CONFIDENTIAL

DATE:

File No.: NS 6652-O3 / 386919

MEMORANDUM FOR THE SENIOR ASSISTANT DEPUTY MINISTER

ENHANCEMENTS TO THE MANAGEMENT OF THE LAWFUL INTERCEPTION CONDITION OF LICENCE REGIME, INCLUDING FORBEARANCE

(Information only)

ISSUE

Overview of recent and proposed enhancements to the management of the forbearance regime with respect to the lawful interception condition of licence.

BACKGROUND

Until passage and full implementation of lawful access legislation, the primary instrument for public safety agencies to compel telecommunications service providers and distributors to meet court authorized intercepts is through including a requirement for lawful interception in their spectrum licence. Part of this requirement is for licensees to abide by the *Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications* (SGES), a set of 23 standards that outline the high level requirements needed by public safety agencies to conduct lawful interception.

An important component of the Lawful Interception (LI) condition of licence is the forbearance regime. The Minister of Industry, in consultation with Public Safety Canada (PS), has the power to grant forbearance to any spectrum licensee from complying with all or part of the SGES. The forbearance regime allows for an important dialogue between the licensee and the Public Safety Portfolio, while ensuring that licence holders are working towards providing the required lawful intercept capabilities. Its objective is to foster relationships for problem resolution, not to deny or revoke licences.

.../2

CONSIDERATIONS

In order to ensure that public safety agencies have the maximum lawful intercept capabilities possible, we are pursuing a stronger, more robust management of the LI condition of licence regime, including the forbearance process within PS. To achieve this objective, Investigative Technologies and Telecommunications Policy (ITTP) has undertaken several program enhancements to bring greater rigour to the forbearance process.

Forbearance Formal Updates

Over the past year, ITTP has revised the approach to recommending approval of forbearance with IC and spectrum licence holders. This revised approach includes having licensees provide a formal update to the Portfolio on their compliance as part of the terms of their forbearance approval. Previously, licensees would often request an extension close to the expiration of their forbearance. This resulted in insufficient time for the Portfolio to work with the licensees to ensure compliance.

Stronger Reporting Tools

In the pursuit of more rigorous management of the forbearance regime, ITTP has begun to develop stronger reporting tools. Beginning with the fourth quarter of FY 2011-12, ITTP will report on the forbearance regime to myself on a quarterly basis The quarterly report will allow for stronger management of the forbearance regime by: regularizing reporting on forbearance requests; providing a tool for comparison and analysis across the difference requests; and offering an audit trail for future work on the file.

We will also be updating the existing forbearance tracking report to ensure that the report has the sufficient level of information, including specifics relating to the nature of the forbearance request, in order to make more informed decisions. This will also permit greater analysis in identifying areas where improvements to the forbearance process or the standards themselves may be required. A more robust tracking system will also allow

greater forward planning and thereby assist in ensuring that the Portfolio's time resources are well managed.

[redacted]

[redacted] *Compliance with Condition of Licence*

[redacted]

The current management of the forbearance regime involves either administering current forbearance requests (licensees that have requested forbearance in the past and have not yet become compliant) or administering requests made by licensees (licensees that proactively tell IC and PS that they are not compliant). [redacted]

Update on LI Condition of Licence –700 MHz Spectrum Auction

On April 25, 2012, IC launched a public consultation on the conditions of licence for the upcoming 700 MHz spectrum auction. As part of this public consultation, IC has agreed to consult on removing references to specific technologies in the Lawful Interception (LI) condition of spectrum licence, notably by removing the term 'circuit-switched'. If this

change to the condition of licence is adopted, this will result in a more relevant and more widely applicable LI condition, as 'circuit-switched' is an older technology that telecommunication service providers will not be using for their new networks.

IC has also included in the public consultation document, a reference to changes to the SGES that PS is currently proposing and directs interested parties to PS for further information. While these are positive developments, PS will need to continue to engage Industry Canada to ensure that the proposed technologically neutral LI condition does in fact become part of the 700 MHz spectrum licences. This could include providing formal and public comments to IC as part of this consultation, which PS did for the last public consultation on this issue. Should PS provide comments we would consult with the Portfolio agencies to ensure a comprehensive Portfolio view is sent to IC. Our comments would need to be submitted to IC no later than June 25, 2012.

NEXT STEPS

ITTP will develop and incorporate the above noted changes and continue to identify ways to manage the condition of licence regime in an effective and efficient manner. A more rigorous management of the forbearance process will allow PS to continue demonstrating leadership and value-added to our Portfolio partners.

Should you require additional information, do not hesitate to contact me at 613-993-4595, or Michèle Kingsley, Director, Investigative Technologies and Telecommunications Policy at 613-949-3181.

Michael MacDonald
Director General
National Security Operations

Prepared by: Shawn Plunkett

ANNEX B – Strategy Implementation Tools

Operationalized

Forbearance Formal Updates: To ensure that TSPs that were granted forbearance continue to work towards developing a lawful interception solution, IC, on the recommendation of ITTP, has been requesting that companies provide a mid term update on their progress as a condition of their forbearance. This allows the PS Portfolio to better monitor progress

Forbearance Quarterly Reports: So far, 5 forbearance quarterly reports have been submitted to the Director General of National Security Operations. These quarterly reports focus on progress made by companies with forbearance to develop interception solutions and provide updates on the implementation of the forbearance

Updated Tracking Report: Sections have been added to the forbearance tracking report, including area of non compliance, schedule for compliance, and next steps. These new fields give a better overview of where potential challenges lie with respect to compliance.

Forbearance Working Group: In fall 2012, ITTP launched a forbearance working group, in which representatives from and PS meet bimonthly to discuss both policy and operational issues related to the forbearance program.

In Progress

Pages 6 to / à 11

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 12

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

Department of Justice Canada

Industry Canada
Legal Services
8th Floor, East Tower
235 Queen Street
Ottawa, ON K1A 0H5

Ministère de la Justice Canada

Industrie Canada
Services juridiques
8ième étage, tour est
235, rue Queen
Ottawa (ON) K1A 0H5

Security classification - Cote de sécurité

Protected/ Solicitor-Client

Our file - Notre référence

Date

August 10th, 2011

Telephone/FAX - Téléphone/Télécopieur

613-952-6430 613-954-

MEMORANDUM NOTE DE SERVICE

TO/DEST: **Claude Pilon, Counsel**
Public Safety Canada Legal Services

FROM/ORIG.: **Diane St-Arnaud**

SUBJECT/
OBJET :

[redacted]

[redacted]

Pages 14 to / à 20

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

[redacted]

Regards,

Diane St-Arnaud
Senior Counsel (Manager)
Telecommunications Law Group

SECRET

DATE:

File No.: NS 6652 / 393945
RDIMS No.: Dragon 5131

MEMORANDUM FOR THE SENIOR ASSISTANT DEPUTY MINISTER

LAWFUL INTERCEPTION CONDITION OF LICENCE FOR THE 700 MHZ SPECTRUM AUCTION

(Information Only)

ISSUE

To provide information on Industry Canada's recent decision regarding the lawful interception condition of spectrum licence for the 700 MHz spectrum band.

BACKGROUND

In Canada, radio spectrum, the frequencies over which wireless communications are transmitted, is managed through a licensing regime. Under the *Radiocommunication Act* (RA), the Minister of Industry has the authority to grant licences with conditions and Telecommunication Service Providers (TSPs) must comply with these conditions when delivering wireless services such as cellular, smart phone and wireless Internet.

Certain licences include a condition to facilitate lawful interception. In those situations where a TSP's network cannot facilitate a lawful interception, the Minister of Industry, in consultation with Public Safety Canada (PS), may grant forbearance for a specified period of time. In the absence of lawful interception legislation, the lawful interception condition of licence remains the only instrument allowing public safety agencies to compel TSPs to implement court authorized interceptions.

CURRENT STATUS

In the context of the upcoming spectrum auctions on the 700 MHz and 2500 MHz spectrum bands, PS engaged Industry Canada (IC) with the intention of modernizing

.../2

the lawful interception condition of spectrum licence. Currently, the condition refers to outdated technologies, is limited to voice services ( ) and does not apply to all spectrum bands.

In April 2012, IC launched a public consultation on the 700 MHz spectrum auction and proposed to make the lawful interception condition both technologically and service neutral. Most TSPs and the Canadian Wireless Telecommunications Association (CWTA) opposed the proposed changes arguing that any modification to the lawful interception regime in Canada would be more appropriately done through legislation.

On March 7, 2013, IC released its decision on the conditions that will apply to spectrum licences on the 700 MHz band. For these licences, the lawful interception condition will now cover all technologies, but will continue to apply only to voice services (, thus excluding data services (i.e., Internet services). Data services are expected to continue to be among the fastest growing portions of the Canadian telecommunications market.

IC has given TSPs and the general public the opportunity to request clarification on any of the conditions of licence for the 700 MHz spectrum band and will respond publicly to these requests by May 20, 2013. The actual auction for this band will not take place until November 19, 2013. Once the auction is held and licences are awarded, law enforcement and national security agencies will approach licence holders offering voice services to assist them in complying with their lawful interception condition. In addition, IC will likely use the same lawful interception condition for the forthcoming auction on the 2500 MHz spectrum band, which is scheduled to take place in early 2014.

CONSIDERATIONS

IC's decision on the lawful interception condition of licence for the 700 MHz spectrum band

.../3

[redacted]

NEXT STEPS

PS is pursuing several options to i[redacted]
IC to ensure the broadest possible

[redacted]

Should you require additional information, do not hesitate to contact me at 613-993-4595, or Marie-Hélène Chayer, Director, Investigative Technologies and Telecommunications Policy at 613-949-3181.

Michael MacDonald
Director General
National Security Operations Directorate

Prepared by: Shawn Plunkett

700 MHz Proposed language for condition of licence:

A licensee ~~using spectrum for circuit switched voice telephony systems~~ operating as a service provider using an interconnected radio-based transmission facility for compensation must~~, from the inception of service,~~ provide for and maintain lawful interception capabilities as authorized by law~~. The requirements for lawful interception capabilities are provided in~~ and in accordance with the Solicitor General's *Enforcement Standards for Lawful Interception of Telecommunication,* ~~(Rev. Nov. 95). These standards may be~~ as amended from time to time.

The licensee may request the Minister of Industry to forbear from enforcing certain assistance capability requirements for a limited period. The Minister, following consultation with Public Safety Canada, may exercise the power to forbear from enforcing a requirement or requirements where, in the opinion of the Minister, the requirement is not reasonably achievable. Requests for forbearance must include specific details and dates indicating when compliance to the requirement can be expected.

NOTES:

(Radiocommunications) service provider is defined in the Radiocommunication Regulations as "a person including a radiocommunications carrier, who operates radio apparatus used by that person or another person to provide radiocommunication services for compensation."

The phrase *interconnected radio-based transmission facility* is defined in the Radiocommunication Regulations as "any radio apparatus that is used for the transmission or reception of intelligence to or from anywhere on a public switched network."

Previous language:

Licensees using spectrum for circuit-switched voice telephony systems must, from the inception of service, provide for and maintain lawful interception capabilities as authorized by law. The requirements for lawful interception capabilities are provided in the Solicitor General's *Enforcement Standards for Lawful Interception of Telecommunications* (Rev. Nov. 95). These standards may be amended from time to time.

The licensee may request the Minister of Industry to forbear from enforcing certain assistance capability requirements for a limited period. The Minister, following consultation with Public Safety Canada, may exercise the power to forbear from enforcing a requirement or requirements where, in the opinion of the Minister, the requirement is not reasonably achievable. Requests for forbearance must include specific details and dates indicating when compliance to the requirement can be expected.

Current language:

~~A licensees using spectrum for circuit-switched voice telephony systems~~

PS portfolio had requested this phrase to be removed. Impact will be that spectrum licences for the 700 MHz licences will not be limited to only circuit-switched technology.

operating as a service provider

Radiocommunications service provider is defined in the Radiocommunication Regulations as "person including a radiocommunications carrier, who operates radio apparatus used by that person or another person to provide radiocommunication services for compensation.

using an interconnected radio-based transmission facility

The phrase *interconnected radio-based transmission facility* is defined in the Radiocommunication Regulations as: "any radio apparatus that is used for the transmission or reception of intelligence to or from anywhere on a public switched network."

for compensation

The term *for compensation* is referred to in the Radiocommunication Regulations under *Radiocommunications service provider* (above) and radiocommunication carrier, which is defined as "a person who operates an interconnected radio-based transmission facility used by that person or another person to provide radiocommunication services for compensation".

must~~, from the inception of service,~~

provide for and maintain lawful interception capabilities as authorized by law~~. The requirements for lawful interception capabilities are provided in~~ and in accordance with

Is there a difference between these two phrases? Perhaps seek legal opinion.

the Solicitor General's *Enforcement Standards for Lawful Interception of Telecommunication,* ~~(Rev. Nov. 95). These standards may be~~ as amended from time to time.

The licensee may request the Minister of Industry to forbear from enforcing certain assistance capability requirements for a limited period. The Minister, following consultation with Public Safety Canada, may exercise the power to forbear from enforcing a requirement or requirements where, in the opinion of the Minister, the requirement is not reasonably achievable. Requests for forbearance must include specific details and dates indicating when compliance to the requirement can be expected.

Page 28

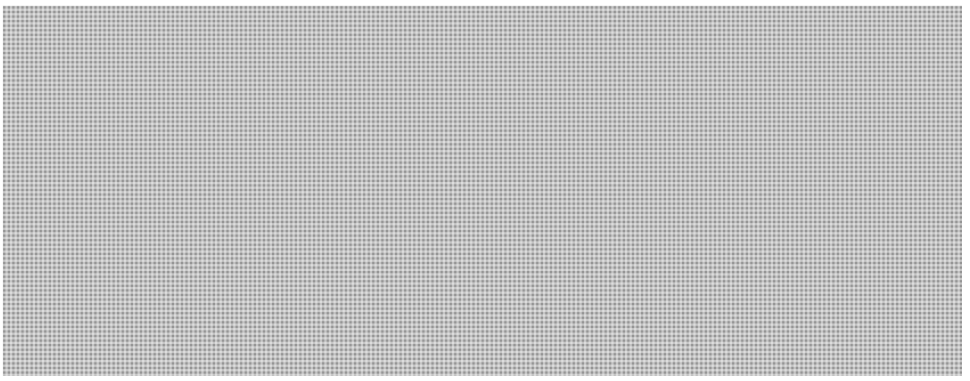
is withheld pursuant to sections

est retenue en vertu des articles

of the Access to Information

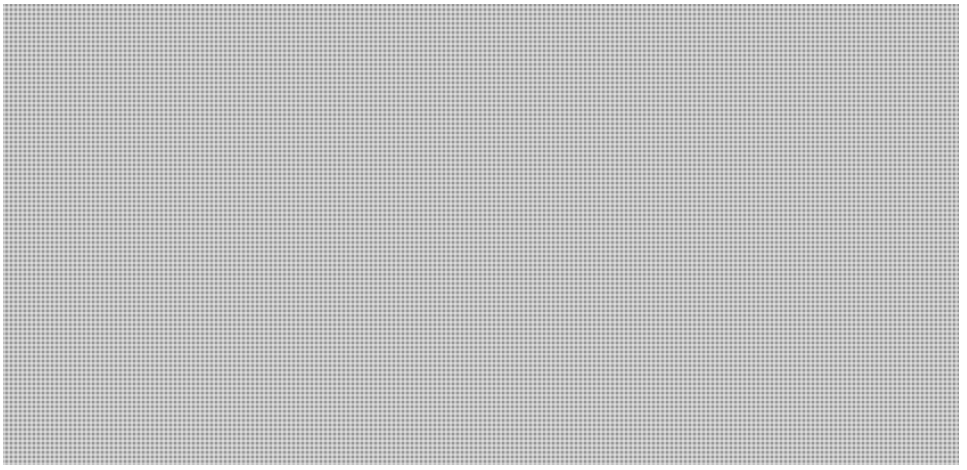
de la Loi sur l'accès à l'information

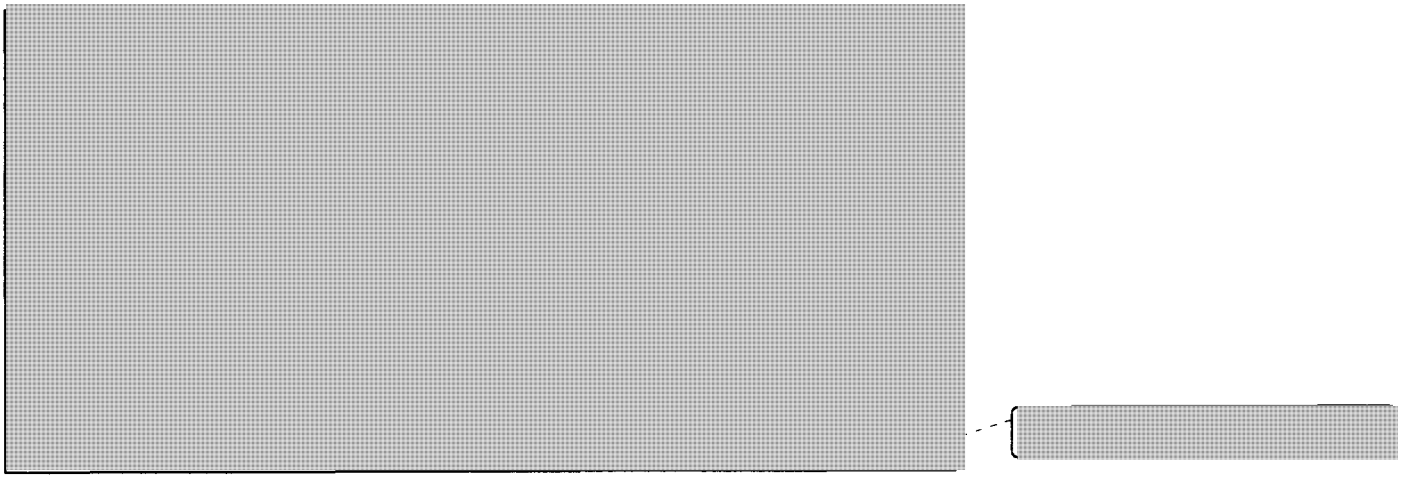
Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications



Standard 1: Law enforcement agencies require access to the entire telecommunications transmitted, or caused to be transmitted, to and from the number or other identifier of the target service used by the interception subject. Law enforcement agencies also require access to the call-associated data that is generated to process the call.

Law enforcement must receive ALL telecommunications that is received or transmitted by the target. This is not limited to the audio portion but must also include any data that is transmitted or received. An example of this would be some sort of short message service (SMS) or other data message that would not require an audio channel allocation. The audio channel must also include any analog transmission of fax or data that the target may transmit or receive. Additionally this may include the interception of voice mail services and/or cloning of same.





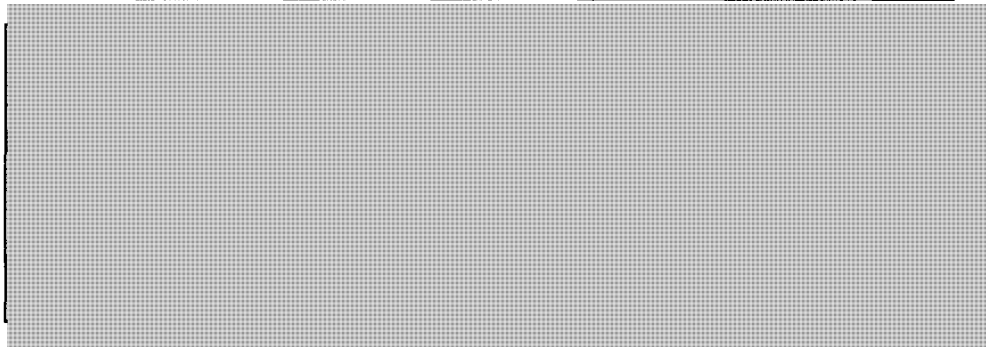
Standard 2: Law enforcement agencies require access to all mobile interception subjects operating temporarily or permanently within a telecommunications system.

Law enforcement requires the same capability on all users of the system whether they reside in the system permanently or on a temporary basis.

Standard 3: Law enforcement agencies require access in cases where the interception subject may be using features to divert calls to other telecommunications service or terminal equipment, including calls that traverse more than one network or are processed by more than one network operator/service provider before completing.

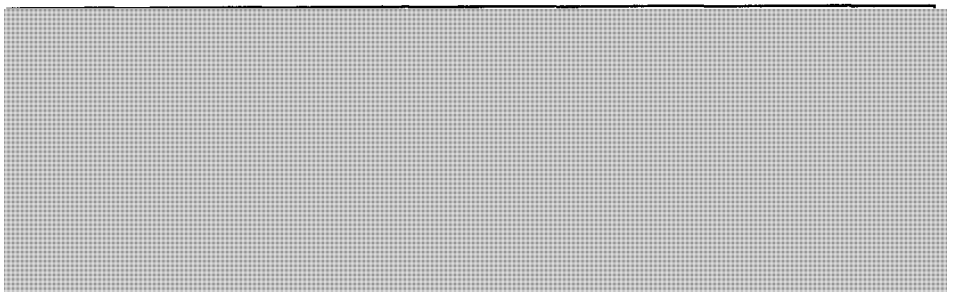
Law enforcement requires access to advanced calling features such as call forwarding and/or call diverting. It is understood that at least two distinct scenarios may exist here. They are inter-network and intra-network. Inter-network refers to calls originating in one service providers' network and terminating in another service provider's network. Intra-network refers to calls both originating and terminating within the same service

providers' network. Capabilities may differ in these scenarios based on the information provided between separate service providers. It is assumed by law enforcement that when the information can be made available and is made available to the customer, it will also be made available to law enforcement. It is important to determine the limitations of this capability in terms of multiple applications of this feature. (i.e. call forwarding a particular phone number several times. 'A' forwarded to 'B', 'B' forwarded to 'C' etc.)



Standard 4: Law enforcement agencies require that the telecommunications to and from a target service be provided to the exclusion of any telecommunications that do not fall within the scope of the interception authorization.

Simply stated, Law enforcement only has the authority to intercept specific target services to the exclusion of other customers served by the service provider. Law enforcement cannot receive any telecommunications that does not fall within the scope of the authorization and its specific time frame. It is the responsibility of the law enforcement agency to appropriately handle all intercepted material once in the possession of the law enforcement agency, which includes the determination of 'privileged call information' and its appropriate handling. Privileged call information is defined as calls which are intercepted but must be handled by law enforcement in a way which the courts define. (i.e. a solicitor/client conversation)



Standard 5: Law enforcement agencies require access to available call associated data such as:

[redacted]

A) Signaling of access ready status

Law enforcement requires some sort of signal to determine that a target phone has become active. The standard methodology is a continuous DTMF 'C' tone during target inactivity (on-hook) and removal of the tone during target activity (off-hook).

[redacted]

B) Called party number for outgoing connections even if there is no successful connection established

Law enforcement requires that the number dialed by the target be available to law enforcement even if the call is deemed incomplete. Examples of incomplete calls are: call, no answer; call, called part busy; call, called party is out of range (assuming wireless); call, all trunks/network busy; call, call forwarding. Law enforcement is also concerned that due to evidentiary rules, call correlation between call associated data and call content is imperative. Law enforcement requires a 1:1 correlation of call content to call data sessions. These outlined examples may cause problems in this area and affect compliance to standard #10 which requires accurate correlation between call content and call associated data. Preferred correlation methods of call content to call data are outlined in interpretation to standard #10

[redacted]

[redacted]

C) Calling party number for incoming connections even if there is no successful connection established

Law enforcement requires the calling number information to be forwarded in all examples as outlined above in 5b. It is understood that at least two distinct scenarios may exist here. They are inter-network and intra-network as defined in standard number 3 above. It is assumed by law enforcement as in standard number 3, that when the information can be made available and is made available to the customer, it will also be made available to law enforcement.

[redacted]

D) All digits dialed by the target, including post-connection dialed digits used to activate features such as conference calling and call transfer

*Law enforcement requires that any and all information transmitted by the target must also be relayed to law enforcement. This includes feature activations that do not necessarily constitute a call. It shall also include any digits dialed or feature activations during the progress of a call. This information may be transmitted to law enforcement in different ways however it is assumed that any 'in-band' information will remain in-band as well as be defined in any call associated data session. An example of this is the target dialing a *67 which activates call forwarding. Law enforcement would expect the in-band signaling to remain intact as well as an indication on the data session as to what feature was activated. All transmission of information should occur post call event rather than post call completion.*

[redacted]

[redacted]

E) Beginning, end, and duration of the connection

Law enforcement requires a time stamp on all sessions to establish dates and time of target calls.

[redacted]

F) Actual destination and intermediate directory numbers if call has been diverted.

Law enforcement requires intermediate destination numbers assuming call forward scenarios. It is understood that at least two distinct scenarios may exist here. They are inter-network and intra-network as defined in standard number 3 above. It is important to determine how many times calls can be diverted and tracked as stated in standard number 3 above

[redacted]

Standard 6: Law enforcement agencies require information on the most accurate geographical location known to the network for mobile subscribers.

There are 5 call scenarios that must be outlined here. They are as follows:
autonomous registration or initial power up of handset
initiation of an outbound call
answer of an incoming call
transfer between cell sites
end of call/hang up of calling party
Additionally, location information needs to be available immediately after the call event rather than after call completion. Further, the resolution of the geographical information sent is important for law enforcement to know. As an example, this information may contain a cell site id, cell sector information, signal strength etc.

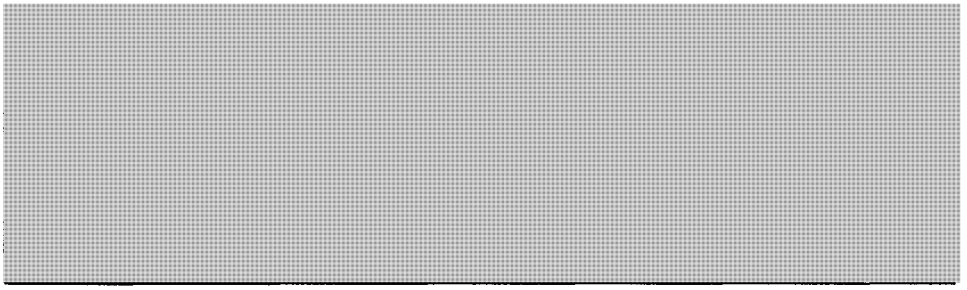
Standard 7: Law enforcement agencies require data on the specific service used by the interception subject and the technical parameters for that type of communication.

Law enforcement will require all information with respect to a targets service, which indicate to us the capabilities the target may have. As an example, this information may contain a list of features that the target has like call forwarding, voice mail, call conference, short message service, paging etc. This information must also include any information with respect to roaming agreements on other networks. This particular information would be limited to being notified of the capability. Other information with respect to his services on other networks would be obtained from the other service provider.

[redacted]

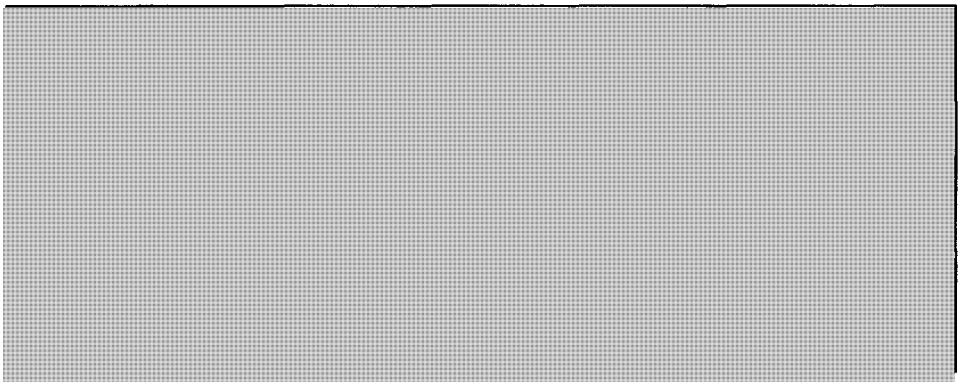
Standard 8: Law enforcement agencies require a real- time, full-time monitoring capability for the interception of telecommunications. Call associated data should also be provided in real-time. If call associated data cannot be made available in real time, law enforcement agencies require the data to be available as soon as possible upon call termination.

Law enforcement assumes that call content information, (audio) will be delivered to the law enforcement agency in real-time. Additionally, call associated data will be made available within milliseconds post call event rather than post call completion. (100ms – 500ms is the desirable target) It is imperative that the call-associated data be made available within this short time frame to allow correlation of call event with audio call details.



Standard 9: Law enforcement agencies require network operators/service providers to provide one or more interfaces from which the intercepted communications can be transmitted to the law enforcement monitoring facility. These interfaces have to be commonly agreed on by the interception authorities and the network operators/service providers. Other issues associated with these interfaces will be handled according to generally accepted practices.

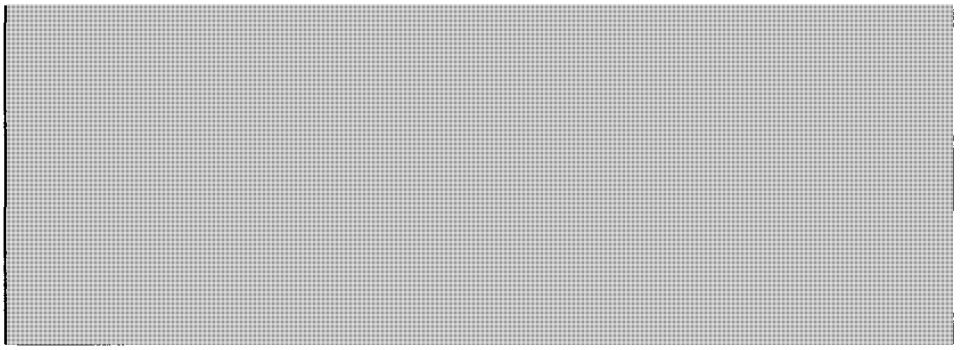
Law enforcement requires that the intercepted material be made available for transmission to law enforcement via industry standard interfaces as well as in a format that conforms to generally accepted practices. Essentially law enforcement would like to see the information available in a non-proprietary format and one that can be easily handled. This formatting of data is wholly dependent on the quantity and type of data made available.



Capability in Legislation/Regulation:

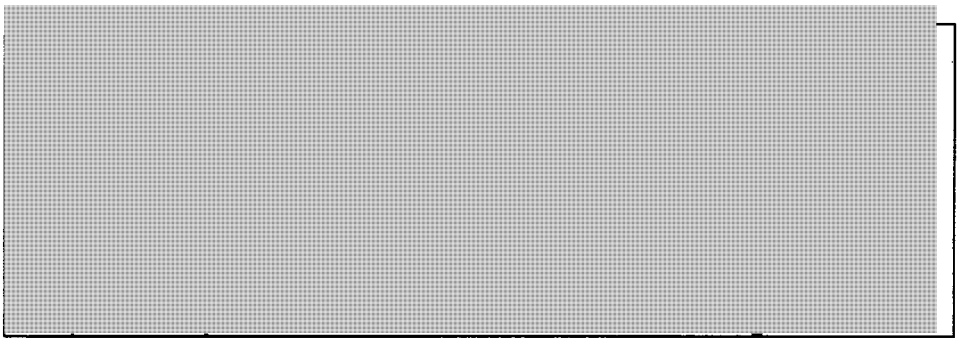
Standard 10: Law enforcement agencies require network operators/service providers to provide call associated data and call content from the target service in a way that allows for the accurate correlation of call associated data with call content.

Law enforcement requires a method of delivery of both the audio content and the data content in a manner that will allow for absolute accuracy of correlation. This is mandatory in terms of evidentiary requirements. Several possibilities are available here. As an example, all audio content and all associated data for each single target are combined in some way and transmitted over the same audio circuit. Another example is all voice content and a pre-determined subset of call associated data for each single target are combined in some way and transmitted over the same audio circuit. In this case, the remaining call associated data must be transmitted via another method to allow correlation of the audio circuit and the data circuit. There are many other options here however the important factor is the absolute accuracy of the audio content and the call-associated data.



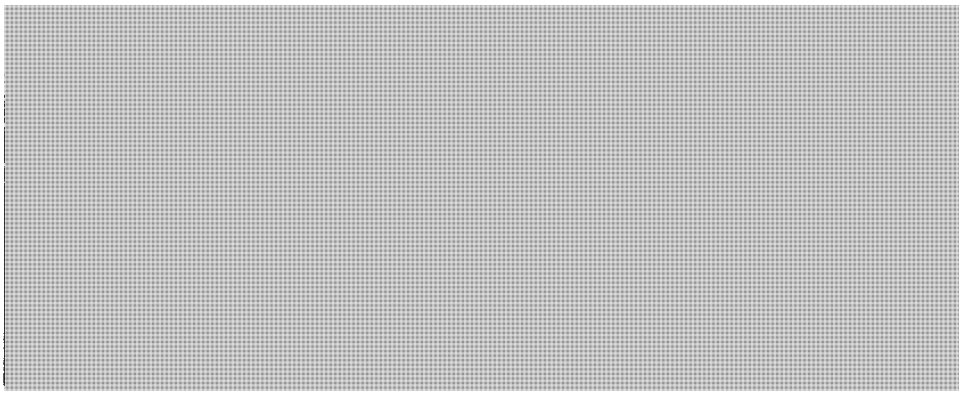
Standard 11: Law enforcement agencies require that the format for transmitting the intercepted communications to the monitoring facility be a generally available format.

Law enforcement requires that the format of the transmissions to law enforcement be standard industry accepted formats. Three different transmission types can be defined here –> in-band data, pure data, and pure audio. Examples of standard formats of each type are as follows but not limited to these examples: In-band data – DTMF, MF, FSK, etc.; Pure data – X.25, serial ASCII, etc.; Pure audio – digital formats, analog formats, etc. Additionally, how many audio paths are required per target to intercept the targets entire service provision. (i.e. Is it possible for the target to be simultaneously utilizing more than one audio path as in a call forward scenario with an inbound call being diverted and allowing outbound calls to be made from target handset.)



Standard 12: If network operators/service providers initiate encoding, compression or encryption of telecommunications traffic, law enforcement agencies require the network operators/service providers to provide intercepted communications en clair.

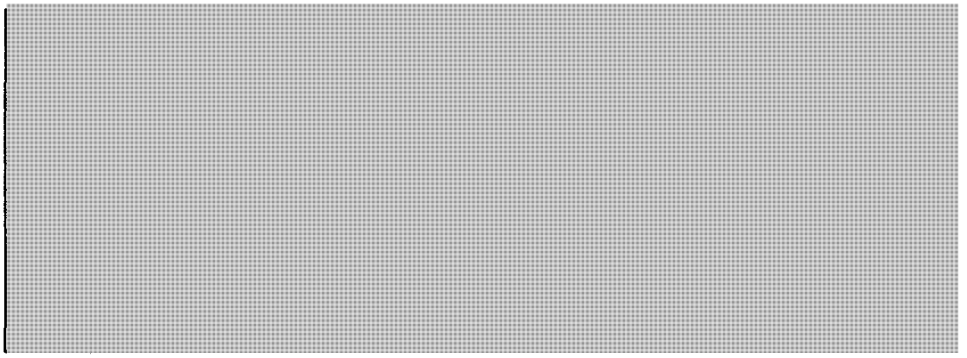
Law enforcement requires that any type of encryption algorithm that is initiated by the service provider must be provided to the law enforcement agency unencrypted. This would include proprietary compression algorithms that are employed in the network. This does not include end to end encryption that can be employed without the service provider's knowledge.



Standard 13: Law enforcement agencies require network operators/service providers to be able to transmit the intercepted communications to the law enforcement monitoring facility via fixed or switched connections.

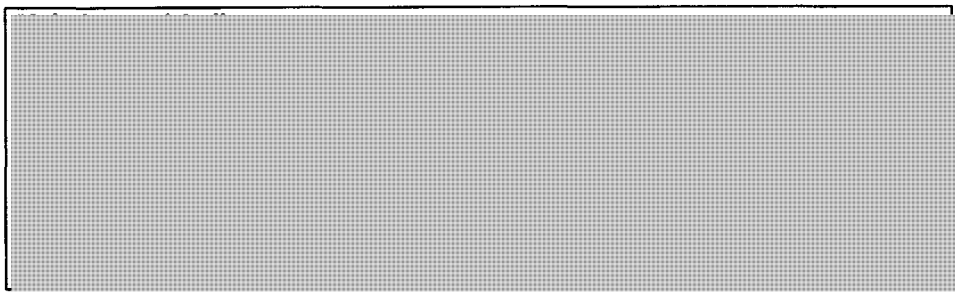
Law enforcement requires the ability to connect to the service providers over both switched (dial-up) and fixed (dedicated) lines at the same time. Different agencies may require different connectivity and therefore both these capabilities must be supported simultaneously. It should also be noted that the type of service connection to the agency

(i.e.: ISDN, T1 etc.) should be supported independently and also simultaneously. An additional concern to law enforcement is the location point of the intercept. A distributed intercept capability on a regional basis is more attractive than a centralized one. The reasoning for this is that lawful interception is done on a regional basis. If a centralized interception point was the only method to gain access to the network, the product would have to be transported back to the regional location.



Standard 14: Law enforcement agencies require that the transmission of the intercepted communications to the monitoring facility meet applicable Government of Canada security requirements.

Government security policies dictate how this must be achieved. The level of security for the RCMP and other Canadian law enforcement agencies will be met if the service providers can achieve the required level of security for CSIS. Copies of the relevant chapters of the Government Security Policy are available upon request.



Standard 15: Law enforcement agencies require interceptions to be implemented so that neither the interception target nor any other unauthorized person is aware of any changes made to fulfill the interception order. In particular, the operation of the target service must appear unchanged to the interception subject.

Law enforcement requires that the interception be conducted so as not to affect the target service in any way. Additionally, no unauthorized personnel are to be made aware of the interception.

[redacted]

Standard 16: Law enforcement agencies require the interception to be designed and implemented to preclude unauthorized or improper use and to safeguard the information related to the interception.

Law enforcement requires the service provider to detail the procedures and safeguards that are implemented to prevent improper use of information related to the interception. All internal security measures should be detailed to comply. This necessitates select individuals to be security cleared to the Top Secret level. Information regarding the security clearance process will be provided.

[redacted]

Standard 17: Law enforcement agencies require network operators/service providers to protect information on which and how many interceptions are being or have been performed, and not disclose information on how interceptions are carried out.

Law enforcement requires the service provider to detail the procedures and safeguards that are implemented to prevent improper use of information related to the interception. All internal security measures should be detailed to comply.

[redacted]

[redacted]

Standard 18: Law enforcement agencies require network operators/service providers to ensure that intercepted communications are only transmitted to the monitoring agency specified in the interception authorization.

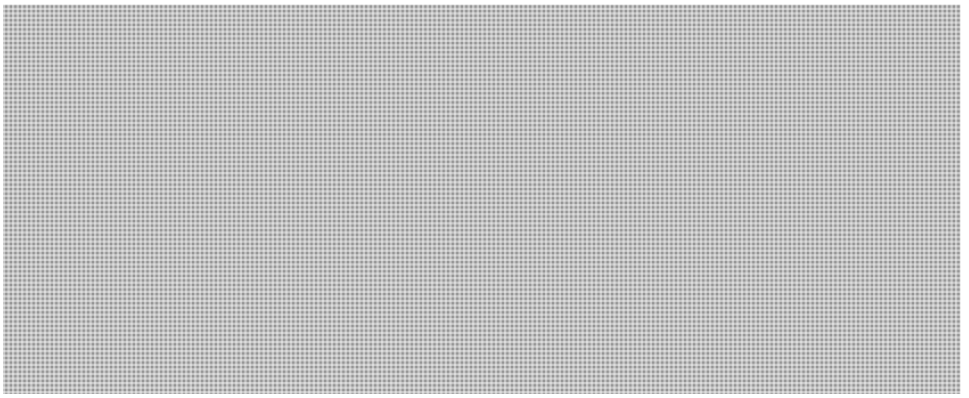
Law enforcement requires only those targets whom have been named by the specific agency and/or department be transmitted to that agency and/or department. By law, it is imperative that other agencies targets are not to be transmitted to any other agency unless specifically named by that agency. Note that different departments within the same agency should be considered as different agencies.

[redacted]

Standard 19: Based on a lawful inquiry and before implementation of the interception, law enforcement agencies require **(1)** the interception subject's identity service number or other distinctive identifier, **(2)** information on the services and features of the telecommunications system used by the interception subject and delivered by network operators/service providers, and **(3)** information on the technical parameters of the transmission to the law enforcement monitoring facility.

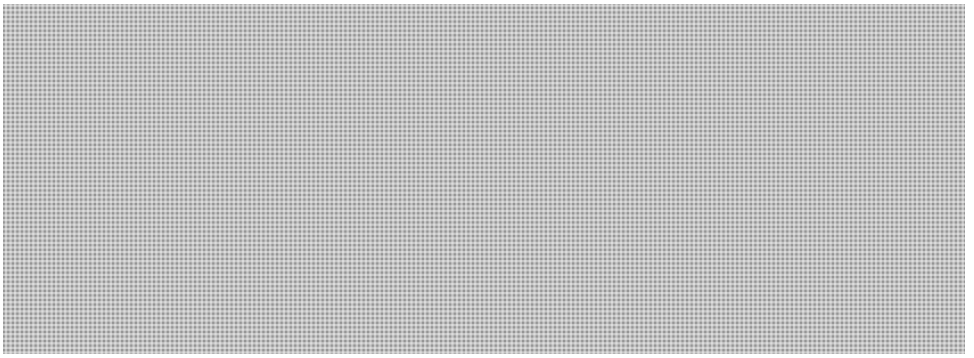
Law enforcement requires all pertinent information about the target in question in order to prepare and present the legal authorization document before the courts. This information would also include any services provided to the target such as voice mail, advanced calling features, roaming capability etc.

[redacted]



Standard 20: During the interception law enforcement agencies may require information and/or assistance from the network operators/service providers to ensure that the communications acquired at the interception interface are those communications associated with the target service.

Law enforcement will require the assistance of the service provider when beginning a lawful interception. This may entail the initial setup and testing of the targets intercepted communications to the law enforcement agency. It may also require the presence of the individual whom assisted law enforcement in a court appearance.

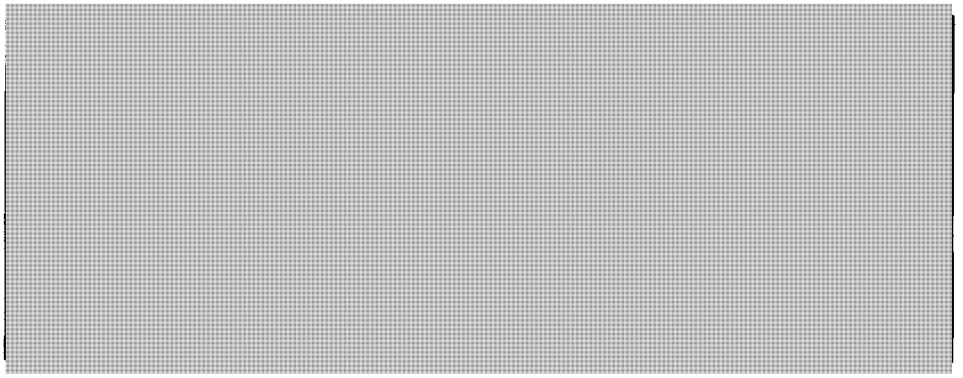


Standard 21: Law enforcement agencies require network operators/service providers to make provisions for implementing a number of simultaneous intercepts. Multiple interceptions may be required for a single target service to allow monitoring by more than one law enforcement agency. In this case, network operators/service providers should take precautions to safeguard the identities of the monitoring agencies and ensure the confidentiality of the investigations.

Law enforcement requires multiple intercepts to be simultaneously operating on an ongoing basis, which can be categorized in at least 3 ways:

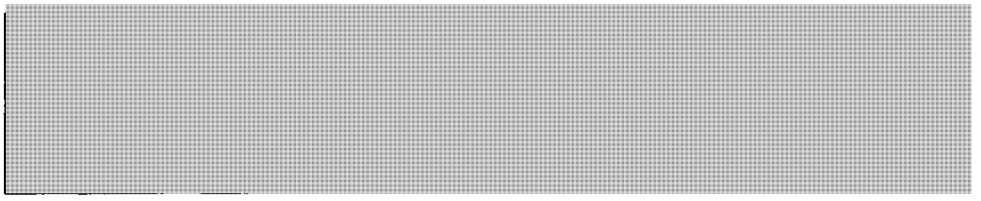
- ***Simultaneous targets*** *– implies a number of simultaneous targets that can be intercepted on a per switch basis. This maximum number is important to law enforcement.*
- ***Simultaneous multi-agency*** *– this implies the support of multiple agencies at one time with the possibility of multiple targets operating independently. The total number of agencies that can be supported is important to law enforcement.*
- ***Single target/multi-agency*** *– this implies the support of simultaneous agencies operating on the same target independently.*

In all cases outlined, law enforcement requires service providers to safeguard the identities of the monitoring agencies to all other agencies involved as well as ensure confidentiality of the separate investigations underway.



Standard 22: Law enforcement agencies require network operators/service providers to implement interceptions as quickly as possible (in urgent cases within a few hours or minutes). The response requirements of law enforcement agencies will vary by the type of target service to be intercepted.

Law enforcement requires various priorities of interception implementations to be carried out by the service providers most of which will have prior notification of 3 to 5 days. There are however emergency and priority situations which may require immediate response from the service provider. An example of this would be a hostage situation where time is of the essence.



[redacted]

Standard 23: For the duration of the interception, law enforcement agencies require that the reliability of the services supporting the interception at least equals the reliability of the target services provided to the interception subject. Law enforcement agencies require the quality of service of the intercepted transmissions forwarded to the monitoring facility to comply with the performance standards of the network operators/service providers.

Law enforcement would expect nothing more/less than the quality of service afforded to any other customer.

[redacted]

SECRET

DATE:

File No.: 6652 /

MEMORANDUM FOR THE DIRECTOR GENERAL

PUBLIC SAFETY CANADA'S ENGAGEMENT WITH TELECOMMUNICATIONS SERVICE PROVIDERS -700 MHZ SPECTRUM

(For decision)

ISSUE

To seek approval for Public Safety Canada (PS) to participate [redacted] for telecommunication service providers (TSPs) that recently acquired 700 MHz spectrum.

BACKGROUND

[redacted]

TSP engagement provides an opportunity to communicate to TSPs the technical requirements needed for lawful interception, including the *Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications* (SolGen Standards); [redacted]

PS, [redacted] engage with TSPs on numerous fronts. [redacted]

…/2

including warrant powers, and outlines how TSPs can provide technical assistance to conduct lawful interception.

Second, PS manages the lawful interception condition of licence with Industry Canada (IC).

The recent 700 MHz spectrum auction These licences will include a lawful interception condition for all voice services. The winners of 700 MHz spectrum (**ANNEX A**) will be required to build new networks in order to provide wireless services such as voice and data services on this spectrum band.

CONSIDERATIONS

The 700 MHz auction produced only one new entrant, Feenix Wireless, who won a licence in the North.

…/3

[redacted]

[redacted]

NEXT STEPS

[redacted]

[redacted] [ANNEX C].

RECOMMENDATION

[redacted]

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.

Lara Dyer

Prepared by: Shawn Plunkett

Pages 49 to / à 51

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 52

is withheld pursuant to section

est retenue en vertu de l'article

of the Access to Information

de la Loi sur l'accès à l'information

Public Safety Canada | Sécurité publique Canada

Ottawa, Canada
K1A 0P8

SECRET

DATE:

File No.: 6951-1 / 378807

MEMORANDUM FOR THE ASSISTANT DEPUTY MINISTER

PUBLIC SAFETY RESPONSE TO INDUSTRY CANADA'S CONSULTATION PAPER ON THE DESIGN OF THE 2500 MHz AUCTION

(Signature Required)

ISSUE

To provide information on the national security implications of a consultation document intended to inform the design of a forthcoming spectrum auction in the 2500 Megahertz (MHz) band.

BACKGROUND

Industry Canada (IC) has released a public consultation paper on a policy and technical framework to auction spectrum in the 2500 MHz band through a Gazette notice. Public responses to this consultation must be submitted before March 31, 2011.

[redacted]

CONSIDERATIONS

[redacted]

[redacted]

[redacted]

There is currently no legislative requirement for service providers to have intercept-capable equipment. As such, even after law enforcement or national security agencies acquire judicial authorization to intercept communications, the service providers may not have the technical ability to do so. Today, authorities work with service providers to [redacted]

[redacted]

Currently, companies applying for certain spectrum licences under the *Radiocommunications Act* must meet the *Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications* (SGES) as a condition of licence.

[redacted]

Therefore, in the absence of lawful access legislation, there is a need to modernize the language of the current interception clause and ensure its application as a condition of spectrum licences for the 2500 MHz band. PS will be consulting with IC separately on the language currently within the conditions of licence and its application as a condition for this and other spectrum bands.

RECOMMENDATION

It is recommended that you send the attached letter to Ms. Helen McDonald, Assistant Deputy Minister, Spectrum, Information Technologies and Telecommunications, Industry Canada.

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

Michael MacDonald

Enclosure: (1)

I approve:

_____

Lynda Clairmont

Prepared by: Julie Thompson

Public Safety Canada | Sécurité publique Canada
Assistant Deputy Minister | Sous-ministre adjoint
Ottawa, Canada
K1A 0P8

SECRET

Helen McDonald
Assistant Deputy Minister
Spectrum, Information Technologies and Telecommunications
Industry Canada
300 Slater Street
Ottawa, Ontario K1A 0C8

Dear Colleague:

I am writing to you regarding the national security concerns that Public Safety Canada (PS) has identified related to the upcoming auction of the 2500-2690 MHz band.

PS consulted its portfolio partners regarding the document entitled: "Decisions on a Band Plan for Broadband Radio Service and Consultation on a Policy and Technical Framework to Licence Spectrum in the Band 2500-2690 MHz", and [redacted] These concerns are similar to those raised in PS's public response to Industry Canada's (IC) 700 MHz consultation and in our classified correspondence of February 25, 2011.

[redacted]

In closing, I would like to reiterate our commitment to work with your department on preserving the integrity of telecommunications networks and maximizing Canada's competitiveness while addressing national security concerns.

.../2

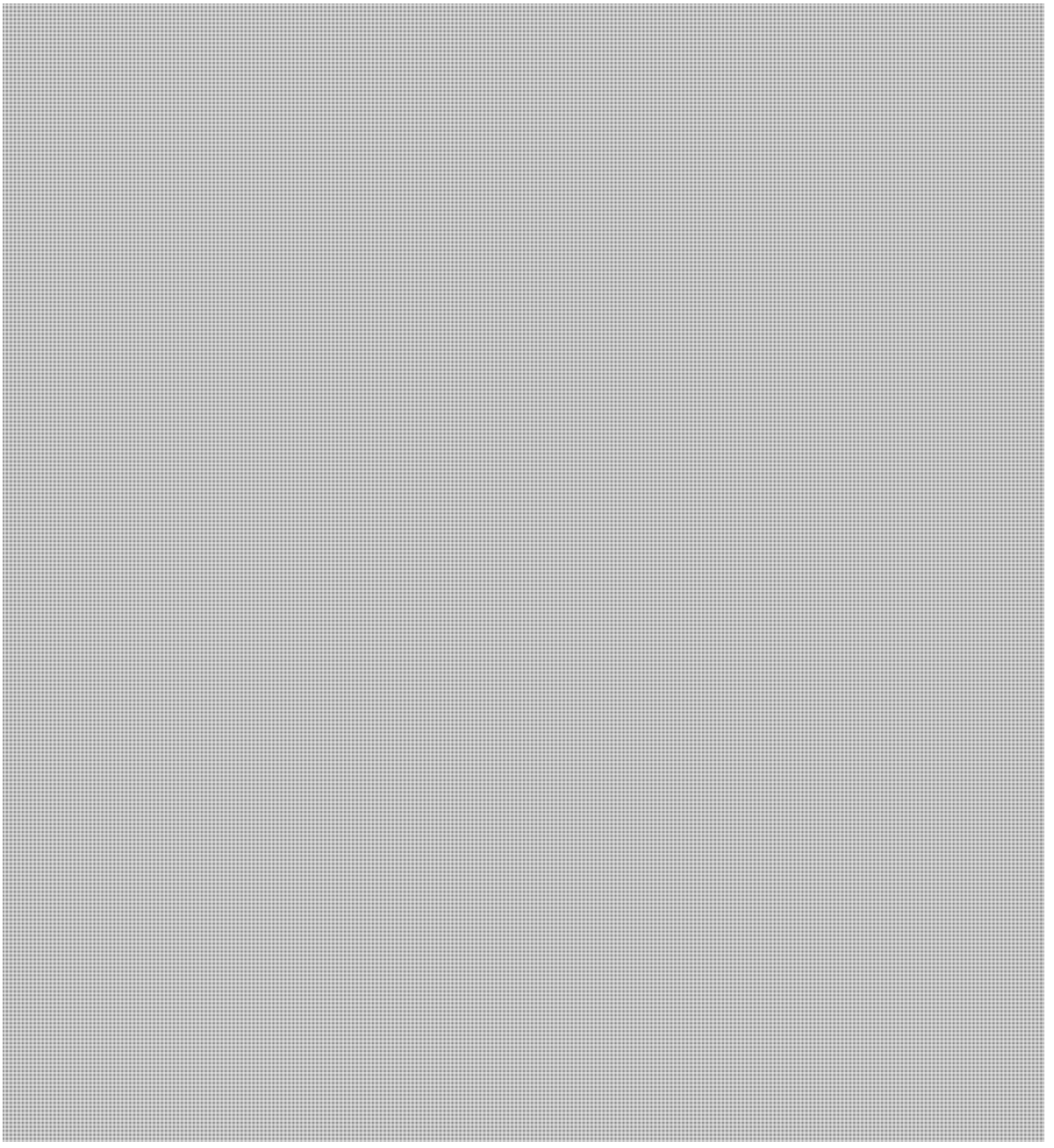
Canada

Should you require additional information, do not hesitate to contact me or Michael MacDonald, Director General, National Security Operations, at 613-993-4595.

Sincerely,

Lynda Clairmont
Assistant Deputy Minister
Emergency Management and National Security

Enclosure: (1)



As work continues on maximizing Canada's competitiveness, my officials will further develop options and will work with your officials to help ensure that any changes to the telecommunications market will be accompanied by necessary mitigation measures and

.../3

Public Safety Canada | Sécurité publique Canada

Assistant Deputy Minister | Sous-ministre adjoint

Ottawa, Canada
K1A 0P8

SECRET

FEV FEB 2 5 2011

Ms. Helen McDonald
Assistant Deputy Minister
Spectrum, Information Technologies and Telecommunications
Industry Canada
300 Slater Street
Ottawa, ON K1A 0C8

Dear Colleague:

Please find enclosed for your consideration a classified response from Public Safety Canada to Notice No. SMSE-018-10: Consultation on a Policy and Technical Framework for the 700 MHz Band and Aspects Related to Commercial Mobile Spectrum. This response is not for publication, but rather is meant to provide your Department with additional context, specifically on the national security concerns related to the 700 MHz auction. Public Safety Canada has also submitted an unclassified response to this consultation outlining the emergency management and national security perspective for publication on the Industry Canada website.

Public Safety Canada recognizes the economic advantages of a prosperous Canadian telecommunications industry and can support the intent of the consultation paper as well as some of the elements intended to foster competition and encourage innovation and the development of products and services that will ultimately offer more choices for Canadians. It is, however, important to fully appreciate the potential impacts that such changes could have on the integrity of Canada's telecommunications sector and ultimately national security.

[redacted] if this initiative were to move forward without the implementation of specific safeguards. These concerns are similar to those raised by Public Safety Canada [redacted] last summer. I have enclosed a copy of the submission we provided to your department for reference as it offers additional detail and potential mitigation strategies to address some of the risks identified below.

.../2

Canada

safeguards. These measures will help preserve the integrity of telecommunications networks, which is critical for the economic wellbeing of Canada and for the prosperity of Canadian industry.

In addition [redacted] we also have concerns related to the conditions of licenses to be issued through this spectrum auction. My officials have identified a need to modernize the language of the current interception requirement clause and ensure its application as a condition of spectrum licenses for the 700 MHz band. As you are aware, currently companies applying for a spectrum license under the *Radiocommunications Act* must meet the *Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications* (SGES) as a condition of license. [redacted]

The 'Next Steps' section of the spectrum consultation document indicates that IC will be consulting on the licensing framework and conditions of license at a future date. [redacted]

Despite the above noted concerns, I want to stress that Public Safety Canada's perspective is not in opposition to the 700 MHz auction. Rather, we want to ensure that the public safety perspective is communicated and incorporated into the consultation process and that appropriate measures are established to protect this vital sector and those who rely on it.

Should you require additional information, please do not hesitate to contact me at 613-990-2743 or Michael MacDonald, Director General National Security Operations at 613-993-4595.

Sincerely,

Daniel Lavoie

Enclosure: (1)

Pages 61 to / à 66

are not relevant

sont non pertinentes

UNCLASSIFIED

December 21, 2012

File No.: NS 6652-O3
RDIMS No.: 745598

MEMORANDUM FOR THE DIRECTOR - ITTP

SECURING INDUSTRY CANADA'S COOPERATION TO ENHANCE THE FORBEARANCE PROGRAM

(For Approval)

ISSUE

To secure Industry Canada's (IC) support to approach Telecommunications Service Providers (TSPs) to determine whether or not they comply with the *Solicitor General Enforcement Standards for Lawful Interception of Telecommunications* (SGES), part of their lawful interception condition of licence (LIC).

BACKGROUND

Presently, there are very few companies with confirmed forbearance, yet there are approximately 150 companies with a valid LIC.

To address this issue, Investigative Technologies and Telecommunications Policy (ITTP) has developed a strategy for enhancing the LIC program to ensure licensees, have lawful interception capabilities.

On November 21, 2012, Public Safety Canada (PS) presented to Portfolio members an overview of this strategy as well as new tools to strengthen the management of the forbearance regime. It was noted during the meeting that such an endeavour would likely increase the resources required to operate the forbearance program. It was also noted that PS would need to engage IC to determine if and how this could be done as IC is responsible for monitoring compliance with the spectrum licence condition. There is some ambiguity, however, regarding IC's role with respect to the SGES.

PROPOSAL TO ENGAGE IC

IC would remain informed during the whole process and can also determine their own level of involvement. The first step of this engagement will be to schedule a meeting between relevant directors/managers at IC and ITTP. The attached one-pager (**ANNEX A**)

CONSIDERATIONS

The proposed approach will require considerable buy-in and likely some resources from IC. It will also likely increase the regulatory and reporting burden for both licence holders and IC. To attempt to mitigate this concern, PS will develop options that ensure that the resource and reporting burden on TSPs and IC will remain low.

It will also be important to ensure the proper choreography of our approach to IC. As IC is still deliberating on decisions related to the lawful interception condition of licence as part of the 700 MHz auction

NEXT STEPS

We are seeking your approval for the following:

- Approve the above approach to IC;
- Agree to meet with relevant directors/managers at IC (David Busquets, wireless and Shari Scott, Richard Hiebert – Satellite)
- Agree to table-drop the attached paper for discussion

ANNEX A

Objective: To ensure that all Telecommunication Service Providers (TSPs) with a Lawful Interception Condition of Licence in their radio or spectrum licence have and maintain lawful interception capabilities.

Rationale: At present, the forbearance program is a responsive program that only engages with companies that pro-actively approach Industry Canada (IC) to request forbearance. [redacted] While we note that licence holders must state in their annual report compliance with their conditions of licence, there is no mechanism to ensure compliance with the *Solicitor General Enforcement Standards for Lawful Interception of Telecommunications* (SGES). [redacted] identify areas where the Public Safety Portfolio can assist TSPs in complying with their lawful interception condition of licence. [redacted]

Proposal: Public Safety Canada (PS) is seeking IC's consent to develop a collaborative proposal to determine compliance with the lawful interception condition of licence and to assist TSPs to comply with this condition.

Options: PS has developed several options for assessing compliance with the SGES:

[redacted]

For all these options, a capacity analysis will need to be undertaken to ensure that there is sufficient resources to accept these responsibilities. Care will also be taken to minimize the reporting burden on licence holders to the greatest extent possible.

We look forward to discussing these proposals with you.

SECRET with attachments

September 24, 2012

File No.:
RDIMS No.: PS-SP-#690086

MEMORANDUM FOR THE DIRECTOR - ITTP

ENHANCEMENTS TO THE MANAGEMENT OF THE LAWFUL INTERCEPTION CONDITION OF LICENCE PROGRAM

(For Approval)

ISSUE

To provide an update on the current Lawful Interception Condition of Licence (LIC) program and to seek your approval on a strategy to enhance its management.

BACKGROUND

Presently, there are over 200 companies with spectrum or radio licences operating in Canada. Investigative Technologies and Telecommunications Policy (ITTP) has developed a strategy for enhancing the LIC program to ensure licensees, are compliant. It also aims to ensure that if they are not compliant, they are monitored through a rigorous forbearance process. The general outline of the strategy has been presented to the Senior Assistant Deputy Minister and received positive feedback (**TAB A**).

STRATEGY FOR ENHANCING THE LAWFUL INTERCEPTION REGIME

Over the past year, ITTP has undertaken a review of the management of the LIC program and has developed a strategy to maximize existing interception capabilities. The objective of the strategy is to bolster the lawful interception regime by: enhancing compliance with the LIC; improving the forbearance program; reviewing the forbearance procedures; and construct a risk-based approach to forbearance.

...2

[redacted]

However, as it is IC who is responsible for compliance with the LIC, their approval and cooperation is essential. ITTP will outline the steps involved in consulting both the Portfolio and IC [redacted]

[redacted]

Tools to Support the Strategy

To support the implementation of this strategy, the forbearance regime has been reinforced with stronger reporting tools and an improved tracking system. The following tools have been developed or revised:

A Forbearance Quarterly Report, addressed to the Director General – National Security Operations, has been implemented to allow for stronger management of the forbearance regime by: regularizing reporting on forbearance requests; providing a tool for comparison and analysis across the different requests; and offering an audit trail for future work on the file (**TAB C**). The report highlights the status of forbearance request and any other issues related to the forbearance regime.

The existing forbearance tracking report has been updated to include specifics relating to the nature of the request (**TAB D**). This improvement allows for a more robust tracking system and includes greater details on the particular standards requiring forbearance.

[redacted]

...3

[redacted]

CONSIDERATIONS

Until the passage and full implementation of the lawful access legislation, the LIC is the primary instrument that holds Telecommunication Service Provider (TSPs) with this condition, accountable to maintain lawful intercept equipment. [redacted]

[redacted]

NEXT STEPS

We seek your approval to begin to implement the strategy for enhancing the current lawful interception regime. It is recognized that this is an iterative process and that further LIC program enhancements will be sought. [redacted]

Should you require additional information, please do not hesitate to contact me.

Enclosures: 7

Prepared by: Julie Thompson

Public Safety Canada | Sécurité publique Canada

SECRET

Subject to ATI exemption 21(1)(a,b)

BUILDING A SAFE AND RESILIENT CANADA

Strategy for Enhancing the Lawful Interception Condition Forbearance Program:

SGES Compliance

May 2013

Canada

Overview

- Strengthen the forbearance program along
-
-

Rationale

- Problem Definition:

Opportunity

- 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

  -
  -
  -
  -

Engaging Licence Holders

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

- With a view to strengthening compliance with the SGES, PS discussed potential approaches with IC

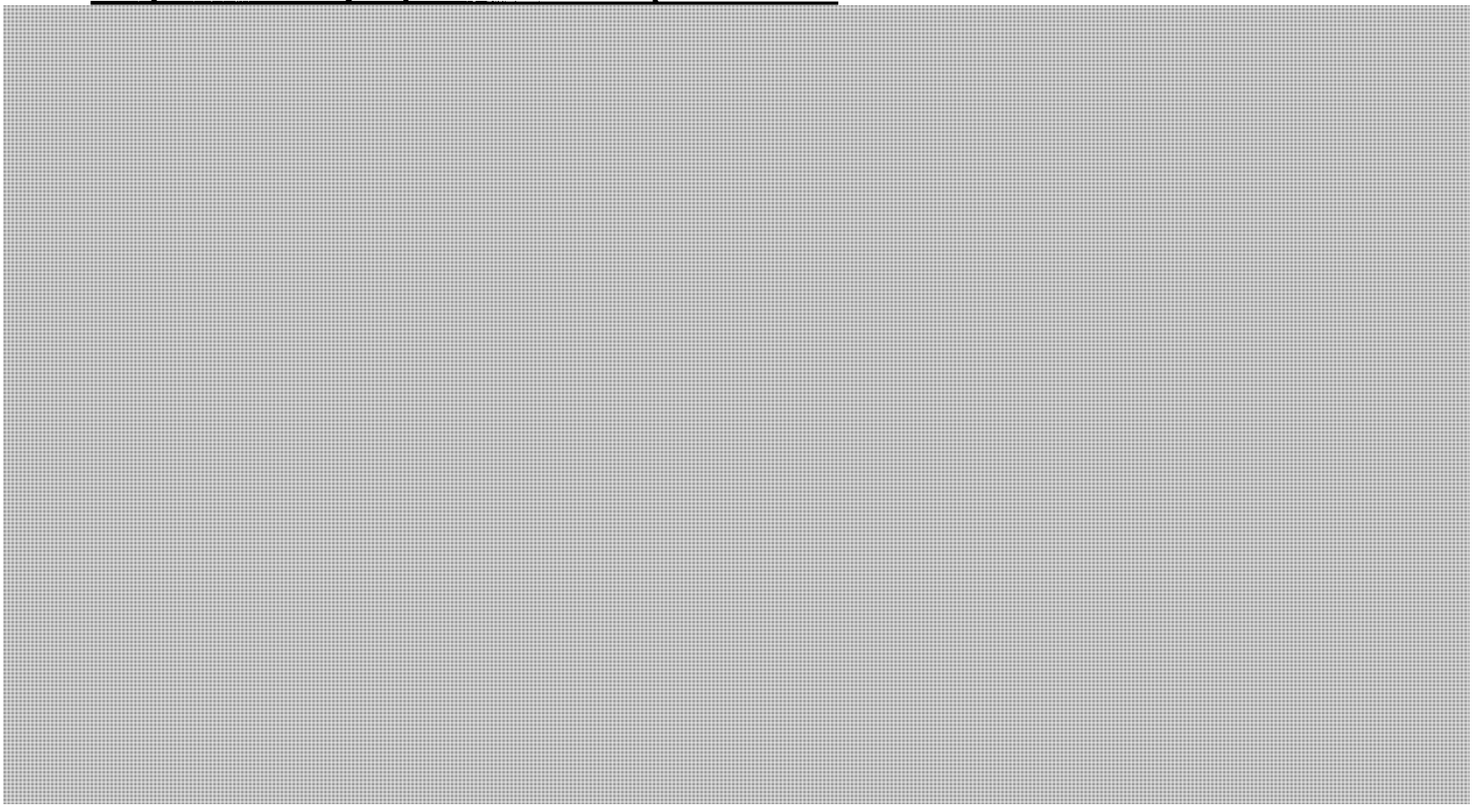
- The preferred approach that emerged involves:
  - [redacted]
  -
  -
  -

Proposed Approach

- We are proposing a 4 step approach:
  - 1)
  - 2)
  - 3)
  - 4)

Operational Requirements

- **Step 1 – Clarify Operational Requirements**



Risk Assessment

- **Step 2 – Undertake a Risk Assessment**
- [redacted]

Engagement

- **Step 3 – Pro Actively Engage Licence Holders**
- [redacted]

Program Management

- **Step 4 – Program Management - Assessment, Monitoring, Reporting**
- *Objective*: The forbearance program is managed in an effective and efficient manner
- [redacted]

Timelines

- Step 1 – Operational Requirements
  - [redacted]
  - [redacted]
- Step 2 – Risk Assessment
  - [redacted]
  - [redacted]
- Step 3 – Engagement
  - [redacted]
  - [redacted]
- Step 4 – Program Management
  - [redacted]
  - [redacted]

Resource Impacts

-
-
-

Draft Business Process

Page 86

is a duplicate

est un duplicata

Benefits

- Short term investments in outlining operational requirements, [redacted] and program management will reap benefits

- A stronger, more structured program will lead to resource savings:
  - [redacted]

Work plan

Forbearance Strengthening

Questions?

Pages 90 to / à 96

are not relevant

sont non pertinentes

Public Safety Canada / Sécurité publique Canada

SECRET

DATE:

File No.: NS 6652-O3 /
RDIMS No.: Dragon 22184

MEMORANDUM FOR THE DIRECTOR GENERAL

OPTIONS FOR THE LAWFUL INTERCEPTION CONDITION OF LICENCE FORBEARANCE PROGRAM

(For decision)

ISSUE

To seek a decision on the lawful interception condition of licence forbearance program.

BACKGROUND

At present, the lawful interception condition of licence is the only regulatory instrument to compel telecommunications service providers (TSPs) to have and maintain lawful interception capabilities on their wireless voice networks.

Part of the condition of licence is that the Minister of Industry, who is responsible for licensing wireless spectrum, can grant a TSP forbearance from complying from all or part of the lawful interception requirements for a limited time, should the Minister, in consultation with Public Safety Canada, be of the opinion that the requirement is not reasonably achievable. Essentially, the forbearance clause allows TSPs to continue to provide services while working to comply with all or part their condition of licence.

As such, it is unclear as to the level of compliance of the other TSPs with an applicable lawful interception condition of licence.

CONSIDERATIONS

Canada

.../2

. The current public environment surrounding law enforcement and national security agencies relationships with TSPs, as well as the call for greater transparency from a series of Parliamentarians, the media, TSPs themselves and academics, leads to a decision point regarding the forbearance program. There are three potential options for moving forward with the forbearance program:

Option 1 –

Option 2 –

[redacted]

Option 3 – [redacted]

[redacted]

RECOMMENDATION

Should you require additional information, please do not hesitate to contact me at 613-949-3181.

Lara Dyer
A/Director, National Security Technology
National Security Operations

Prepared by:

(377254)

SECRET

DATE:

File No. :

MEMORANDUM FOR THE DEPUTY MINISTER

SOLICITOR GENERAL ENFORCEMENT STANDARDS AND CONDITIONS OF LICENSING

(Decision sought)

ISSUE

To provide an overview of current interception challenges resulting from outdated language in the lawful interception condition of spectrum licences and to request that you forward a letter to your counterpart at Industry Canada (IC) outlining these concerns.

BACKGROUND

To help ensure that lawful intercept capabilities for law enforcement and national security agencies are available, a condition of licensing requiring that licensees of circuit-switched systems meet the *Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications* (SGES) (**TAB A**) is included for spectrum licensed under the *Radiocommunications Act*. IC is responsible for issuing these licences. The SGES are dated and do not have the force of law. However, until Bill C-52, the *Investigating and Preventing Criminal Electronic Communications Act* comes into force, the SGES remain law enforcement and national security agencies' only leverage to compel Telecommunication Service Providers (TSPs) to provide an interception capability.

[redacted]

CONSIDERATIONS

The first concern lies with the use of the term "circuit-switched" as it refers to dated technology that was used at the time the clause was being negotiated. Since that time, most companies have, or are in the process of, decommissioning these types of switches as they deploy newer technologies. As such, linking interception requirements to an outdated technology is rendering the licence condition obsolete.

Second, the condition only applies to Personal Communications Services licences, which includes higher frequency spectrum above the 1900 MHz range. Therefore, the condition does not apply to all spectrum required for intercept purposes (e.g. cellular licences).

[redacted]

CURRENT STATUS

Over the last two months, Public Safety (PS) officials had engaged IC to address these licence concerns, ideally before March 31st, as 219 cellular frequency licences are up for renewal on that date. PS suggested that the term "circuit-switched" and the caveat that the Lawful Interception condition applies only to PCS licences be removed. These amendments would modernize the framework, allow for a broader application of interception requirements and satisfy the Department, [redacted]

IC was open to recommending this approach to senior management. However, PS officials were informed on January 21, 2011 that IC would be unable to implement the changes for the licence renewals in the short term as extensive consultations would have to occur prior to such changes.

[redacted] IC is currently designing two spectrum auctions to take place in 2012 that will allocate additional spectrum to new and existing market players (700 MHz band and 2500 MHz band). IC officials indicated that their recommendation to senior management would be to include both of PS' suggested revisions in these new licences. However, any amendments to the conditions of license are under the purview of the Minister of Industry and ultimately require consultation with licensees. IC has posted a consultation paper for the 700 MHz auction on its website and PS is preparing a response that will include amending the Lawful Interception condition of license and a request to include these proposed changes in future consultation papers for both forthcoming spectrum auctions to ensure that potential licensees have an opportunity to comment on these proposed changes.

[redacted] As such, enclosed is a letter for your review and signature to your counterpart at IC requesting that officials

from both departments work together to put these amendments in place as soon as possible (**TAB B**).

RECOMMENDATION

[redacted] it is recommended that you forward the enclosed letter to your counterpart at IC.

Should you require additional information, please do not hesitate to contact me or Mr. Michael MacDonald, Director General National Security Operations Directorate at 613-993-4595.

Lynda Clairmont

Enclosures: (2)

I agree:

_____
William V. Baker

SECRET

DATE:

File No.: NS 6652 / 395256
RDIMS No.: DRAGON 10481

MEMORANDUM FOR THE DIRECTOR GENERAL

PRIMER ON THE SOLICITOR GENERAL'S ENFORCEMENT STANDARDS FOR LAWFUL INTERCEPTION OF TELECOMMUNICATIONS

(Information only)

ISSUE

To provide background information and considerations related to the Solicitor General's Enforcement Standards for lawful interception of telecommunications (SGES).

BACKGROUND

Following the passage of the *Communication Assistance for Law Enforcement Act* (CALEA) in the United States in 1994, officials from Industry Canada (IC), the Royal Canadian Mounted Police (RCMP), the Canadian Security Intelligence Service (CSIS) and the then Department of the Solicitor General decided that a condition of spectrum licence, under the authority of the Minister of Industry, would be an effective means to compel telecommunication service providers (TSPs) to have and maintain some lawful interception capabilities. These officials came to agree on including a lawful interception condition of licence as part of the Personal Communications Systems (PCS) spectrum licences. This condition required TSPs using "circuit switched voice telephony" systems to have and maintain lawful interception capabilities, and noted that the requirements for lawful interception in Canada are provided for in the SGES, version 1995 (**ANNEX A**).

The SGES are not technically standards, as this term is reserved for specific technical standards set by standards bodies. Rather the SGES outline the high level requirements that TSPs must meet with regard to lawful interception capabilities. The SGES do not provide detailed engineering specifications. As such, TSPs have flexibility to develop their own solutions in order to meet the requirements.

The 23 'standards' that make up the SGES can be divided into two broad categories: engineering requirements and operational protocols (**ANNEX B**). The engineering requirements cover such issues as what content and call associated data are to be provided, how the information should be delivered to authorized agencies, as well as the decryption of communications (where the TSP applies the encryption). The operational protocols outline the requirements for the non-technical components of the lawful interception process, such as target identifiers, and the quality and security of service.

As communications began to migrate from voice calls to other electronic forms of communications, explanatory annotations for each of the standards were added to address these emerging forms of communication and to provide additional clarity on the requirements (**ANNEX C**).

The SGES are based on a document entitled: "International User Requirements for Electronic Surveillance" (IUR), which outlines internationally recognized requirements to conduct the lawful interception of communications. The IURs were developed

was successful in having the IURs tabled in the European Parliament in 1995 as part of a resolution regarding lawful interception requirements for member states. In Canada, the IURs were modified slightly to become the SGES. The 1995 version of the SGES was first included in the lawful interception condition on PCS licences. The 1995 version continues to be applied to spectrum licences, including the upcoming 700 MHz licences.

CONSIDERATIONS

While the SGES continue to be useful in outlining agencies' high level lawful interception requirements, some challenges remain. Despite being fairly broad in scope, the SGES are limited by the language of the condition of licence, which refers to outdated technology (except for the upcoming 700 MHz licences) and specific services

In addition, the actual wording of the lawful interception condition of licence is not consistent across all spectrum licences. For example, some spectrum licences refer to the 1995 SGES version, while others refer only to the SGES. Furthermore, IC officials have indicated that should amendments to the SGES be required, a public consultation would need to be held before they could apply these SGES to the condition of licence.

PS is leading a working group to review the SGES and clarify requirements for each standard, as well as to ensure there is only one official version circulated to licence holders. The SGES

.../3

working group will develop a common understanding and interpretation of each standard as well as identify gaps in interception requirements. This is being done with a view towards ensuring that law enforcement and national security agencies are receiving the maximum capabilities under the existing regulations.

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

ANNEX B

SGES Engineering Requirements

The engineering requirements of the SGES can be grouped into five subcategories: content and call associated data, service data, location data, encryption, and handover interface requirements.

Content and Call Associated Data (standards 1, 2, 5, and 8)
These standards require TSPs to provide telecommunications content in real time, as well as the provision of call associated information such as the origin, direction, destination, duration, or termination of the telecommunication, and whether the telecommunication was sent or received successfully.

Service Data (standards 3 and 7)
The SGES require TSPs to provide a list of all services and features associated with an interception subject. They further establish requirements in cases involving multiple call forwarding/call diverting for different systems.

Location Data (standard 6)
The SGES require information on the most accurate geographical location of targets.

Handover Interface Requirements (standards 9, 10, 11, 13 and 21)
These standards provide technical specifications regarding how the intercepted communications will be processed and delivered from the TSPs to the law enforcement or national security agencies. They also specify delivery methods for different telecommunications content and ensuring that there is a means to correlate this information.

Encryption (standard 12)
This standard required TSPs to provide telecommunication traffic to authorized agencies 'en clair' (i.e., without encryption, compression or encoding).

SGES Operational Protocols

The second category of requirements is the operational protocols, which can be grouped into four subcategories: identifiers, quality of service, security, and scope warrant. These standards are more general and less technical

Identifiers (standards 19)
The SGES stipulate the types of user identifiers and technical parameters that TSPs must provide based on a lawful inquiry

Security (standards 14, 16 and 17)
These standards require that the transmission of the intercepted telecommunications to the monitoring facility meet applicable Government of Canada security. They also require that the interception be designed and implemented to preclude unauthorized or improper use and to safeguard the information related to the interception. They further require TSPs to detail implemented procedures and safeguards to prevent improper use of information related to the interception.

Quality of Service (standards 15, 22 and 23)
The SGES require that the interception be undetectable to the interception subject and other unauthorized persons. It also requires that interceptions are implemented as quickly as possible and that the quality of service for law enforcement and national security agencies is equal to the quality of service for customers.

Scope of Warrant (standards 4, 18 and 20)
The SGES require that telecommunications to and from a target's TSP be within the scope of the authorization and be provided only to the authorized agency as specified in the interception authorization.

Page 108

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 109

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 110 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

Pages 117 to / à 124

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 125 to / à 126

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 127

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 128

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 129 to / à 130

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 131 to / à 132

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

DRAFT (July 2013)

TERMS OF REFERENCE

SOLICITOR GENERAL'S ENFORCEMENT STANDARDS FOR LAWFUL INTERCEPTION OF TELECOMMUNICATIONS WORKING GROUP

PURPOSE

The Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications Working Group (WG) was established at the May 8, 2013 meeting of the Forbearance WG.

The SGES WG's purpose is to review the SGES with a view to developing a common and consistent understanding of requirements, and to identify any potential gaps in the regulatory framework regarding interception requirements.

SGES WORKING GROUP STRUCTURE

The SGES WG meetings will be chaired by the Investigative Technologies and Telecommunications Policy division at Public Safety Canada (PS) and will include representatives [redacted] The SGES WG work will be conducted through meetings, teleconferences and email exchanges.

The discussions will be scheduled on an as-required basis and will begin in summer 2013 until the end of 2013 (prior to the 700 MHz spectrum auction in January 2014). Following this date, any issues related to the SGES can be brought forward through the Forbearance WG.

OBJECTIVES

The objectives of the SGES WG are as follows:

1- Develop a common understanding and interpretation of each standard.
2- Identify gaps in SGES requirements and capabilities.
3- Formalize the SGES document and create guidelines for its distribution to relevant stakeholders.

Pages 134 to / à 135

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

Department of Justice Canada
Ministère de la Justice Canada

Public Safety and Emergency Preparedness Canada
269 Laurier Avenue West, 16th Floor
Ottawa, Ontario
K1A 0P8

Sécurité publique et Protection civile Canada
269, avenue Laurier Ouest, 16e étage
Ottawa (Ontario)
K1A 0P8

Security classification -- Côte de sécurité
Solicitor-Client privilege | Secret professionnel de l'avocat
Protected B
File number -- Numéro de dossier
10037-2
Date
June 25, 2012
Telephone / FAX – Téléphone / Télécopieur
613-991-4364

MEMORANDUM / NOTE DE SERVICE

TO / DEST: Shawn Plunkett
Senior Policy Advisor
Investigative Technologies and Telecommunications Policy (ITTP)
National Security Operations

FROM / ORIG: Claude Pilon
Counsel
Public Safety Legal Services

SUBJECT / OBJET:

Comments/Remarques

Pages 137 to / à 140

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

Paragraph for DM transition deck – April 25, 2012

Telecommunications Security

The telecommunications sector is of considerable strategic importance to Canada. While this sector is a strong engine for economic growth, it is also vulnerable to a disparate number of threats to national security and poses challenges to law enforcement investigations. These threats and challenges are multi-faceted as telecommunications are not only a potential target of criminal activity; they are also a vehicle for perpetuating malicious acts.

The Canadian telecommunications industry has undergone considerable and rapid change in recent years. As this sector continues to develop, including through the introduction of new communication technologies, the removal of foreign investment restrictions for telecommunications companies in Canada and the increase in foreign provided equipment and services, it will be important to implement sufficient security measures to mitigate against potential threats to national security, such as cyber attacks, disruptions to critical infrastructure and espionage, among others.

To this end, Public Safety Canada (PS) is working with Portfolio agencies and the Security and Intelligence (S&I) Community to develop measures to protect and secure a prosperous and innovative telecommunications sector in Canada. PS is working to coordinate a comprehensive Public Safety Portfolio position on the issue of telecommunications security. This will assist in aligning and prioritizing our security concerns within the telecommunications sector and assist in developing appropriate mitigation measures. In addition, PS and IC are working together to ensure that law enforcement and national security agencies have lawful interception capabilities, prior to the passage and implementation of Lawful Access legislation, through IC's telecommunications licencing regime.

Page 142

is not relevant

est non pertinente

CONFIDENTIAL (When completed)

SOLICITOR GENERAL'S ENFORCEMENT STANDARDS FOR LAWFUL INTERCEPTION OF TELECOMMUNICATIONS
EXISTING VERSUS IDEAL REQUIREMENTS

STANDARD	SHORT NAME (STANDARDS)	CAPABILITIES (WHAT INFORMATION DO WE PRESENTLY RECEIVE FROM TSPs)	GAPS (WHAT INFORMATION DO WE NOT RECEIVE)	OPTIONS FOR ADDRESSING GAPS
1	Access to telecommunications			
2	Roaming			
3	Access to call features			
4	Isolation of target telecommunication			
5	Call-associated data			
5A	*Access ready status*			
5B	*Outgoing connections*			
5C	*Incoming connections*			
5D	*Digits dialed*			
5E	*Beginning, end, duration*			
5F	*Destination, diversions*			
6	Geographical location			
7	Target's services, technical parameters			
8	Real-time, full-time monitoring capability (and call-associated data)			
9	Handover interfaces			
10	Accurate correlation			
11	Handover format			
12	Encoding, encryption, compression			
13	Handover connections			
14	GoC security requirements			

SOLICITOR GENERAL'S ENFORCEMENT STANDARDS FOR LAWFUL INTERCEPTION OF TELECOMMUNICATIONS
EXISTING VERSUS IDEAL REQUIREMENTS

15	No target awareness			
16	No unauthorized or improper use			
17	Protection of intercept information/process			
18	Transmission to Authorized agency			
19	Subscriber Information			
19 (1)	Subscriber Identification Number			
19 (2)	Subscriber Services			
19 (3)	Technical Parameters (Subscriber Services)			
20	Assistance with interception (testing and follow-up)			
21	Simultaneous Intercepts			
22	Response Time			
23	Quality of Service			

SECRET

Helen McDonald
Assistant Deputy Minister
Industry Canada
Spectrum, Information Technologies and Telecommunications
300 Slater Street
Ottawa, Ontario K1A 0C8

Dear Colleague:

Please find enclosed for your consideration a classified response from Public Safety Canada to Notice No. SMSE-018-10: Consultation on a Policy and Technical Framework for the 700 MHz Band and Aspects Related to Commercial Mobile Spectrum. Public Safety Canada has also submitted an unclassified response to this consultation outlining the emergency management and national security perspective for publication on the Industry Canada website. This version is not for publication but rather is meant to provide your Department with additional context specifically on the national security concerns related to the 700 MHz auction.

Public Safety Canada recognizes the economic advantages of a prosperous Canadian telecommunications industry and can support the intent of the consultation paper as well as some of the elements intended to foster more competition, and, encourage innovation and the development of products and services that will ultimately offer more choices for Canadians. It is, however, important to fully appreciate the potential impacts that such changes could have on the integrity of Canada's telecommunications sector and ultimately national security.

Several proposed elements of the spectrum auction raise national security concerns if this initiative were to move forward without the implementation of specific safeguards. These concerns are similar to those raised by Public Safety Canada [redacted] last summer. I have enclosed a copy of the submission we provided to your department for reference as it offers additional detail and potential mitigation strategies to address some of the risks identified below.

[redacted]

.../2

[redacted]

As work continues on maximizing Canada's competitiveness, my officials will further develop options and will work with your officials to help ensure that any changes to the telecommunications market will be accompanied by necessary mitigation measures and safeguards. These measures will help preserve the integrity of telecommunications networks, which is critical for the economic wellbeing of Canada and for the prosperity of Canadian industry.

In addition to the national security implications, we also have concerns related to the conditions of licenses to be issued through this spectrum auction. My officials have identified a need to modernize the language of the current interception requirement clause and ensure its application as a condition of spectrum licenses for the 700 MHz band. As you are aware, currently companies applying for a spectrum license under the *Radiocommunications Act* must meet the *Solicitor General's Enforcement Standards for Lawful Interception of Telecommunications* (SGES) as a condition of license. [redacted]

[redacted]

.../3

The 'Next Steps' section of the spectrum consultation document indicates that IC will be consulting on the licensing framework and conditions of license at a future date.

Despite the above noted concerns, I want to stress that Public Safety Canada's perspective is not in opposition to the 700 MHz auction. Rather, we want to ensure that the public safety perspective is communicated and incorporated into the consultation process and that appropriate measures are established to protect this vital sector and those who rely on it.

Should you require additional information, do not hesitate to contact me or Michael MacDonald, Director General National Security Operations at 613-993-4595.

Sincerely,

Daniel Lavoie
Associate Assistant Deputy Minister

Page 148

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