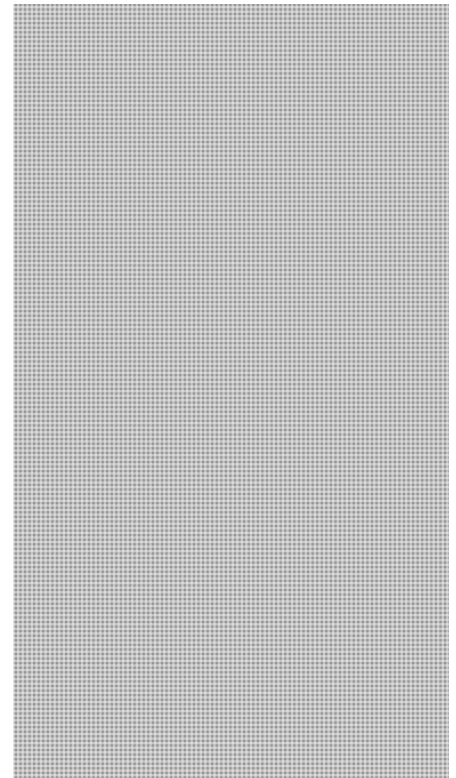
- We are proposing a 4 step approach:



Public Safety Canada / Sécurité publique Canada

5

- For each step we have proposed an objective and some outputs.



**Pages 375 to / à 376
are withheld pursuant to section
sont retenues en vertu de l'article**

21(1)(a)

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

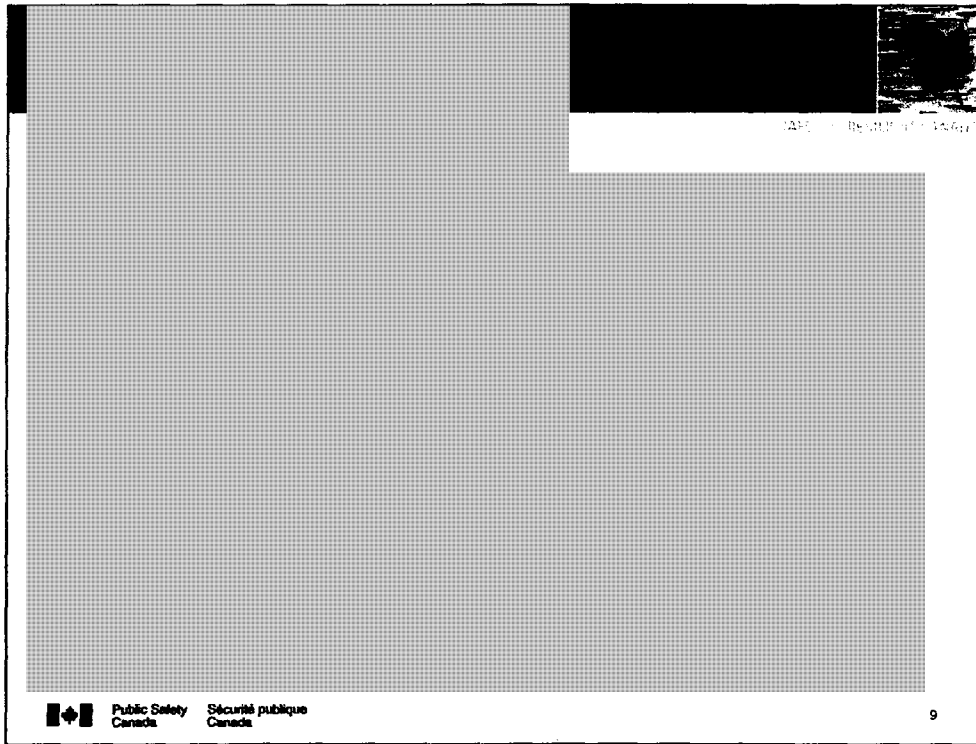
Page 377

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

21(1)(a), 21(1)(b)

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

s.21(1)(a)



- Finally, we want to ensure that the forbearance program runs smoothly and effectively
- [REDACTED]
- We have already started some of this work.
- [REDACTED]
- [REDACTED] We will endeavor to send these to you for consultation shortly.
- [REDACTED] are also something we are working on.
- We have some preliminary [REDACTED] which we will also consult with you shortly, but recognize that these may be evolving as the program strengthens. As we move forward, we hope to have more information track and better ways to gauge performance.

Timelines

SAFETY AND SECURITY OF CANADA

s.21(1)(a)

- Step 1 – [REDACTED]
 - Timelines: May – Sep 2013
 - Responsibility Centres: PS, RCMP, CSIS
- Step 2 – [REDACTED]
 - Timelines: Sep- Dec 2013
 - Responsibility Centres: RCMP/CSIS (lead), PS
- Step 3 – [REDACTED]
 - Timelines: Jan 2014 and ongoing
 - Responsibility Centres: IC/PS (lead), RCMP, CSIS
- Step 4 – [REDACTED]
 - Timelines: Ongoing
 - Responsibility Centres: PS (lead), RMCP, CSIS



Public Safety Canada / Sécurité publique Canada

10

- These timelines are a bit of a placeholder.
- I think we might be able to be more aggressive with these timelines.
- **Thoughts?**

Page 380

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

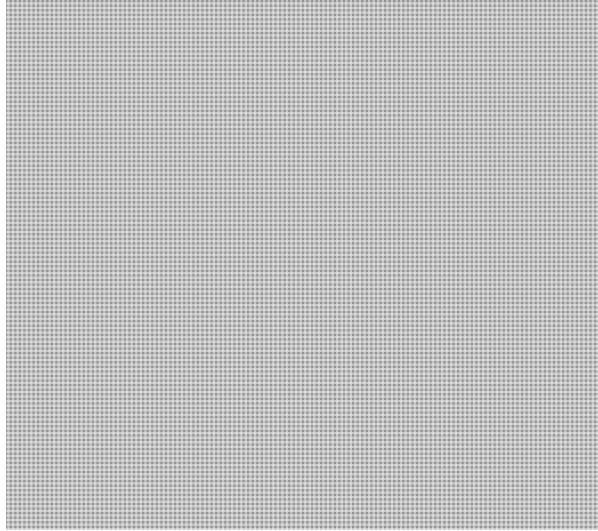
21(1)(a), 21(1)(b)

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

Draft Business Process



PROTECTOR GENERAL'S OFFICE - BUREAU GÉNÉRAL DU PROTECTEUR



s.21(1)(a)

- Visual of business process.

s.21(1)(a)

Benefits

SAFE - RESILIENT CANADA

- Short term investments in outlining [redacted] will reap benefits
- A stronger, more structured program will lead [redacted]

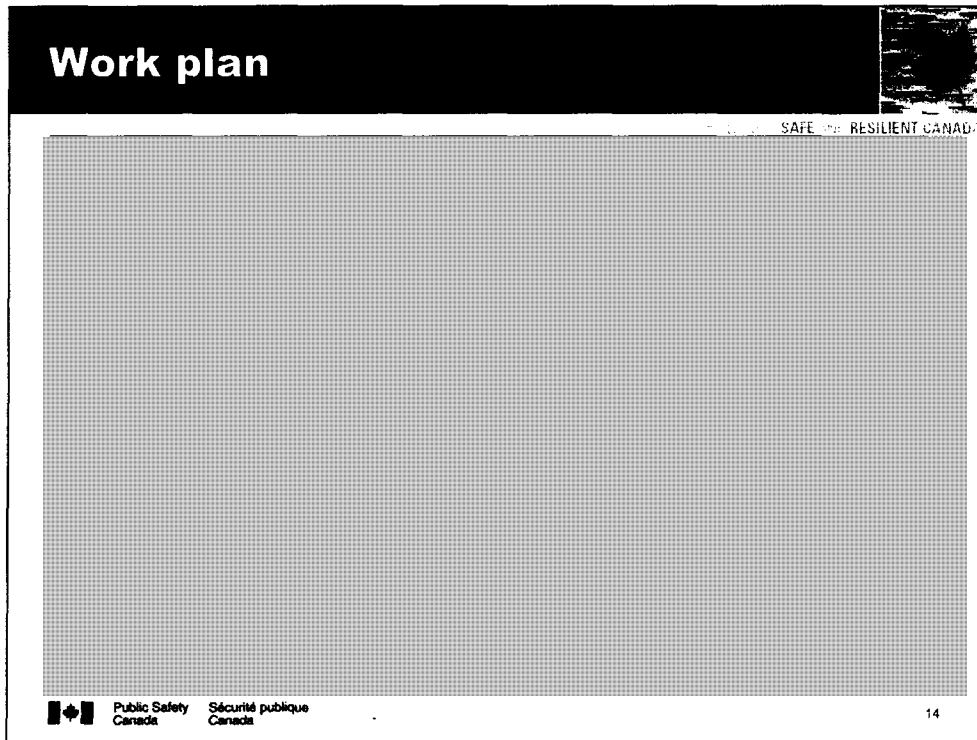
Public Safety Canada / Sécurité publique Canada

13

- As with any program, some initial heavy lifting can lead to longer term benefits.

Work plan

s.21(1)(a)



- We have also put together a work plan based on the outputs of this strategy.
- Not yet started, delayed, significantly delayed, in progress, done.
- This workplan will be adjusted as we adjust the strategy.

Forbearance Strengthening



Public Safety Canada

Questions?



Public Safety
Canada

Sécurité publique
Canada

15

s.21(1)(a)

s.23

Hawrylak, Maciek

From: Pilon, Claude
Sent: April-25-13 4:08 PM
To: Hawrylak, Maciek
Subject: RE: Report - Lawful Access - Trip Report from UK - 2013-02-25

Maciek,

Thanks

Claude

From: Hawrylak, Maciek
Sent: March-12-13 1:13 PM
To: Pilon, Claude
Subject: Report - Lawful Access - Trip Report from UK - 2013-02-25

Claude,

Attached is the trip report I referenced in yesterday's conversation.

Best,
Maciek

Senior Policy Advisor | Conseiller principal
National Security Operations Directorate | Direction-générale des opérations de la sécurité nationale
Public Safety Canada | Sécurité publique Canada
Maciek.hawrylak@dragon.ps.gc.ca
613-991-6036



SECRET

DATE:

File No.: NS 6652-O3 /394413
RDIMS No.: DRAGON 6411

MEMORANDUM FOR THE DIRECTOR GENERAL

FORBEARANCE QUARTERLY REPORT, FY 2012-2013, Q4

(Information only)

s.16(1)(c)
s.16(2)
s.21(1)(a)
s.21(1)(b)

ISSUE

To provide an update on forbearance requests for the fourth quarter of FY 2012-2013; from January 1, 2013, to March 31, 2013. The next report is due July 12, 2013.

STATUS OF FORBEARANCE REQUESTS

[Redacted]

Status:

[Redacted]

Report:

[Redacted]

should/can we clarify better?

Next Steps:

[Redacted]

[Redacted]

Status:

[Redacted]

Report:

- s.16(1)(c)
- s.16(2)
- s.21(1)(a)
- s.21(1)(b)

[Redacted]

[Redacted]

[Redacted]

[Redacted]

Next Steps:

[Redacted]

[Redacted]

Status:

[Redacted]

Report:

[Redacted]

[Redacted]

Next Steps:

[Redacted]

[Redacted]

Status:

[Redacted]

Report:

[Redacted]

Next Steps:

[Redacted]

[Redacted]

[Redacted]

Status:

[Redacted]

CBCF
topic?
PS/DA
stand-alone
topic?

SECRET

s.16(1)(c)
s.16(2)
s.21(1)(a)
s.21(1)(b)

Report: [Redacted]

Next Steps: [Redacted]

FORBEARANCE PROGRAM ENHANCEMENT

*Good stuff.
Should we
do a 2pg
memo to
SADM?*

In February 2013, PS met again with the RCMP, CSIS and IC to further discuss a strategy to enhance the forbearance program. [Redacted]

[Redacted]

LOOK AHEAD

- April 2013
 - Bi-monthly Forbearance Working Group (April, 29, 2013- TBC)
- May 2013
 - Conference call with [Redacted] (Forbearance expires June 30, 2013)
- June 2013
 - Conference call with [Redacted] for progress update (Forbearance expires September 30, 2013)
 - Conference call with [Redacted] (Forbearance expires June 28, 2013)

Should you require additional information, please do not hesitate to contact me at 613-949-3181 or Shawn Plunkett, Senior Policy Advisor, Investigative Technologies and Telecommunications Policy at 613-990-7066.

MHC
Marie-Hélène Chayer
Director, Investigative Technologies and Telecommunications Policy
National Security Operations

Prepared by: Julie Thompson

April 17, 2013



Public Safety / Sécurité publique
Canada / Canada

*Good work.
MM.*

SECRET

s.16(1)(c)
s.16(2)
s.21(1)(a)
s.21(1)(b)

DATE:

File No.: NS 6652-O3 / 392858
RDIMS No.: DRAGON 4920

MEMORANDUM FOR THE DIRECTOR GENERAL

FORBEARANCE QUARTERLY REPORT, FY 2012-2013, Q3

(Information only)

ISSUE

To provide an update on forbearance requests for the third quarter of FY 2012-2013; from October 1, 2012, to December 31, 2012. The next report is due April 12, 2013.

STATUS OF FORBEARANCE REQUESTS

[Redacted]

Status:

[Redacted]

Report:

[Redacted]

Next Steps:

[Redacted]

SECRET

s.16(1)(c)

s.16(2)

s.21(1)(a)

s.21(1)(b)

[Redacted]

Status:

[Redacted]

Report:



[Redacted]

Next Steps:

[Redacted]

[Redacted]

Status:

[Redacted]

Report:



[Redacted]

Next Steps:

[Redacted]

SECRET

[Redacted]

Status: [Redacted]
[Redacted]

Report: [Redacted]

s.16(1)(c)

s.16(2)

s.21(1)(a)

s.21(1)(b)

Next Steps: [Redacted]
[Redacted]

[Redacted]

Status: [Redacted]
[Redacted]

Report: [Redacted]
[Redacted]

Next Steps: [Redacted]
[Redacted]

In November 2012, PS met with the RCMP and CSIS to discuss a strategy to enhance the forbearance program. PS presented new tools to strengthen the management of this regime, including a draft performance dashboard, a draft compliance table and the Forbearance Quarterly Report. The agencies supported the overall strategy, [Redacted]



[Redacted]

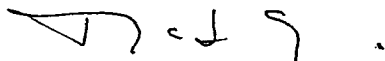
SECRET

- 4 -

LOOK AHEAD

- January 2013
 - Meeting with the RCMP and CSIS to align positions [REDACTED] (Jan 28)
 - s.16(1)(c) ○ Meeting with [REDACTED] (Jan 29) – *POSTPONED*
 - s.16(2) ○ Forbearance Expiry – [REDACTED] (Jan 31)
 - s.21(1)(a)
- February 2013
 - Bi-monthly meeting with the agencies (second week of Feb)
 - [REDACTED] (TBD)
 - PS will participate in the agencies' [REDACTED] (Feb 27)
- March 2013
 - Nil

Should you require additional information, please do not hesitate to contact me at 613-949-3181 or Shawn Plunkett, Senior Policy Advisor, Investigative Technologies and Telecommunications Policy at 613-990-7066.



Marie-Hélène Chayer
Director, Investigative Technologies and Telecommunications Policy
National Security Operations

Prepared by: Julie Thompson

s.20(1)(b)

s.21(1)(a)

Emmett, Jamie

From: Plunkett, Shawn
Sent: March-21-13 5:19 PM
To: Grigsby, Alexandre
Cc: Chayer, Marie-Helene; Binne, Christine (Christine.Binne@ps-sp.gc.ca); Hawrylak, Maciek
Subject: RE: Application service providers and lawful access - Revised version
Attachments: PS-SP-#795622-v3-Briefing_Note_-_Application_Service_Providers_-_2013-03....doc

Hi Alex,

Please use this revised version instead of the one I sent earlier?

Sorry about this.

Thanks.

From: Plunkett, Shawn
Sent: March-21-13 4:52 PM
To: Grigsby, Alexandre
Cc: Chayer, Marie-Helene; Binne, Christine (Christine.Binne@ps-sp.gc.ca); Hawrylak, Maciek
Subject: FW: Application service providers and lawful access

Alex,
As requested, please find a briefing note on Application Service Providers for SADM's meeting next week. Grateful if you could advise should any changes be required.

Let us know if you need anything further.

Thanks.

From: Grigsby, Alexandre
Sent: March-20-13 11:53 AM
To: Plunkett, Shawn
Cc: Binne, Christine
Subject: Application service providers and lawful access

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

Hi Shawn,

I'm e-mailing you in Maciek's absence with the hopes that you can help me out with something.

s.13(1)(a)

s.15(1) - Int'l

Now I've already talked to Justice on this issue and they've given me a rundown of what's happening on this in the Quintet (the five Attorneys General) and will be providing me some background briefs. Do you know if NSOps has provided any briefing notes on this particular topic to Lynda? I want to make sure that whatever briefing note I draft is consistent with what you have provided to her in the past on this issue, if at all.

Thanks

alex

Alexandre Grigsby
Analyst | Analyste
National Cyber Security Directorate | Direction générale de la cybersécurité nationale
Public Safety Canada | Sécurité publique Canada
tel. 613.949.4243
www.publicsafety.gc.ca | www.securitepublique.gc.ca

UNCLASSIFIED

BRIEFING NOTE

APPLICATION SERVICE PROVIDERS

STRATEGIC OBJECTIVES

s.13(1)(a)

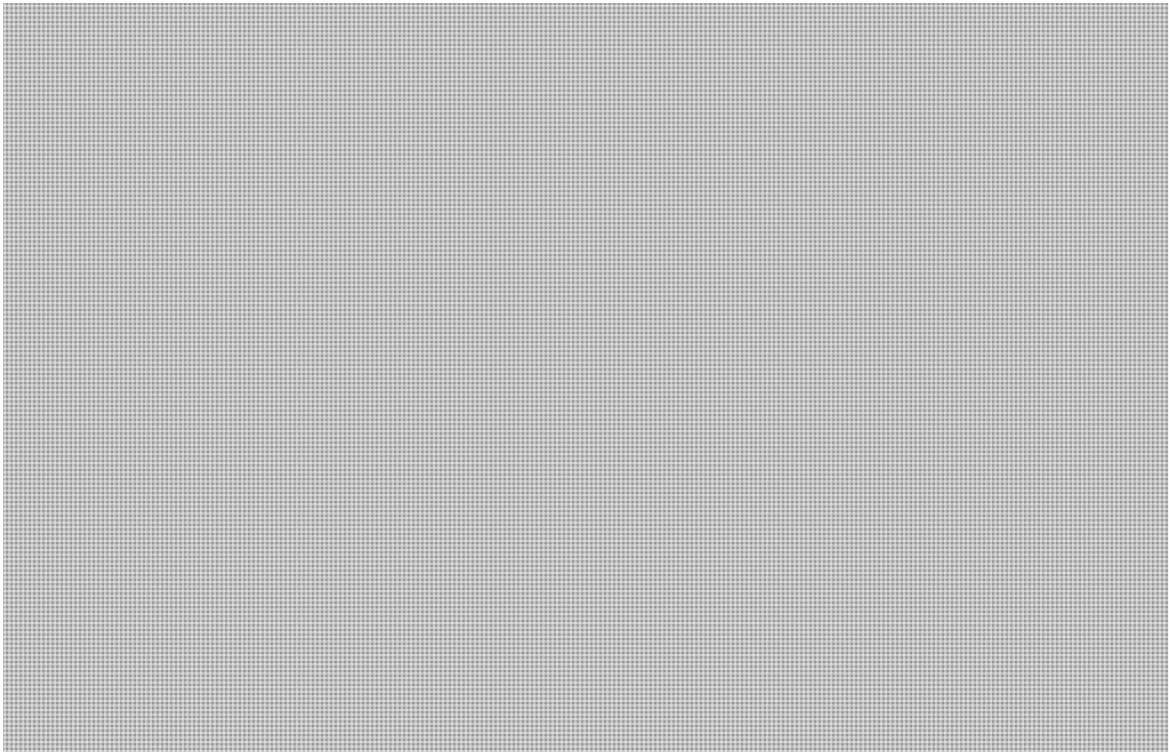
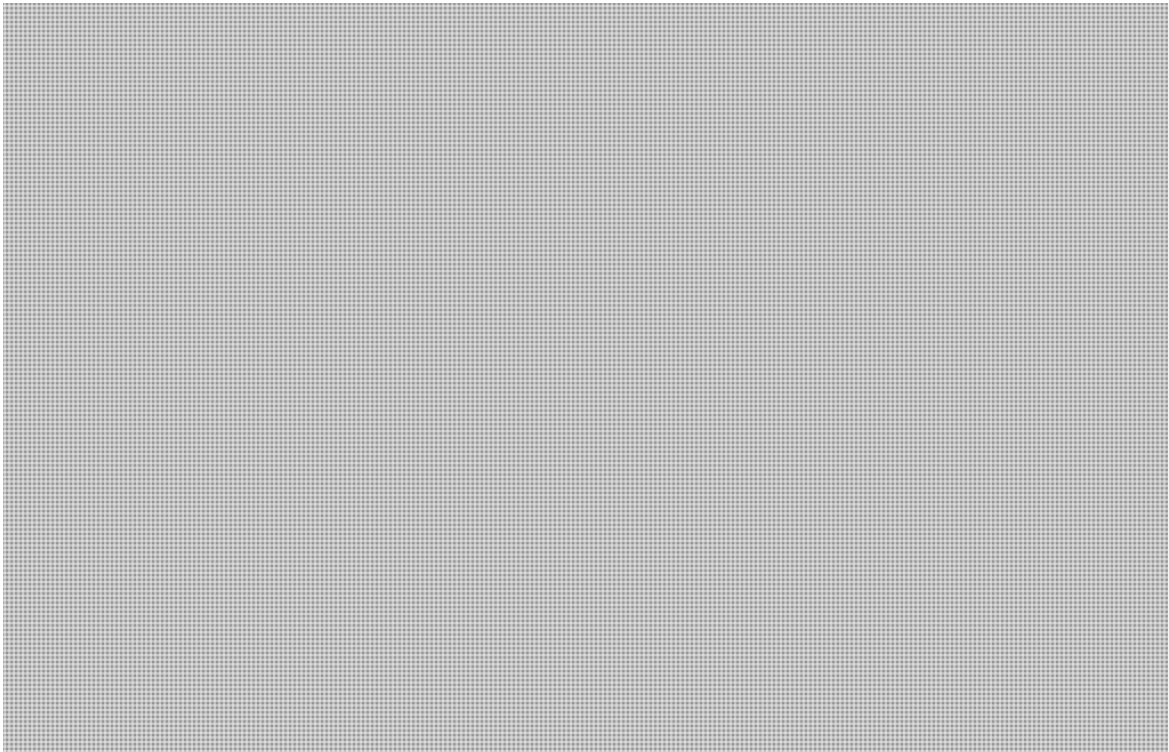
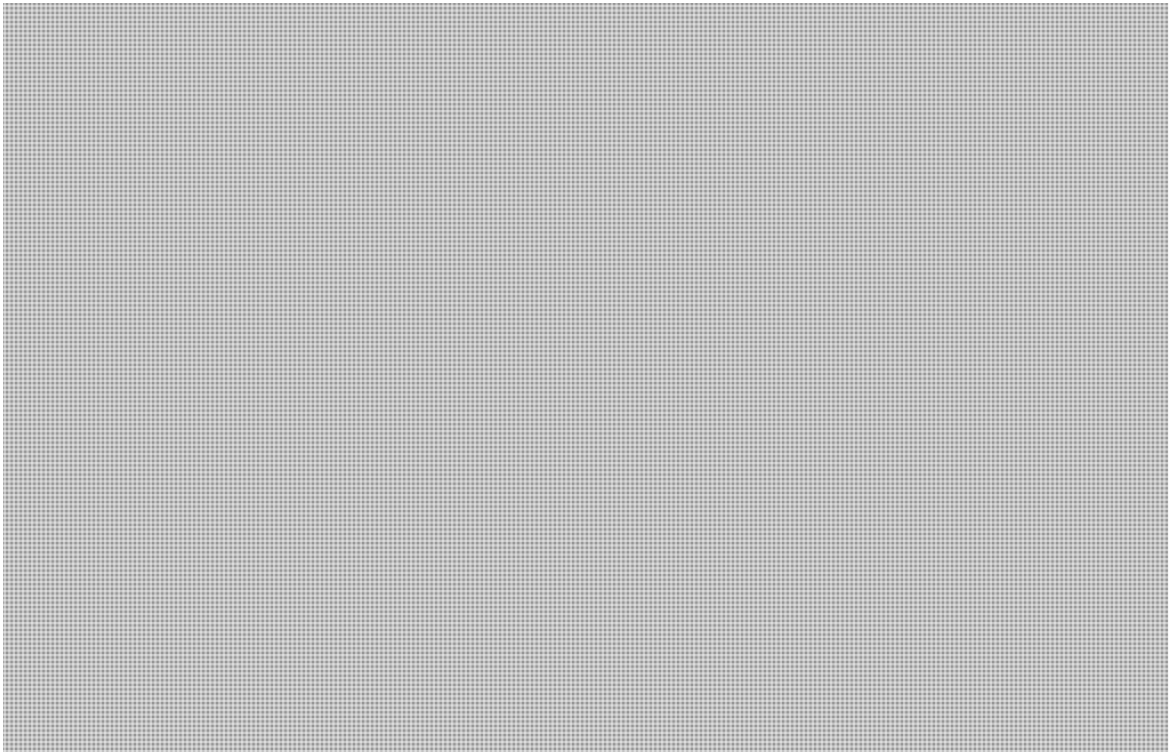
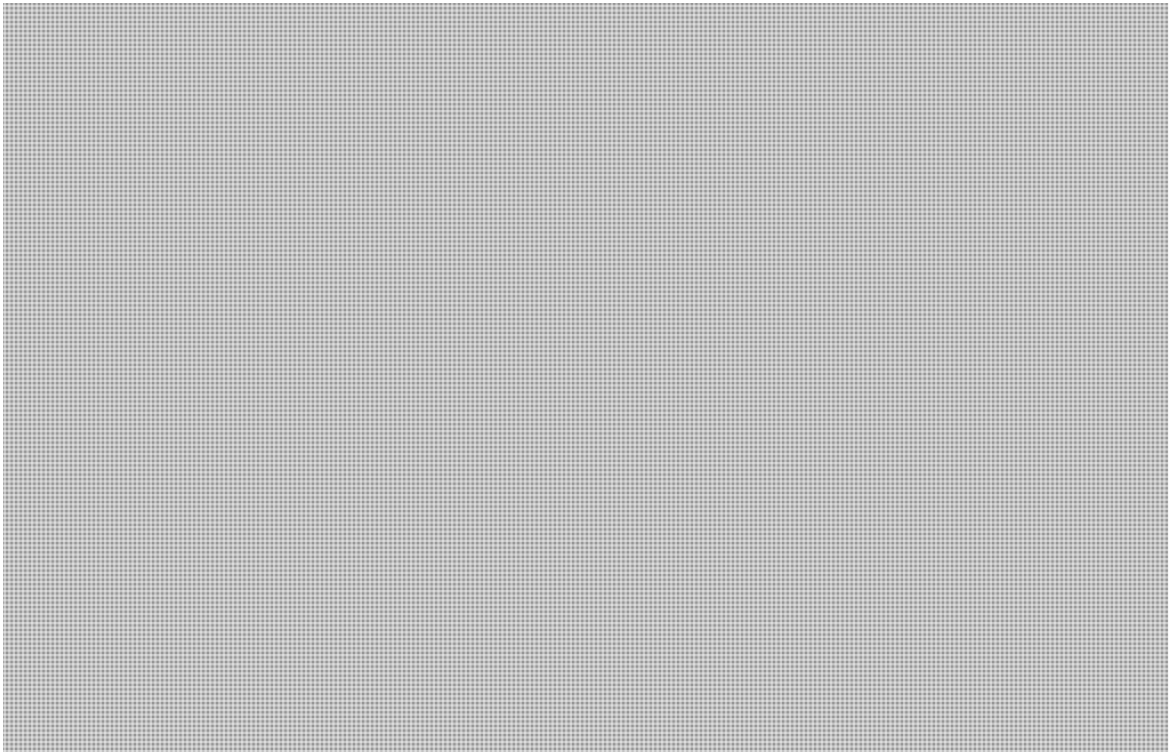
s.15(1) - Int'l

s.16(1)(b)

s.16(1)(c)

- Ensure that work to address challenges posed by Application Service Providers (ASPs) incorporate policy, legal and operational considerations.
- Ensure that any new initiative to address this issue will align with and build on ongoing multilateral efforts.

CONSIDERATIONS

- 
- 
- 
- 

BACKGROUND

ASPs are web-based services, such as VoIP (Voice Over Internet Protocol) and webmail (Hotmail, Gmail), that are accessed or downloaded by users over the Internet. The number and use of ASPs is growing as a result of the popularity of services such as Skype, FaceTime and other newer forms of communication.



UNCLASSIFIED

[REDACTED]

There is no formal mechanism for Canada to obtain intercepted communication or electronic data from other countries. In fact, the legislative framework of some countries (e.g. US) prevents service providers from conducting interceptions for or sharing personal information on their customers with foreign countries. [REDACTED]

[REDACTED]

The interception capability requirement included in Bill C-30, the *Protecting Children From Internet Predators Act*, would have applied to Canadian ASPs, and thus would have compelled those companies to assist agencies in obtaining intercepted communications or other electronic data. [REDACTED]

[REDACTED]

CURRENT STATUS

[REDACTED]

- s.13(1)(a)
- s.14(a)
- s.15(1) - Int'l
- s.16(1)(b)
- s.16(1)(c)

UNCLASSIFIED

TALKING POINTS

- Obtaining information and interceptions of communications from Application Services Providers is a growing operational challenge for Canadian law enforcement and national security agencies, especially regarding encrypted communications.
- I understand that officials from our respective security and legal communities are already working together to tackle this issue. We welcome any further suggestions to help address this complex challenge in an effective and timely manner.

Hawrylak, Maciek

From: Grigsby, Alexandre
Sent: March-21-13 5:06 PM
To: Plunkett, Shawn
Cc: Chayer, Marie-Helene; Binne, Christine; Hawrylak, Maciek
Subject: RE: Application service providers and lawful access

Excellent. Thanks!

I'm not going to make any changes to the note save for some formatting stuff to ensure consistency across the binder.

Thanks again for the really quick turn-around!

alex

Grigsby, Alexandre
March 21, 2013 5:06 PM

From: Plunkett, Shawn
Sent: Thursday, March 21, 2013 4:52 PM
To: Grigsby, Alexandre
Cc: Chayer, Marie-Helene; Binne, Christine; Hawrylak, Maciek
Subject: FW: Application service providers and lawful access

Alex,
As requested, please find a briefing note on Application Service Providers for SADM's meeting next week. Grateful if you could advise should any changes be required.

Let us know if you need anything further.

Thanks.

s.13(1)(a)

s.15(1) - Int'l

From: Grigsby, Alexandre
Sent: March-20-13 11:53 AM
To: Plunkett, Shawn
Cc: Binne, Christine
Subject: Application service providers and lawful access

Hi Shawn,

I'm e-mailing you in Maciek's absence with the hopes that you can help me out with something.



Now I've already talked to Justice on this issue and they've given me a rundown of what's happening on this in the Quintet (the five Attorneys General) and will be providing me some background briefs. Do you know if NSOps has provided any briefing notes on this particular topic to Lynda? I want to make sure that whatever briefing note I draft is consistent with what you have provided to her in the past on this issue, if at all.

Thanks

alex


Alexandre Grigsby
Analyst | Analyste
National Cyber Security Directorate | Direction générale de la cybersécurité nationale
Public Safety Canada | Sécurité publique Canada
tel. 613.949.4243
www.publicsafety.gc.ca | www.securitepublique.gc.ca

s.13(1)(a)

s.15(1) - Int'l

Emmett, Jamie

From: Plunkett, Shawn s.13(1)(a)
Sent: March-20-13 12:11 PM s.15(1) - Int'l
To: Chayer, Marie-Helene s.21(1)(a)
Subject: FW: Application service providers and lawful access s.21(1)(b)

Hi, please see below message from Cyber. 



From: Grigsby, Alexandre
Sent: March-20-13 11:53 AM
To: Plunkett, Shawn
Cc: Binne, Christine
Subject: Application service providers and lawful access

Hi Shawn,

I'm e-mailing you in Maciek's absence with the hopes that you can help me out with something.



Now I've already talked to Justice on this issue and they've given me a rundown of what's happening on this in the Quintet (the five Attorneys General) and will be providing me some background briefs. Do you know if NSOps has provided any briefing notes on this particular topic to Lynda? I want to make sure that whatever briefing note I draft is consistent with what you have provided to her in the past on this issue, if at all.

Thanks

alex

Alexandre Grigsby
Analyst | Analyste
National Cyber Security Directorate | Direction générale de la cybersécurité nationale
Public Safety Canada | Sécurité publique Canada
tel. 613.949.4243
www.publicsafety.gc.ca | www.securitepublique.gc.ca

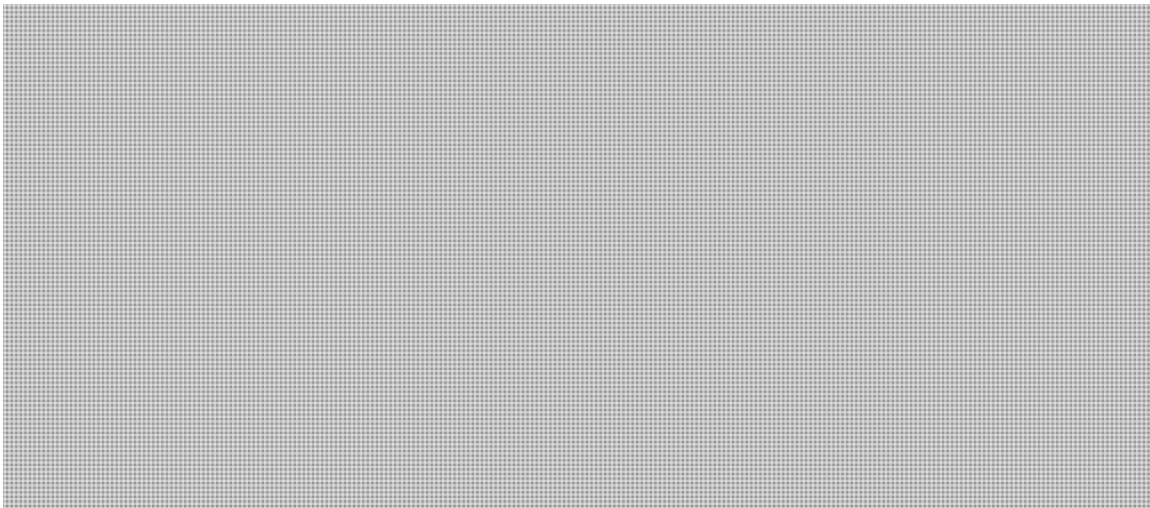
CONFIDENTIAL

s.15(1)(i) and 21(1)(a) of ATI Act apply

**Deputy Minister's meeting with James Cole, US Deputy Attorney General
Background Information and Talking Points
for a Potential Lawful Access Discussion
March 14, 2013**

BACKGROUND

Under the 1994 *Communications Assistance for Law Enforcement Act* (CALEA), telecommunications service providers (TSPs) in the United States (US) must maintain the capability to intercept communications. While CALEA was originally drafted to cover managed wireline voice technologies (i.e. the public telephone system) that were prevalent in the early 1990s, the scope of the law was extended in 2004 to cover new types of telecommunications developed since the law's introduction, including some high speed internet services.



Canada does not have legislation similar to CALEA. An attempt in 2012 to introduce lawful access legislation was met with much criticism, and the Government of Canada has since announced that it will not be pursuing current Bill C-30. This Bill included a suite of legislative measures aimed at:

1. compelling TSPs to build and maintain intercept capable systems;
2. requiring TSPs to provide limited basic subscriber information (such as a subscriber's name, address, telephone number, and e-mail address) to designated authorities and to police officers in certain circumstances;
3. streamlining the warrant application process for multiple investigative techniques involving an interception;
4. modernizing some investigative powers; and
5. introducing safeguards for the use of warrantless interceptions conducted in exceptional circumstances (in response to a 2012 Supreme Court decision, which ruled that the current *Criminal Code* provisions on emergency wiretapping are unconstitutional).

s.13(1)(a)

s.15(1) - Int'l

CONFIDENTIAL

s.15(1)(i) and 21(1)(a) of ATI Act apply

On February 11, 2013, the Minister of Justice introduced Bill C-55, the *Response to the Supreme Court of Canada Decision in R. v. Tse Act*, which mainly consists of C-30's provisions to introduce safeguards for the use of warrantless interceptions conducted in exceptional circumstances (number 5 above). The Government publicly indicated that the provisions in Bill C-30 pertaining to interception capability and access to basic subscriber information (numbers 1 and 2 above) would not go forward. [REDACTED]

TALKING POINTS

- Technological changes in the telecommunications sector are affecting how law enforcement and national security agencies around the world do their job. We must all adapt to these changes.
- We are following with interest your discussions [REDACTED] If we can provide any assistance, please do not hesitate to contact my officials.

(If pressed on Bill C-30)

- The Government recently introduced legislation to increase the safeguards related to the conduct of warrantless interceptions in exceptional circumstances.
- Specifically, the proposed amendments would include notification and reporting requirements, and would limit the authority to use emergency wiretapping to police officers for specific offences.
- Providing law enforcement and national security agencies with the tools they need to do their job remains a priority, and we continue to look at ways to more effectively fight crime in the digital age.
- Our aim is to strike the right balance between investigative needs and privacy protection.

s.15(1) - Int'l

s.21(1)(a)

s.15(1)(i) and 21(1)(a) of ATI Act apply

**Background Information and Talking Points
for a Potential Lawful Access Discussion
March 2013**

BACKGROUND

Under the *Regulation of Investigatory Powers Act* (RIPA, 2000), telecommunications service providers (TSPs) in the UK must maintain the capability to intercept communications. The content of interceptions are used by British authorities to build cases and gather intelligence, but cannot be used in court in order to protect the integrity of interception techniques. However, the communications data of interceptions (who was communicating, when, from where, and with whom) is used in court proceedings, given that the techniques involved to obtain that data are less sensitive.

In June 2012, the UK Government published draft legislation, the *Communications Data Bill*. The proposed Bill would amend RIPA to preserve the ability of British authorities to obtain certain types of data in the face of evolving technologies. The idea behind publishing draft legislation was to allow Parliamentary committees and the public to comment on the text of the proposed legislation prior to the official tabling in Parliament.

The draft Bill proposes to allow UK authorities to order a TSP to generate, collect or retain certain types of communications data that it might not otherwise have. The move towards internet based communications makes it increasingly difficult for police and security agencies to obtain this type of data because TSPs have fewer business reasons for retaining it than in the past. UK police and security agencies estimate that, without legislation, up to 25% of communications data that could be useful to operations would not be available to them.

A UK Joint Parliamentary committee was charged with reviewing the draft Bill and submitted its report in December 2012. The report notably recommended to:

- narrow the ability of the Government to order a TSP to retain data to only those instances where a clear gap was identified;
- conduct another round of public consultations;
- revise cost estimates which the Committee felt were too low; and
- improve the detail of reporting and auditing done by the UK's Interception Commissioner.

UK Privacy advocates have also sharply criticized the draft Bill as being too expansive in scope and unnecessary. The UK Government accepted the Joint Parliamentary committee's recommendations in principle, and is planning to consult further with industry and privacy advocates. A new draft Bill is expected in the coming weeks.

Canada does not have legislation similar to the UK's existing RIPA or draft *Communications Data Bill*. An attempt in 2012 to introduce lawful access legislation that was not nearly as ambitious as the UK's proposed and existing legislation was met

s.15(1)(i) and 21(1)(a) of ATI Act apply

with much criticism, and the Government of Canada has since announced that it will not be pursuing it. The legislation was Bill C-30, the *Protecting Children from Internet Predators Act*. This Bill included a suite of legislative measures aimed at:

1. compelling TSPs to build and maintain intercept capable systems;
2. requiring TSPs to provide basic subscriber information (such as a subscriber's name, address, telephone number, and -mail address) to designated authorities and to police officers in certain circumstances.
3. streamlining the warrant application process for multiple investigative techniques involving an interception;
4. modernizing some investigative powers;
5. introducing safeguards for the use of warrantless interceptions conducted in exceptional circumstances (in response to a 2012 Supreme Court decision, which ruled that the current *Criminal Code* provisions on emergency wiretapping are unconstitutional).

In February 2013, the Minister of Justice introduced Bill C-55, the *Response to the Supreme Court of Canada Decision in R. v. Tse Act*, which mainly consists of C-30's provisions to introduce safeguards for the use of warrantless interceptions conducted in exceptional circumstances (number 5 above). The Bill received Royal Assent on March 27, 2013. The Government indicated that the provisions in Bill C-30 pertaining to interception capability and access to basic subscriber information (numbers 1 and 2 above) would not go forward.

TALKING POINTS

- Technological changes in the telecommunications sector are affecting how law enforcement and national security agencies around the world do their job. We must all adapt to these changes. We are following with interest the discussions about the new *Communications Data Bill*.

(If pressed on Bill C-30)

- Our Government recently introduced legislation to increase the safeguards related to the conduct of warrantless interceptions in exceptional circumstances.
- Specifically, the proposed amendments would include notification and reporting requirements, and would limit the authority to use emergency wiretapping to police officers for specific offences.
- We remain committed to provide law enforcement and national security agencies with the tools they need to do their job, and continue to look at ways to more effectively fight crime in the digital age. As always, we will aim to strike the right balance between investigative needs and privacy protection.