



2017

Réseau à large bande de
sécurité publique

Demande de renseignements

Table des matières

Définitions clés.....	2
1. INTRODUCTION.....	3
1.1. Qu'est-ce qu'un RL BSP?.....	3
1.2. Activités récemment entreprises au Canada concernant le RL BSP.....	3
1.3. Objectif de la demande de renseignements (DDR).....	4
1.4. Contexte opérationnel actuel.....	4
1.5. Approches internationales.....	5
2. LIGNES DIRECTRICES.....	7
2.1. Nature de la demande de renseignements (DDR).....	7
2.2. Nature et traitement des réponses attendues.....	7
2.2.1. Coût de réponses.....	7
2.2.2. Traitement des réponses.....	7
2.3. Contenu de la présente DDR.....	8
2.4. Format des réponses.....	8
2.5. Demandes de renseignements.....	8
2.6. Présentation des réponses.....	8
3. QUESTIONNAIRE.....	10
3.1. Un modèle d'affaires viable.....	10
3.2. Modèle de gouvernance.....	11
3.3. Écosystème d'applications, de services et de dispositifs.....	12
Documents de référence.....	13

Définitions clés

Modèle d'affaires	Approche consistant à bâtir, exploiter et entretenir un réseau à large bande de sécurité publique (RLBSP) qui est abordable et durable et qui répond aux objectifs changeants ayant trait à la sécurité publique.
Disponibilité de communication	La disponibilité de communication se définit par plusieurs facteurs tels que les droits de priorité et de préemption, la durée d'établissement de la communication et le taux de succès de l'accès par les utilisateurs, le taux de succès du transfert intercellulaire et l'étendue de latence, le débit de données et les pertes de données subies par les utilisateurs du réseau.
Couverture	La couverture du réseau peut être établie en ciblant un pourcentage de la population qui réside dans la zone de couverture ou en fixant un objectif de couverture d'une superficie terrestre ou d'une longueur de route couverte par le réseau. La couverture réseau sans fil peut être étendue de façon temporaire en utilisant des systèmes déployables dans une zone d'incident localisée ou en ayant recours à l'itinérance à l'échelle de plusieurs réseaux.
Modèle de gouvernance	Structure d'une ou de plus d'une entité potentielle nationale ou régionale régissant le RLBSP, et les rôles et les responsabilités, y compris la coordination nationale des normes, la possession de licences du spectre sans fil, l'harmonisation des procédures d'exploitation et les relations entre les utilisateurs du réseau et l'industrie.
Interopérabilité	Capacité du personnel d'urgence de communiquer entre les administrations, les disciplines et les ordres de gouvernement au moyen de systèmes divers, au besoin et en fonction des autorisations ¹ . Cela inclut l'atteinte d'une opérabilité nationale totale au moyen d'identifiants d'utilisateur courants sans égard au mode de déploiement du réseau ainsi qu'à l'interopérabilité du RLBSP avec les services de radio mobile à court et à moyen terme.
Réseau à large bande de sécurité publique (RLBSP)	Réseau sans fil national, sécurisé et à haut débit, qui offrirait une plateforme améliorée, interopérable et résiliente pour la transmission de données ayant trait à la sécurité publique entre les administrations (fédérale, provinciales, territoriales et municipales) et, potentiellement, avec les États-Unis.
Résilience	Capacité du réseau à fournir et à maintenir un niveau de service acceptable compte tenu des diverses déficiences et difficultés liées à l'exploitation normale d'un réseau. L'infrastructure résiliente du RLBSP serait renforcée pour faire face aux menaces telles que les pannes de courant, les inondations, les secousses sismiques, le terrorisme et le vandalisme et, en cas de panne, pour rétablir rapidement les communications.
Sécurité	Capacité de protéger et de sécuriser l'infrastructure physique du réseau et de prévenir les actes malveillants tels que les cyberattaques au niveau du système ou des applications.

¹ Comme défini dans la Stratégie d'interopérabilité des communications pour le Canada (SICC), janvier 2011.

1. INTRODUCTION

Pour intervenir efficacement dans les cas de catastrophes majeures, d'urgences et d'événements de tous les jours, il faut être en mesure d'utiliser des moyens de communication de voix et de données fiables et interopérables entre les administrations et les divers intervenants d'urgence. À l'heure actuelle, la communauté des premiers intervenants du Canada n'a pas accès de façon générale et constante à ces capacités; ils s'appuient principalement sur des systèmes de communication vocale par radio et des services commerciaux de données sans fil. La plupart des systèmes radio de sécurité publique fonctionnent sur des fréquences différentes et les systèmes commerciaux de communication vocale et de données deviennent congestionnés durant les urgences. La création d'un réseau à large bande de sécurité publique (RLBSP) aiderait à résoudre ces problèmes en mettant à la disposition des intervenants d'urgence du Canada un outil qui leur donnerait un accès prioritaire à un réseau sans fil sécurisé et fiable pour la transmission de données à haut débit.

1.1. Qu'est-ce qu'un RLBSP?

Un RLBSP est un réseau national sans fil sécurisé, à haut débit, abordable et durable, utilisé pour la transmission de données. Ce réseau offre une plateforme améliorée, résiliente et interopérable pour la transmission de données ayant trait à la sécurité publique entre les administrations (fédérale, provinciales, territoriales et municipales, par exemple) et les communautés de la sécurité publique. S'il est mis en œuvre au Canada, il sera idéalement capable d'interagir avec FirstNet (First Responder Network Authority) des États-Unis². La plateforme permettrait d'améliorer la planification, la coordination et l'exécution des activités quotidiennes et l'efficacité des interventions en situation de crise. Entre autres, les utilisateurs se serviraient de ce réseau pour :

- accéder de manière fiable à des applications de transfert de données à haut débit pour transférer des données, des images et du contenu connexe;
- accéder à des applications partagées (par exemple à des services de gestion des dossiers et de répartition assistée par ordinateur [RAO]);
- obtenir des renseignements essentiels à la compréhension de situations en temps opportun;
- communiquer sans interruption partout au pays au moyen d'une infrastructure permanente ou temporaire.

1.2. Activités récemment entreprises au Canada concernant le RLBSP

Le gouvernement du Canada (GC) a entrepris plusieurs activités visant l'étude d'un RLBSP, notamment la désignation d'un spectre à large bande pour la sécurité publique et des consultations avec les intervenants.

En mars 2012, Innovation, Sciences et Développement économique Canada (ISDE) (Industrie Canada à cette époque) a désigné 10 MHz du spectre de 700 MHz, qui est très prisé, aux communications à large bande de la sécurité publique. Dans le budget de 2015, le gouvernement du Canada a annoncé que 10 MHz additionnels du spectre de 700 MHz seraient réservés pour l'utilisation des services à large bande par la sécurité publique.

² Le 30 mars 2017, le gouvernement américain a signé un contrat avec AT&T visant la construction, l'exploitation et l'actualisation du réseau national à large bande de sécurité publique de First Responder Network Authority (FirstNet). FirstNet sera la mise en œuvre d'un RLBSP aux États-Unis.

On peut tirer profit des 20 MHz du spectre réservés dans la bande de 700 MHz³ en vue du déploiement d'un RL BSP national et interopérable au Canada.

En mai 2016, les ministres fédéral/provinciaux/territoriaux (FPT) responsables de la gestion des interventions d'urgence se sont réunis à Toronto et se sont engagés à accélérer la mobilisation des intervenants par rapport à la mise en œuvre potentielle d'un RL BSP.

Le 19 mai 2017, le gouvernement du Canada a annoncé un engagement de 3 millions de dollars en 2017-2018 pour mobiliser divers intervenants et pour recueillir et analyser les données relatives aux modèles potentiels de mise en œuvre du réseau.

Les intervenants mobilisés comprennent les gouvernements provinciaux et territoriaux, les administrations municipales, les premiers intervenants, les représentants de l'industrie, les exploitants d'infrastructures essentielles, les représentants de collectivités plus petites ou éloignées, les représentants des collectivités autochtones, les représentants du milieu universitaire et des homologues étrangers de la sécurité publique.

Par cet exercice de mobilisation, on pourra mieux comprendre les avantages possibles d'un RL BSP et éclairer la prise de décision. Ces consultations tiennent compte de la gouvernance, des coûts, des sources de revenus, de la couverture, des besoins des utilisateurs dans la sécurité publique, de l'utilisation efficace du spectre et des occasions d'innover.

1.3. Objectif de la demande de renseignements (DDR)

Par l'entremise du présent processus de DDR, Innovation, Sciences et Développement économique Canada (ISDE) cherche à obtenir les points de vue de l'industrie des technologies de l'information et des communications (TIC) et des télécommunications sur les sujets suivants, afin d'éclairer l'approche du gouvernement du Canada relativement à un RL BSP au Canada :

- modèle d'affaires viable;
- modèle de gouvernance;
- écosystème d'applications, de services et de dispositifs.

1.4. Contexte opérationnel actuel

Depuis des décennies, les systèmes radio mobiles terrestres (RMT) existants constituent le point d'ancrage de la transmission de données ayant trait à la sécurité publique. Cependant, leur mise en œuvre fragmentée dans l'ensemble du Canada a compliqué l'interopérabilité des communications dans les différentes administrations et à la frontière avec les États-Unis, étant donné que ces systèmes fonctionnent souvent sur des segments différents du spectre des radiofréquences. La technologie elle-même présente des limites, bien que des mesures positives aient été prises pour harmoniser les systèmes RMT.

³ Décisions se rapportant au cadre politique, technique et de délivrance de licences pour l'utilisation du spectre à large bande destiné à la sécurité publique, et ce, dans les bandes de 758 à 763 MHz et de 788 à 793 MHz (bloc D), ainsi que de 763 à 768 MHz et de 793 à 798 MHz (bloc SPLB), juin 2017.

À l'heure actuelle, les intervenants d'urgence comptent sur des réseaux sans fil commerciaux pour obtenir l'accès à des applications riches en données, par l'intermédiaire de l'Internet public. Ces réseaux peuvent être encombrés durant les situations d'urgence, ce qui augmente le risque d'un refus de service pour les premiers intervenants.

1.5. Approches internationales

Plusieurs pays ont décidé de mettre à exécution des plans d'installation d'un RL BSP à l'échelle nationale. Les démarches adoptées par ces pays reposent sur des facteurs comme la géographie, la dynamique dans l'industrie des télécommunications, le statut de la couverture des services à large bande, les politiques de gestion du spectre et la répartition des pouvoirs fédérés. Nous vous présentons trois de ces démarches ci-dessous :

Les États-Unis

Le gouvernement américain a pris des mesures en vue du déploiement d'un RL BSP national par l'entremise d'un partenariat public-privé. En vertu de la *Middle Class Tax Relief and Job Creation Act (2012)*, le First Responder Network Authority (FirstNet) a été créé à titre d'autorité indépendante au sein de la National Telecommunications and Information Administration (NTIA). Son mandat est de fournir aux intervenants d'urgence le premier réseau national haute vitesse américain consacré à la sécurité publique. Le gouvernement a réservé 20 MHz de la bande de 700 MHz à l'usage de la sécurité publique en plus d'investir des fonds dans la construction du réseau FirstNet.

Le contrat de construction du RL BSP national a été attribué à AT&T en mars 2017. Il stipulait que l'entrepreneur devait, dans un délai de six mois, fournir une couverture nationale en se servant des bandes commerciales utilisant les déploiements des services sans fil existants. Le déploiement de la bande de fréquence 14 comportera plusieurs phases qui seront étalées sur une période de quatre ans et le réseau devrait être prêt en 2022.

Verizon a récemment fait part de son intention de construire et d'exploiter un réseau central privé consacré à ses clients de la sécurité publique qui sera distinct de son réseau central commercial et qui fournira à ses clients un accès prioritaire à son réseau LTE national. Verizon offrirait ce service sans accéder au spectre de la sécurité publique de 700 MHz et sans financement gouvernemental.

Royaume-Uni

Le Home Office du Royaume-Uni échange avec les intégrateurs système et les opérateurs commerciaux de services sans fil en vue de développer un réseau de services d'urgence (RSU) de remplacement en améliorant les réseaux commerciaux d'évolution à long terme (LTE) afin de satisfaire aux normes essentielles à la mission en ce qui a trait à la couverture, à la sécurité et à la disponibilité. Le RSU vise à remplacer complètement le réseau national (RMT) TETRA actuellement exploité par AirWave Solutions. Le réseau de remplacement incorporera un réseau commercial LTE principalement dédié au RSU. Au cours du troisième trimestre de 2015, le Home Office a annoncé que le premier contrat de RSU avait été attribué à Kellogg Brown & Root (KBR) en tant que partenaire de la prestation du programme. Plus tard, le Home Office a attribué les contrats de services aux utilisateurs et de services mobiles à Motorola Solutions et à l'opérateur commercial de services sans fil EE. La transition des communications sur bande étroite aux communications sur large bande devrait commencer à l'été 2018 et se terminer en septembre 2020.

Corée du Sud

Le gouvernement de la Corée du Sud prévoit déployer un réseau LTE national consacré à la sécurité publique, en utilisant 20 MHz du spectre désigné dans la bande 28 de 700 MHz. Le réseau appuiera les opérations de tous les ministères et organismes du gouvernement, y compris les bureaux militaires, les réseaux d'électricité, les systèmes d'alimentation en gaz, le réseau maritime et les systèmes ferroviaires.

2. LIGNES DIRECTRICES

2.1. Nature de la demande de renseignements (DDR)

L'objet de la présente DDR est de solliciter la rétroaction de l'industrie des technologies de l'information et des communications/des télécommunications pour orienter la meilleure marche à suivre dans la mise en œuvre possible d'un réseau à large bande de sécurité publique (RLBSP) au Canada. La présente DDR ne constitue pas un appel d'offres et il n'en résultera aucune demande de proposition ni attribution de contrat. Par conséquent, les fournisseurs éventuels des biens ou des services décrits dans la présente DDR ne devraient pas réserver des biens ou des installations ni affecter des ressources en fonction des renseignements présentés dans la DDR. De plus, la présente DDR ne donnera pas lieu à la création de listes de fournisseurs. En outre, la présente DDR n'entraînera pas nécessairement l'achat de l'un ou l'autre des biens et services qui y sont décrits.

2.2. Nature et traitement des réponses attendues

Les répondants sont invités à répondre par écrit aux questions de la DDR et à présenter leurs commentaires, suggestions, préoccupations, et, le cas échéant, des recommandations pertinentes sur la façon de réaliser les objectifs ou les résultats définis dans la présente DDR. Les répondants sont priés d'expliquer les hypothèses qu'ils avancent dans leur réponse.

Les répondants peuvent choisir de répondre uniquement à un sous-ensemble des questions.

2.2.1. Coût de réponses

Le GC ne remboursera pas aux répondants les frais engagés pour répondre à la présente DDR.

2.2.2. Traitement des réponses

1. **Utilisation des réponses** : Les réponses reçues peuvent être utilisées par le gouvernement du Canada, les provinces et les territoires ainsi que les municipalités pour orienter des stratégies d'approvisionnement futures ou tout document de passation de contrats ou toute clause et modalité. Le GC peut produire un rapport général anonyme résumant les résultats de la DDR qui peuvent être rendus publics.
2. **Équipe d'examen** : Toutes les réponses reçues à la date de clôture de la DDR seront examinées. Le GC pourra, à sa discrétion, examiner les réponses reçues après cette date. Le GC se réserve le droit d'embaucher des experts-conseils indépendants ou d'utiliser des ressources du gouvernement, s'il le juge nécessaire, pour l'examen des réponses.
3. **Confidentialité** : Les répondants devraient indiquer clairement les parties de leur réponse qui, selon eux, sont de nature exclusive ou confidentielle. Le GC traitera les réponses conformément à la *Loi sur l'accès à l'information*, L.R. 1985, ch. A-1, et à la *Loi sur la protection des renseignements personnels*, L.R. 1985, ch. P-21. Les réponses ne seront pas transmises aux autres répondants ni aux fournisseurs, mais pourraient être transmises à d'autres échelons gouvernementaux, conformément au paragraphe 1.

-
4. **Activité de suivi** : Le gouvernement du Canada peut, à son entière discrétion, communiquer avec les répondants afin de leur poser des questions supplémentaires ou de leur demander des précisions sur tout aspect d'une réponse dans le cadre de rencontres bilatérales.

2.3. Contenu de la présente DDR

Les répondants ne doivent pas tenir pour acquis qu'aucune des clauses ou des exigences ne sera supprimée ou révisée. Les commentaires concernant tout aspect du document sont les bienvenues. Si les répondants estiment qu'une question ou un aspect clé a été omis, ils sont invités à formuler des observations ou à fournir des renseignements à cet égard dans leur réponse.

2.4. Format des réponses

1. **Page titre** : La première page de chaque document de la réponse doit contenir ce qui suit :
 - 1.1. le titre de la réponse et le numéro de document (si la réponse est formée de multiples documents);
 - 1.2. le nom légal complet du répondant;
 - 1.3. le nom, l'adresse et le numéro de téléphone de la personne-ressource du répondant;
 - 1.4. la date;
 - 1.5. le numéro de la DDR.
2. **Système de numérotation** : Les répondants doivent préparer leur réponse en utilisant un système de numérotation correspondant à celui utilisé dans la présente DDR. Les références à des documents descriptifs, à des manuels techniques et à des brochures accompagnant la réponse doivent respecter ce même système.

2.5. Demandes de renseignements

La présente demande de renseignement (DDR) ne constitue pas une demande de soumissions. Le gouvernement du Canada ne répondra pas nécessairement aux demandes de renseignements par écrit ou en envoyant les réponses à tous les répondants potentiels. Les questions concernant la présente DDR peuvent être adressées à :

Stéphanie Cléroux

Stephanie.Cleroux2@canada.ca

Agente de contrats et d'acquisitions, Secteur de la gestion intégrée

Innovation, Sciences et Développement économique Canada / Gouvernement du Canada

2.6 Présentation des réponses

Délai de présentation des réponses et adresse d'expédition : Les répondants qui souhaitent fournir une réponse doivent l'envoyer à l'autorité contractante susmentionnée, par courriel, d'ici le 5 janvier 2018 à midi (HAE). Les répondants qui désirent présenter leurs réponses autrement que par courriel doivent communiquer avec l'autorité contractante indiquée ci-dessus.

Responsabilité en ce qui a trait à la présentation des réponses dans les délais prescrits : Il incombe à chaque répondant de s'assurer que sa réponse est présentée dans les délais prescrits et qu'elle est envoyée à la bonne adresse électronique.

Identification des réponses : Les répondants doivent s'assurer d'être bien identifiés en vérifiant que leur nom et leur adresse de courriel, ainsi que le numéro et le titre de la DDR, sont clairement indiqués dans le courriel.

3. QUESTIONNAIRE

3.1. Un modèle d'affaires viable

Pour fournir un RL BSP tel que décrit à la section 1.1 de la présente DDR, le RL BSP doit : 1) appuyer les objectifs changeants de la communauté de la sécurité publique en ce qui concerne la disponibilité, la sécurité, la résilience, l'interopérabilité et la couverture des communications; 2) assurer l'utilisation efficace du spectre; 3) déployer le réseau en temps opportun et d'une façon abordable et durable.

Les besoins des utilisateurs de la sécurité publique relatifs aux communications à large bande varient en fonction de leurs activités et de la nature des événements ou des incidents auxquels ils font face. Le RL BSP doit à tout le moins appuyer les activités dans les trois catégories suivantes :

- Activités quotidiennes courantes — telles que répondre aux incidents qui impliquent un nombre limité d'agents de sécurité publique ou d'équipes d'intervention. Pendant ces périodes, on s'attend à ce que la demande de services de communication soit plus faible, ainsi que plus stable et prévisible, par rapport aux autres catégories de services.
- Événements prévus — tels que des événements sportifs importants, des festivals de musique ou des réunions auxquelles participent des dirigeants étrangers (p. ex. G20), qui exigent une présence plus importante qu'à l'habitude de personnel de la sécurité publique. Pendant ces événements, on s'attend à ce que la demande de services de communication soit relativement élevée dans les zones localisées, mais prévisible.
- Situations d'urgence à grande échelle — telles que les catastrophes naturelles, les attaques terroristes ou d'autres incidents peu fréquents qui exigent une importante intervention d'urgence inter-organismes. Pendant ces incidents, la demande à l'égard des communications devrait être très forte dans les zones touchées, en plus d'être très pressante. Dans certains cas, la situation d'urgence en tant que telle peut perturber l'infrastructure ou la capacité de communication. Une forte résilience du réseau est essentielle pour répondre à un tel événement.

Toute mise en œuvre d'une solution de RL BSP doit pouvoir répondre aux besoins futurs des utilisateurs de la sécurité publique.

Le nombre d'utilisateurs potentiel de la sécurité publique au Canada pour un RL BSP est estimé aux alentours de 300 000 à 350 000. Ce nombre comprend entre autres la police, les premiers intervenants et les opérateurs de l'infrastructure essentielle.

Q1. En vous appuyant, entre autres, sur les approches internationales à titre d'exemples, quel(s) modèle(s) d'affaires recommandez-vous pour le Canada afin de concrétiser la vision d'un RL BSP?

Veillez énoncer vos hypothèses en ce qui concerne :

- a) Les principales considérations relatives au coût, y compris les dépenses en capital et les dépenses d'exploitation, les sources de financement (p. ex. le financement extérieur) et les sources de revenus constants (utilisateurs et autres);

-
- b) La nouvelle infrastructure clé requise, une occasion de mettre à profit l'infrastructure existante, y compris les infrastructures essentielles⁴, et d'autres actifs appartenant à la Couronne à tous les niveaux;
 - c) La nécessité d'accéder au spectre désigné au RL BSP et à d'autres spectres, et dans quelles conditions;
 - d) La contribution positive à l'analyse de rentabilisation de la mise à profit du spectre à large bande de la sécurité publique pour le trafic commercial, si disponible.
 - e) Le niveau de couverture probable au Canada, en particulier dans les régions rurales et éloignées, et les calendriers de déploiement possibles avec étapes suggérées et compte tenu des droits de priorité et de préemption;
 - f) Les types de services et l'éventail de prix pour un RL BSP comparativement aux offres commerciales;
 - g) Le nombre d'opérateurs canadiens impliqués, et s'il y en a plus d'un, la nature des partenariats entre eux;
 - h) Les options pour donner aux organismes de sécurité publique le contrôle direct et en temps réel de l'accès et des profils des utilisateurs sur un RL BSP;
 - i) Toute autre hypothèse qui devrait être présentée explicitement pour faciliter la compréhension, y compris les principaux risques et les conditions essentielles à la réussite.

S'il y a lieu, veuillez ajouter des précisions au sujet des coûts particuliers ou des considérations opérationnelles en ce qui concerne :

- a) Les conséquences sur les utilisateurs commerciaux du fait de donner des droits de priorité et de préemption aux utilisateurs de la sécurité publique;
- b) Les objectifs visant à obtenir une empreinte nationale complète, une interopérabilité harmonisée, un renforcement des systèmes et une continuité des services, que ce soit au moyen des capacités existantes ou en partenariat avec d'autres entreprises;
- c) Les obstacles technologiques ou les défis associés à l'atteinte de ces objectifs en fonction de la technologie d'aujourd'hui et de demain;
- d) L'intégration d'un RL BSP aux systèmes radio mobiles terrestres existants utilisés pour les services de sécurité publique;
- e) L'interopérabilité entre les intervenants d'urgence américains et canadiens longeant ou traversant la frontière internationale;
- f) Comment les capacités 5G amélioreront le service ou transformeront le modèle d'affaires d'un RL BSP national;
- g) Toute autre hypothèse qui devrait être présentée explicitement pour une meilleure compréhension.

Q2. Avez-vous l'intention d'offrir des services commerciaux à large bande aux communautés de la sécurité publique, au moyen des normes 3GPP existantes relatives aux droits de priorité et de préemption? Dans l'affirmative, quel serait l'échéancier?

3.2. Modèle de gouvernance

Étant donné qu'un RL BSP national pourrait possiblement servir un éventail d'intervenants au sein de diverses administrations et entités, une structure de gouvernance possédant une entité (ou plus) sera requise. L'entité peut être

⁴ Comme le définit Sécurité publique Canada, <https://www.securitepublique.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/index-fr.aspx>

tenue responsable d'une variété de fonctions. Par exemple, il pourrait incomber à l'entité d'harmoniser les normes et les applications communes. De plus, l'entité pourrait possiblement détenir des licences de spectre et assumer l'entière responsabilité de la négociation avec le secteur privé à propos de la mise en œuvre et du fonctionnement continu du réseau. Il pourrait y avoir une seule entité nationale, un ensemble d'entités régionales, ou les deux.

Q3. En tenant compte de l'encadrement législatif et réglementaire actuel et entre autres, des approches internationales, quel modèle de gouvernance serait selon vous le plus adéquat pour soutenir un RL BSP canadien?

Veuillez énoncer vos hypothèses relativement à ce qui suit :

- a) l'existence et les responsabilités d'une entité nationale;
- b) l'existence et les responsabilités des entités régionales;
- c) si a) et b) sont nécessaires, la gouvernance entre les deux niveaux;
- d) les titulaires de licence d'utilisation du spectre du RL BSP;
- e) l'écosystème des applications, des services et des dispositifs connexes du RL BSP;
- f) tous les autres obstacles, défis et hypothèses qui devraient être présentés de façon explicite pour une meilleure compréhension.

3.3. Écosystème d'applications, de services et de dispositifs

La clé du succès d'un RL BSP passe par un écosystème qui offre des services, des applications et des capacités pertinentes et novatrices en matière de sécurité publique.

Voici quelques exemples de fonctionnalités :

- a) diffusion vidéo en continu et transmission en direct de vidéos;
- b) externalisation et filtrage en temps réel des médias sociaux pour favoriser la connaissance de la situation;
- c) transmission d'images en haute résolution et services basés sur la localisation;
- d) applications vocales, comme celles permettant l'utilisation d'un bouton de microphone (PTT), la répartition et les communications de groupe;
- e) utilisation des services de gestion de l'identité, des justificatifs d'identité et de l'accès;
- f) communication en mode direct et services de proximité;
- g) interopérabilité avec les systèmes RMT, le Système national d'alerte publique, les systèmes 9-1-1 actuels et les systèmes 9-1-1 de prochaine génération (9-1-1 de PG).

Q4. Quel est l'état actuel et prévu de l'écosystème de RL BSP?

- a) Quels types d'applications, de services et de dispositifs sont en cours d'élaboration pour les RL BSP? Par quelles entreprises et dans quels pays?
- b) Quels points forts le Canada possède-t-il (notamment en ce qui a trait à la recherche, aux universités et aux affaires) pouvant permettre la création d'applications, de services et de dispositifs?

Documents de référence

1. The Public Safety LTE & Mobile Broadband Market: 2016 – 2030 – Opportunities, Challenges, Strategies & Forecasts, SNS Telecom Research, 2016. <http://www.reportsnreports.com/reports/560702-the-public-safety-lte-mobile-broadband-market-2016-2030-opportunities-challenges-strategies-forecasts.html>
2. The Los Angeles Regional Interoperable Communications System (LA-RICS), Request for Information for Public Safety Broadband Network (PSBN) Devices, DDR N° LA-RICS 009, Septembre 2014. http://www.la-rics.org/wp-content/uploads/2014/02/RFI_LARICS_009_PSBN_DEVICES_090214.pdf
3. Public Safety Mobile Broadband, Productivity Commission Issues Paper, gouvernement de l’Australie, avril 2015. <http://www.pc.gov.au/inquiries/completed/public-safety-mobile-broadband/issues/public-safety-mobile-broadband-issues.pdf>
4. Public Safety Mobile Broadband, Productivity Commission Research Report, gouvernement de l’Australie, décembre 2015. <http://www.pc.gov.au/inquiries/completed/public-safety-mobile-broadband/report/public-safety-mobile-broadband.pdf>
5. FirstNet Request for Information for Comprehensive Network Solution(s), septembre 2014. <https://www.fbo.gov/utills/view?id=1ef697f901b1c4b347bb17ae77c5a485>
6. FirstNet’s Request for Information (RFI) with a draft Statement of Objectives (SOO) for Comprehensive Network Solution(s), septembre 2015. <https://www.firstnet.gov/sites/default/files/rfi-draft-soo-comp-network-solution-faqs.pdf>
7. Public Safety LTE Market Analysis and Forecasts 2016 – 2020, Mind Commerce Publishing, 2016. https://mindcommerce.com/public_safety_lte_market_analysis_and_forecasts_2016_2020.php
8. Décisions se rapportant au cadre politique, technique et de délivrance de licences pour l’utilisation du spectre à large bande destiné à la sécurité publique, et ce, dans les bandes de 758 à 763 MHz et de 788 à 793 MHz (bloc D), ainsi que de 763 à 768 MHz et de 793 à 798 MHz (bloc SPLB), juin 2017.