Conseil de la radiodiffusion et des télécommunications canadiennes
Canadian Radio-television and Telecommunications Commission

Avis de consultation de télécom CRTC 2025-226

Version PDF

Gatineau, le 4 septembre 2025

Dossier public : 1011-NOC2025-0226

Appel aux observations – Élaboration d'une politique réglementaire sur des mesures en vue d'améliorer la résilience des réseaux de télécommunication et la fiabilité des services de télécommunication

Date limite de dépôt des interventions : 3 décembre 2025

Date limite de dépôt des répliques : 30 jours suivant la date de réception d'une lettre adressée à tous les intervenants leur conseillant de déposer des observations en réplique

[Soumettre une intervention ou voir les documents connexes]

[Soumettre vos points de vue en utilisant la plateforme de mobilisation en ligne]

Sommaire

La population canadienne doit avoir accès à des services de communication fiables, abordables et de grande qualité pour tous les aspects de sa vie quotidienne.

Les interruptions des services de télécommunication, même si elles sont de courte durée, sont très perturbantes et peuvent avoir de graves répercussions sur la vie quotidienne de la population canadienne. Toutes les interruptions peuvent avoir des effets néfastes sur les personnes, en particulier lorsqu'elles ne peuvent pas se connecter aux services d'urgence en cas de besoin.

Le Conseil, les fournisseurs de services de télécommunication et d'autres autorités gouvernementales jouent tous un rôle dans la prévention et la gestion des interruptions de services de télécommunication. Il s'agit notamment de ministères fédéraux comme Innovation, Sciences et Développement économique Canada et Sécurité publique Canada, ainsi que d'organismes provinciaux et territoriaux de gestion des urgences et de centres d'appels des services 9-1-1.

Dans le cadre de la présente consultation, le Conseil examinera des mesures que les fournisseurs de services de télécommunication (FST) devraient prendre pour améliorer la résilience des réseaux de télécommunication et la fiabilité des services de télécommunication. Le Conseil sollicite des observations portant sur : i) les principes qui devraient guider l'élaboration et la mise en œuvre de la politique réglementaire; ii) la façon dont les FST devraient concevoir et exploiter leurs réseaux pour les rendre plus résilients; et iii) la façon dont la politique réglementaire peut contribuer à la sécurité de la

population canadienne dans toutes les régions du pays, y compris les collectivités rurales et éloignées et les communautés autochtones.

Parallèlement à cette consultation, le Conseil prend deux autres mesures dans le cadre de sa stratégie plus large pour aider à atténuer les effets perturbateurs des interruptions de service sur la population canadienne. Premièrement, le Conseil aidera à améliorer la coordination en cas d'interruption majeure par l'entremise de la décision de télécom 2025-225. Il exigera des fournisseurs de services de télécommunication qu'ils informent le Conseil et les autres autorités gouvernementales dans des délais précis et qu'ils déposent des rapports complets après une interruption. Deuxièmement, le Conseil envisage des protections supplémentaires pour les consommateurs lorsque les Canadiennes et les Canadiens subissent une interruption de leurs services Internet, de leurs services sans fil, de leurs services filaires ou de leurs services de télévision, par le biais de l'avis de consultation de télécom et de radiodiffusion 2025-227. Ces protections comprennent une communication plus claire de la part des fournisseurs de services pendant les interruptions et des remboursements pour les services perdus.

Une liste complète des questions se trouve dans la section « Appel aux observations » du présent avis. Des renseignements sur les modalités de participation à la présente instance figurent plus loin dans cet avis.

Un résumé de cet avis est disponible en langue des signes québécoise (LSQ) et en American Sign Language (ASL) sur le site Web du Conseil. Le Conseil acceptera les interventions vidéo et les répliques en LSQ et en ASL.

Introduction

Pourquoi nous amorçons la présente instance

1. La population canadienne a connu des interruptions de services de télécommunication en raison de phénomènes météorologiques extrêmes, de pannes techniques ou d'autres facteurs. Ces interruptions, même si elles sont de courte durée, sont très perturbantes et peuvent avoir de graves répercussions sur la vie quotidienne de la population canadienne. Toutes les interruptions peuvent avoir des effets néfastes sur les personnes, en particulier lorsqu'elles ne peuvent pas se connecter aux services d'urgence en cas de besoin. Les réseaux doivent être résilients pour s'assurer que les services de télécommunication demeurent fiables pour la population canadienne.

2. Bien que certains fournisseurs de services de télécommunication (FST) ont fait des démarches de leur propre chef pour améliorer la résilience des réseaux et la fiabilité des services, un ensemble d'exigences minimales communes pour tous les FST favorisera la cohérence et aidera à garantir que la population canadienne continue de bénéficier de services de télécommunication fiables.

3. Avant de lancer cette instance, le Conseil a sollicité l'aide d'experts tiers pour qu'ils contribuent à déterminer des mesures réglementaires qui pourraient être nécessaires pour aider à améliorer la résilience des réseaux et la fiabilité des services. Dans le

cadre de la présente instance, on examinera les recommandations des rapports d'experts suivants, et on sollicite les observations sur celles-ci :

- Rapport sur les points de référence pour l'analyse de la résilience dans les télécommunications : Le Conseil et Innovation, Sciences et Développement économique Canada (ISDE) ont demandé à Gartner Canada Co. d'analyser et de comparer les mesures réglementaires liées à la résilience dans d'autres territoires. L'étude et le rapport qui en a découlé couvraient le Canada, les États-Unis, le Royaume-Uni, l'Australie, l'Union européenne, la France, l'Allemagne, le Japon, la Nouvelle-Zélande et la Corée du Sud.

- Évaluation de la résilience et de la fiabilité du réseau de Rogers liée à la panne du 8 juillet 2022 : Le Conseil a retenu les services de Xona Partners Inc. pour enquêter sur les causes de la panne de Rogers Communications Canada Inc. (Rogers) en juillet 2022 et pour évaluer si Rogers avait pris des mesures satisfaisantes pour remédier aux causes de la panne. Leurs conclusions ont été présentées dans un rapport, qui fournissait également des recommandations sur les mesures que peuvent prendre tous les FST pour éviter des pannes similaires.

- Résilience des réseaux de télécommunications au Canada : Une voie à suivre : Le Groupe de travail sur la résilience des réseaux canadiens de télécommunications[1] a présenté un rapport à la ministre de l'Industrie contenant une série de recommandations en matière de résilience à l'intention des FST.

- Le Groupe de travail sur la protection cybernétique des télécommunications canadiennes[2] a rédigé des rapports pour le Comité consultatif canadien pour la sécurité des télécommunications (CCCST) sur la façon d'améliorer la résilience des réseaux, et comprennent une politique sur les pratiques exemplaires en matière de sécurité, une norme de surveillance de la sécurité du réseau et de détection des risques, une norme d'intervention en cas d'incident de sécurité, une norme de gestion des fournisseurs ainsi qu'une norme de protection des infrastructures essentielles.

---

[1] Ce groupe de travail a été mis sur pied par le Comité consultatif canadien pour la sécurité des télécommunications (CCCST) et a comme objectif de formuler des recommandations pour améliorer la fiabilité des réseaux de télécommunication du Canada. Il est composé de représentants d'ISDE et de plusieurs FST.

[2] Ce groupe de travail est un sous-comité du CCCST; il travaille à promouvoir la confidentialité, l'intégrité et la disponibilité du réseau public de télécommunication dans une optique de détection, de protection, d'atténuation et de rétablissement en lien avec les cyberattaques et les indicateurs de compromission.

Cadre législatif

4. Les décisions du Conseil doivent promouvoir les objectifs stratégiques énoncés à l'article 7 de la *Loi sur les télécommunications*. La présente instance traite de trois de ces objectifs :

   - favoriser le développement ordonné des télécommunications partout au Canada en un système qui contribue à sauvegarder, enrichir et renforcer la structure sociale et économique du Canada et de ses régions (alinéa 7a));
   - permettre l'accès aux Canadiennes et aux Canadiens dans toutes les régions – rurales ou urbaines – du Canada à des services de télécommunication sûrs, abordables et de qualité (alinéa 7b));
   - satisfaire les exigences économiques et sociales des utilisateurs des services de télécommunication (alinéa 7h)).

5. En rendant ses décisions, le Conseil doit aussi mettre en œuvre les Instructions de 2023 du gouvernement du Canada[3]. Elles énoncent que le Conseil doit tenir compte de la manière dont ses décisions promeuvent la concurrence, l'abordabilité, les intérêts des consommateurs et l'innovation. Il s'agit notamment de faire en sorte qu'un accès abordable à des services de télécommunication de haute qualité, fiables et robustes soit disponible dans toutes les régions du Canada, notamment les régions rurales, les régions éloignées et les communautés autochtones[4]. Les Instructions indiquent également que le Conseil devrait continuer à prendre des mesures pour appuyer l'objectif de l'accès universel à des services Internet fixes et mobiles sans fil de haute qualité, fiables et robustes[5].

Instances connexes

6. La présente consultation, qui a pour but d'améliorer la résilience et la fiabilité des réseaux et des services de télécommunication, est un élément du Plan d'action pour protéger les consommateurs du Conseil. Dans le cadre de ce plan, le Conseil prend des mesures pour réduire la fréquence et la durée des interruptions de service dans toutes les régions du Canada, y compris dans les collectivités rurales et éloignées ainsi que les communautés autochtones.

7. En s'appuyant sur les travaux d'ISDE et du CCCST, le Conseil a annoncé un plan d'action décliné en plusieurs étapes pour élaborer un cadre réglementaire en vue d'améliorer la résilience des réseaux de télécommunication et la fiabilité des services.

---

[3] *Décret donnant au CRTC des instructions sur une approche renouvelée de la politique de télécommunication*, DORS/2023-23, 10 février 2023

[4] Voir l'alinéa 2c).

[5] Voir le paragraphe 18.

8. Comme première étape du cadre réglementaire, le Conseil a publié l'avis de consultation de télécom 2023-39, qui a mené aux exigences en matière de transmission d'avis et de production de rapports lors d'interruptions de services majeures établies dans la décision de télécom 2025-225. Le Conseil a ensuite publié la décision de télécom 2025-65, qui impose des mesures qui visent à améliorer la résilience des services 9-1-1 et du service d'alerte au public afin de réduire les répercussions des interruptions de services.

9. Au début de cette année, le Conseil a publié la politique réglementaire de télécom 2025-9, qui a pour but d'améliorer la fiabilité et l'abordabilité des services Internet dans le Grand Nord. Le Conseil a également publié l'avis de consultation de télécom et de radiodiffusion 2025-227 pour obtenir des opinions sur la manière d'améliorer les mesures de protection des consommateurs canadiens qui sont touchés par une panne ou une interruption de service. Cette consultation portera sur les mesures de protection des consommateurs pouvant aider les Canadiennes et les Canadiens à être mieux informés sur l'état de leurs services et à recevoir un remboursement ou un crédit pour un service qu'ils ne peuvent utiliser.

10. De plus, dans le cadre de son examen continu du Fonds pour la large bande, lancé par l'avis de consultation de télécom 2023-89, le Conseil examine si ce programme peut fournir du financement pour des projets qui amélioreraient la résilience des réseaux, surtout dans les régions rurales et éloignées.

11. Dans le cadre de la présente instance, le Conseil réfléchira aux mesures que les FST peuvent prendre pour améliorer la résilience des réseaux et la fiabilité des services de télécommunication en s'appuyant sur les recommandations formulées dans les rapports d'experts et les pratiques exemplaires de l'industrie.

Qu'examine le Conseil dans le cadre de la présente instance?

12. Le Conseil sollicite des observations portant sur l'élaboration et la mise en œuvre d'une politique réglementaire en vue d'aider à améliorer la résilience des réseaux de télécommunication et la fiabilité des services (politique réglementaire sur la résilience). Pour ce faire, le Conseil examinera les enjeux suivants :

    - les principes qui devraient guider l'élaboration et la mise en œuvre de la politique réglementaire sur la résilience;
    - les mesures en matière de résilience que les FST devraient prendre en considération lors de la conception de leurs réseaux;
    - les mesures en matière de résilience que les FST devraient prendre en considération dans leurs activités relatives aux réseaux;
    - l'amélioration de la fiabilité des services 9-1-1 et du service d'alertes sans fil au public;

- l’amélioration de la fiabilité des services d’accessibilité;
- l’accès aux services de télécommunication durant une situation d’urgence;
- la mise en application de la politique réglementaire sur la résilience.

13. Le Conseil invite les intéressés à lui faire part de leurs observations sur les questions susmentionnées, ainsi que sur les questions précises dans l’appel aux observations ci-dessous. Des renseignements sur la manière dont vous pouvez participer à cette instance et demander du financement figurent à la fin du présent avis.

Appel aux observations

14. Le Conseil sollicite des observations sur les questions ci-dessous. Dans chacune de vos réponses à ces questions, fournissez une justification ou encore des éléments de preuve à l’appui de votre position, y compris toute justification technique, physique ou économique.

Principes qui devraient guider l’élaboration et la mise en œuvre de la politique réglementaire sur la résilience

15. Plusieurs principes de haut niveau pourraient guider la politique réglementaire sur la résilience du Conseil. Par exemple, la politique pourrait prendre en considération que les FST devraient, entre autres choses, réaliser ce qui suit :

- s’efforcer d’assurer la disponibilité permanente des services;
- concevoir des réseaux résilients qui résistent aux perturbations;
- mettre en œuvre de solides processus d’exploitation des réseaux;
- aspirer à avoir des mécanismes immédiats d’atténuation des défaillances et de rétablissement rapide;
- déployer un réseau de communication résilient pour le personnel de rétablissement en cas d’urgence;
- s’efforcer d’établir des partenariats fiables avec des vendeurs et des fournisseurs tiers;
- se soutenir mutuellement en cas de besoin.

Q1. Quels principes, y compris ceux indiqués au paragraphe 15 ou ailleurs, le Conseil devrait-il prendre en considération dans l’établissement de la politique réglementaire sur la résilience? Comment chacun de ces principes peut-il améliorer la résilience du réseau ainsi que la fiabilité des services?

Mesures en matière de résilience que les FST devraient prendre en considération lors de la conception de leurs réseaux

16. La politique réglementaire sur la résilience relèvera des mesures de conception que les FST pourraient devoir mettre en œuvre pour garantir la résilience du réseau et la fiabilité des services. Le Conseil a relevé les domaines de conception de réseau suivants à explorer :

    a) Redondance du réseau : La redondance du réseau consiste à éliminer les points de défaillance uniques. On vise notamment à améliorer la redondance des composants du réseau, des chemins de réseau, de la géographie et de l'accès de gestion du réseau. Le déploiement d'éléments de réseau provenant de plusieurs fournisseurs ou basés sur différentes technologies peut aider à améliorer la redondance.

    b) Sécurité du réseau : La sécurité du réseau protège la confidentialité, l'intégrité et la disponibilité des réseaux. On améliore la sécurité des réseaux lorsqu'on les protège contre les accès non autorisés, les cyberattaques, les atteintes à la sécurité et la divulgation inappropriée de renseignements confidentiels sur le réseau.

    c) Infrastructure des réseaux : Les réseaux reposent sur des infrastructures physiques intérieures et extérieures qui sont souvent exposées et vulnérables aux menaces, notamment les catastrophes naturelles[6], les dommages accidentels, le vol, le vandalisme et la dégradation des structures. La mise en place de normes minimales pour protéger ces infrastructures pourrait aider les FST à éviter les dommages ou à atténuer les répercussions de ces menaces. Ces mesures comprennent le renforcement du site[7] et la détection précoce[8] des catastrophes naturelles.

    d) Alimentation électrique du réseau : Les réseaux ont besoin d'énergie électrique, qui peut provenir de diverses sources, notamment le réseau électrique, les générateurs à gaz, les batteries et l'énergie solaire. Les pannes de réseau et les interruptions de service sont souvent causées par une interruption de l'alimentation électrique en raison des catastrophes naturelles. La mise en œuvre de mesures visant à promouvoir l'approvisionnement en

---

[6] Les catastrophes naturelles comprennent les phénomènes météorologiques extrêmes tels que les tremblements de terre, les inondations, les glissements de terrain, les tsunamis et les feux incontrôlés. Pour obtenir de plus amples renseignements, consultez la page Dangers Naturels.

[7] Le renforcement du site fait référence aux mesures proactives prises par les FST pour protéger les sites du réseau contre les menaces humaines et environnementales.

[8] Des mesures de détection précoce, comme l'installation de capteurs ou de caméras ou l'utilisation de l'intelligence artificielle, peuvent aider les FST à détecter les catastrophes naturelles imminentes, ce qui les aide à mieux réagir aux menaces à leurs réseaux.

électricité ininterrompue du réseau peut contribuer à améliorer la fiabilité des services.

e) Modularisation du réseau : La modularisation du réseau est le processus de division d'un réseau en sections plus petites et plus faciles à gérer qui peuvent être facilement mises à l'échelle, remplacées ou isolées pour les mises à niveau et le dépannage. Cette pratique peut aider à éviter les pannes de réseau à grande échelle.

Q2. Les rapports d'experts au dossier de la présente instance recommandent des mesures de conception de la résilience du réseau pour les FST (voir l'annexe 1 du présent avis). Indiquez les mesures supplémentaires que les FST devraient mettre en œuvre pour les domaines de conception figurant au paragraphe 16.

a) Pour chacune de ces mesures, indiquez lesquelles devraient être obligatoires et lesquelles devraient être estimées comme des pratiques exemplaires.

b) À quels FST[9] chacune de ces mesures de résilience devraient-elles s'appliquer, et à quelle partie de leur réseau sont-elles pertinentes?

Q3. Quelles menaces pourraient endommager les infrastructures physiques du réseau[10]?

a) Comment les FST peuvent-ils évaluer ces menaces, et quelles mesures peuvent-ils prendre pour protéger les infrastructures physiques du réseau?

b) Comme il peut être nécessaire de réévaluer les mesures d'atténuation des menaces au fil du temps pour tenir compte de l'évolution de celles-ci, à quelle fréquence les FST devraient-ils réévaluer les menaces à un site du réseau?

Q4. Comment et pour quels scénarios les FST devraient-ils effectuer des simulations de crise[11]?

---

[9] Par exemple, les fournisseurs de services sans fil (FSSF), les fournisseurs de services Internet (FSI), les entreprises de services locaux (ESL)

[10] Les infrastructures physiques du réseau comprennent les câbles de transmission, les immeubles ou les vastes enceintes où on trouve de l'équipement critique du réseau de télécommunication (station cellulaire, central, tête de ligne d'un câblodistributeur, station terrestre pour les services par satellite, etc.).

[11] Une simulation de crise d'un réseau de télécommunication est le processus d'évaluer la performance et la stabilité d'un réseau en le soumettant à de fortes charges et à des conditions qui simulent un trafic élevé ou des scénarios opérationnels extrêmes. Cet exercice aide à cerner les vulnérabilités, les goulots d'étranglement et les limites des infrastructures de réseau.

Q5. Que peuvent faire les FST pour s'assurer que les abris de télécommunication[12] protègent l'équipement du réseau contre divers éléments et menaces, y compris les changements de température extrêmes, l'humidité, les vents forts et les feux?

a) Lesquelles de ces mesures devraient être obligatoires et lesquelles devraient être estimées comme des pratiques exemplaires?

Q6. Quelles mesures pourraient améliorer la résilience des réseaux ou de l'équipement dans les régions éloignées, dont certains éléments pourraient prendre des jours avant d'y accéder pour être réparés?

a) Lesquelles de ces mesures devraient être obligatoires et lesquelles devraient être estimées comme des pratiques exemplaires?

Q7. Comment les FST doivent-ils s'assurer de l'approvisionnement en électricité ininterrompue à leurs sites de réseau?

a) Comment les FST devraient-ils déterminer quels sites de réseau doivent être prioritaires pour l'alimentation de secours?

b) De quoi les FST devraient-ils tenir compte lorsqu'ils déterminent les options d'alimentation de secours les plus appropriées (p. ex. énergie solaire, batteries, génératrice à carburant)?

c) Quels paramètres les FST devraient-ils utiliser pour déterminer la durée d'alimentation de secours appropriée pour chaque type de site de réseau?

d) Comment les FST devraient-ils assurer un approvisionnement ininterrompu en carburant aux sites du réseau qui sont principalement alimentés par des génératrices à carburant, ou dont l'alimentation de secours est fournie par des génératrices à carburant?

Q8. Quelles mesures les FST peuvent-ils prendre pour tirer parti des progrès dans les services par satellite afin d'améliorer la résilience des réseaux et la fiabilité des services? Utilisez les scénarios suivants dans votre réponse :

a) Intégrer des réseaux de satellites pour améliorer la résilience de la connectivité de la liaison de raccordement et de transport;

[12] Les abris de télécommunication sont des bâtiments ou des structures qui abritent et protègent l'équipement de télécommunication, comme l'équipement radio et la fibre optique. Ils offrent également un abri pour l'équipement de données, les systèmes d'alimentation, les génératrices, l'éclairage, les systèmes d'extinction d'incendie, l'entrée de câbles, le chauffage, la ventilation et la climatisation, le rayonnage, etc.

b) Intégrer des capacités de connexion par satellite à un appareil sans intermédiaire pour améliorer la connectivité des services mobiles pendant les pannes de service ou les urgences.

Q9. Parmi les recommandations formulées dans les rapports du Groupe de travail sur la protection cybernétique des télécommunications canadiennes, indiquez lesquelles le Conseil devrait rendre obligatoires, et lesquelles devraient être estimées comme des pratiques exemplaires : Norme de protection des infrastructures essentielles pour les fournisseurs canadiens de services de télécommunications (FCST), Politique sur les pratiques exemplaires en matière de sécurité pour les fournisseurs canadiens de services de télécommunications (FCST) et Norme de surveillance de la sécurité du réseau et de détection des risques pour les fournisseurs canadiens de services de télécommunications (FCST).

Mesures en matière de résilience que les FST devraient prendre en considération dans leurs activités relatives aux réseaux

17. Les mesures de résilience dans les activités de réseau comprennent i) la création de processus pour prévenir les défaillances de réseau qui entraînent des interruptions de service, et ii) le rétablissement des services touchés le plus rapidement possible. Le Conseil a relevé les domaines d'exploitation de réseau suivants à explorer :

a) Gestion des changements : La gestion des changements comprend les processus et les pratiques utilisés par les FST lorsqu'ils apportent des modifications à un réseau. Il s'agit notamment des changements et des mises à jour de l'infrastructure réseau, du matériel et des logiciels, des configurations et des arrangements des éléments de réseau. Une bonne gestion des changements peut atténuer le risque que les changements ou les mises à jour du réseau causent une panne de service.

b) Gestion des incidents : La gestion des incidents est une approche structurée pour gérer et résoudre les perturbations imprévues au sein du réseau, y compris les défaillances matérielles et logicielles. La gestion efficace des incidents garantit qu'un incident est traité rapidement afin de minimiser l'impact sur la performance du réseau et l'expérience client.

c) Gestion de la chaîne d'approvisionnement : Les FST comptent souvent sur différents fournisseurs pour les composants et les matériaux essentiels au fonctionnement du réseau afin d'assurer des services fiables. Une chaîne d'approvisionnement résiliente comprend des fournisseurs qui offrent de l'équipement fiable et le soutien nécessaire face aux perturbations du réseau. Il s'agit également de maintenir et de situer stratégiquement un inventaire de l'équipement essentiel pour intervenir en temps opportun en cas d'interruption du réseau.

d) Gestion des risques : Des processus et des stratégies systématiques peuvent aider à cerner et à atténuer les risques complexes auxquels les FST sont confrontés. Connaître et combattre les menaces potentielles – que ce soit des menaces liées à l'infrastructure (y compris la modernisation ou la mise hors service des réseaux), ou des menaces opérationnelles, financières ou techniques (y compris la mise à niveau du réseau) – peut minimiser les résultats négatifs.

e) Modernisation de l'infrastructure : Les réseaux de télécommunication sont des infrastructures essentielles qui doivent être modernisées à mesure que la technologie évolue pour répondre aux besoins économiques et sociaux de toute la population canadienne. La modernisation de l'infrastructure consiste à remplacer les anciennes composantes du réseau par de nouvelles pièces d'équipement plus modernes. On améliore ainsi la performance, l'efficacité, la fiabilité et la sécurité d'un réseau. Prévoir et prendre des mesures proactives pour résoudre les problèmes potentiels pendant la modernisation peut aider à réduire les répercussions sur les consommateurs.

f) Préparation aux situations d'urgence : Les réseaux de télécommunication sont essentiels en cas d'urgence, et de nombreux services et agents locaux de gestion des urgences comptent sur les réseaux commerciaux. La préparation aux situations d'urgence permet de s'assurer que les FST peuvent continuer à fournir des services fiables en cas d'urgence ainsi que soutenir les efforts d'intervention en cas d'urgence et aider les collectivités à rester connectées.

g) Soutien mutuel : En septembre 2022, 12 FST ont signé un Protocole d'entente sur la fiabilité des télécommunications (protocole d'entente) pour assurer l'itinérance en cas d'urgence[13], l'assistance mutuelle et les communications avec le public et les autorités gouvernementales, en cas de défaillance critique du réseau. Le soutien mutuel entre les FST permet à la population canadienne de continuer à accéder à des services de télécommunication lorsque leur fournisseur de services subit une panne de réseau, par exemple grâce au service d'itinérance d'urgence entre les fournisseurs de services sans fil (FSSF) mis en place dans le cadre du protocole d'entente.

Q10. Les rapports d'experts versés au dossier de la présente instance présentent des recommandations de mesures de résilience que les FST devraient mettre en œuvre pour améliorer l'exploitation du réseau (voir l'annexe 2 du présent avis). Indiquez les mesures supplémentaires que les FST devraient mettre en œuvre pour les domaines d'exploitation de réseau figurant au paragraphe 17.

[13] L'itinérance en cas d'urgence permet aux clients d'un FSSF qui subit une panne de réseau d'utiliser le réseau d'un autre FSSF.

a) Pour chacune de ces mesures, indiquez lesquelles devraient être obligatoires et lesquelles devraient être estimées comme des pratiques exemplaires.

b) À quels FST[14] chacune de ces mesures de résilience devraient-elles s'appliquer, et à quelle partie de leur réseau sont-elles pertinentes?

Q11. Le Conseil devrait-il obliger les FST à préparer et à mettre en œuvre un processus de gestion des changements? Dans la négative, veuillez indiquer pourquoi et expliquer s'il faudrait plutôt considérer ces mesures comme une pratique exemplaire.

a) Quelles étapes faut-il inclure dans un processus de gestion des changements?

b) Comment les changements à un réseau doivent-ils être classés (p. ex. en fonction de l'importance de l'élément ou de la fonction de réseau qui fait l'objet du changement pour la fourniture du service) et qui devrait approuver ces changements de réseau?

c) Les FST devraient-ils être tenus de tenir un registre des changements apportés au réseau?

Q12. Le Conseil devrait-il obliger les FST à préparer et à mettre en œuvre un plan de gestion des incidents? Dans la négative, veuillez indiquer pourquoi et expliquer s'il faudrait plutôt considérer ces mesures comme une pratique exemplaire.

a) Que faudrait-il inclure dans un plan de gestion des incidents?

b) Comment les FST peuvent-ils détecter rapidement les incidents et les défaillances du réseau et déclencher le plan de gestion des incidents?

Q13. Le Conseil devrait-il obliger les FST à préparer et à mettre en œuvre des plans de gestion de la chaîne d'approvisionnement? Dans la négative, veuillez indiquer pourquoi et expliquer s'il faudrait plutôt considérer ces mesures comme une pratique exemplaire.

a) Que faudrait-il inclure dans un plan de gestion de la chaîne d'approvisionnement?

b) Quelles mesures les FST devraient-ils inclure dans leur plan de gestion de la chaîne d'approvisionnement pour réduire le temps nécessaire à la restauration des composants essentiels du réseau dans les collectivités éloignées?

Q14. Le Conseil devrait-il obliger les FST à préparer et à mettre en œuvre des stratégies d'évaluation et de gestion des risques? Dans la négative, veuillez indiquer

[14] Par exemple, les FSSF, les FSI ou les ESL

pourquoi et expliquer s'il faudrait plutôt considérer ces mesures comme une pratique exemplaire.

a) Que faudrait-il inclure dans la stratégie d'évaluation et de gestion des risques?

b) Comment les FST devraient-ils promouvoir une culture de sensibilisation au risque au sein de leur organisation dans le cadre de la stratégie de gestion des risques?

Q15. Comment les FST peuvent-ils s'assurer que leurs services de télécommunication demeurent fonctionnels pendant les pannes de courant aux installations de leurs clients?

a) Le Conseil devrait-il exiger des FST qu'ils fournissent des routeurs et des modems domestiques ayant une batterie de secours intégrée? Dans la négative, veuillez indiquer pourquoi et expliquer s'il faudrait plutôt considérer ces mesures comme une pratique exemplaire.

Q16. Le Conseil devrait-il obliger les FST à préparer et à mettre en œuvre des plans d'intervention en cas d'urgence? Dans la négative, veuillez indiquer pourquoi et expliquer s'il faudrait plutôt considérer cette mesure comme une pratique exemplaire.

a) Que faudrait-il inclure dans un plan d'intervention en cas d'urgence?

b) Les FST devraient-ils être tenus de développer et d'installer stratégiquement des installations de réseau déployables[15]? Dans la négative, veuillez indiquer pourquoi et expliquer s'il faudrait plutôt considérer cette mesure comme une pratique exemplaire.

c) Serait-il avantageux pour les FST de former les résidents des collectivités éloignées pour les aider dans les processus de rétablissement du service (p. ex. dépannage mineur du système ou redémarrage du système sous supervision à distance)? Dans l'affirmative, comment faudrait-il donner cette formation?

[15] Les installations de réseau déployables sont des installations temporaires qui peuvent être déplacées dans des zones sans couverture pour fournir une connectivité cellulaire. Elles comprennent les cellules sur roues ou les tours de téléphonie cellulaire aéroportées pour la couverture d'urgence et des génératrices mobiles.

Q17. Comment les FST peuvent-ils se soutenir mutuellement pour améliorer la résilience du réseau et la fiabilité des services, en particulier en cas d'urgence et de panne de service, par exemple par l'assistance mutuelle[16] et l'itinérance d'urgence?

a) En vertu de quel arrangement les FSSF qui ne sont pas parties au protocole d'entente devraient-ils mettre en œuvre l'assistance mutuelle et l'itinérance en cas d'urgence?

   i) Comment un FSSF offrant l'itinérance en cas d'urgence pourrait-il bénéficier d'un tel arrangement, et quelle incidence cela aurait-il sur les services du FSSF?

   ii) Quels services et niveaux de service minimaux devraient être soutenus pendant l'itinérance en cas d'urgence?

b) En vertu de quels arrangements les FST qui fournissent des services filaires mettraient-ils en œuvre l'assistance mutuelle? Ces arrangements nécessiteraient-ils des ententes ou des protocoles d'entente entre les FST? Comment devraient-ils être établis?

Q18. Le Groupe de travail sur la protection cybernétique des télécommunications canadiennes a élaboré les Normes d'intervention en cas d'incident de sécurité pour les fournisseurs canadiens de services de télécommunications pour la gestion des incidents de cybersécurité. Le Conseil devrait-il exiger que les FST mettent en œuvre ces normes? Dans la négative, veuillez indiquer pourquoi et expliquer s'il faudrait plutôt considérer ces normes comme une pratique exemplaire.

Q19. Le Groupe de travail sur la protection cybernétique des télécommunications canadiennes a élaboré la Norme de gestion des fournisseurs pour les fournisseurs canadiens de services de télécommunications. Le Conseil devrait-il exiger que les FST mettent en œuvre cette norme? Dans la négative, veuillez indiquer pourquoi et expliquer s'il faudrait plutôt considérer cette norme comme une pratique exemplaire.

Amélioration de la fiabilité des services 9-1-1 et du service d'alertes sans fil au public

18. Le système des services 9-1-1 est un pont qui relie la population canadienne aux services d'urgence en cas de besoin, et les alertes sans fil au public avertissent la population des dangers imminents ou possibles tels que les inondations, les tornades, les feux et d'autres catastrophes. Les gouvernements fédéral, provinciaux, territoriaux et municipaux, ainsi que les FST, jouent tous un rôle important pour s'assurer que la population canadienne puisse accéder aux services 9-1-1 et recevoir

[16] L'assistance mutuelle est l'aide temporaire fournie par un FST à un autre FST sous diverses formes, par exemple, le partage de biens matériels, d'équipement ou de ressources humaines, la fourniture de services demandés ou l'accès aux réseaux 9-1-1.

les alertes d'urgence. Le rôle du Conseil est de réglementer les FST qui connectent les appels 9-1-1 aux premiers répondants et qui distribuent à la population canadienne les alertes sans fil provenant des organismes de gestion des urgences gouvernementaux.

19. Les services 9-1-1 et d'alertes sans fil au public sont essentiels à la santé et à la sécurité de la population canadienne et doivent être du plus haut niveau de fiabilité. Ces services sont fournis au moyen de réseaux distincts ou spécialisés et nécessitent des considérations particulières lors de l'établissement des exigences en matière de résilience.

20. Dans les décisions de télécom 2016-165, 2018-217 et 2019-353, le Conseil a établi des exigences relatives à la résilience des réseaux 9-1-1. Dans la décision de télécom 2025-65, le Conseil a exigé des FST qu'ils mettent en œuvre des mesures supplémentaires pour améliorer la résilience des services 9-1-1 et d'alertes sans fil au public et réduire les répercussions des interruptions. Le Conseil examine actuellement un rapport (ESRE0098b) reçu du Groupe de travail Services d'urgence du Comité directeur du CRTC sur l'interconnexion portant sur la fiabilité et la résilience des réseaux 9-1-1 de prochaine génération et les pratiques exemplaires et normes en matière de sécurité *(Next Generation 9-1-1 Reliability, Resiliency, and Security Best Practices & Standards)* pour déterminer si les FST devraient mettre en œuvre les mesures recommandées.

    Q20. Quelles mesures supplémentaires les FST devraient-ils mettre en œuvre pour améliorer la fiabilité des services 9-1-1? Les mesures proposées doivent tenir compte du mandat du Conseil en tant que tribunal indépendant quasi-judiciaire dans la réglementation des FST, sans surveillance réglementaire des centres d'appels intermédiaires ou des centres d'appels de la sécurité publique.

    a) Lesquelles de ces mesures devraient être obligatoires et lesquelles devraient être estimées comme des pratiques exemplaires?

    b) Qui devrait mettre en œuvre ces mesures (p. ex. les fournisseurs de réseaux d'origine sur lesquels les appels au 9-1-1 sont effectués ou les fournisseurs de réseaux 9-1-1 responsables d'acheminer ces appels aux centres d'appels de la sécurité publique)?

    Q21. Quelles mesures supplémentaires les FSSF devraient-ils mettre en œuvre pour améliorer davantage la fiabilité du service d'alerte sans fil au public?

    a) Lesquelles de ces mesures devraient être obligatoires et lesquelles devraient être estimées comme des pratiques exemplaires?

    b) Qui devrait mettre en œuvre ces mesures (p. ex. les FSST dont les réseaux sont utilisés pour diffuser les alertes au public ou l'exploitant du Système d'agrégation et de dissémination national d'alertes qui connecte ces FSST pour diffuser les alertes sans fil au public par ces réseaux)?

Amélioration de la fiabilité des services d'accessibilité

21. Les services d'accessibilité constituent des services de télécommunication spécialisés utilisés par les personnes ayant une déficience auditive ou un trouble de la parole. Les services d'accessibilité visés dans la présente instance constituent les services de relais par téléscripteur[17] et les services de relais par protocole Internet[18]. Contrairement aux services d'urgence, les services d'accessibilité sont fournis au moyen de réseaux de télécommunication habituels. La fiabilité du service de relais vidéo a été abordée dans l'avis de consultation de télécom 2021-102 et ne sera pas prise en considération dans le cadre de la présente instance.

    Q22. Quelles mesures les FST devraient-ils mettre en œuvre pour améliorer la fiabilité des services de relais par téléscripteur et les services de relais par protocole Internet? Lesquelles de ces mesures devraient être obligatoires et lesquelles devraient être estimées comme des pratiques exemplaires?

    Q23. Quelles mesures les fournisseurs de services tiers, embauchés par les FST pour fournir des services de relais par téléscripteur et de relais par protocole Internet, devraient-ils mettre en œuvre pour améliorer la fiabilité de ces services?

    a) Comment les FST peuvent-ils s'assurer que ces fournisseurs de services tiers ont bien mis en œuvre les mesures requises?

Accès aux services de télécommunication durant une situation d'urgence

22. La population canadienne peut prendre des mesures précises pour assurer un accès continu aux services de télécommunication durant une situation d'urgence, comme les pannes de courant, les phénomènes météorologiques extrêmes et d'autres catastrophes naturelles. Le Conseil établit des politiques et des exigences en vue de s'assurer que les FST fournissent des services fiables. ISDE est l'agent de liaison en matière de préparation aux situations d'urgence concernant les télécommunications entre l'industrie des télécommunications et les organismes fédéraux, provinciaux et territoriaux de gestion des urgences. Dans le cadre de ce rôle, ISDE propose une ressource intitulée Conseils destinés aux Canadiens pour maintenir le contact durant une situation d'urgence. L'Association canadienne des télécommunications défend les intérêts des FST et informe la population canadienne des initiatives de l'industrie comme la protection des consommateurs. L'Association canadienne des télécommunications a également fourni des conseils intitulés Préparation aux

---

[17] Le service de relais par téléscripteur (SRT) est offert à tous les abonnés d'un service téléphonique de résidence au Canada. Lors d'un appel effectué à l'aide du SRT, une personne ayant une déficience auditive ou un trouble de la parole utilise un SRT et compose le 7-1-1 pour joindre un agent de relais.

[18] Le service de relais par protocole Internet est offert à tous les abonnés d'un service téléphonique de résidence ou mobile au Canada. Lors d'un appel effectué à l'aide du service de relais par protocole Internet, une personne ayant une déficience auditive ou un trouble de la parole utilise un appareil pouvant accéder à Internet (un ordinateur de bureau, un ordinateur portable, une tablette, un cellulaire, etc.) pour joindre un agent de relais en se connectant au portail Web de relais par IP du fournisseur.

phénomènes météorologiques violents et autres situations d'urgence, décrivant comment la population canadienne peut rester en contact en cas de catastrophe naturelle, de phénomène météorologique violent ou de situation d'urgence.

Q24. Compte tenu des directives fournies par ISDE et l'Association canadienne des télécommunications sur la façon dont la population canadienne peut se préparer et rester en contact durant une situation d'urgence :

a) Y a-t-il des renseignements supplémentaires que les FST devraient être responsables de fournir à la population canadienne?

b) Les FST devraient-ils être tenus d'informer la population canadienne sur la façon de se préparer et de maintenir le contact durant une situation de situations d'urgence? Dans l'affirmative, pour quels services, et quelles méthodes de communication les FST devraient-ils utiliser?

Mise en application de la politique réglementaire sur la résilience

23. Le Conseil pourrait exiger des FST qu'ils mettent en œuvre certaines mesures à la suite de la présente instance. Dans ces circonstances, le Conseil pourrait devoir imposer des mécanismes de mise en conformité et d'application de la loi.

Q25. Quelles mesures de conformité précises le Conseil devrait-il envisager pour s'assurer que les FST respectent les exigences de la politique réglementaire sur la résilience (p. ex. rapports de mise en conformité, vérifications relatives à la résilience ou surveillance)?

a) Ces mesures de conformité devraient-elles s'appliquer également à tous les FST? Dans la négative, veuillez expliquer pourquoi.

b) Comment le Conseil pourrait-il quantifier et évaluer la résilience des réseaux des FST ainsi que la fiabilité de leurs services?

Ce qu'il faut savoir pour participer à la présente instance

Procédure

24. Les *Règles de pratique et de procédure du Conseil de la radiodiffusion et des télécommunications canadiennes* (*Règles de procédure*) s'appliquent à la présente instance. Les Lignes directrices à l'égard des *Règles de pratique et de procédure du CRTC* (bulletin d'information de radiodiffusion et de télécom 2010-959) ont pour but d'aider le public à comprendre les *Règles de procédure* afin qu'il puisse participer plus efficacement aux instances du Conseil.

Déposer une intervention

25. Le Conseil invite les intéressés à déposer des observations au sujet des enjeux et des questions identifiées dans le présent avis. Il les acceptera jusqu'au **3 décembre 2025**.

26. Les intéressés qui ont besoin d'aide pour déposer des observations peuvent communiquer avec le groupe des audiences et des instances publiques du Conseil à l'adresse électronique audience@crtc.gc.ca.

27. Le Conseil encourage la participation des parties prenantes ayant de l'expertise pour garantir la résilience des réseaux de télécommunication. Cela comprend les FST, d'autres parties prenantes de l'industrie comme les organismes de normalisation et les fournisseurs d'équipement, les gouvernements (provinciaux, territoriaux et municipaux) et les organisations et communautés autochtones.

28. Tous les FST sont automatiquement désignés parties à la présente instance. Les intéressés qui déposent une intervention deviennent automatiquement partie à l'instance. Seules les parties à l'instance peuvent participer à ses étapes ultérieures.

29. Les parties peuvent recueillir, organiser et déposer, en un mémoire unique, des interventions au nom d'autres personnes intéressées qui font part de leur opinion. Des renseignements sur la manière de déposer ce type de mémoire, qu'on appelle une intervention favorable conjointe, ainsi qu'un modèle de la lettre d'accompagnement qui doit être déposée par les parties, sont présentés dans le bulletin d'information de télécom 2011-693.

30. Les mémoires doivent être déposés auprès du secrétaire général du Conseil au moyen de l'une des façons suivantes :

    - en remplissant le formulaire d'intervention du Conseil;
    - en déposant une vidéo en langue des signes québécoise (LSQ) ou en American Sign Language (ASL) à l'aide du formulaire d'intervention;
    - en envoyant une télécopie au 819-994-0218;
    - en écrivant par courrier à l'adresse suivante : CRTC, Gatineau (Québec) K1A 0N2.

31. Les mémoires de plus de cinq pages doivent comprendre un résumé. Les mémoires seront affichés dans la langue et le format officiels dans lesquels ils ont été reçus.

32. L'heure limite de dépôt des interventions au Conseil est fixée à 17 h, heure de Vancouver (20 h, heure de Gatineau). Les parties doivent veiller à ce que leurs mémoires soient déposés en temps opportun. Elles ne seront pas informées si leurs mémoires sont reçus après la date limite. Les mémoires déposés en retard ne seront pas pris en compte par le Conseil et ne seront pas versés au dossier public.

Demandes de renseignements

33. Le Conseil peut adresser des demandes de renseignements à toutes les parties à l'instance.

Déposer une réplique

34. Les parties peuvent déposer des répliques auprès du Conseil dans les **30 jours** suivant la date de réception d'une lettre adressée à tous les intervenants leur conseillant de déposer des observations en réplique. Cette lettre sera envoyée après la fin du processus de demande de renseignements ainsi que l'affichage des transcriptions des interventions vidéo en LSQ et en ASL sur le site Web du Conseil.

Avis de confidentialité

35. Veuillez porter attention aux points suivants :

- Les documents seront affichés sur le site Web du Conseil exactement comme ils ont été reçus. Ces documents comprennent tous les renseignements personnels qu'ils contiennent, tels que le nom complet, le courriel, l'adresse postale et les numéros de téléphone et de télécopieur.

- Tous les renseignements personnels que les parties fournissent dans le cadre du présent processus public, à l'exception des renseignements désignés comme confidentiels, seront affichés sur le site Web du Conseil et pourront être consultés par d'autres personnes.

- Toutefois, les renseignements et les transcriptions des vidéos en LSQ et en ASL que les parties fournissent ne peuvent être consultés qu'à partir de la page Web de ce processus public. Par conséquent, une recherche généralisée du site Web du Conseil, à l'aide de son moteur de recherche ou de tout autre moteur de recherche, ne permettra pas d'accéder directement aux renseignements fournis dans le cadre de ce processus public.

- Les renseignements personnels fournis par les parties peuvent être divulgués et seront utilisés aux fins auxquelles ils ont été recueillis ou compilés par le Conseil, ou pour un usage qui est compatible avec ces fins.

Confidentialité

36. Les instances du Conseil sont conçues pour permettre au public d'apporter leur contribution afin qu'il puisse prendre de meilleures décisions plus éclairées. Par conséquent, la règle générale est que tous les renseignements déposés auprès du Conseil sont versés au dossier public et peuvent être examinés par toutes les parties et le public.

37. Cependant, le Conseil a souvent besoin de renseignements détaillés de la part des entreprises qu'il réglemente et supervise pour prendre une décision éclairée. Ces

renseignements peuvent être commercialement sensibles, d'autant plus que l'environnement dans lequel les entreprises exercent leurs activités devient de plus en plus concurrentiel. Le Conseil acceptera donc de considérer certains renseignements confidentiels.

38. Les parties peuvent demander que ces renseignements soient déposés à titre confidentiel en vertu du paragraphe 39(1) de la *Loi sur les télécommunications*, avec une justification détaillée des raisons pour lesquelles ces renseignements doivent être considérés confidentiels. Le Conseil rappelle aux parties qui font une telle demande que lorsqu'un document contenant des renseignements confidentiels est déposé, une version abrégée doit également être déposée afin d'être incluse dans le dossier public.

Formats accessibles

39. Le Conseil exige des entités réglementées qu'elles déposent leurs mémoires dans le cadre des instances du Conseil dans des formats accessibles (p. ex. des formats de fichier texte dont le texte peut être agrandi ou modifié, ou lu par un lecteur d'écran), et il encourage toutes les parties à faire de même. Pour lui faciliter la tâche, le Conseil a affiché sur son site Web des lignes directrices pour la préparation des documents en formats accessibles.

40. Si un document n'a pas été déposé dans un format accessible, vous pouvez communiquer avec le groupe des audiences et des instances publiques du Conseil à l'adresse électronique audience@crtc.gc.ca pour demander au personnel du Conseil d'obtenir ce document dans un format accessible auprès de la partie qui l'a initialement déposé.

41. Le Conseil accepte les mémoires en LSQ ou en ASL en format vidéo. Le Conseil publiera les liens vers les vidéos des parties sur son site Web. Les autorisations sur les vidéos doivent être publiques. Le Conseil n'acceptera pas les liens qui exigent que quelqu'un demande l'accès aux vidéos. Les liens sur le site Web du Conseil redirigeront les utilisateurs vers les vidéos telles qu'elles ont été téléchargées, et les utilisateurs auront accès à tous les renseignements personnels affichés sur la plateforme d'hébergement vidéo. Les vidéos seront entièrement traduites en texte et une transcription sera disponible en français pour les vidéos en LSQ et en anglais pour les vidéos en ASL.

Faire part de vos points de vue sur Conversations CRTC

42. Les personnes ont jusqu'au **3 décembre 2025** pour transmettre leurs points de vue sur Conversations CRTC, la plateforme de mobilisation en ligne.

43. La plateforme facilite la participation des personnes qui pourraient moins bien connaître les processus du Conseil. Elle comprend certaines questions seulement.

44. Toutes les observations reçues au moyen de Conversations CRTC seront versées au dossier public de la présente instance.

45. Veuillez noter que :

- les renseignements fournis sont saisis dans une base de données consultable sur la plateforme de mobilisation;
- les observations seront attribuées au nom d'utilisateur donné lors du processus d'inscription sur la plateforme;
- ces observations et noms d'utilisateur sont consultables à l'aide de moteurs de recherche tiers;
- les renseignements personnels fournis par l'intermédiaire de cette plateforme pourraient être retrouvés lors d'une recherche. Ces renseignements peuvent être divulgués et seront utilisés aux fins auxquelles ils ont été recueillis ou compilés par le CRTC, ou pour un usage qui est compatible avec ces fins.

46. Les personnes qui donnent leur avis au moyen de Conversations CRTC ne seront pas considérées comme des parties à l'instance. En général, cela signifie qu'elles ne recevront pas d'avis concernant d'autres observations, des requêtes procédurales ou des changements, qu'elles ne pourront pas participer à une audience, et qu'elles ne pourront pas être nommées dans le cadre de tout appel de la décision du Conseil (ni tenues d'y participer).

47. Pour devenir partie à la présente instance, les personnes intéressées doivent déposer une intervention formelle au moyen du formulaire en ligne, par télécopieur, par la poste ou par vidéo en LSQ ou en ASL. Les détails sur la façon de déposer une intervention formelle sont fournis ci-dessus.

Accéder aux documents

48. On peut accéder aux interventions, ainsi qu'à d'autres documents dont il est question dans le présent avis, en cliquant sur les liens dans la page Consultations et audiences : donnez votre avis du Conseil.

49. Les documents sont disponibles sur demande, pendant les heures normales de bureau. Veuillez contacter :

Centre de documentation
Examinationroom@crtc.gc.ca
Tél. : 819-997-4389
Téléc. : 819-994-0218

Service à la clientèle
Téléphone sans frais : 1-877-249-2782
ATS sans frais : 1-877-909-2782

50. Les intéressés peuvent trouver les versions électroniques des documents en cliquant sur « [Soumettre une intervention ou consulter les documents connexes] » en haut du présent avis.

Secrétaire général

Documents connexes

- *Appel aux observations – Protection des consommateurs en cas de panne ou d'interruption de service*, Avis de consultation de télécom et de radiodiffusion CRTC 2025-227, 4 septembre 2025

- *Exigences en matière de transmission d'avis et de production de rapports lors d'interruptions de services de télécommunication majeures*, Décision de télécom CRTC 2025-225, 4 septembre 2025

- *Groupe de travail Services d'urgence et Groupe de travail Réseau du Comité directeur du CRTC sur l'interconnexion – Rapport de consensus NTRE081 sur les mesures en vue d'améliorer la résilience des services 9-1-1 et des services d'alertes au public et de réduire les répercussions des pannes*, Décision de télécom CRTC 2025-65, 28 février 2025

- *Les télécommunications dans le Grand Nord*, Politique réglementaire de télécom CRTC 2025-9, 16 janvier 2025

- *Appel aux observations – Examen de la politique sur le Fonds pour la large bande*, Avis de consultation de télécom CRTC 2023-89, 23 mars 2023; modifié par les Avis de consultation de télécom CRTC 2023-89-1, 17 avril 2023; et 2023-89-2, 25 juillet 2024

- *Appel aux observations – Élaboration d'un cadre réglementaire pour améliorer la fiabilité et la résilience des réseaux – Obligations en matière de transmission d'avis et de production de rapports lors d'interruptions de services de télécommunication majeures*, Avis de consultation de télécom CRTC 2023-39, 22 février 2023; modifié par l'Avis de consultation de télécom CRTC 2023-39-1, 11 septembre 2023

- *Appel aux observations – Examen du service de relais vidéo*, Avis de consultation de télécom CRTC 2021-102, 11 mars 2021; modifié par les Avis de consultation de télécom CRTC 2021-102-1, 26 avril 2021; 2021-102-2, 30 juin 2021; 2021-102-3, 14 mars 2022; et 2021-102-4, 19 septembre 2023

- *Groupe de travail Services d'urgence du CDCI – Rapport de consensus sur les questions liées à la compatibilité, à la fiabilité, à la résilience et à la sécurité des services 9-1-1 de prochaine génération*, Décision de télécom CRTC 2019-353, 22 octobre 2019

- *Rapports de consensus du Groupe de travail Services d'urgence du CDCI – Service 9-1-1 de prochaine génération – Facteurs techniques et opérationnels et éléments logistiques des essais*, Décision de télécom CRTC 2018-217, 28 juin 2018

- *Questions ayant trait à la fiabilité et à la résilience des réseaux 9-1-1*, Politique réglementaire de télécom CRTC 2016-165, 2 mai 2016

- *Dépôt de mémoires en formats accessibles pour les instances du Conseil*, Bulletin d'information de radiodiffusion et de télécom CRTC 2015-242, 8 juin 2015

- *Dépôt d'interventions favorables conjointes*, Bulletin d'information de télécom CRTC 2011-693, 8 novembre 2011

- *Lignes directrices à l'égard des* Règles de pratique et de procédure du CRTC, Bulletin d'information de radiodiffusion et de télécom CRTC 2010-959, 23 décembre 2010

Annexe 1 de l'Avis de consultation de télécom CRTC 2025-226

Recommandations concernant des mesures de conception favorisant la résilience

Les recommandations suivantes sont tirées du rapport *Évaluation de la résilience et de la fiabilité du réseau de Rogers liée à la panne du 8 juillet 2022* (rapport de Xona Partners) :

1	Mettre en œuvre une protection contre la surcharge des routeurs dans les réseaux IP [protocole Internet] centraux et de distribution.
2	Séparer physiquement et logiquement la couche de gestion du réseau du réseau de données.
3	Fournir au centre d'exploitation du réseau et à d'autres sites distants critiques une connectivité de secours sécurisée provenant d'exploitants de réseaux de télécommunication tiers.

Les recommandations suivantes sont tirées du rapport *Résilience des réseaux de télécommunications au Canada : Une voie à suivre* (rapport du Comité consultatif canadien pour la sécurité des télécommunications [CCCST]) :

4	Lorsque cela est possible, la conception des réseaux cœurs des FCST [fournisseurs canadiens de services de télécommunication] doit tenir compte de la possibilité d'une perte d'accès physique des travailleurs aux centres d'opérations, bâtiments ou sites. En cas de restriction temporaire de l'accès du personnel, des procédures doivent être mises en place pour informer les employés qui travaillent habituellement dans un centre d'opérations, un bâtiment ou un site donné. Les plans d'urgence devraient englober les aspects liés à la communication avec les services d'intervention d'urgence concernant l'accès physique afin de maintenir les services essentiels.
5	Il convient d'avoir recours à des équipements et systèmes fiables (provenant de fournisseurs compétents), lorsque cela est possible, conçus dans le but de prévenir les effets des conditions extrêmes, notamment la perte de l'alimentation électrique, et de résister à de telles conditions.
6	Lorsque cela est possible, les FCST devraient avoir recours à des méthodes telles que l'acheminement prioritaire, les tentatives répétées, le réacheminement et la réservation de circuits afin d'éviter de dépendre d'un seul ensemble d'équipements pour le traitement du trafic d'urgence en provenance du public.
7a	Dans le cas d'équipements contrôlés par un logiciel, celui-ci doit être conçu, lorsque cela est possible, de manière à réduire au minimum la possibilité qu'une erreur logicielle se propage dans tout le système ou à d'autres équipements, et à être protégé contre les interférences externes involontaires.

7b	En outre, la fonctionnalité d'« application automatique » doit être désactivée sur les équipements de réseau afin d'éviter les risques liés à l'application immédiate d'un nouveau logiciel ou correctif sur le réseau.
8	Afin d'éviter les défaillances en chaîne, il convient d'envisager, dans la mesure du possible, la mise en place de réseaux à couches doubles ou à double maillage fournis par des fournisseurs distincts.
9	Les FCST doivent planifier au mieux de leurs capacités les mesures à prendre pour atténuer les menaces liées à la signalisation. Lorsque cela est possible, les FCST devraient s'efforcer de minimiser les répercussions des messages de signalisation inappropriés susceptibles d'entraîner un mauvais fonctionnement du réseau ou des systèmes connexes.
10	Les FCST doivent planifier au mieux de leurs capacités les mesures à prendre pour atténuer les menaces liées au volume de trafic. Les FCST doivent appliquer, dans la mesure du possible, des contrôles de gestion des réseaux pour limiter les répercussions et la transmission de volumes de trafic excessifs, mais pas plus que ce qui est raisonnablement nécessaire pour maximiser l'établissement d'appels vocaux efficaces ou de connexions de données en temps opportun.
11	Les FCST doivent avoir pour objectif de se conformer aux normes techniques de mise en réseau applicables, compte tenu notamment du fait que des mauvais signaux reçus de l'extérieur du domaine d'un FCST peuvent interférer avec le bon fonctionnement de son réseau. Ces signaux peuvent être bénins et découler d'un mauvais fonctionnement accidentel de l'équipement. Cependant, les mauvais signaux peuvent aussi être le fait de tentatives délibérées d'interférer avec un réseau. On peut mentionner par exemple les tentatives délibérées de ne pas payer adéquatement les services d'un réseau (fraude téléphonique), les dénis de service à des tiers et les tentatives de corruption de données ou de logiciels stockés. Plusieurs niveaux de sécurité doivent être envisagés pour contrer ces menaces, notamment des mécanismes de surveillance de la signalisation, des pare-feu, des processus de communication entre les intervenants concernés et des instruments opérationnels pour assurer l'harmonisation de la compréhension des effets et de la planification des interventions.
12	Les FCST peuvent envisager des mesures appropriées pour veiller à ce que leurs réseaux soient protégés des problèmes liés à la signalisation ou aux couches de commande dans un contexte caractérisé par l'interconnexion des réseaux. La méthode du filtrage (ou surveillance) pourrait être utilisée à la périphérie des réseaux par les FCST pour se protéger contre les risques de fonctionnement inadéquat des réseaux connectés. Il serait raisonnable de prévoir le filtrage des liens d'interconnexion pour s'assurer que seules les utilisations répondant aux modalités convenues sont autorisées et entreprises. En outre, la surveillance de protocoles tels que le protocole SS7 faciliterait la détection du trafic anormal, permettant aux FCST de gérer les possibles menaces de manière appropriée.
13	Lorsque cela est approprié et économiquement possible, les FCST peuvent envisager de mettre en œuvre diverses voies ou routes de conduits, car la séparation physique des fibres ne garantit pas à elle seule la disponibilité. Si cela est économiquement et physiquement possible, il est recommandé aux FCST de chercher à combiner plusieurs routes physiques distinctes afin de renforcer la redondance et la résilience de leur infrastructure de réseau.

14	Lorsque cela est approprié, les FCST doivent s'assurer que tous les éléments des réseaux cœurs sont accessibles par l'entremise d'un réseau physique séparé hors bande ou d'un lien vers les éléments du réseau essentiel.
15	Pendant la conception de réseaux de routage IP, il convient d'envisager des mesures de protection appropriées afin d'éviter que les bases de données ou les tables de routage des routeurs ne soient surchargées. Cela permettra d'éviter les défaillances en cascade dans le réseau de routage et d'accélérer les délais de rétablissement en cas de défaillance imprévue.
16	Lorsque cela est possible, les FCST devraient viser une segmentation générale de base des services et des éléments du réseau. Les FCST doivent veiller, au mieux de leurs capacités, à ce que la défaillance d'un ou de plusieurs éléments de réseau dans un segment ou une région n'entraîne pas de défaillance des services dans d'autres segments ou régions.
17	Il doit y avoir une diversité et une redondance adéquates au sein des différents segments et régions du réseau, de sorte qu'une défaillance dans un segment ou une région n'ait pas d'incidence sur la prestation globale du service.
18	Lorsque cela est possible, les FCST doivent s'efforcer d'éviter les points de défaillance uniques dans n'importe quelle partie du réseau essentiel, afin de réduire au minimum les pertes de service causées par les défaillances d'éléments individuels du réseau.
19	Lorsque cela est économiquement et physiquement possible, les FCST doivent s'efforcer de fournir une géo-redondance adéquate pour tous les éléments et serveurs centralisés des réseaux cœurs, notamment les serveurs d'authentification, les serveurs DHCP (protocole de configuration dynamique des hôtes), les serveurs de routage, etc.
20	Les FCST sont tenus de fournir, dans la mesure du possible, des mécanismes adéquats de ralentissement artificiel du trafic et de priorisation pour tous les systèmes de contrôle et de signalisation afin d'éviter les tempêtes de signaux et les défaillances des systèmes susceptibles d'en résulter.
21	Adoption des pratiques exemplaires et des normes du CCCST : Il convient que les FCST examinent les principes de conception et les contrôles décrits dans la Politique sur les pratiques exemplaires en matière de sécurité du CCCST et dans la Norme de protection des infrastructures essentielles connexe et les appliquent à leurs réseaux, le cas échéant.
22	Mise en œuvre d'une infrastructure à clé publique (ICP) de ressource : Les FCST doivent poursuivre leurs efforts pour mettre en place une ICP de ressource, qui correspond à la signature cryptographique de la propriété des routes BGP (protocole de passerelle frontière) dans leur infrastructure de réseau.
23	Surveillance des routes BGP : Afin d'améliorer la capacité d'intervention nationale en cas d'événements relatifs au protocole BGP menaçant la résilience des réseaux de télécommunications, les FCST doivent mettre en place un processus de surveillance des routes pour détecter et consigner toute activité anormale.

24	Filtrage anti-usurpation : Les FCST sont invités à mettre en œuvre un mécanisme de filtrage anti-usurpation pour bloquer le trafic provenant d'adresses IP usurpées, lorsque cela est possible.
25	Authentification multifactorielle (AMF) : Les FCST devraient mettre en œuvre des mécanismes d'AMF robustes pour l'accès aux dispositifs des réseaux cœurs, et élargir le processus d'authentification à facteurs multiples aux comptes des opérateurs et des administrateurs des réseaux. Des directives détaillées sur l'AMF doivent être incorporées dans la Politique sur les pratiques exemplaires en matière de sécurité du CCCST et dans la Norme de protection des infrastructures essentielles qui l'accompagne.
26	Les considérations relatives aux contrôles supplémentaires, ou équivalents, nécessaires pour limiter ou réduire l'incidence des réactions en chaîne résultant d'un événement cybernétique, peuvent inclure les mesures suivantes : • la redondance des couches d'utilisateurs; • la segmentation du réseau; • la diversité de la chaîne d'approvisionnement.
27	Lorsque cela est possible, les systèmes contrôlés par logiciel doivent être tolérants aux anomalies et être conçus et déployés de manière à réduire au minimum la possibilité qu'une erreur logicielle se propage dans tout le système ou à d'autres équipements, et être protégés contre les interférences externes accidentelles ou planifiées.
28	Les FCST et le gouvernement devraient influencer conjointement les fabricants de pièces d'origine afin de normaliser le comportement des appareils mobiles si un événement déclencheur a une incidence sur les services 911.
29	Lorsque c'est physiquement et économiquement possible, il convient d'envisager et de mettre en place un réseau de liaison mobile pour le réseau cellulaire en ayant recours à la diversité physique et logique, de manière à disposer d'un minimum de deux chemins indépendants et distincts.
30	La diversité des chemins peut faire appel à plusieurs technologies pour éviter la congestion et, en cas de panne, chaque chemin doit pouvoir accueillir un niveau raisonnablement élevé de trafic prioritaire (p. ex. services d'urgence), lorsque cela est possible.
31	En cas de congestion à la suite d'une panne sur un réseau multiservice, lorsque cela est possible, il est recommandé de configurer des mécanismes d'assurance de qualité du service et d'établissement de priorités pour protéger le trafic et les services classés comme essentiels ou hautement prioritaires.

32	Les FCST doivent, lorsque cela est possible, évaluer les menaces environnementales qui pèsent sur leurs installations extérieures et, lorsque cela est économiquement et physiquement possible, chercher à atténuer ou à prévenir les dommages éventuels que pourraient causer à leurs installations des phénomènes météorologiques tels que (liste non exhaustive) : • la pression exercée par les vents extrêmes et les vibrations causées par le vent; • les vibrations causées par les tremblements de terre; • les dommages causés par la foudre; • les feux de forêt et les incendies en général; • l'eau (inondations, immersion dans l'eau, tsunamis); • la glace et les périodes prolongées sous le point de congélation; • les vents chargés de sel; • les gaz corrosifs; • les poussières; • les températures extrêmes et les variations de température; • l'humidité et la rouille causée par l'humidité.
33	Les FCST doivent, lorsque cela est possible, évaluer les menaces environnementales qui pèsent sur leurs installations intérieures et, lorsque cela est économiquement et physiquement possible, chercher à atténuer ou à prévenir les dommages éventuels que pourraient causer à leurs installations des phénomènes météorologiques tels que (liste non exhaustive) : • les tremblements de terre de petite ou grande ampleur; • les dommages causés par la foudre; • les incendies; • les inondations.

34	Au moment de déterminer l'emplacement et la composition structurelle d'un bâtiment abritant des infrastructures de télécommunications, les FCST doivent s'assurer que le bâtiment pourra résister, lorsque cela est possible, aux répercussions négatives des éléments suivants (liste non exhaustive) : • des tempêtes; • les inondations; • les dommages causés par le vent ou l'eau; • les champs électromagnétiques puissants – des écrans électromagnétiques doivent être installés dans les salles de machines, le cas échéant; • les tremblements de terre; • les incendies – des mécanismes d'extinction des incendies doivent être installés de manière appropriée.
35	En ce qui concerne les nouvelles installations hébergeant ou offrant des services essentiels ou lorsque les sites ont subi une inondation ou un tremblement de terre par le passé, il faut prendre des mesures particulières pour veiller à ce que les services essentiels puissent, lorsque cela est possible, être maintenus en cas d'inondation ou de tremblement de terre (le service peut être assuré à partir d'un site de rechange non exposé aux mêmes risques que le site principal). Les répercussions d'une inondation ou d'un tremblement de terre sur les intrants clés doivent également être prises en compte (intrants en énergie comme l'électricité ou le mazout, accès du personnel).
36	Dans la mesure du possible, il convient d'éviter de concentrer les équipements essentiels au point de compromettre la sécurité globale du réseau, en particulier dans un seul bâtiment. Lorsque des équipements essentiels sont situés au même endroit (par exemple, dans un site hébergeant des processeurs multiples), il faut privilégier une séparation physique telle qu'un coupe-feu afin de réduire la possibilité d'une défaillance de mode commun.
37	Lorsque cela est approprié et réalisable, il faut prévoir divers points d'entrée et de sortie (p. ex. des sites ou des bâtiments), y compris en ce qui concerne les entrées de câbles.
38	Lorsque cela est approprié et réalisable, les FCST doivent utiliser divers chemins ou routes de conduits. (Remarque : La séparation physique n'est pas suffisante en soi pour garantir la disponibilité, celle-ci étant généralement le fruit d'une combinaison de facteurs comprenant la séparation physique, la redondance et la résilience.)
39	Les équipements extérieurs doivent être placés de manière à minimiser les risques, lorsque cela est possible, par exemple les risques associés aux accidents de la route ou au vandalisme, et doivent être verrouillés et étanches.
40	Dans la mesure du possible, pour chaque nouvelle installation de fibre optique ou modification d'un réseau de fibre optique existant, les FCST doivent envisager de mettre

	en place un processus interne pour consigner les coordonnées géographiques précises dans une base de données interne.
41	Dans la mesure du possible, les principaux centres régionaux des FCST doivent être décentralisés.
42	Le centre régional principal d'un FCST doit pouvoir bénéficier du soutien d'autres centres régionaux, lorsque cela est possible.
43	Lorsque cela est possible, les centres régionaux essentiels doivent être reliés à d'autres centres régionaux par un chemin de déviation afin de minimiser l'impact d'une interruption du chemin de connexion initial.
44	Les installations de transport reliant les principaux centres régionaux doivent être physiquement redondantes (chemins multiples), lorsque cela est possible.
45	Les installations principales d'accès à la fibre optique doivent être installées de manière à constituer deux ou plusieurs chemins physiquement distincts chaque fois que cela est possible.
46	Les lignes de télécommunication reliant les principaux centres régionaux doivent être installées dans des installations de transport différentes chaque fois que cela est possible.
47	Les principales installations de transport des FCST doivent permettre de transférer les liaisons de télécommunications vers d'autres liaisons aussi rapidement que possible, si nécessaire.
48	Les principales installations de transport et les liaisons de télécommunications doivent être dotées d'une fonction permettant de surveiller l'exploitation, de détecter immédiatement les défaillances et de rendre compte de l'état des opérations, et ce de manière intégrée.
49	Lors de l'installation d'installations de transmission à chemins multiples, les FCST doivent prévoir de mettre en place des chemins géographiquement séparés et diversifiés dans la mesure où cela est physiquement et économiquement possible, afin d'atténuer les risques locaux provenant des autres chemins.
50	Lorsque l'accès de routine à un site aux fins d'entretien risque d'être compromis en raison du mauvais temps, il convient de prévoir dans les plans d'urgence des dispositions relatives à l'utilisation de moyens de transport de rechange appropriés (p. ex., véhicules à quatre roues motrices, dameuses à neige, hélicoptères). Dans les lieux sujets aux inondations, les bâtiments doivent être conçus pour que les fonctions les plus importantes soient réalisées dans les zones les moins exposées.
51	Les FCST doivent s'efforcer de disposer d'équipements redondants et d'équipement de rechange en cas de défaillance ou de dégradation des équipements d'origine, qu'ils soient intérieurs ou extérieurs.

52	Les FCST doivent envisager de mettre en place dans les installations intérieures importantes une fonction d'alerte capable de détecter sans délai les défaillances et de les signaler. Lorsque cela est possible, les installations intérieures dépourvues de personnel doivent disposer d'une fonction de rapport à distance en cas de défaillance, ou d'un système d'alerte de rechange comparable.
53	L'emplacement de toutes les installations de lignes externes telles que les câbles souterrains et aériens doit être communiqué aux autorités compétentes lorsque cela est approprié (p. ex. adhésion au service provincial d'appel unique ou aux services équivalents).
54	Des processus opérationnels appropriés doivent être mis en place pour coordonner les activités des différents services publics et des administrations routières pour veiller à réduire au minimum les risques de dommages.
55	Dans la mesure du possible, les poteaux doivent être installés aux emplacements les moins risqués en fonction de leur utilisation. L'emplacement des câbles aériens et des fils d'embranchement est soumis à des règlements plus larges; ces derniers doivent être installés de manière à permettre un espace libre suffisant pour les véhicules, les terrains et les bâtiments. Les fournisseurs de services publics doivent s'assurer de l'intégrité physique continue des infrastructures partagées comme les poteaux et les pylônes au moyen d'enquêtes régulières. Ils doivent évaluer et communiquer aux FCST tout nouveau risque pour l'intégrité des structures partagées (p. ex. la croissance des arbres).
56	Lorsqu'un système de ventilation ou de climatisation est employé, il faut éviter, dans la mesure du possible, qu'une seule défaillance ne dégrade les installations, et surveiller à distance les infrastructures essentielles de refroidissement pour pouvoir intervenir rapidement en cas d'incident.
57	Il est recommandé d'installer, au besoin, des systèmes appropriés de détection et d'extinction des incendies, des systèmes de détection des gaz explosifs et asphyxiants, et des systèmes de détection des inondations.
58	Dans la mesure du possible, les alarmes incendie automatiques et les systèmes d'extinction doivent être déployés de manière appropriée dans les bâtiments et les salles des machines.
59	L'entretien normal du site devrait être effectué régulièrement, dans la mesure du possible. Dans le cas où l'accès à un site est compromis à cause du mauvais temps, des redondances doivent être mises en place pour soutenir la stabilité du service.
60	La sécurité des lieux est un facteur clé du maintien de l'intégrité des services de télécommunications. La protection dont bénéficie un bâtiment doit être évaluée et correspondre à un protocole de sécurité.
61	Les bâtiments doivent être protégés contre toute intrusion de personnes non autorisées. Il convient d'être en mesure de démontrer que le niveau de sécurité des bâtiments est adéquat et proportionnel à l'évaluation des niveaux de risque et de vulnérabilité. Il peut être nécessaire de mettre en place des systèmes d'entrée sécurisés, des détecteurs de

	mouvement et des systèmes de vidéosurveillance. Dans les grands bâtiments, un système de sécurité périmétrique et cellulaire peut être approprié.
62	L'alimentation électrique des équipements clés ne doit pas être interrompue en cas de défaillance de l'alimentation principale et, lorsque cela est approprié et faisable, les FCST peuvent chercher à acquérir diverses sources d'alimentation principale pour protéger les principaux sites contre les défaillances de l'alimentation électrique.
63a	Dans la mesure du possible en cas de défaillance de l'alimentation principale, l'alimentation de secours doit être d'une capacité suffisante pour supporter toute la charge opérationnelle pendant la période entre le début de la défaillance et le transfert à l'alimentation de secours disponible.
63b	Dans la mesure du possible, des génératrices doivent être disponibles grâce à une combinaison de génératrices sur place dans les installations désignées comme prioritaires et de génératrices hors ligne entreposées à des endroits stratégiques du réseau pour soutenir les efforts de reprise après sinistre lorsque la liaison est encore fonctionnelle et qu'une protection est nécessaire.
64	Dans les sites où il n'est pas possible de fournir une alimentation de secours sur place (c.-à-d. des génératrices), les FCST doivent envisager de concevoir des batteries capables de couvrir la durée des interruptions généralement observées de l'alimentation principale ou le temps nécessaire au déplacement d'une génératrice portative sur place.
65	Lorsque l'alimentation provient de batteries, les FCST doivent tenir compte des points suivants en ce qui concerne l'utilisation des batteries : • Les batteries sont capables d'assurer le maintien des services, quel que soit le stade de leur durée de vie; • Les conditions relatives au site, l'espace et les autorisations nécessaires au bon fonctionnement des batteries sont planifiés à l'avance; • Les batteries sont entretenues conformément aux recommandations des fabricants, ce qui comprend le respect des recommandations concernant la décharge complète des batteries de manière régulière; • Le motif et la durée de l'utilisation des batteries sont dûment consignés.
66	Les FCST doivent effectuer des essais et un entretien régulier de leurs systèmes d'alimentation de secours pour veiller à ce qu'ils fonctionnent de manière satisfaisante dans des situations de défaillance.
67	Les FCST doivent prendre des dispositions adéquates pour disposer de réserves de carburant pour les génératrices de secours et mettre en place des contrats de réapprovisionnement.
68	Les FCST doivent prendre des dispositions pour atténuer la menace que représentent les conditions électriques et s'efforcer de mettre en place des interfaces de réseau capables de soutenir ou d'empêcher la transmission de signaux électriques ou les conditions qui se situent en dehors des valeurs de fonctionnement normalement prévues.

69	Dans la mesure du possible, les emplacements non couverts par un chevauchement des services doivent être équipés d'une batterie de secours.
70	En cas d'urgence, les FCST devraient bénéficier d'un accès prioritaire à leurs installations, d'un accès prioritaire et fiable aux carburants et aux génératrices, et d'un rétablissement prioritaire de l'alimentation électrique.

Annexe 2 de l'Avis de consultation de télécom CRTC 2025-226

Recommandations de mesures en vue d'améliorer la résilience d'exploitation du réseau

Les recommandations suivantes sont tirées du rapport *Évaluation de la résilience et de la fiabilité du réseau de Rogers liée à la panne du 8 juillet 2022* (rapport de Xona Partners) :

1	Veiller à ce que le processus de vérification des changements de configuration du réseau soit efficace et implique différentes équipes au sein de l'organisation, comme l'ingénierie, les opérations et la gestion de projet. Il est également conseillé d'impliquer les fournisseurs d'équipement lorsque les changements de configuration concernent des infrastructures critiques, comme le réseau central IP [protocole Internet].
2	Effectuer des tests en laboratoire des changements de configuration prévus et s'assurer que l'équipement de laboratoire et les scénarios de test reflètent fidèlement le réseau de production.
3	Gérer avec soin le nombre de changements de configuration effectués au cours d'une seule fenêtre de maintenance et tirer parti des outils et des processus pour le retour automatisé des paramètres de configuration.
4	Mettre en œuvre une solution automatisée de hiérarchisation des alarmes afin de supprimer les alarmes inutiles pour chaque type de changement et de permettre au personnel de se concentrer sur les alarmes importantes.
5	Fournir au personnel critique des moyens de communication secondaires, tels que des cartes SIM [Subscriber Identity Module (module d'identité d'abonné)] d'exploitants de réseaux tiers.
6	Simuler et pratiquer des scénarios de défaillance et de panne du réseau afin de mettre en évidence les lacunes de l'architecture du réseau et du processus de gestion des incidents.
7	Mettre en œuvre des formations et des exercices de réponse aux incidents afin de découvrir les faiblesses de l'architecture, des opérations et des processus opérationnels qui ont une incidence négative sur les efforts de rétablissement des pannes.
8	Mettre en place des indicateurs de rendement clés pour la réponse à la gestion des incidents afin d'évaluer l'effort de réponse aux incidents et d'en améliorer l'efficacité.
9	Définir clairement les rôles et les responsabilités du personnel afin de mieux répondre aux pannes de réseau.
10	Envisager de calculer l'incidence financière d'une panne de réseau afin d'atténuer les conséquences des incidents en prenant des décisions sur l'affectation des ressources et en communiquant avec les intervenants pour préserver l'image de marque et la stabilité financière.

Les recommandations suivantes sont tirées du rapport *Résilience des réseaux de télécommunications au Canada : Une voie à suivre* (rapport du Comité consultatif canadien pour la sécurité des télécommunications [CCCST]) :

11	Autant que possible, les FCST [fournisseurs canadiens de services de télécommunication] devraient conserver des stocks adéquats de pièces de rechange et de fournitures consommables sur place ou dans un dépôt facile d'accès situé à proximité des sites. De plus, les FCST peuvent envisager de conclure des contrats avec des fournisseurs pour qu'ils conservent des stocks tampons au nom du prestataire. Une attention particulière doit être portée aux articles provenant de l'étranger, qui sont susceptibles d'être touchés par des perturbations de transport ou de communication. Les risques pour la sécurité posés par les interruptions possibles de la chaîne d'approvisionnement doivent être pris en compte.
12	Lorsque cela est possible, les FCST devraient avoir des processus opérationnels efficaces englobant au minimum les domaines suivants : a) Gestion des anomalies b) Travaux et entretien prévus c) Gestion de la configuration et des changements d) Gestion du rendement e) Gestion des risques f) Gestion de la capacité g) Essais
13	Les FCST doivent informer les parties concernées, dans un délai raisonnable, de tous travaux ou opérations d'entretien prévus qui comportent un risque important d'atteinte aux services essentiels des FCST interconnectés.
14	Les FCST doivent s'assurer, lorsque cela est possible, que des processus de gestion des changements et des configurations sont établis : une bonne gestion des configurations et des changements suppose de tenir un inventaire fiable des ressources du réseau et de disposer de processus solides et documentés pour l'affectation des ressources et la gestion des changements pouvant présenter des risques importants pour la continuité des services.
15	Les FCST doivent s'efforcer, lorsque cela est possible, de mettre en place des systèmes, des processus et des pratiques opérationnels solides en matière de gestion de la performance. Une gestion efficace des performances requiert d'utiliser les données provenant des systèmes de gestion du réseau et d'autres sources pour contrôler les performances du réseau, les évaluer en fonction de normes établies et gérer la capacité du réseau afin de répondre à des niveaux de service déterminés.
16	Lorsque cela est possible, les FCST devraient disposer de systèmes, de processus et de pratiques opérationnels robustes en matière de gestion de la sécurité; il convient de citer les autres sections des présentes recommandations relatives à la gestion de la sécurité.

17	Lorsque cela est possible, les FCST devraient disposer de pratiques robustes en matière de gestion des risques. Dans ce contexte, une gestion efficace des risques implique d'évaluer les exigences relatives à la conception des processus, procédures, réseaux, systèmes et services, d'identifier les éventuelles vulnérabilités ou lacunes, d'évaluer leur incidence potentielle et, le cas échéant, de concevoir des contrôles d'atténuation pour la gestion des risques qui représentent une menace importante pour la continuité des opérations.
18	Les FCST doivent mettre au point des processus de gestion des capacités et des pratiques opérationnelles. La gestion de la capacité en temps réel suppose d'être en mesure de rassembler des données provenant de diverses parties du réseau pour permettre d'évaluer les options réelles de gestion du routage en temps réel. Ce processus peut également comprendre la collecte de données provenant de liaisons de signalisation, de passerelles Internet et de routes d'interconnexion avec d'autres FCST.
19	Les systèmes complexes évoluent et font l'objet de mises à jour en continu. Par conséquent, les FCST devraient maintenir un effectif qui possède les capacités, les compétences et l'expertise requises pour concevoir, exploiter et entretenir ces systèmes.
20	Globalement, la résilience du réseau et des services doit être assurée par une combinaison appropriée d'équipements résilients, de redondance ainsi que de mesures de rétablissement, de réparation et d'examen.
21	En cas de congestion à la suite d'une panne sur un réseau multiservice, lorsque cela est possible, il est recommandé de configurer des mécanismes d'assurance de qualité du service et d'établissement de priorités pour protéger le trafic et les services classés comme essentiels ou hautement prioritaires.
22	Lorsque cela est techniquement et économiquement possible, les FCST peuvent déployer des réseaux cellulaires temporaires pendant la période de rétablissement après un sinistre. La possibilité et la pertinence d'une telle opération dépendent de la disponibilité des équipements, de la sécurité des accès routiers et de la capacité de liaison secondaire dans la zone concernée, ainsi que de la durée prévue de la panne.
23	Les FCST peuvent étudier la possibilité d'un partage temporaire du spectre disponible avec un autre FCST au cas où l'un d'entre eux connaîtrait une importante panne de réseau ayant des répercussions sur les services aux clients. Un FCST peut réduire les répercussions négatives sur les clients en faisant appel au spectre d'un autre FCST pour une courte période en vue d'augmenter rapidement la capacité du réseau. Le soutien d'ISDE serait nécessaire pour permettre la mise en œuvre rapide de cette recommandation dans toute panne grave du réseau.
24	Dans le but de gérer les perturbations de service, l'infrastructure de service doit supporter plusieurs niveaux de disponibilité de service en fonction de la gravité de la perturbation et des ressources disponibles dans le réseau.
25	Pour chaque niveau de disponibilité du service, l'infrastructure de service doit prendre en charge plusieurs catégories de services (voix, vidéo, navigation sur Internet, etc.). Les ressources doivent être affectées aux différents services par ordre de priorité avant de prendre en charge les services moins prioritaires.

26	En cas de défaillance ou de charge excessive, les FCST doivent, dans la mesure du possible, prendre en charge la migration ou la mise à l'échelle de l'infrastructure de service sur place (sur la même infrastructure de service ou sur une infrastructure différente) ou sur une infrastructure de service distincte dans un emplacement différent (y compris le nuage public).
27	Chaque FCST peut envisager de tirer parti de ses propres processus robustes de gestion des problèmes et d'analyse des causes profondes pour s'assurer de tirer des leçons des défaillances et des défaillances évitées de justesse. Les leçons apprises peuvent être transmises en cascade à l'ensemble du FCST concerné à la suite du processus de gestion des incidents et d'analyse des causes profondes.
28	Les FCST sont encouragés à consigner officiellement leurs processus de continuité des services. Les principaux domaines à prendre en compte sont les suivants : La description du processus, la portée du plan, les hypothèses, les dépendances, la responsabilité, l'évaluation des risques, l'analyse des incidences sur les activités, la hiérarchisation, la mise à l'essai du plan, la formation et la tenue à jour du plan.
29	Lors d'incidents nécessitant la mise en œuvre du plan de continuité des services, les FCST sont encouragés, lorsque cela est possible, à désigner un centre d'opérations d'urgence qui présente une diversité géographique.
30	Les FCST devraient envisager de mettre en place des plans de rétablissement en cas de défaillance du réseau et, si de tels plans existent, ils devraient mettre à l'essai leur plan de continuité des services.
31	Les FCST devraient envisager le recours à plusieurs dispositifs, systèmes et fournisseurs de services de communication de rechange pour leurs employés essentiels en cas d'urgence.
32	Les FCST sont encouragés à maintenir leur participation au Groupe de travail sur la préparation et la gestion des urgences dans le secteur canadien des télécommunications et au Groupe de travail sur la protection cybernétique des télécommunications canadiennes, qui sont tous deux des sous-comités du Comité consultatif canadien pour la sécurité des télécommunications (CCCST). Ces sous-comités proposent notamment des séances de consultation, des exercices, des séances sur les pratiques exemplaires et des possibilités de formation connexes. Il est recommandé aux fournisseurs d'examiner les pratiques exemplaires reconnues et proposées et d'envisager leur mise en œuvre.
33	Les FCST doivent tenir une liste des personnes-ressources et la fournir au ministère de l'Innovation, des Sciences et du Développement économique (ISDE). Ils doivent la mettre à jour à mesure que des changements surviennent ou à la demande d'ISDE.
34	Les FCST devraient envisager la création d'une stratégie d'accès aux systèmes à distance pouvant être utilisée lors de la reprise des activités en cas d'urgence.
35	Les FCST doivent disposer de listes de personnes-ressources pour les diverses fonctions spécialisées et les principaux fournisseurs à contacter en cas d'urgence pour que les équipements et les spécialistes compétents puissent être déployés sur les lieux lors des

	situations d'urgence majeure. Les FCST peuvent envisager de fournir des cartes SIM doubles aux fournisseurs essentiels.
36	Les FCST doivent, lorsque cela est possible, élaborer et tenir à jour des processus permettant d'archiver régulièrement les sauvegardes du système et de les stocker sur un support externe sécurisé situé dans un emplacement géographiquement distinct.
37	Pour éviter d'être vulnérables à la défaillance d'une seule partie du système, les FCST devraient, lorsque cela est possible, évaluer les risques et prioriser les recommandations d'investissements en résilience.
38	Les recommandations relatives à l'itinérance d'urgence sont abordées dans le protocole d'entente du 9 septembre 2022 du CCCST.
39	Pour que la gestion des anomalies soit efficace, les FCST devraient, lorsque cela est possible, disposer de personnel, de systèmes et de processus capables de détecter et de surveiller les anomalies 24 heures sur 24 et 7 jours sur 7, documenter les anomalies et analyser leurs effets, en déterminer la ou les causes (analyse des causes profondes) et les moyens de les contourner afin de maintenir la performance du réseau et de corriger les anomalies.
40	Dans le cas de FCST interconnectés, il est attendu, dans la mesure du possible, que : a) Toute partie ayant connaissance d'une anomalie dans le service d'interconnexion doit en informer tous les autres opérateurs associés. b) Dans un tel cas, une action rapide pour résoudre l'anomalie doit être prise par la partie responsable du système dans lequel cette dernière est apparue. c) La gestion des opérations d'entretien prévues et des défaillances entre opérateurs interconnectés doit faire partie des procédures plus générales de fonctionnement et entretien (F et E) des opérateurs interconnectés.
41a	Lorsque cela est possible, les FCST devraient disposer de procédures pour tester le réseau, notamment en testant les composants du réseau de façon proactive. Il est entendu qu'il est impossible de réaliser des tests avec une certitude totale sur un système aussi complexe qu'un réseau de télécommunications moderne.
41b	Les FCST doivent être en mesure de démontrer que des scénarios de défaillance potentiels ont été envisagés et que des plans d'urgence pour le rétablissement du service ont été préparés, mis à l'essai et adoptés. L'objectif des plans d'urgence devrait être de maintenir la capacité des FCST à remplir, au minimum, leurs obligations de service en cas de défaillance du réseau.
42	Les FCST doivent mettre en place, le cas échéant, des programmes d'entretien préventif pour les systèmes de support des réseaux des installations, notamment des génératrices de secours et des systèmes d'alimentation sans coupure, de courant continu, de haute tension et d'extinction des incendies.