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

Telecom Notice of Consultation CRTC 2025-226

PDF version

Gatineau, 4 September 2025

Public record: 1011-NOC2025-0226

Call for comments – Development of a regulatory policy on measures to improve the resiliency of telecommunications networks and the reliability of telecommunications services

Deadline for submission of interventions: 3 December 2025

Deadline for submission of replies: 30 days from the date of receipt of the letter to all interveners advising them to submit reply comments

[Submit an intervention or view related documents]

[Submit your views using the online engagement platform]

Summary

Canadians need access to reliable, affordable, and high-quality communications services for every part of their daily lives.

Telecommunications service outages, even if they are short, are highly disruptive and can seriously impact Canadians' day-to-day lives. All outages can have harmful effects on people, especially when they cannot connect to emergency services in times of need.

The Commission, along with telecommunications service providers (TSPs) and other government authorities, all play a role in preventing and managing telecommunications service outages. This includes federal departments like Innovation, Science and Economic Development Canada and Public Safety Canada, as well as provincial and territorial emergency management organizations, and 9-1-1 call centres.

In this consultation, the Commission is developing a regulatory policy on measures that TSPs should take to help improve the resiliency of telecommunications networks and the reliability of telecommunications services. The Commission is gathering views on (i) what principles should guide the development and implementation of the regulatory policy, (ii) how TSPs should design and operate their networks to help make them more resilient, and (iii) how the regulatory policy can help support the safety of Canadians in all regions of the country, including rural, remote, and Indigenous communities.

Alongside this consultation, the Commission is taking two additional actions as part of its broader strategy to help lessen the disruptive impact of service outages on Canadians. First, the Commission is helping improve coordination whenever a major outage happens through

Telecom Decision 2025-225. The Commission is requiring TSPs to notify it and other government authorities within specific timeframes, as well as file comprehensive post-outage reports. Second, the Commission is considering additional consumer protections when Canadians experience an outage with their Internet, cellphone, telephone, or television services through Telecom and Broadcasting Notice of Consultation 2025-227. These protections include clearer communication from service providers during outages and refunds for lost services.

A complete list of questions can be found in the "Call for comments" section of this notice. Information on how to participate in this proceeding can be found later in this notice.

A summary of this notice is available in American Sign Language (ASL) and Langue des signes québécoise (LSQ) on the Commission's website. The Commission will accept video interventions and replies in ASL and LSQ.

Introduction

Why we are launching this proceeding

1. Canadians have experienced telecommunications service outages due to extreme weather events, technical failures, and other factors. These outages, even if they are short, are highly disruptive and can seriously impact Canadians' day-to-day lives. All outages can have harmful effects on people, especially when they cannot connect to emergency services in times of need. Networks need to be resilient to help ensure that telecommunications services remain reliable for Canadians.

2. While some telecommunications service providers (TSPs) have taken voluntary steps to improve network resiliency and service reliability, a common set of minimum requirements for all TSPs will promote consistency and will help ensure that Canadians continue to have reliable telecommunications services.

3. Before launching this proceeding, the Commission sought assistance from third-party experts to help determine what regulatory action may be required to address network resiliency and service reliability. This proceeding will gather views on the recommendations in the following expert reports:

    - Telecommunications Resilience Analysis Benchmarks Report: The Commission and Innovation, Science and Economic Development Canada (ISED) commissioned Gartner Canada Co. to analyze and benchmark resiliency-related regulatory measures in other jurisdictions. The study and resulting report covered Canada, the United States, the United Kingdom, Australia, the European Union, France, Germany, Japan, New Zealand, and South Korea.

    - Assessment of Rogers Networks for Resiliency and Reliability Following the 8 July 2022 Outage: The Commission engaged Xona Partners Inc. to investigate the causes of the Rogers Communications Canada Inc. (Rogers) July 2022 outage and to evaluate whether Rogers had taken satisfactory measures to address the causes

of the outage. They detailed their findings in a report, which also provided recommendations on the measures all TSPs can take to avoid similar outages.

- Telecommunications Network Resiliency in Canada: A Path Forward: The Canadian Telecommunications Network Resiliency Working Group (CTNR-WG)[1] submitted a report to the Minister of Industry containing a set of resiliency recommendations for TSPs.

- The Canadian Telecommunications Cyber Protection (CTCP) working group[2] authored reports for the Canadian Security Telecommunications Advisory Committee (CSTAC) on how TSPs can improve network resiliency, and include a security best practice policy, a network security monitoring and detection standard, a security incident response standard, a vendor management standard, and a critical infrastructure protection standard.

Legal framework

4. The Commission's decisions must advance the policy objectives set out in section 7 of the *Telecommunications Act* (the Act). This proceeding addresses three of those objectives:

    - to facilitate the orderly development throughout Canada of a telecommunications system that serves to safeguard, enrich and strengthen the social and economic fabric of Canada and its regions (paragraph 7(a));

    - to render reliable and affordable telecommunications services of high quality accessible to Canadians in both urban and rural areas in all regions of Canada (paragraph 7(b)); and

    - to respond to the economic and social requirements of users of telecommunications services (paragraph 7(h)).

5. In making decisions, the Commission must also implement the Government of Canada's 2023 Policy Direction.[3] The Policy Direction states that the Commission should consider how its decision would promote competition, affordability, consumer interests, and innovation. This includes ensuring that affordable access to high-quality, reliable, and resilient telecommunications services is available in all regions of Canada, including in rural, remote, and Indigenous communities.[4] The Policy Direction also notes that the

---

[1] The CTNR-WG was established by the Canadian Security Telecommunications Advisory Committee (CSTAC) to focus on delivering recommendations to improve the reliability of Canada's telecommunications networks. It is made up of representatives from ISED and several TSPs.

[2] The CTCP working group is a sub-committee of CSTAC and works to promote the confidentiality, integrity, and availability of the public telecommunications network as it may detect, protect, mitigate, and recover from cyber attacks and indicators of compromise.

[3] *Order Issuing a Direction to the CRTC on a Renewed Approach to Telecommunications Policy*, SOR/2023-23, 10 February 2023.

[4] See paragraph 2(c).

Commission should continue taking measures to support the objective of universal access to high-quality, reliable and resilient fixed Internet and mobile wireless services.[5]

Related proceedings

6. This consultation, which aims to improve the resiliency of telecommunications networks and reliability of telecommunications services, is one piece of the Commission's Consumer Protections Action Plan. As part of this plan, the Commission is taking action to reduce the frequency and length of service outages in all regions of Canada, including rural, remote, and Indigenous communities.

7. Building on the work of ISED and CSTAC, the Commission announced a multi-stage action plan for a regulatory framework to help improve the resiliency of telecommunications networks and reliability of telecommunications services.

8. As a first step of the regulatory framework, the Commission launched Telecom Notice of Consultation 2023-39, which led to the major service outage notification and reporting requirements established in Telecom Decision 2025-225. The Commission then published Telecom Decision 2025-65, mandating measures to improve the resiliency of 9-1-1 and public alerting services and reduce the impacts of service outages.

9. Earlier this year, the Commission published Telecom Regulatory Policy 2025-9, which aims to improve reliability and affordability of Internet services in the Far North. The Commission also launched Telecom and Broadcasting Notice of Consultation 2025-227 to gather views on improving consumer protections in the event of a service outage or disruption. The consultation will focus on how consumer protections can help Canadians be better informed about the status of their services and receive a refund or credit for a service they could not use.

10. Furthermore, through its continuing review of the Broadband Fund, initiated by Telecom Notice of Consultation 2023-89, the Commission is considering whether that program can provide funding for projects that would improve the resiliency of networks, especially in rural and remote areas.

11. In the present proceeding, the Commission will consider what steps TSPs can take to help improve resiliency of telecommunications networks and reliability of telecommunications services by building on recommendations from expert reports and industry best practices.

What we are examining in this proceeding

12. The Commission is gathering views on the development and implementation of a regulatory policy to help improve the resiliency of telecommunications networks and the

[5] See paragraph 18.

reliability of telecommunications services (the resiliency regulatory policy). To do this, the Commission will consider the following issues:

- principles that should guide the development and implementation of the resiliency regulatory policy;
- resiliency measures TSPs should consider when designing their networks;
- resiliency measures TSPs should consider in their network operations;
- improving the reliability of 9-1-1 and wireless public alerting services;
- improving the reliability of accessibility services;
- accessing telecommunications services during an emergency; and
- enforcing the resiliency regulatory policy.

13. The Commission invites comments on the above issues, as well as on the specific questions in the call for comments section below. Information on how to participate in this proceeding and how to apply for funding can be found at the end of this notice.

Call for comments

14. The Commission calls for comments on the following questions. In each of your responses to these questions, provide the rationale or evidence to support your position, including any technical, practical, or economic justifications.

Principles that should guide the development and implementation of the resiliency regulatory policy

15. Several principles could guide the Commission's resiliency regulatory policy. For example, the policy could consider that TSPs should, among other things:

- strive for always-on service availability;
- design resilient networks to withstand disruptions;
- implement robust network operation processes;
- aspire to have immediate fault mitigation and rapid restoration mechanisms;
- deploy resilient communications networks for emergency recovery personnel;
- strive for reliable partnerships with third-party vendors and suppliers; and
- support each other during times of need.

Q1. Which principles, including those in paragraph 15, or others, should the Commission consider in establishing the resiliency regulatory policy? How can each of these principles improve network resiliency and service reliability?

Resiliency measures TSPs should consider when designing their networks

16. The resiliency regulatory policy will identify design measures that TSPs may be required to implement to help ensure network resiliency and service reliability. The Commission has identified the following network design areas to explore:

    (a) Network redundancy: Network redundancy involves eliminating single points of failure. Examples include redundancy in network components, network paths, geography, and network management access. Deploying network components sourced from multiple vendors or based on different technologies may help increase redundancy.

    (b) Network security: Network security safeguards the confidentiality, integrity, and availability of networks. Protecting networks from unauthorized access, cyber-attacks, security breaches, and the improper disclosure of confidential network information all help improve network security.

    (c) Network infrastructure: Networks rely on both indoor and outdoor physical infrastructure that is often exposed and vulnerable to threats, including natural hazards,[6] accidental damage, theft, vandalism, and structural degradation. Establishing minimum standards to protect this infrastructure could help TSPs avoid damage or mitigate the impact of such threats. Such measures include site hardening[7] and the early detection[8] of natural hazards.

    (d) Network power supply: Networks need electrical power, which can come from various sources, including the electricity grid, gas generators, batteries, and solar power. The interruption of electrical power due to natural hazards is a common cause of network outages and service interruptions. Implementing measures to promote the supply of uninterrupted power to the network can help improve service reliability.

    (e) Network modularization: Network modularization is the process of dividing a network into smaller, more manageable sections that can be easily scaled, replaced, or isolated for network upgrades and troubleshooting. This practice can help avoid network outages.

    Q2. The expert reports on the record of this proceeding have recommended network resiliency design measures for TSPs (see Appendix 1 to this notice). Identify any

---

[6] Natural hazards include extreme weather events such as earthquakes, floods, landslides, tsunamis, and wildfires. For more information refer to Natural Hazards.

[7] Site hardening refers to the proactive steps taken by TSPs to protect network sites from human and environmental threats.

[8] Early detection measures like installing sensors, cameras, or artificial intelligence can help TSPs identify impending natural hazards, thereby enabling them to better react to threats to their networks.

additional measures that TSPs should implement for the design areas listed in paragraph 16.

(a) For each of these measures, identify which should be mandatory and which should be considered best practices.

(b) Which TSPs[9] should each of these resiliency measures apply to, and to what part of their networks would the measures be relevant?

Q3. What threats could damage physical network infrastructure?[10]

(a) How can TSPs evaluate these threats, and what measures can they take to protect physical network infrastructure?

(b) Since threat mitigation measures may need to be reassessed as threats change over time, how often should TSPs reassess threats to a network site?

Q4. How and under what different scenarios should TSPs conduct stress tests?[11]

Q5. What can TSPs do to ensure that telecommunications shelters[12] protect network equipment from various elements and threats, including extreme temperature changes, moisture, strong winds, and fire?

(a) Which of these measures should be mandatory, and which should be considered best practices?

Q6. What measures could improve the resiliency of networks or equipment in remote areas, some of which could take days to access for repairs?

(a) Which of these measures should be mandatory, and which should be considered best practices?

Q7. How should TSPs ensure the supply of uninterrupted power to their network sites?

(a) How should TSPs identify network sites that must be prioritized for backup power?

(b) What criteria should TSPs assess when determining the most suitable backup power options (e.g., solar, battery, fuel-powered generator)?

---

[9] For example, wireless service providers (WSPs), Internet service providers (ISPs), or local exchange carriers (LECs).

[10] Physical network infrastructure includes transmission cables and buildings or large enclosures that accommodate critical telecommunications network equipment (e.g., cell site, central office, cableco headend, satellite earth station, etc.).

[11] Telecommunications network stress testing is a process of evaluating the performance and stability of a network by subjecting it to heavy loads, and conditions that simulate high traffic or extreme operational scenarios. This helps to identify vulnerabilities, bottlenecks, and limitations within network infrastructure.

[12] Telecommunications shelters are buildings or structures that house and protect telecommunications equipment, such as radio equipment and fibre optics. They also provide shelter for data equipment, power systems, generators, lighting, fire suppression, cable entry, heating, ventilation, and air conditioning, racking, and more.

(c) What parameters should TSPs use to determine an appropriate backup power run time for each type of network site?

(d) How should TSPs ensure an uninterrupted fuel supply to network sites that are primarily powered or have backup power from fuel-powered generators?

Q8. What measures can TSPs take to benefit from advancements in satellite services to improve the resiliency of networks and reliability of services? Include the following scenarios in your response:

(a) Integrating satellite networks to improve the resiliency of backhaul transport connectivity.

(b) Integrating direct-to-device satellite capabilities to improve mobile service connectivity during service outages or emergencies.

Q9. Which recommendations in the following CTCP working group reports should the Commission require TSPs to implement, and which should be considered best practices: Critical Infrastructure Protection Standard for Canadian Telecommunications Service Providers, Security Best Practice Policy for Canadian Telecommunications Service Providers and Network Security Monitoring and Detection Standard for Canadian Telecommunications Service Providers?

Resiliency measures TSPs should consider in their network operations

17. Resiliency measures in network operations include (i) creating processes to prevent network failures that result in service disruptions, and (ii) restoring affected services as quickly as possible. The Commission has identified the following network operations areas to explore:

(a) Change management: Change management consists of the processes and practices TSPs follow when making modifications to a network. This includes changes and updates to network infrastructure, hardware and software, network element arrangements, and network configurations. Proper change management can mitigate the risk that network changes or updates cause a service outage.

(b) Incident management: Incident management is a structured approach to handling and resolving unexpected disruptions within the network, including hardware and software failures. Effective incident management ensures that an incident is addressed quickly to minimize the impact on network performance and customer experience.

(c) Supply chain management: TSPs often rely on multiple vendors for components and materials critical to network operation to ensure reliable services. A resilient supply chain includes suppliers that provide reliable equipment and necessary support in the face of network disruptions. It also involves maintaining and

strategically situating an inventory of critical equipment to respond to network disruptions in a timely manner.

(d) Risk management: Systematic processes and strategies can help identify and mitigate the complex risks that TSPs face. Understanding and controlling potential threats – whether infrastructure-related (including modernization or decommissioning of networks), operational, financial, or technical (including network upgrades) – can minimize adverse outcomes.

(e) Infrastructure modernization: Telecommunications networks are critical infrastructure that need to be modernized as technology evolves to respond to all Canadians' economic and social requirements. Infrastructure modernization involves replacing old network components with new and more modern equipment. This improves a network's performance, efficiency, reliability, and security. Anticipating and taking proactive steps to address potential issues during modernization can help reduce any impact on consumers.

(f) Emergency preparedness: Telecommunications networks are critical during emergencies, with many local emergency management departments and officers relying on commercial networks. Emergency preparedness ensures that TSPs can continue to deliver reliable services during emergencies, support emergency response efforts, and help communities stay connected.

(g) Mutual support: In September 2022, 12 TSPs signed a Memorandum of Understanding on Telecommunications Reliability (the MoU) to provide emergency roaming,[13] mutual assistance, and communications to the public and government authorities during a critical network failure. Mutual support between TSPs enables Canadians to continue to access telecommunications services when their service provider has a network outage, for example, emergency roaming between wireless service providers (WSPs) as implemented within the MoU.

Q10. The expert reports on the record of this proceeding have recommended resiliency measures TSPs should implement to improve network operations (see Appendix 2 to this notice). Identify any additional measures that TSPs should implement for the network operations areas listed in paragraph 17.

(a) For each of these measures, identify which should be mandatory and which should be considered best practices.

[13] Emergency roaming enables the customers of a WSP experiencing a network outage to roam on another WSP's network.

(b) Which TSPs[14] should each of these resiliency measures apply to, and to what part of their networks would they be relevant?

Q11. Should the Commission require TSPs to prepare and implement a change management process? If not, provide reasons why and explain whether this should instead be considered a best practice.

(a) What steps should a change management process include?

(b) How should changes to a network be classified (e.g., based on how critical the network element or function undergoing the change is to providing service), and who should approve these network changes?

(c) Should TSPs be required to keep and maintain a record of network changes?

Q12. Should the Commission require TSPs to prepare and implement an incident management plan? If not, provide reasons why and explain whether this should instead be considered a best practice.

(a) What should an incident management plan include?

(b) How can TSPs detect network incidents and failures early to trigger the incident management plan?

Q13. Should the Commission require TSPs to prepare and implement supply chain management plans? If not, provide reasons why and explain whether this should instead be considered a best practice.

(a) What should a supply chain management plan include?

(b) What measures should TSPs include in a supply chain management plan to reduce the time required to restore critical network components in remote communities?

Q14. Should the Commission require TSPs to prepare and implement risk assessment and management strategies? If not, provide reasons why and explain whether this should instead be considered a best practice.

(a) What should a risk assessment and management strategy include?

(b) How should TSPs promote a risk-aware culture within their organizations as part of the risk management strategy?

[14] For example, WSPs, ISPs, or LECs.

Q15. How can TSPs ensure that their telecommunications services remain functional during power outages at their customers' premises?

(a) Should the Commission require TSPs to provide home routers and modems with integrated battery backup? If not, provide reasons why and explain whether this should instead be considered a best practice.

Q16. Should the Commission require TSPs to prepare and implement emergency response plans? If not, provide reasons why and whether this should instead be considered a best practice.

(a) What should an emergency response plan include?

(b) Should TSPs be required to develop and strategically locate deployable network facilities?[15] If not, provide reasons why and explain whether this should instead be considered a best practice.

(c) Would it be beneficial for TSPs to train residents of remote communities to assist in service restoration processes (e.g., minor system troubleshooting or system reboot under remote supervision)? If so, how should the training be accomplished?

Q17. How can TSPs support each other to improve network resiliency and service reliability, especially during emergencies and service outages such as through mutual assistance[16] and emergency roaming?

(a) Under what arrangements should WSPs not party to the MoU implement mutual assistance and emergency roaming?

  (i) How might a WSP providing emergency roaming benefit from such an arrangement, and how would it impact the WSP's services?

  (ii) What minimum services and service levels should be supported during emergency roaming?

(b) Under what arrangements would wireline TSPs implement mutual assistance? Would these arrangements require agreements or memorandums of understanding between TSPs? How should they be established?

Q18. The CTCP working group developed the Security Incident Response Standard for Canadian Telecommunications Service Providers to manage cyber security incidents.

---

[15] Deployable network facilities are temporary facilities that can be moved in areas without coverage to provide cellular connectivity. Such facilities include cell-on-wheel or airborne cell towers for emergency coverage, and movable generators.

[16] Mutual assistance is the temporary assistance provided by a TSP to another TSP in various forms, for example, the sharing of physical assets, equipment or human resources, the provision of requested services or access to 9-1-1 networks.

Should the Commission require TSPs to implement this standard? If not, provide reasons why and explain whether this should instead be considered a best practice.

Q19. The CTCP working group developed the Vendor Management Standard for Canadian Telecommunications Service Providers. Should the Commission require TSPs to implement this standard? If not, provide reasons why and explain whether this should instead be considered a best practice.

Improving the reliability of 9-1-1 and wireless public alerting services

18. 9-1-1 is a bridge that connects Canadians to emergency services in times of need, and wireless public alerts warn the public about imminent or possible dangers such as floods, tornados, fires, and other disasters. Federal, provincial, territorial, and municipal governments, as well as TSPs, all play a role in ensuring that Canadians can access 9-1-1 services and receive emergency alerts. The Commission's role is to regulate the TSPs that connect 9-1-1 calls to first responders and that distribute wireless public alerts from the emergency management organizations of these governments to Canadians.

19. 9-1-1 and wireless public alerting services are critical to the health and safety of Canadians and must be of the highest level of reliability. These services are provided using separate or dedicated networks and require special considerations when establishing resiliency requirements.

20. In Telecom Decisions 2016-165, 2018-217, and 2019-353, the Commission established requirements for the resiliency of 9-1-1 networks. In Telecom Decision 2025-65, the Commission mandated TSPs to implement additional measures to improve the resiliency of 9-1-1 and wireless public alerting services and reduce the impact of outages. The Commission is currently reviewing a report (ESRE0098b) received from the CRTC Interconnection Steering Committee (CISC) Emergency Services Working Group on *Next Generation 9-1-1 Reliability, Resiliency, and Security Best Practices & Standards* to determine whether TSPs should implement the recommended measures.

Q20. What additional measures should TSPs implement to further improve the reliability of 9-1-1 services? The proposed measures should take into consideration the Commission's mandate as an independent quasi-judicial tribunal in regulating TSPs, with no regulatory oversight of public safety answering points or third-party call centres.

(a) Which of these measures should be mandatory, and which should be considered best practices?

(b) Who should implement these measures (i.e., the originating network providers on whose networks the 9-1-1 calls are made and/or the 9-1-1 network providers responsible for delivering these calls to public safety answering points)?

Q21. What additional measures should WSPs implement to further improve the reliability of wireless public alerting services?

(a) Which of these measures should be mandatory, and which should be considered best practices?

(b) Who should implement these measures (i.e., WSPs on whose networks public alerts are disseminated to the public and/or the National Alert Aggregation and Dissemination system operator who connects with these WSPs to relay wireless public alerts through those networks)?

Improving the reliability of accessibility services

21. Accessibility services are specialized telecommunications services used by persons with hearing or speech disabilities. Accessibility services addressed in this proceeding are teletypewriter (TTY) relay[17] and Internet Protocol (IP) relay[18] services. Unlike emergency services, accessibility services are provided using regular telecommunications networks. The reliability of Video Relay Service was addressed in Telecom Notice of Consultation 2021-102 and will not be considered in this proceeding.

    Q22. What measures should TSPs implement to improve the reliability of TTY relay and IP relay services? Which of these measures should be mandatory, and which should be considered best practices?

    Q23. What measures should third-party service providers, hired by the TSPs to provide TTY relay and IP relay services, implement to improve the reliability of those services?

    (a) How can TSPs ensure these third-party service providers have implemented the required measures?

Accessing telecommunications services during an emergency

22. Canadians can take specific measures to ensure continued access to telecommunications services during emergencies, such as power outages, extreme weather events, and other natural disasters. The Commission establishes policies and requirements to help ensure TSPs provide reliable services. ISED is the telecommunications emergency preparedness liaison between the telecommunications industry and federal, provincial, and territorial emergency management organizations. As part of this role, ISED has provided Guidance for Canadians to stay connected during an emergency. The Canadian Telecommunications Association (CTA) advocates on behalf of TSPs and informs Canadians about industry initiatives such as consumer protection. The CTA has also provided guidance on Preparing for Severe Weather Events & Other Emergencies, outlining how Canadians can stay connected in the event of a natural disaster, a severe weather event, or an emergency.

---

[17] TTY relay service is offered to all home telephone subscribers in Canada. In a TTY relay service call, a person with a hearing or speech disability uses a TTY and dials 7-1-1 to reach a relay operator.

[18] IP relay service is offered to all subscribers of home or mobile telephone service in Canada. In an IP relay service call, a person with a hearing or speech disability uses an Internet-enabled device (e.g., computer, laptop, tablet, or mobile phone) to reach a relay operator by logging into the IP relay provider's web portal.

Q24. Given the guidance provided by ISED and the CTA on how Canadians can prepare and stay connected during emergencies,

(a) Is there additional information that TSPs should be responsible for providing to Canadians?

(b) Should TSPs be required to inform Canadians about how to prepare and stay connected during emergencies? If so, for which services, and what methods of communication should TSPs use?

Enforcing the resiliency regulatory policy

23. The Commission may require TSPs to implement certain measures as an outcome of this proceeding. In those circumstances, the Commission may need to impose compliance and enforcement mechanisms.

Q25. What specific compliance measures should the Commission consider to help ensure TSPs adhere to the resiliency regulatory policy requirements (e.g., compliance reporting, resiliency audits, or monitoring)?

(a) Should these compliance measures apply equally to all TSPs? If not, explain why.

(b) How could the Commission quantify and evaluate the resiliency of TSPs' networks and the reliability of their services?

What you need to know to participate in this proceeding

Procedure

24. The *Canadian Radio-television and Telecommunications Commission Rules of Practice and Procedure* (the Rules of Procedure) apply to this proceeding. The Guidelines on the CRTC Rules of Practice and Procedure (Broadcasting and Telecom Information Bulletin 2010-959) are meant to help members of the public understand the Rules of Procedure so that they can more effectively participate in Commission proceedings.

Submitting an intervention

25. The Commission invites comments that address the issues and questions set out in this notice. The Commission will accept interventions that it receives no later than **3 December 2025**.

26. Interested persons who require assistance submitting comments can contact the Commission's Hearings & Public Proceedings group at hearing@crtc.gc.ca.

27. The Commission encourages stakeholders who have expertise in ensuring the resiliency of telecommunications networks to participate. This includes TSPs, other industry stakeholders such as standards organizations and equipment vendors, governments (provincial, territorial, and municipal), and Indigenous organizations and communities.

28. All TSPs are automatically made parties to this proceeding. Interested persons who file an intervention also automatically become a party to this proceeding. Only parties to the proceeding can participate in further stages of the proceeding.

29. Parties can coordinate, organize, and file, in a single submission, interventions by other interested persons who share their position. Information on how to file this type of submission, known as a joint supporting intervention, as well as a template for the accompanying cover letter to be filed by parties, can be found in Telecom Information Bulletin 2011-693.

30. Submissions must be filed by sending them to the Secretary General of the Commission using only one of the following means:

    - completing the Commission's intervention form;
    - Submitting an ASL or LSQ video using the intervention form;
    - sending a fax to 819-994-0218; or
    - writing by mail to CRTC, Gatineau, Quebec K1A 0N2.

31. Submissions longer than five pages should include a summary. Submissions will be posted in the official language and format in which they are received.

32. The deadline to submit an intervention to the Commission is 5 p.m. Vancouver time (8 p.m. Gatineau time). Parties are responsible for ensuring the timely delivery of their submissions and will not be notified if their submissions are received after the deadline. Late submissions will not be considered by the Commission and will not be made part of the public record.

Requests for information

33. The Commission may request information, in the form of interrogatories, from any party to the proceeding.

Submitting a reply

34. Parties can file replies with the Commission within **30 days** from the date of receipt of a letter to all interveners advising them to submit reply comments. This letter will be sent after the completion of the request for information process and the posting of the transcripts of ASL and LSQ video interventions on the Commission's website.

Privacy notice

35. Please note the following:

    - Documents will be posted on the Commission's website exactly as received. This includes any personal information contained in them, such as full names, email addresses, postal/street addresses, and telephone and fax numbers.

- All personal information parties provide as part of this public proceeding, except information designated as confidential, will be posted on the Commission's website and can be accessed by others.
- However, the information and transcripts of the ASL or LSQ videos that the parties provide can only be accessed from the web page of this public proceeding. As a result, a general search of the Commission's website using either its search engine or a third-party search engine will not provide access to the information that was provided as part of this public process.
- The personal information that parties provide will be used and may be disclosed for the purpose for which the information was obtained or compiled by the Commission or for a use consistent with that purpose.

Confidentiality

36. The Commission's proceedings are designed to allow members of the public to provide input so that it can make better, more informed decisions. As a result, the general rule is that all information filed with the Commission is placed on the public record and can be reviewed by all parties and members of the public.

37. However, the Commission also often needs detailed information from the companies it regulates and supervises to make an informed decision. This information can be commercially sensitive, especially as the environment in which the companies operate becomes more competitive. The Commission will therefore accept certain information as confidential.

38. Parties can request that information be filed in confidence under subsection 39(1) of the Act with a detailed rationale as to why that information should be considered confidential. The Commission reminds parties that make such a request that when a document is filed with confidential information, an abridged version must also be filed so that it can be included in the public record.

Accessible formats

39. The Commission requires regulated entities and encourages all parties to file submissions in accessible formats (for example, text-based file formats that enable text to be enlarged or modified or read by screen readers) for this proceeding. To help in this regard, the Commission has posted on its website guidelines for preparing documents in accessible formats.

40. If submitted documents have not been filed in accessible formats, you can contact the Commission's Hearings & Public Proceedings group at hearing@crtc.gc.ca to request that Commission staff obtain those documents in accessible formats from the party that originally submitted the documents in question.

41. The Commission is accepting submissions in ASL or LSQ in video format. The Commission will publish the links to the parties' videos on its website. The permissions on the videos must be set to public. The Commission will not accept links that require

anyone to request access to the videos. The links on the Commission's website will redirect users to parties' videos as they are uploaded, and users will have access to any of the parties' personal information displayed on the video-hosting platform. The videos will be fully translated into text, and transcripts will be available in English and French for ASL and LSQ videos.

Sharing views on CRTC Conversations

42. Views can be shared on CRTC Conversations, the online engagement platform, until **3 December 2025**.

43. The platform facilitates participation among people who may be less familiar with Commission processes. It includes only select questions.

44. All submissions received via CRTC Conversations will be placed on the public record of this proceeding.

45. Please note the following:

- The information provided is entered into a searchable database on the engagement platform.
- The comments provided will be attributed to the username given during the registration process on the platform.
- These comments and usernames are searchable with the help of third-party search engines.
- Any personal information submitted through the platform will also be searchable. Any information will be used and may be disclosed for the purposes for which the information was obtained or compiled by the Commission, or for a use consistent with that purpose.

46. Participants who provide their views via CRTC Conversations will not be considered parties to this proceeding. In general, this means that they will not receive notice of other comments or procedural requests or changes, they may not participate in an oral hearing, and they may not be named (or required to participate) in any appeal of the Commission's decision.

47. To become a party to this proceeding, people must submit a formal intervention via the online form, fax, traditional mail, or by ASL or LSQ video. Details on how to submit a formal intervention are provided above.

Accessing documents

48. Links to interventions, replies, and other documents referred to in this notice, are available on the Commission's "Consultations and hearings: have your say" page.

49. Documents are available upon request during normal business hours by contacting:

Documentation Centre
Examinationroom@crtc.gc.ca
Tel.: 819-997-4389
Fax: 819-994-0218

Client Services
Toll-free telephone: 1-877-249-2782
Toll-free TTY: 1-877-909-2782

50. Interested persons can find electronic versions of the documents by clicking on "[Submit an intervention or view related documents]" at the top of this notice.

Secretary General

Related documents

- *Call for comments – Consumer protections in the event of a service outage or disruption*, Telecom and Broadcasting Notice of Consultation CRTC 2025-227, 4 September 2025

- *Mandatory notification and reporting of major telecommunications service outages*, Telecom Decision CRTC 2025-225, 4 September 2025

- *CISC Emergency Services Working Group and Network Working Group – Consensus report NTRE081 on measures to improve the resiliency of 9-1-1 and public alerting services and reduce the impacts of outages*, Telecom Decision CRTC 2025-65, 28 February 2025

- *Telecommunications in the Far North*, Telecom Regulatory Policy CRTC 2025-9, 16 January 2025

- *Call for comments – Broadband Fund policy review*, Telecom Notice of Consultation CRTC 2023-89, 23 March 2023, as amended by Telecom Notices of Consultation CRTC 2023-89-1, 17 April 2023, and 2023-89-2, 25 July 2024

- *Call for comments – Development of a regulatory framework to improve network reliability and resiliency – Mandatory notification and reporting about major telecommunications service outages*, Telecom Notice of Consultation CRTC 2023-39, 22 February 2023, as amended by Telecom Notice of Consultation CRTC 2023-39-1, 11 September 2023

- *Call for comments – Review of video relay service*, Telecom Notice of Consultation CRTC 2021-102, 11 March 2021, as amended by Telecom Notices of Consultation CRTC 2021-102-1, 26 April 2021, 2021-102-2, 30 June 2021, 2021-102-3, 14 March 2022, and 2021-102-4, 19 September 2023

- *CISC Emergency Services Working Group – Consensus report on matters related to compatibility, reliability, resiliency, and security for next-generation 9-1-1*, Telecom Decision CRTC 2019-353, 22 October 2019

- *CISC Emergency Services Working Group consensus items – Next-generation 9-1-1 technical and operational considerations and trial logistics*, Telecom Decision CRTC 2018-217, 28 June 2018

- *Matters related to the reliability and resiliency of the 9-1-1 networks*, Telecom Regulatory Policy CRTC 2016-165, 2 May 2016

- *Filing submissions for Commission proceedings in accessible formats*, Broadcasting and Telecom Information Bulletin CRTC 2015-242, 8 June 2015

- *Filing of joint supporting interventions*, Telecom Information Bulletin CRTC 2011-693, 8 November 2011

- *Guidelines on the CRTC Rules of Practice and Procedure*, Broadcasting and Telecom Information Bulletin CRTC 2010-959, 23 December 2010

Appendix 1 to Telecom Notice of Consultation CRTC 2025-226

Recommendations on resiliency design measures

The following recommendations are from *Assessment of Rogers Networks for Resiliency and Reliability Following the 8 July 2022 Outage* (the Xona Partners Report):

1	Implement router overload protection in the Internet Protocol (IP) core and distribution networks.
2	Separate network management layer physically and logically from the data network.
3	Provide the network operation centre and other critical remote sites with a secure backup connectivity from third-party telecom network operators.

The following recommendations are from *Telecommunications Network Resiliency in Canada: A Path Forward* (the Canadian Security Telecommunications Advisory Committee [CSTAC] Report):

4	Where practicable, designs for the core networks of Canadian Telecommunications Service Providers (CTSPs) should consider the possibility of loss of human physical access to operations centres, buildings or sites. In cases where human access is temporarily restricted, procedures should be in place to notify staff who would normally work at a given operations centre, building or site. Contingency plans should aim to cover the liaison with emergency responders concerning physical access in order to maintain essential services.
5	The use of reliable equipment and systems (sourced from capable suppliers) should be designed, where practicable, with the intent to prevent or withstand the effects of extreme conditions, including the loss of commercial utility power.
6	CTSPs should, where practicable, aim to use techniques such as priority routing, repeat attempts, alternative routing, and trunk reservation, where practicable, in order to avoid dependence on a single set of equipment for the handling of public emergency traffic.
7a	Where equipment is software controlled, the software should be designed to minimize the possibility of a software error propagating throughout the system or to other equipment, and be secured against unintended external interference, where practicable.
7b	In addition, ‘auto-apply’ functionality should be disabled on network equipment to avoid the risk of immediate application of new software/patch to the network.
8	In order to avoid cascade failures, to the extent practicable, consideration should be given to dual plane or dual meshed networks provided by different suppliers.

9	To the best of their ability, CTSPs should plan accordingly to mitigate signaling threats. CTSPs, where practicable, should aim to minimize the impact of inappropriate signaling messages which may cause mis-operation of the network or supporting systems.
10	To the best of their ability, CTSPs should plan accordingly to mitigate traffic load threats. CTSPs, where practicable, should apply network management controls to limit the impact and onward transmission of excessive traffic volumes, but no more than is reasonably required to maximize the establishment of effective voice calls or timely data connections.
11	CTSPs should aspire to comply with applicable technical networking standards, especially considering that incorrect signals received from outside of a CTSP's domain can interfere with the correct operation of a CTSP's network. Such signals may be benign in intent and be caused by accidental mis-operation of equipment. However, incorrect signals may also be deliberate attempts to interfere with a network. An example of a deliberate attempt could be the avoidance of the proper charging for network services (phone fraud); a denial of service to others; or an attempt to corrupt stored data or software. Multiple levels of security should be considered to counter such threats, including, but not limited to, signaling 'policing' mechanisms, firewalls, and communication processes across relevant stakeholders and operational tools to ensure alignment in understanding impacts and planned response.
12	CTSPs may consider appropriate measures to ensure that their networks can be protected from signaling / control plane problems in an interconnected network environment. Screening (also known as policing) is a technique that could be used, if appropriate, at the edge of the network to protect CTSPs from mis-operation of connected networks. It may be reasonable to provide screening of an interconnect link to ensure that only the agreed upon use of the interconnect is allowed and undertaken. Additionally, monitoring of protocols such as SS7 would assist in detecting anomalous traffic enabling CTSPs to manage potential threats appropriately.
13	Where appropriate and where commercially feasible, CTSPs may consider implementing diverse duct tracks or routes as physical separation of fibre on its own does not deliver guaranteed availability. If economically and physically feasible, CTSPs should aspire to have a combination of physically diverse routes to achieve stronger redundancy and resilience of their network infrastructure.
14	Where appropriate, CTSPs should ensure that all core network elements are accessible by an out of band (OOB) separate physical network or link to the core network elements.
15	When designing IP Routing networks, appropriate safeguards can be considered in order to prevent routing database or tables on routers from getting overloaded. This will help in preventing cascading failures across the routing network and will speed up the recovery times in case of an unforeseen failure.
16	As far as practicable, CTSPs should strive for general core segmentation of services and network elements. To the best of a CTSP's ability, failure of network element(s) in one segment or region should not affect the failure of services in other segments or regions.
17	Within network segments or regions, there should be adequate diversity and redundancy so that individual failure in the segment or region does not impact overall service delivery.

18	To the extent practicable, CTSPs should strive to avoid single points of failure in any part of the Core network, so that service loss pursuant to the events of failures of individual network elements are minimized.
19	Where physically possible and economically feasible, CTSPs should strive to provide adequate geo-redundancy for all centralized core network elements and servers such as, but not limited to, authentication servers, Dynamic Host Configuration Protocol (DHCP servers), route servers, etc.
20	CTSPs should, to the extent practicable, provide adequate throttling and prioritization mechanisms for all control and signaling systems in order to avoid signaling storms and failure of systems thereof.
21	Adoption of CSTAC Best Practices and Standards: CTSPs should review and apply to their network(s), as appropriate, the design principles and controls outlined in the CSTAC's Security Best Practices Policy and its accompanied Critical Infrastructure Protection Standard or future releases.
22	Resource Public Key Infrastructure (RPKI) Implementation: CTSPs should continue to pursue the implementation of RPKI, the cryptographic signing of Border Gateway Protocol (BGP) route ownership, into their network infrastructure.
23	BGP Route Monitoring: To enhance the national response to BGP events threatening telecommunications network resiliency CTSPs should implement route monitoring to identify and record anomalous activity.
24	Anti-spoofing filtering: Where practicable, CTSPs should implement anti-spoofing filtering to prevent traffic with spoofed source IP addresses.
25	Multi-Factor Authentication (MFA): CTSPs should implement robust multi-factor authentication for access to core network devices, also extend multi-factor authentication to operator and administrator network accounts. Detailed guidance on MFA should be incorporated into the CSTAC Security Best Practices Policy and its accompanied Critical Infrastructure Protection Standard.
26	Considerations for additional controls, or equivalent, to contain or reduce the impact of cascading issues as a result of a possible cyber event, may include, but not be limited to: • User Plane Redundancy • Network Segmentation • Supply Chain Diversity
27	As practicable, software-controlled environments should be fault tolerant and should be designed and deployed to minimize the possibility of a software error propagating throughout the system or to other equipment and be secured against accidental or planned external interference.
28	CTSPs and government should jointly influence original equipment manufacturers (OEM) in order to standardize the behavior of mobile devices should a triggering event impact 911 services.

29	Where it is physically and commercially practicable, cell site mobile backhaul networks should be designed and built using physical and logical diversity, to have a minimum of two independent and diverse paths.
30	Path diversity can use several technologies to avoid congestion and, in the case of an outage, each path should be able to accommodate a reasonably high-level of priority (e.g., emergency services) traffic, to the extent practicable.
31	If there is congestion following an outage on a multi-services network, Quality of Service (QoS) and prioritization mechanisms should be configured, where practicable, to protect traffic and services that are marked critical or higher priority
32	CTSPs should, to the extent practicable, assess the environmental threats to their outdoor facilities and where physically and economically feasible, seek to mitigate or prevent possible damage to their facilities from weather events such as (list is not exhaustive): • Extreme wind pressures and the vibration caused by wind • Vibration caused by earthquakes • Damage from lightning strikes • Wildfires, fire generally • Water - floods, water immersion, tidal waves • Ice, prolonged freezing temperatures • Salt-laden winds • Corrosive gasses • Dust • Extreme temperatures and temperature swings • Humidity and rust caused by humidity
33	CTSPs should to the extent practicable, assess the environmental threats to their indoor facilities and where physically and economically feasible, seek to mitigate or prevent possible damage to their facilities from weather or situational events such as (list is not exhaustive): • Small or large-scale earthquakes • Damage from lightning strikes • Fires • Flooding
34	When determining the location and structural make-up of a telecommunications building, CTSPs should strive to ensure that the building will, to the extent practicable, resist damaging effects of (list is not exhaustive): • Storms • Floods • Breakdown by wind or water • Strong electromagnetic fields - electromagnetic shields for machine rooms should be installed where appropriate • Earthquakes • Fire - fire suppression mechanisms should be appropriately installed

35	For new sites hosting or supporting critical services and/ or where sites have experienced flooding or earthquake historically, special consideration should be made to ensure that, to the extent practicable, the critical services can be maintained during a flooding or earthquake incident (the service may be supported by delivery from an alternative site which should not be exposed to the same set of risks as the primary site) the impacts of flooding or earthquake to key inputs should also be considered (energy inputs such as electricity, fuel oil and human access).
36	Wherever reasonable, essential equipment should not be concentrated, particularly in one building, to the extent that overall network security is jeopardized. Where essential equipment is co-located (for example, at multiprocessor sites), priority should be given to physical separation, such as a fire break, to reduce the possibility of common mode failure.
37	Where appropriate and practicable, diverse entry and exit points, e.g., to sites or buildings, should be provided (including cable entries).
38	Where appropriate, and practicable, CTSPs should use diverse duct tracks or routes (NB: physical separation on its own does not deliver guaranteed availability, and this is usually achieved by a combination of physical separation, redundancy and resilience).
39	Outside equipment should be positioned to minimize risk, where practicable, for example from road accidents or vandalism, as well as being locked and weather sealed.
40	Where possible, for every new fibre installation or modification to an existing fibre network, CTSPs should consider implementing an internal process to record the precise geolocation into an internal database.
41	Where possible, CTSPs should strive to have their main regional centres placed in a decentralized manner and region.
42	A CTSP's main regional centre should be backed up by other regional centres, to the extent practicable.
43	Critical regional centres should be connected, where practicable, to other regional centres via a detour route to minimize the impact when the original connection route is broken.
44	The transport facilities that connect the main regional centres should be physically redundant, where practicable (i.e., multi-routed).
45	The main fibre access facilities should be installed as two or more physically diverse routes whenever practicable.
46	The telecommunication lines that connect the main regional centres should be laid in different transport facilities whenever practicable.
47	A CTSP's main transport facilities should allow for telecommunications links to be switched to alternate telecommunications links as quickly as practicable, when necessary.

48	The main transport facilities and telecommunications links should be provided with a function to monitor the operation, detect failures immediately, and report the status of operation, and do so in an integrated manner.
49	When installing multi-routed transmission facilities, CTSPs should plan for each route to be as geographically separated and diverse as physically and commercially practicable, in order to mitigate local risks from the other routes.
50	Where normal maintenance access to a site may be jeopardized because of bad weather, arrangements for use of suitable alternative transport should be covered by contingency plans (e.g., four-wheel drive vehicles, snow cats, helicopters, etc.). At sites prone to flooding, building utilization should be such that the least critical functions are performed in the areas of highest risk.
51	CTSPs should strive to have the redundant and spare equipment on hand and readily available in the event that original indoor and/or outdoor equipment fails or is degraded.
52	CTSPs should consider having an alert function implemented in important indoor facilities that immediately detects failures and reports those failures. Where practicable, unmanned indoor facilities should have a remote reporting function in the event of a failure, or a comparable alternative alerting system.
53	The location of all external line plant, such as underground and aerial cables, should be notified to the relevant authorities as and when appropriate (e.g. membership with the Provincial One Call agencies or equivalent).
54	Suitable business processes should be in place to coordinate the activities of the various utilities and highway authorities to ensure that risk of damage is minimized.
55	Poles should be placed in the lowest risk positions consistent with their use, where practicable. The positioning of aerial cables and drop-wires is subject to broader regulation and must be installed to ensure adequate clearance of vehicles, land and buildings. Utility providers should ensure the continued physical integrity of shared infrastructure, such as poles, towers, etc., through regular surveys, and assess and communicate with CTSPs any new risks to the integrity of shared structures (e.g. tree growth).
56	Where possible, where ventilation or air conditioning is used, a single failure should not degrade the facility and essential cooling infrastructure should be remotely monitored for timely action in the event of an incident.
57	It is recommended that where appropriate, suitable detection and extinguishing or suppressant systems for fire, detection systems for explosive and asphyxiating gasses, and flood detection systems are installed.
58	Automatic fire alarms and, where appropriate, fire suppressants should be deployed appropriately for buildings and machine rooms.

59	Where possible, normal site maintenance should occur on a regular basis. In the event access to a site is jeopardized because of bad weather, redundancies should be in place to support service stability.
60	A secure environment is a key factor in maintaining the integrity of telecommunications service. The protection given to a building should be assessed and follow a security protocol.
61	Buildings should be secure against entry by unauthorized people. An adequate level of building security should be demonstrable and commensurate with the assessment of levels of risk and vulnerability. Secure entry systems, movement detectors and video surveillance may be necessary, and both perimeter and cellular security may be appropriate in large buildings.
62	Where appropriate, the power supply to key equipment should not be interrupted in the event of a mains power supply failure, and where appropriate and feasible, CTSPs may seek to acquire diverse feeds of mains supply to protect major sites from power supply failure.
63a	Where possible, in the event of a mains power supply failure, standby power should be of sufficient capacity to fully support the operational power load in the period between power failure and the cut over to any alternative supply which is available.
63b	Where practical and feasible, generators should be available through a combination of onsite generators at designated high priority sites as well as offline generators stored at strategic locations through the network to support disaster recovery efforts where backhaul is still functional and coverage is required.
64	At sites where it is not practical to provide an alternative on-site supply (i.e., generators), CTSPs should consider designing battery capacity to cover the typical likely interruption of the mains supply or the time to travel to site with portable generating equipment.
65	Where power is provided by batteries, CTSPs should consider the following pertaining to their battery power usage: • The batteries are capable of maintaining service irrespective of their stage of design life; • Site conditions, space, and any required permits for proper battery function are prepared ahead of time; • Batteries are maintained to manufacturers' recommendations, including but not limited to recommendations regarding the full discharge of the batteries on a regular basis; and • The reason for and duration of battery usage is properly documented.
66	CTSPs should undertake regular testing and maintenance of their standby power systems to ensure that they perform satisfactorily under failure conditions.
67	CTSPs should make adequate arrangements to ensure that a supply of fuel for back-up generators is available, with contracts in place for replenishment.

68	CTSPs should plan to mitigate the threat of electrical conditions and strive for network interfaces that can withstand or prevent onward transmission of electrical signals or conditions that are outside normally expected operating values.
69	Where practical and feasible, sites without overlapping coverage from other locations should have backup battery power.
70	During emergencies, CTSPs should be afforded prioritized access to their sites, prioritized and reliable access to fuels and generators, and prioritized restoration of utility power.

Appendix 2 to Telecom Notice of Consultation CRTC 2025-226

Recommendations on resiliency measures for network operation

The following recommendations are from *Assessment of Rogers Networks for Resiliency and Reliability Following the 8 July 2022 Outage* (the Xona Partners Report):

1	Ensure that the audit process for network configuration changes is effective and involves different teams within the organization, such as engineering, operations, and project management. It is also advisable to involve equipment vendors where the configuration changes pertain to critical infrastructure, such as the Internet Protocol (IP) core network.
2	Conduct lab tests of planned configuration changes and ensure that the lab equipment and test scenarios accurately reflect the production network.
3	Carefully manage the number of configuration changes completed in a single maintenance window and leverage tools and processes for automatic rollback of configuration parameters.
4	Implement an automated alarm prioritization solution to suppress unnecessary alarms for every type of change and to allow staff to focus on the important alarms.
5	Provide critical staff with secondary means to communicate, such as Subscriber Identity Module (SIM) cards from third-party network operators.
6	Simulate and practice network failure and outage scenarios to uncover deficiencies in the network architecture and the incident management process.
7	Implement incident response training and drills to uncover weaknesses in architecture, operations, and business processes that adversely impact outage recovery efforts.
8	Implement incident management response key performance indicators to benchmark the incident response effort and improve its effectiveness.
9	Designate clear roles and responsibilities for personnel to better respond to network outages.
10	Consider calculating the cost impact of a network outage to help mitigate the consequences of incidents through decision-making on resource allocation and communication with stakeholders to preserve brand-image and financial stability.

The following recommendations are from *Telecommunications Network Resiliency in Canada: A Path Forward* (the Canadian Security Telecommunications Advisory Committee [CSTAC] Report).

11	Where practicable, Canadian Telecommunications Service Providers (CTSPs) should keep adequate stocks of spare parts and consumable materials on site or at a convenient depot located within a short distance to sites. Additionally, CTSPs may consider contracts with suppliers to hold buffer stocks on behalf of the provider. Particular care should be taken for items sourced from overseas in the event of transport or communication disruptions. Security risks posed by practicable supply chain interruptions should be considered.
12	CTSPs should, where practicable, have effective operational processes in place, covering at least the following areas: a) Fault management b) Planned works and planned maintenance c) Configuration/change management d) Performance management e) Risk management f) Capacity management g) Testing
13	CTSPs should provide reasonable notice to the affected parties of any planned work/maintenance that carries significant risk of impairment to essential services of interconnected CTSPs.
14	CTSPs should, where practicable, ensure Change and Configuration Management processes are established: good configuration/change management entails keeping a reliable inventory of network resources and having documented robust processes for the allocation of resources and management of changes that may pose significant risks to the continued delivery of services.
15	CTSPs should, where practicable, aim for robust performance management systems, processes and operational practices. Effective performance management involves the use of data from the network management systems and elsewhere to monitor network performance, to gauge performance against specified standards and to manage network capacity to meet specified grades of service.
16	CTSPs should, where practicable, have robust security management systems, processes and operational practices and reference should be made to other sections in these recommendations relating to security management.
17	CTSPs should, where practicable, have robust risk management practices. Effective risk management in this context involves assessing the design requirements of process, procedure, networks, systems and services, identifying any vulnerabilities or shortfalls and assessing potential impacts and where appropriate designing mitigating controls to manage those risks where they have been assessed as posing a significant threat to continued operations.
18	CTSPs should develop capacity management processes and operational practices. Real time capacity management involves the ability to gather data from various parts of the network to allow assessments to be made concerning real options to manage routing in real time. This may also include the gathering of data from signaling links, Internet gateways and interconnect routes with other CTSPs.

19	Complex systems are constantly evolving and being updated. Consequently, CTSPs should maintain a workforce that possesses the required capabilities, skills and expertise to design, operate and maintain such systems.
20	Overall, resilience of the network and services should be delivered through an appropriate combination of resilient equipment, redundancy, restoration, repair and review.
21	If there is congestion following an outage on a multi-services network, Quality of Service (QoS) and prioritization mechanisms should be configured, where practicable, to protect traffic and services that are marked critical or higher priority.
22	Where technically and economically practicable, CTSPs may deploy temporary cell sites during disaster recovery situations. The ability and suitability of such a deployment will depend on availability of equipment, safe road access and backhaul capability in the required area, as well as the expected duration of the outage.
23	CTSPs may explore the feasibility of temporarily sharing available spectrum with a fellow CTSP in the event one is experiencing a severe network outage resulting in customers' services being impacted. A CTSP may be able to minimize negative customer impacts by using another CTSPs spectrum for a short period of time to quickly increase network capacity. Support from ISED, would be required to enable the expeditious implementation of this recommendation in any particular severe network outage event.
24	In order to manage service disruptions, service infrastructure should support multiple levels of service availability depending on the severity of the disruption and the remaining available resources in the network.
25	Within each service availability level, the service infrastructure should support multiple grades of service depending on the service (voice, video, web-browsing, etc.). Resources should be assigned to higher priority services prior to supporting those further down the list.
26	Under failure or excessive load conditions, where practical and feasible, CTSPs should support migrating or scaling out the service infrastructure onsite (on the same or different service infrastructure) or on a separate service infrastructure at a different site (including the public cloud).
27	Each CTSP may consider leveraging their own robust problem management and root cause analysis processes to ensure lessons are identified from "near misses" or actual failures. Lessons learned may be cascaded across the impacted CTSP as an outcome of the problem management and root cause analysis process.
28	CTSPs should consider formally documenting their service continuity processes. Key areas for consideration include: Process Description, Plan Scope, Assumptions, Dependencies, Responsibility, Risk Assessment, Business Impact Analysis, Prioritization, Plan Testing, Training and Plan Maintenance.
29	During incidents which result in the invoking of their service continuity plan, CTSPs should, if practicable, establish a designated Emergency Operations Centre that is geographically diverse.

30	CTSPs should consider having recovery plans in place should a network failure occur and where such plans exist, they should test their service continuity plan.
31	CTSPs should consider making use of multiple alternative communication devices, systems and service providers for use by their critical staff during emergencies.
32	CTSPs should maintain their participation in the Canadian Telecom Emergency Preparedness and Management (CTEPM) and Canadian Telecommunication Cyber Protection (CTCP) working groups, both of which are sub committees of the Canadian Security Telecommunications Advisory Committee (CSTAC). These sub-committees include advisory sessions, exercises, best practices and opportunities for related training. They should review existing and proposed best practices and consider implementation.
33	CTSPs should maintain a contact roster and provide it to the Ministry of Innovation, Science and Economic Development (ISED) and update this contact roster as changes occur or at the request of ISED.
34	CTSPs should consider creating a remote system access strategy for use during emergencies recovery.
35	CTSPs should have contact lists for the various specialist functions and key vendors needed during emergencies so that equipment and skilled specialists can be deployed to emergency sites in the most significant cases. CTSPs may consider supplying dual SIM cards for critical suppliers.
36	CTSPs should, where practicable, develop and maintain processes to routinely archive system media backups and provide storage in a "secure off-site" facility which would provide geographical diversity.
37	To prevent being vulnerable to the failure of a single part of the system, CTSPs should, where practicable, assess the risks and prioritize recommendations for resiliency investments.
38	Recommendations pertaining to emergency roaming are covered under the September 9, 2022 CSTAC Memorandum of Understanding (MOU).
39	For fault management to be effective, CTSPs should, where practicable, have staffing, systems and processes for 24/7 fault detection and fault monitoring, fault documentation and impact analysis, a process for determining the cause(s) of faults (Root Cause Analysis), and means to bypass faults to maintain network performance and fault fixing.
40	In the case of interconnected CTSPs, it is expected that when and where practicable: a) Any party becoming aware of an interconnect service fault will inform all other associated operators. b) In such an event, prompt action to resolve the fault should be taken by the party in whose system the fault has arisen. c) The management of planned maintenance and faults between interconnected operators should be part of more general operations and maintenance (O&M) procedures between interconnected operators.

41a	Where practicable, CTSPs should have procedures in place for testing the network, including proactive testing of network components. It is recognized that it is impossible to test something as complicated as a modern telecommunications network with complete certainty.
41b	CTSPs should be able to demonstrate that potential failure scenarios have been envisaged and that contingency plans for service restoration have been prepared, tested, and are in place. The objective of the contingency plan should be to maintain the CTSPs ability to fulfil, as a minimum, its service obligations in the event of network failure.
42	CTSPs should, as appropriate, run preventative maintenance programs for network site support systems including emergency generators, Uninterruptible power supply (UPS), Direct Current (DC) plant, High Voltage (HV), and fire suppression systems.