AGENCE MUNICIPALE DE FINANCEMENT ET DE DÉVELOPPEMENT DES CENTRES D'URGENCE 9-1-1 DU QUÉBEC

ASSOCIATION DES CENTRES D'URGENCE DU QUÉBEC

CAUCA Experts en appels d'urgence

Le 23 mai 2018

M. Claude DOUCET
Secrétaire général
Conseil de la radiodiffusion et des télécommunications canadiennes
GATINEAU (Québec)
K1A 0N2

Objet : Observations
Avis de consultation de télécom **CRTC 2018-105,** *Appel aux observations, Gains d'efficacité liés à la conception des réseaux 9-1-1 de prochaine génération*
Dossier ***1011-NOC2018-0105***

Monsieur le Secrétaire général,

1. La **COALITION POUR LE SERVICE 9-1-1 AU QUÉBEC**, ci-après la COALITION, répond par la présente à l'appel aux observations de l'Avis de consultation de télécom **CRTC 2018-105** du 26 mars 2018, modifié par l'ACT CRTC 2018-105-1 ainsi que par l'ACT CRTC 2018-105-2. Elle est formée de :

    a. L'**AGENCE MUNICIPALE DE FINANCEMENT ET DE DÉVELOPPEMENT DES CENTRES D'URGENCE 9-1-1 DU QUÉBEC** (l'Agence), constituée et administrée selon la *Loi sur la fiscalité municipale*[1] du Québec par **l'UNION DES MUNICIPALITÉS DU QUÉBEC** (UMQ), la **FÉDÉRATION QUÉBÉCOISE DES MUNICIPALITÉS** (FQM) et la **VILLE DE MONTRÉAL**;

    b. L'**ASSOCIATION DES CENTRES D'URGENCE DU QUÉBEC** (ACUQ), qui représente la presque totalité des centres d'urgence 9-1-1, des centres de communication santé du Québec (urgences préhospitalières) ainsi que divers autres centres d'appels d'urgence secondaires ou spécialisés de la province;

    c. La **CENTRALE DES APPELS D'URGENCE DE CHAUDIÈRE-APPALACHES** (CAUCA), qui offre le service 9-1-1 à plus de 560 municipalités québécoises dans plusieurs régions de la province et n'est pas représentée par l'ACUQ.

2. La COALITION souhaite être considérée comme une partie à l'instance. Elle se réserve le droit de réplique à toutes les observations ou réponses qui seront produites au dossier.

---

[1] *Recueil des lois et règlements du Québec*, RLRQ, chapitre F-2.1, article 244.68 et suivants.

REMARQUES PRÉLIMINAIRES

3. La COALITION s'est réjouie de la partie de la décision[2] du Conseil qui a déterminé un modèle de gouvernance et de financement des réseaux 9-1-1 de prochaine génération (PG) par les entreprises de services locaux titulaires, sous sa supervision. Il s'agissait de l'une de nos recommandations, lors des audiences publiques de janvier 2017.

4. La COALITION note que selon le paragraphe 17° de l'Avis, le Conseil annonce qu'il n'examinera **pas** *les propositions de gains d'efficacité liés à la conception des réseaux 9-1-1PG portant sur les composantes des réseaux ou sur les éléments fonctionnels qui relèvent de la responsabilité des centres d'appels de la sécurité publique (CASP), conformément à la politique réglementaire de télécom 2017-182 et à la norme i3*. Il faut rappeler que les éléments « *qui relèvent de la responsabilité des CASP* » ne sont **pas vraiment connus** par les CASP **ou déterminés** et qu'il n'y a eu aucune communication auprès des CASP sur ce qui pourrait changer à l'avenir, les conséquences prévisibles et les mesures à prendre. S'en remettre simplement à la norme i3 de NENA, **incompréhensible pour la majorité des gens** et d'ailleurs **toujours en évolution**, ne devrait pas satisfaire le Conseil.

5. Nous ne croyons pas que le respect normal et attendu de la juridiction des provinces et des territoires sur les CASP doive aveugler le Conseil. Dans le cadre de la présente instance, l'**intérêt public** devrait prévaloir, sans dogmatisme. Bien que le passage au service 9-1-1PG puisse offrir de nouvelles possibilités sur le plan technologique, cela ne devrait pas constituer une occasion ou une justification de transférer en douce aux CASP de nouveaux coûts ou responsabilités. Rappelons qu'il existe un mécanisme efficace et peu coûteux de financement du réseau 9-1-1 par les usagers dont personne ne se plaint (*mais avec plus de transparence qu'actuellement quant aux sommes et à leur gestion, toutefois*).

6. La COALITION est d'avis que les décisions que le Conseil pourrait prendre à la suite de la présente instance sont susceptibles d'avoir des répercussions **techniques, opérationnelles et financières** pour les centres d'appels de la sécurité publique (CASP). Les éléments cruciaux permettant l'administration et la gestion de bout en bout du service 9-1-1PG devraient être considérés et évalués, afin d'en minimiser l'impact pour les contribuables autant que faire se peut ainsi que sur la complexité du travail des CASP, afin de permettre une uniformisation des opérations et ce, même si la juridiction du Conseil ne porte effectivement que sur les entreprises de télécommunication.

7. Les CASP sont des **partenaires** du Conseil relativement au service 9-1-1 au pays et contribuent significativement aux travaux du Groupe de travail Services d'urgence (GTSU) du Comité directeur du Conseil sur l'interconnexion. Leurs préoccupations et intérêts, afin de desservir et de protéger les Canadiens selon les plus hauts standards et au meilleur coût, doivent être pris en compte **dans l'évaluation des diverses solutions** qui s'offrent au Conseil.

[2] Politique réglementaire de télécom CRTC 2017-182, *9-1-1 de prochaine génération – Modernisation des réseaux 9-1-1 afin de satisfaire aux besoins des Canadiens en matière de sécurité publique*.

8. Toute mesure permettant d'augmenter les gains d'efficacité technique et la réduction des coûts pour l'ensemble des parties prenantes du service 9-1-1 est la bienvenue, **à la condition** que la fiabilité, la sécurité, la cyber-sécurité et la résilience ne soient jamais sacrifiés ou occultés. Il doit toujours y avoir, clairement, **un responsable imputable** à qui les CASP ou le Conseil peuvent en référer au besoin, sans partie de *ping pong* possible entre divers fournisseurs en cas de problème ou de défaillance de certaines constituantes/parties communes du réseau 9-1-1PG.

9. Le service 9-1-1 est l'un des éléments constitutifs de la sécurité nationale au pays, et le service 9-1-1PG le sera davantage encore. Il faut donc travailler ensemble, et viser à faire un succès de ce vaste chantier pour toutes les parties prenantes.

RÉPONSES AUX QUESTIONS

Serveurs de données de localisation (paragraphes 2 à 13 du rapport)

***Q1**. Le rapport indique que selon la norme i3, les FST qui exploitent des réseaux d'origine sont responsables de la fonctionnalité SDL. Cependant, les fournisseurs de réseaux 9-1-1 PG pourraient offrir un service SDL hébergé à ces FST pour les aider à fournir cette fonctionnalité.*

***a**. Croyez-vous qu'au Canada les FST qui détiennent et exploitent des réseaux d'origine devraient être responsables de la fourniture de la fonctionnalité SDL? Expliquez votre réponse en fournissant une justification et des preuves à l'appui.*

10. La COALITION privilégie une fourniture hébergée de serveurs de données de localisation (SDL). Ces derniers stockent des données de localisation liées aux points d'extrémité IP connectés à un réseau IP et ce, afin de normaliser la gestion uniformisée de la prise en charge des appels d'urgence provenant de ces points d'extrémité et d'en faciliter la disponibilité, l'accessibilité et l'interopérabilité avec les systèmes du 9-1-1PG des CASP.

b. Donnez votre opinion concernant la faisabilité ainsi que les avantages et les désavantages d'un modèle selon lequel les fournisseurs de réseaux 9-1-1PG offrent un service SDL hébergé aux FST qui détiennent et exploitent des réseaux d'origine.

11. Dans leur rapport soumis au CRTC le 21 décembre et annexé à l'Avis de consultation dans la présente instance, les fournisseurs de réseaux 9-1-1PG ont déjà fait connaître leur préférence[3] et offert de fournir ce genre de service aux FST. La simplification des interactions avec les CASP lors d'appels 9-1-1PG et pour la gestion des accréditations d'accès de la cyber-sécurité constituerait alors un avantage assuré.

***c.** Les FST devraient-ils avoir le choix de fournir leur propre fonctionnalité SDL ou de s'abonner au service SDL hébergé proposé des fournisseurs de réseaux 9-1-1PG? Expliquez votre réponse en fournissant une justification et des preuves à l'appui.*

[3] Paragraphes 3° à 11°

12. Bien que nous n'ayons pas de position arrêtée actuellement sur cette option, nous préconisons une normalisation de la gestion de toute donnée cruciale pour l'acheminement des appels et la répartition des services d'urgence.

d. *Les fournisseurs de réseaux 9-1-1PG devraient-ils être obligés de fournir un service SDL hébergé tarifé de gros aux FST, et, le cas échéant, le coût de la fourniture de ce service devrait-il être compris dans le tarif d'accès aux réseaux 9-1-1PG ou être un tarif distinct pour les FST qui s'abonnent au service SDL hébergé?*

13. Bien que nous n'ayons pas de position arrêtée sur cette option actuellement, nous préconisons la standardisation de l'administration et de la gestion des données.

Q2*. Le rapport indique que les FST qui exploitent des réseaux d'origine sont les propriétaires des données de localisation des utilisateurs finals utilisées par la fonctionnalité SDL et sont responsables de leur mise à jour.*

a*. Croyez-vous que chaque FST qui offre des services aux utilisateurs finals visés devrait être propriétaire des données de localisation des utilisateurs finals utilisées par la fonctionnalité SDL et être responsable de leur mise à jour? Expliquez votre réponse en fournissant une justification et des preuves à l'appui.*

14. Oui. La gestion des renseignements et des données validées de localisation des utilisateurs finals relève du FST ayant des liens avec l'usager et lui fournissant un service. De plus, le CASP doit être en mesure d'identifier et de pouvoir communiquer rapidement avec la source responsable des renseignements et des informations de localisation.

b. *Quelles exigences devraient être imposées aux FST en ce qui concerne la mise à jour des données de localisation des utilisateurs finals et leur transmission au SDL lorsque les FST fournissent le SDL ou que les fournisseurs de réseaux 9-1-1PG fournissent un service SDL hébergé aux FST?*

15. Les mêmes exigences d'administration, de gestion et d'intégrité des renseignements devraient être imposées aux FST, en ce qui concerne la mise à jour des données de localisation des utilisateurs finals et leur transmission au SDL et ce, peu importe de qui relève l'administration et la gestion du SDL. Un processus permanent de validation de l'intégrité des données doit aussi être exigé.

Q3*. Le Conseil devrait-il tenir compte d'autres considérations stratégiques relativement à la fourniture de la fonctionnalité SDL et des données de localisation?*

16. Probablement. Le positionnement des SDL, la fiabilité, la redondance, la sécurité, les processus de gestion et de validation de l'intégrité des renseignements, etc. pourraient faire l'objet de recommandations du GTSU que le Conseil devrait requérir. Le CASP doit être en mesure d'avoir accès rapidement et de façon standardisée aux données requises.

Répertoires de données additionnelles (paragraphes 14 à 24 du rapport)

Q4*. Le rapport indique que conformément à la norme i3, la fonctionnalité RDA ne fait pas partie d'ESInet et que les FST qui exploitent des réseaux d'origine sont responsables de la*

fonctionnalité RDA et des données qu'ils contiennent. Cependant, les fournisseurs de réseaux 9-1-1PG pourraient offrir un service RDA hébergé à ces FST pour les aider à fournir cette fonctionnalité.

***a**. Croyez-vous qu'au Canada les FST qui détiennent et exploitent des réseaux d'origine devraient être responsables de la fonctionnalité RDA? Expliquez votre réponse en fournissant une justification et des preuves à l'appui.*

17. Bien que la COALITION reconnaisse la responsabilité de base des FST en matière du contenu et d'intégrité de données concernant leur clientèle, nous privilégions la fourniture hébergée de banques de données sur les clients pour le 9-1-1PG, appelées répertoires de données additionnelles (RDA). Celles-ci fournissent des données supplémentaires sur l'appel, la localisation de l'appelant et, notamment, des données sur les abonnés des FST qui pourraient être utiles aux CASP, comme le nom et un numéro de rappel de l'abonné.

***b.** Donnez votre opinion concernant la faisabilité ainsi que les avantages et les désavantages d'un modèle selon lequel les fournisseurs de réseaux 9-1-1PG offrent un service RDA hébergé aux FST.*

18. Les fournisseurs de réseaux 9-1-1PG ont déjà fait connaître leur préférence et offert de fournir ce genre de service aux FST[4]. La simplification des interactions avec les CASP lors d'appels 9-1-1PG et pour la gestion des accréditations d'accès de la cyber-sécurité constituerait alors un avantage assuré.

***c.** Les FST devraient-ils avoir le choix de fournir leur propre fonctionnalité RDA ou de s'abonner au service RDA hébergé proposé des fournisseurs de réseaux 9-1-1PG? Expliquez votre réponse en fournissant une justification et des preuves à l'appui.*

19. Bien que nous n'ayons pas de position arrêtée sur cette option actuellement, nous préconisons une standardisation des outils permettant la gestion rapide des appels (par exemple, les renseignements utiles pour le transfert d'un appel à un autre CASP) et des données requises pour la répartition des services d'urgence.

***d**. Les fournisseurs de réseaux 9-1-1PG devraient-ils être obligés de fournir un service RDA hébergé tarifé de gros aux FST, et, le cas échéant, le coût de la fourniture de ce service devrait-il être compris dans le tarif d'accès aux réseaux 9-1-1PG ou être un tarif distinct pour les FST qui s'abonnent au service RDA hébergé?*

20. Nous n'avons pas de position arrêtée à ce sujet actuellement. Dans la mesure où les abonnés et les usagers sont ceux qui assument ultimement ces frais, nous favorisons un mécanisme visant l'**efficacité**, la **simplicité** et la **transparence** complète du processus de financement du réseau 9-1-1 canadien.

***Q5.** Le rapport indique que les FST qui exploitent des réseaux d'origine sont les propriétaires des données sur les abonnés finals utilisées par la fonctionnalité RDA et sont responsables de leur mise à jour.*

[4] Voir la note 3 précédente. Idem.

***a**. Croyez-vous que chaque FST qui offre des services aux abonnés finals visés devrait être propriétaire des données sur les abonnés finals utilisées par la fonctionnalité RDA et être responsable de leur mise à jour? Expliquez votre réponse en fournissant une justification et des preuves à l'appui.*

21. **Oui**. La gestion des renseignements et données valides sur les abonnés finals utilisées par la fonctionnalité RDA relèvent du FST ayant des liens d'affaires avec l'usager et lui fournissant le service. Le CASP doit être en mesure d'identifier et de pouvoir communiquer rapidement avec la source responsable des renseignements additionnels pouvant lui être utiles, afin d'assumer ses responsabilités de protection du public.

***b.** Quelles exigences devraient être imposées aux FST en ce qui concerne la validation et la mise à jour des données sur les abonnés finals et leur transmission au RDA lorsque les FST fournissent le service RDA ou que les fournisseurs de réseaux 9-1-1PG fournissent aux FST un service RDA hébergé?*

22. Les **mêmes exigences** d'administration, de gestion et d'intégrité des renseignements devraient être imposées aux FST, relativement à la mise à jour des données de localisation des utilisateurs finals et leur transmission au RDA et ce, peu importe qui sera le responsable de l'administration et de la gestion du RDA. Un processus permanent de validation de l'intégrité des données **doit aussi être exigé**.

***Q6**. Le Conseil devrait-il tenir compte d'autres considérations stratégiques relativement à la fourniture de la fonctionnalité RDA et des données qu'il contient?*

23. Probablement. Le positionnement des RDA, la fiabilité, la redondance, la sécurité, les processus de gestion et de validation de l'intégrité des renseignements, etc. pourraient faire l'objet de recommandations du GTSU que le Conseil pourrait requérir. Le CASP doit être en mesure d'avoir accès rapidement et de façon standardisée aux renseignements requis.

Partage des composantes des réseaux 9-1-1PG (paragraphes 25 et 26 du rapport)

***Q7.** Le rapport indique qu'étant donné que le réseau 9-1-1PG est un cadre évolutif qui comprend un certain nombre de normes et de spécifications d'interface, dont quelques-unes n'ont pas encore été finalisées, aucune composante fondamentale du réseau ne pourrait être partagée pour l'instant pour bénéficier d'économies d'échelle. Indiquez précisément les composantes fondamentales des réseaux 9-1-1PG qui pourraient être partagées pour bénéficier d'économies d'échelle qui n'ont pas été étudiées dans le rapport ou qui ont déjà été étudiées dans le cadre de l'instance ayant mené à la politique réglementaire de télécom 2017-182, et fournissez une justification et des preuves à l'appui.*

24. La COALITION n'a pas de position arrêtée sur cette option actuellement, mais elle préconise la simplification des interfaces et la standardisation des opérations de gestion des appels. Une **approche proactive** immédiate, prévoyant et permettant une **architecture souple** *de bout en bout* du service 9-1-1PG est préférable, selon nous, à des changements en cours de route. Une telle situation regrettable occasionnerait inutilement le gaspillage de temps et d'argent, un luxe inabordable.

Ententes d'interconnexion (paragraphes 27 à 42 du rapport)

***Q8** : Le rapport recommande de permettre à un fournisseur de réseaux 9-1-1PG de choisir de déployer plus de deux PI 9-1-1PG dans son territoire de desserte, selon les facteurs liés à la géographie, à la résilience et autres. Cependant, le rapport ne contient aucune recommandation concernant l'emplacement des PI 9-1-1PG, le nombre de PI que devraient compter les territoires de desserte des fournisseurs de réseaux 9-1-1PG, ni les critères nécessaires pour tirer des conclusions relativement à l'interconnexion.*

Commentez la question de savoir si, compte tenu de la transition vers des réseaux 9-1-1PG, le Conseil devrait continuer ou cesser d'appliquer ses politiques actuelles sur l'interconnexion des réseaux IP pour les services de voix (dont il est question au paragraphe 5 ci-dessus) dans les situations où les ESLT, qui agissent à titre de fournisseurs de réseaux 9-1-1PG, sont tenues d'établir des PI pour les réseaux d'origine exploités par les FST afin que soit acheminé le trafic des réseaux 9-1-1PG sur le réseau 9-1-1PG. Veuillez fournir une justification et des preuves à l'appui, ainsi que votre opinion sur les questions suivantes :

***a.** Le Conseil devrait-il établir des critères concernant la façon de définir les régions d'interconnexion du réseau 9-1-1PG (p. ex., pour chaque RIL, chaque province ou chaque ESInet)?*

25. L'emplacement ainsi que le nombre des points d'interconnexions (PI) du 9-1-1PG dans les territoires de desserte des fournisseurs de réseaux 9-1-1 PG restent à déterminer, selon des critères rigoureux de fiabilité, de résilience et de sécurité. La COALITION fait remarquer que le modèle d'interconnexion actuel (9-1-1 évolué) exige que chaque FST établisse deux faisceaux de liaisons par CU 9-1-1[5]. Le modèle du 9-1-1PG préconisé par le Conseil **élimine cette exigence**, **sans toutefois clairement requérir que chaque appel d'urgence soit acheminé immédiatement soit à un CASP désigné ou, par défaut, à un CASP alternatif de réponse**. Cela nous inquiète. Le processus requis à cet égard devrait être défini clairement et recommandé au préalable de façon consensuelle par le GTSU, sans improvisation de la part du Conseil sur une telle question.

***b**. Combien de PI 9-1-1PG devraient être établis dans chacune des régions d'interconnexion proposées, selon quels critères et qui devrait déterminer ce nombre et ces critères (p. ex., le Conseil, les fournisseurs de réseaux 9-1-1PG, les FST, les fournisseurs de réseaux 9-1-1PG et les FST au moyen de négociations)?*

26. Peu importe qui déterminera le nombre et les critères physiques d'interconnexion, la COALITION est clairement d'avis que les **CASP** (destinataires finaux) **doivent être consultés** concernant les critères opérationnels, en particulier quant au choix à effectuer et aux critères d'acheminement par défaut des appels d'urgence.

***c.** Dans quelles municipalités ou régions du pays des PI 9-1-1PG devraient-ils être établis?*

27. Nous préconisons la rationalisation et la simplification des opérations, sans toutefois mettre en péril un accès rapide et approprié aux services d'urgence régionaux. Avec les connaissances dont nous disposons, nous sommes toutefois d'avis que les cinq

[5] Voir le rapport de consensus ESREE0065 du GTSU (cas d'espèces 1,7, 1.11, 4.t5 et 4.6)

grandes régions du pays (Atlantique, Québec, Ontario, Prairies et Pacifique), le Nord étant possiblement rattaché à l'une des deux dernières, devraient, **au minimum**, disposer de PI 9-1-1PG. Le Canada est le deuxième plus vaste pays sur Terre. Rappelons également les conséquences de la coupure accidentelle de deux fibres optiques presque en simultané au Québec et au Nouveau-Brunswick en 2017. Celle-ci avait entraîné des coupures massives de services téléphoniques, y compris du service 9-1-1 et le chaos dans plusieurs activités économiques dans presque toutes les provinces de l'Atlantique.

***Q9**. Le rapport recommande que chaque FST qui exploite des réseaux d'origine établisse une interconnexion avec au moins deux PI situés dans différents emplacements géographiques dans chaque région d'interconnexion. Êtes-vous d'accord avec cette recommandation? Expliquez votre réponse en fournissant une justification et des preuves à l'appui, et proposez une définition de la diversité géographique en ce qui a trait aux PI.*

28. Bien que nous n'ayons pas actuellement de position arrêtée sur cette question, nous préconisons la résilience, la fiabilité et la sécurité pour l'acheminement des appels et des données. Néanmoins, l'architecture retenue ne devrait jamais constituer la source de conflits de gestion des appels pour les CASP déterminés pour l'acheminement par défaut.

***Q10**. Le rapport ne traite pas spécifiquement des ententes concernant les PI 9-1-1PG qui ont été conclues entre les FST et les petites ESLT qui agissent à titre de fournisseurs de réseaux 9-1-1PG dans leurs territoires de desserte. Compte tenu de vos réponses aux questions précédentes, la même approche devrait-elle être appliquée à l'établissement des PI dans les territoires de desserte des petites ESLT ou des facteurs spéciaux devraient-ils être pris en compte? Expliquez votre réponse en fournissant une justification et des preuves à l'appui.*

29. Bien que nous n'ayons pas actuellement de position arrêtée sur cette question, nous préconisons la résilience, la fiabilité et la sécurité pour l'acheminement des appels et des données et ce, peu importe le territoire de desserte. L'architecture retenue ne devrait jamais constituer la source de conflits de gestion des appels pour les CASP déterminés pour l'acheminement par défaut.

***Q11**. Le rapport recommande que tous les appels et toutes les communications de données connexes présentés à un PI 9-1-1PG donné soient localisés, c'est-à-dire qu'ils soient associés au domaine du fournisseur de réseaux 9-1-1PG qui offre le service (p. ex., un appel provenant de Vancouver doit être acheminé à l'un des PI 9-1-1PG de TCI). Êtes-vous d'accord avec cette recommandation? Expliquez votre réponse en fournissant une justification et des preuves à l'appui.*

30. Bien que nous n'ayons pas de position arrêtée sur cette question actuellement, nous préconisons la résilience, la fiabilité et la sécurité pour l'acheminement des appels et des données. On doit toutefois garder les choses simples, sans complexité ou risques inutiles pouvant mettre en péril un accès approprié aux services d'urgence régionaux.

***Q12.** Le rapport indique que l'interconnexion Internet publique ne sera pas prise en charge pour des raisons de sécurité. Êtes-vous d'accord avec cette affirmation? Expliquez votre réponse en fournissant une justification et des preuves à l'appui.*

31. Selon nos renseignements, la **norme i3** de la NENA (*NENA-STA-010.2*) et le document d'information de l'architecture du réseau 9-1-1 des services d'urgence (ESIND) (*NENA-INF-016.2*) **indiquent la possibilité d'interconnexion avec et à partir de l'Internet public.** Nous joignons en annexe des extraits des normes susmentionnées de la NENA.

32. La COALITION recommande au Conseil de requérir le GTSU d'examiner cette question technique et de lui formuler des recommandations sur les différentes options, afin de ne pas restreindre l'accès au service d'urgence canadien à certaines sources d'appels, ou pour la gestion permettant d'accéder à certaines banques de données externes. La COALITION préconise la résilience, la fiabilité et la sécurité pour l'acheminement des appels et la gestion des données.

33. Nous demeurons à la disposition du Conseil et vous prions d'agréer, Monsieur le Secrétaire général, l'expression de nos salutations distinguées.

Pour la COALITION,

M^e^ Serge ALLEN, avocat, MAP
sallen@agence9-1-1.org
300 - 2954, boulevard Laurier
Québec (Québec) G1V 4T2
Téléphone: 418 653-3911, poste 222
Télécopieur: 418 653-6198

ANNEXES A ET B À NOS OBSERVATIONS (*les soulignés sont de nous*)

A - *Extraits de la norme i3 de la NENA - NENA Detailed Functional and Interface Standards for the NENA i3 Solution – Document NENA-STA-010.*

« 2.3 Security Impacts Summary

This document introduces many new security mechanisms that will impact network and PSAP operations. The most significant changes to current practice are:

- *Of necessity, PSAPs will be connected, indirectly through the ESInet, to the global Internet to accept calls. This means that PSAPs will likely experience deliberate attacks on their systems. The types of vulnerabilities that NG9-1-1 systems must manage and protect against will fundamentally change and will require constant vigilance to create a secure and reliable operating environment. NG9-1-1 systems must have robust detection and mitigation mechanisms to deal with such attacks.*

3.7 Emergency Services IP Networks

ESInets must be accessible from the global Internet, with calls going through the Border Control Function (BCF). This Internet interconnect is recommended at the state ESInet level with local or regional ESInets getting Internet connectivity via the state ESInet. Origination networks should be connected to any ESInet they regularly deliver volume traffic to via a

private connection, through the BCF of that ESInet. Connection through the Internet is acceptable, preferably through a Virtual Private Network (VPN).

Access to ESInets must be controlled. Only public safety agencies and their service providers may be connected directly to the ESInet. Call origination sources, gateways, and similar elements are outside the ESInet and interconnected through the BCF. However, for security reasons, the ESInet should not be assumed to be a "walled garden".

4.1.17 Maintaining connections and NAT Traversal

All elements in an ESInet that implement SIP interfaces must comply with RFC 5626 [109] (Outbound) to maintain connections from User Agents. PSAPs, IMRs, bridges and other elements that terminate calls from entities outside an ESInet that may be behind NATs must implement "Interactive Connectivity Establishment (ICE)", RFC 5245 [128]. ESInets should maintain a "Traversal Using Relays around NAT (TURN)" [156] server for use by entities inside the ESInet placing calls towards the Internet.

5.3.8 Operational Considerations

The NG9-1-1 architecture allows for a hierarchy of ESInets, with replicas of ECRF/LVFs at different levels of the hierarchy as well as in access/origination networks. It is expected that ECRFs that are provided as local copies to network operators will only have the layers necessary to route to the correct originating ESRP, whereas ECRFs that are inside the ESInet(s) will have all available layers and use authorization to control who has access to what information. Since it is not possible that all entities that need to access an ECRF will have one in their local domain, an ECRF for each 9-1-1 Authority must be accessible from the Internet.

Since it is not possible that all entities that need to access a LVF will have one in their local domain, a LVF must be accessible from the Internet[33]*.*

[33] *The Internet accessible ECRF/LVF may be a state or regional ECRF/LVF containing the local data of all PSAPs within the state or region.*

External ECRFs must be accessible to all devices and services, including those on the Internet. »

B ***- Extraits de NENA Emergency Services IP Network Design Information***
Document NENA-INF-016.2-2018

« 4.3 Security Impacts Summary

ESInets are utilized to provide IP transport between a number of different agencies and resources including PSAPs, regional host sites, and state-level Next Generation Core Services (NGCS). Many of the agencies connected to an ESInet will also be connected to untrusted networks including the Internet. Given the operating environment that NG9-1-1 requires, it seems likely that PSAPs, regional 9-1-1 entities, and state authorities will experience deliberate attacks on their systems. Maintaining high degrees of reliability, resiliency and security in this new environment will require a fundamental change in the approach taken to both physical and cyber security. The NENA Security for NG9-1-1 standard (NENA 75-001) is applicable and recommended. Qualified security engineers should be consulted when designing and deploying ESInets.

2.11.4 Internet Access within a PSAP

*As ESInets are planned and implemented, a review of the physical and logical security mechanisms is necessary. Presently, the most utilized method of security is to "wall off" or create a zone of protection specifically within the PSAP. If an ESInet is implemented with a walled-off approach, it may limit the full capabilities of an ESInet and minimize some of the effectiveness of full functional NG9-1-1. While legacy networks are in place this method is effective, but can limit the greater advantages that an ESInet can offer. ESInets will increase the PSAP exposure to the public int**ernet** and PSAPs must be prepared to alter their policies to accommodate the new capabilities available.*

In the strictest sense, Internet access at a PSAP must be controlled. This can be accomplished through the use of Access Control Lists (ACLs) at the edge of the ESInet. Non-ESInet authorized personnel may be granted guest Internet access on a separate service.

2.12.4 Dimensioning ESInet Data Circuits

The circuits upon which Internet-based emergency 9-1-1 calls will be delivered have some unique design considerations. Some of the following may impact final ESInet data circuit design:

- *Access to online mapping tools*
- *Potentially social media access*
- *Additional supplemental data (floor plans, campus maps)*
- *Streaming media*

2.14 Network Architecture

Connections to Internet border controllers from outside an ESInets are shown at both the regional hosts and state-level host sites. Among other things these connections could be utilized to support requirements to receive emergency 9-1-1 calls via the Internet and/or to support remote access requirements for monitoring and maintenance. »

*****Fin du document*****