Telecommunications Network Resiliency in Canada: A Path Forward

Canadian Telecommunications Network Resiliency Working Group

March 2023

Table of Contents

1. Introduction

Surrounded by three oceans, Canada is the second largest country by land mass and 39th in terms of population, with most of its population clustered along its southern border and vast areas of low population density. In addition, much of the country's terrain is challenging and subject to extreme environmental and weather events, many of which are becoming increasingly pronounced due to the impacts of climate change.

Building, maintaining, and ensuring the effective operation of a telecommunications network is a daunting task in any circumstance, but building networks is exceptionally difficult in Canada given the fundamental characteristics of our country. These challenges are further complicated by jurisdictional divisions between different levels of governments, some current and potential legal requirements that could impede the ability of Canadian Telecommunications Service Providers (CTSPs) to respond to outages.

Despite this complex and challenging environment, CTSPs, through investment and ingenuity, have built remarkable telecommunications networks.

CTSPs seek to outpace the global telecommunications industry in network resilience, availability, and reliability, and the drive for continuous improvement on behalf of their customers is at the core of their collective raison d'être. Canadians, industry and other infrastructure sectors increasingly depend on telecommunications services to conduct economic and social activities, as well as access basic and emergency services. This connectivity expectation became acute during the recent COVID-19 pandemic, during which remote connectivity was both necessary for our health, as well as our economic productivity. Moreover, the increasing frequency and intensity of environmental events, such as floods and wildfires, has made the availability of network connectivity even more important to helping ensure the physical well-being of Canadians. CTSPs' drive for improved resilience, availability, reliability, and fast recovery, is also consistent with the Minister of Innovation, Science and Industry's mandate to increase the resilience of CTSP networks.

Taking these realities into consideration, the Minister of Innovation, Science, and Industry requested that the industry convene a working group to develop recommendations aimed at reducing the likelihood of severe network outages and mitigating their impact when one occurs. Accordingly, the Canadian Telecommunications Network Resiliency Working Group (CTNR-WG) was created with representatives from CTSPs and Innovation Science and Economic Development Canada (ISED). Its aim has been to build upon the accomplishments of the Canadian Security Telecommunications Advisory Committee (CSTAC) and to develop recommendations on which CTSPs are aligned.

The CTNR-WG recommendations are guiding principles for CTSPs to continue improving the reliability and resiliency of their networks. The recommendations may be adapted and implemented in a manner that aligns with the individual circumstances of each CTSP. CTSPs are encouraged to implement these recommendations, to the extent practicable (including physically, operationally, technically, and commercially), as they strive for dependable connectivity and resiliency for the benefit of their customers.

This document is meant to guide CTSPs, not impose obligations, and recommendations contained in this document are neither directive nor mandatory. Any recommendation that uses words such as, "*should*"

or "*may*", is to be understood as a recommendation to be considered to the extent practicable that a CTSP can implement it, given their individual business circumstances and operational, physical, and regulatory realities.

Fundamentally, network resiliency and reliability require that CTSPs strive for always-on availability of service, to the maximum extent practicable, from a commercial, operational, and technical perspective, in the context of operating complex networks across the Canadian landscape. Effective network resiliency suggests that CTSPs aspire to have immediate fault-mitigation and rapid restoration mechanisms to reduce the impact of an adverse event on service delivery should the first line of connection degrade or fail. Such mechanisms may be either passive and/or active. CTSPs should also work towards ensuring, to the extent practicable, the deployment and maintenance of resilient communication networks for emergency recovery personnel (e.g., emergency operations, network operations centers and other CTSP personnel involved in emergency response). This includes striving for reliable partnerships between a CTSP and any third party vendors that may be involved in the delivery of a CTSP's communications service. Further, to the extent practicable, CTSPs should support each other during times of need, to help preserve the connectivity of all users of Canada's telecommunications networks.

1.1. General Recommendations on Telecommunications Network Resiliency

The high-level recommendations for network resiliency proposed by the CTNR-WG, are to be implemented to the extent practicable by a CTSP in view of its commercial, operational, technical and physical circumstances, and are subject to applicable laws and regulations. These serve as a basis for the more particular recommendations set out in this Report, and are as follows:

1. Seek to establish redundant pathways, in particular, facilities that support main fiber access should have physically diverse fiber routes between critical infrastructures, especially those routes with access to emergency services such as 911.

2. Attempt to identify and mitigate single points of failure and strive for geographic diversity of services and network elements. Where essential equipment is co-located, priority should be given to physical separation, such as a fire break, to reduce the possibility of common mode failure.

3. Design physical structures (both indoor and outdoor) to be as resilient as practicable, in the circumstances, to withstand extreme environmental conditions and weather events (e.g., wildfires, floods, windstorms, ice, etc.), as well as the loss of commercial utility (e.g. hydroelectric) power supplies. Further, CTSPs should strive to source their equipment and systems from reliable, capable, and reputable suppliers.

4. Strive to install communications cables underground to mitigate damage from possible structural degradation and/or natural disasters. Should communications cables be buried, known risks attributed to this design should be documented and mitigated to the extent practicable.

5. Endeavor to establish robust business practices that enable rapid assessment of network issues, along with service continuity plans that support strong communication and responsiveness when adverse events cause major outages to critical services.

1.2. CTSP Asks of the Government of Canada

To strengthen CTSPs' efforts to improve the resiliency of Canada's telecommunications networks, the CTNR-WG recommends that the Government of Canada take timely action (including, where appropriate, initiating a process to liaise with other relevant levels of government) in priority areas, as follows:

1. Create an article of federal law that specifically protects CTSPs' critical and ancillary infrastructure and maximizes criminal penalties in the event of willful or negligent damage to, and/or acts of vandalism or theft of critical network infrastructure. As a reference, the U.S. Criminal Code criminalizes such acts through financial penalties, imprisonment, or both [1]. CTSPs will endeavour to provide data to ISED on a strictly confidential basis that could include information such as (but not specific to or limited to) the type of damage (e.g., a fiber cut) and/or the relevant details.

2. Implement a timely approval process by ISED for short-term emergency spectrum sharing in the event of a severe network outage, when it is jointly requested by the CTSPs involved. Such a process could be helpful when a "Triggering Event Declaration" is made under the September 9, 2022 Memorandum of Understanding [2] but also in other emergency circumstances which may not qualify as or rise to the level of a Triggering Event [2].

3. Liaise with provincial and territorial governments with a view to enhancing measures to enforce compliance with existing regulations related to "Dial Before You Dig" legislation [3] or other similar underground infrastructure notification regulations, in order to minimize any potential damage to underground telecom facilities resulting from non-compliant or careless excavation practices.

4. Liaise with the telecom and electricity/hydro sector participants, including the Canadian Standards Association (CSA), to collaborate on improving critical infrastructure resiliency through changes to the Canadian Electrical Code or other construction standards.

5. Facilitate network construction and reliability access to public places and publicly owned passive infrastructure. Specifically, through amendments to the *Telecommunications Act* and *Radiocommunication Act* [4]:

    a. Expand the CRTC's authority over publicly-owned passive infrastructure to clearly include access to all public property capable of supporting [network] facilities, such as street furniture.
    b. Assert federal jurisdiction in the wireless tower siting and develop new site approval processes that avoid unnecessary delay and burden and expedite the delivery of wireless services to Canadians.
    c. Expand the scope of the CRTC's authority over support structures to include CTSPs access to the support structures of provincially regulated utilities.

6. Telecommunications networks are critical infrastructure that, while federally regulated, are highly dependent on provincial/territorial regulated utilities and services. The CTNR-WG asks that the federal government coordinate the following amongst both federal and provincial/territorial emergency management organizations:

    a. Priority access, at all times (including during emergencies) for CTSP technicians to their sites to effect repairs and fuel generators;
    b. Priority access for CTSPs to fuels during recovery efforts following major emergencies and consider reliable/resilient fuel dispensaries; and
    c. Priority restoration of utility power to CTSP sites by provincial/territorial utility companies.

7. Exemption from labour regulations and legislation that is fundamentally inconsistent with the Minister's prioritization of network resiliency – specifically the legislation prohibiting the use of replacement workers, which, if applied to CTSPs, could result in outages during work stoppages and Hours of Work limitations under Part III of the Labour Code in the contexts of emergencies, which would limit the ability of CTSPs to respond to outages.

8. In regions where there is no wireless coverage, or where there exists service from only one CTSP, the federal government should provide funding or tax credits to bolster that CTSPs' reliability. This will support the CTSP in supplying backup batteries, generators, diverse backhaul investments, etc.

9. Encourage and liaise with provincial, territorial and municipal governments to ensure that local processes support accelerated tower construction and other radio apparatus siting approval times.

1.3. Scope of Recommendations

The CTNR-WG brings forth these recommendations with the understanding that certain telecommunications technologies are out of scope and therefore have not been considered in this document. For example, the resiliency, availability, and reliability of submarine communications cables and cloud-based software have not been considered. Emerging and future communications technologies are also considered out of scope. Nevertheless, it is the aim of the CTNR-WG that the recommendations herein are broad enough for CTSPs to consider them, where, commercially, operationally, technically, and physically practicable, in connection with CTSPs' provision of communications technologies to their customers in the future.

As well, the recommendations have been developed based on what the industry looks like today, at the date of the publishing of this report. The recommendations could be revisited in the future as the telecommunications industry evolves to ensure that they remain relevant and helpful in a future context.

Customer experience is at the heart of the CTNR-WG's effort in developing these recommendations. Canadians demand uninterrupted availability of their services and CTSPs strive to deliver on this front. As CTSPs make every effort to meet this demand, they also seek to bring to the attention of government and relevant stakeholders the fact that third party partners that deliver a service using a CTSPs network

also have a duty to provide reliable service to the best of their ability. For example, government and relevant stakeholders may wish to consider asking third parties, especially those that support critical business operations, such as financial services, to develop their own resiliency and business continuity plans in the event of a customer and/or business impacting outage or degradation to their communications and information systems and infrastructure. To the extent that jurisdictional challenges exist, ISED should consider engaging with appropriate provincial counterparts to this end.

It is the CTNR-WG's desire that CTSPs work to strengthen the resiliency of their networks consistent with the recommendations to the extent practicable given the circumstances and facilities of each CTSP. The recommendations have been prepared in the spirit of collaboration, with the understanding that the Government of Canada is also committed to supporting network reliability. To that end, as described above, the CTNR-WG encourages the Government of Canada to work to evolve the policy environment (as described in Section 1.2.) to better enable CTSPs to provide reliable and high-quality services to Canadians. Reliable networks require effective long-term planning, significant capital investments, access to expertise and resources, and unrelenting rigor and discipline. To continue to do that successfully requires the federal government to be a partner in the quest to maintain Canada as a leader in telecommunications. Government action on the listed priority areas in Section 1.2. will enhance the resiliency collaboration with CTSPs.

1.4. Acknowledgements

Led by Co-Chairs, Juan Ramos, Vice President, Network Engineering, Vidéotron, Brian Lakey, Vice President, Reliability Centre of Excellence, TELUS, and Wen Kwan, Senior Director, ICT Resilience, ISED, the CTNR-WG is comprised of twelve of Canada's telecommunications industry participants (full membership is listed in the Appendix), who gathered on a weekly basis for six months with a collective vision to develop a policy document for the advancement of telecommunications network resiliency. The CTNR-WG is grateful to have had this opportunity to collaboratively share our experience, knowledge and best practices and is proud of the dedication and collaboration that was achieved in order to align on industry best practices and a collective direction for the future of network resiliency in Canada. The CTNR-WG would like to thank Minister Champagne for spearheading the initiation of the CTNR-WG, and for providing the space to have collaborative conversations about the importance of network resiliency across Canada. To the knowledgeable public servants of ISED, the Canadian Centre for Cyber Security and Public Safety Canada, the CTNR-WG is deeply appreciative of your steady and thoughtful guidance and facilitation throughout the development of this document.

The CTNR-WG leveraged the United Kingdom's Electronic Communications Resilience & Response Group's (EC-RRG) report of June 2021 entitled, *Resilience Guidelines for Providers of Critical National Telecommunications Infrastructure* [5], as well as ITU-T Focus Group on Disaster Relief Systems, Network Resilience and Recovery's technical report of May 2014 entitled, *Requirements for Network Resilience and Recovery* [6], to help inform and guide the structure of this reports' recommendations for telecommunications resiliency in Canada.

1.5. Executive summary

Six sub-groups were constituted to address key elements that are intrinsic to network resiliency.

Accordingly, the CTNR-WG has organized and grouped their recommendations for network resiliency by the following six key element headings:

1. Core Networks
2. Physical Structures
3. Services and Applications
4. Internet Services and Infrastructure
5. Access Networks
6. Processes

Members of the CTNR-WG agree that the recommendations below, respecting the key elements of network resiliency, should be implemented, by a given CTSP, to the extent commercially, operationally, technically and physically practicable as it determines given its particular circumstances. Each set of recommendations below is, therefore, to be read and understood in that context.

2. Core Networks

Core networks should be protected against single points of failure. If a network element fails in a particular region, that failure should not spill over into other regions. Geo-redundant measures for centralized core network elements should be taken to protect against regional-based failures, and measures to protect against signaling storms should be implemented for control and signaling systems.

2.1. Core Infrastructure Resiliency

CIR-01	Where practicable, designs for the core networks of CTSPs should consider the possibility of loss of human physical access to operations centers, 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 center, building or site. Contingency plans should aim to cover the liaison with emergency responders concerning physical access in order to maintain essential services.
CIR-02	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.
CIR-03	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.
CIR-04	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. 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.
CIR-05	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.
CIR-06	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.
CIR-07	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.
CIR-08	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.
CIR-09	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.

CIR-10	Where appropriate and where commercially feasible, CTSPs may consider implementing diverse duct tracks or routes as physical separation of fiber 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.
CIR-11	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.

2.2. Core Network Failures

CNF-01	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.
CNF-02	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.
CNF-03	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.
CNF-04	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.
CNF-05	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.

CNF-06	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.

2.3. CSTAC Best Practices

CBP-01	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 [7] and its accompanied Critical Infrastructure Protection Standard [8] or future releases.
CBP-02	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.
CBP-03	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.
CBP-04	Anti-spoofing filtering: Where practicable, CTSPs should implement anti-spoofing filtering to prevent traffic with spoofed source IP addresses.
CBP-05	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 [7] and its accompanied Critical Infrastructure Protection Standard [8].
CBP-06	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

3. Physical Structures

The location of CTSPs' physical structures and their security features should, where feasible practicably, economically, and physically, be at or above industry standards of environmental preparedness while offering geographically separate and diverse network paths, where practicable.

3.1 Structural Environmental Resilience

SER-01	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
SER-02	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
SER-03	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

SER-04	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).

3.2 Major Fiber Cuts

MFC-01	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.
MFC-02	Where appropriate and practicable, diverse entry and exit points, e.g., to sites or buildings, should be provided (including cable entries).
MFC-03	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).
MFC-04	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.
MFC-05	Where possible, for every new fiber installation or modification to an existing fiber network, CTSPs should consider implementing an internal process to record the precise geolocation into an internal database.

3.3 Transport Network Facilities

TNF-01	Where possible, CTSPs should strive to have their main regional centres placed in a decentralized manner and region.
TNF-02	A CTSP's main regional center should be backed up by other regional centres, to the extent practicable.
TNF-03	Critical regional centres should be connected, where practicable, to other regional centers via a detour route to minimize the impact when the original connection route is broken.
TNF-04	The transport facilities that connect the main regional centres should be physically

	redundant, where practicable (i.e., multi-routed).
TNF-05	The main fiber access facilities should be installed as two or more physically diverse routes whenever practicable.
TNF-06	The telecommunication lines that connect the main regional centres should be laid in different transport facilities whenever practicable.
TNF-07	A CTSP's main transport facilities should allow for telecommunications links to be switched to alternate telecommunications links as quickly as practicable, when necessary.
TNF-08	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.
TNF-09	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.
TNF-10	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.
TNF-11	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.
TNF-12	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.

3.4 Equipment Location, Energy and Materials

LEM-01	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).
LEM-02	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.
LEM-03	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).
LEM-04	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.
LEM-05	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.
LEM-06	Automatic fire alarms and, where appropriate, fire suppressants should be deployed appropriately for buildings and machine rooms.
LEM-07	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.
LEM-08	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.
LEM-09	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. • 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.
LEM-10	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.
LEM-11	• 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.
LEM-12	CTSPs should undertake regular testing and maintenance of their standby power systems to ensure that they perform satisfactorily under failure conditions.
LEM-13	CTSPs should make adequate arrangements to ensure that a supply of fuel for back-up generators is available, with contracts in place for replenishment.
LEM-14	Where practicable, 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.
LEM-15	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.

3.5 Authorized Access and Input

AAI-01	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.
AAI-02	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.

4. Services and Applications

Equipment controlled and supported by software should be designed to protect against accidental or planned external interference, and to automatically restart when interference nevertheless occurs. Service infrastructure should support an array of different grades of services and Public Safety Answering Point (PSAP) architectures should consider diverse connectivity.

4.1. Failure of System and Software

FSS-01	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.
FSS-02	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.

5. Internet Services and Infrastructure

The Internet is the global communications network that allows any endpoint connected (with a globally reachable IP (Internet Protocol) address) to communicate directly with any other endpoint. An endpoint could be a laptop, a smartphone, an information server, a smart device (a.k.a. IoT, Internet of Things), etc.

Typically, when a server (or a group of servers) endpoint is responding with contents that a user endpoint has requested, the server is delivering an ***Internet service***. For example, when a user types a term or a group of text in the search window of the Internet browser and hits “Enter”, the user is requesting a “search” from one search engine service connected on the Internet (e.g., Google, Bing). By way of another example, when a user sends an email from a smartphone, the user is requesting the email to be relayed through a series of email servers connected on the Internet; the email will eventually be delivered into the electronic mailbox of the intended recipient(s).

Except for a small number of Internet infrastructure services (and the associated servers) that support the delivery of the Internet connectivity services provided to the users (endpoints) by a CTSP, the CTSP is responsible only for the connectivity between the user endpoint and the Internet services (and the associated servers). Each CTSP should strive to ensure the data traffic between the endpoints is delivered in a timely manner (traffic can be sent back and forth). CTSPs arrange for global reachability and exchange of traffic by establishing network connections with interconnection partners (such as Internet transit providers, internet peering partners, 3rd party Content Delivery Network (CDN) providers and caching infrastructure providers. The CTSP is not aware of, or responsible for, the delivery of the actual applications and services that the user is transacting over the Internet. CTSPs are only responsible

for components of the end-to-end delivery of Internet services. The end-to-end delivery of most Internet services depends on services, resources, servers and network infrastructures provided by 3rd party providers, including the interconnection partners, cloud services providers, and the actual content and services providers distributed globally over the public Internet. Reliable and resilient operations of these 3rd party providers therefore are also essential components of delivering Internet services in Canada.

In order for any user (Internet endpoint) to enjoy a range of applications and services over the Internet, such as streaming video (e.g., Netflix, YouTube), messaging (e.g., iMessage, WhatsApp), e-commerce (e.g., shopping on Amazon, Alibaba), social media (e.g., Facebook, Instagram), government services (e.g., Canada.ca), gaming, banking, etc., a CTSP typically provides its users with access to the CTSP's Internet infrastructure services, such as DNS (Domain Name Service) and Email.

DNS and Email are amongst the most critical Internet infrastructure services typically offered by a CTSP. DNS is the "phone book" of the Internet. The globally distributed DNS platform is responsible for the real time translation of domain names (e.g. www.canada.ca) to the corresponding IP address of corresponding endpoint or server (e.g., IP address for the www.canada.ca server). If there is a disruption in the DNS services offered by a CTSP, users using the CTSP provided DNS servers will experience a severe degradation of Internet services as most Internet services, such as web browsing, will stop working.

The following recommendations aim to ensure the highest level of reliability and resiliency of the critical Internet infrastructure services, DNS (if offered) and Email services (if offered) in particular, delivered within the control of a CTSP as part of the Internet connectivity services by the CTSP.

ISI-01	To the extent practicable, CTSPs should consider deploying redundant DNS servers with geo-diversity and resiliency consistent with CSTAC Critical Infrastructure (CI) Protection Standard, Section 1.2.3.6 (dated January 2020) [8]. CTSPs should also consider deploying redundant Email servers using similar geo-diversity and resiliency standards.
ISI-02	To the extent practicable, CTSPs should consider establishing a roadmap of implementation of protections of Domain Name Service (DNS) services as recommended by the Canadian Centre for Cyber Security as per ITSAP.40.021 (dated August 2022) [9] and the DNS Service Protection Controls in the CSTAC Critical Infrastructure Protection Standard [9].
ISI-03	To the extent practicable, CTSPs should strive for their DNS servers to operate within acceptable performance parameters (e.g., response time, latency) and connect effectively and securely to the global distributed DNS architecture.
ISI-04	To the extent practicable, CTSPs should consider establishing a roadmap of implementation of email domain and server protection as recommended by the Canadian Centre for Cyber Security as per ITSP.40.065 (dated August 2021) [10].

ISI-05	To the extent practicable, CTSPs should strive for their email relay servers to operate within acceptable performance parameters including, but not limited to, by effectively filtering unsolicited emails (a.k.a. SPAM emails).
ISI-06	Third party Internet services and content providers may leverage their own caching servers or commercial CDN caching servers deployed within a CTSPs network. To the extent practicable, CTSPs should consider establishing a mutually agreed operating framework (including maintenance planning, outage notification and other operational procedures) with the 3rd parties or CDN/cache providers in order to minimize unexpected behaviour of the caches or traffic overload situation in order to maintain overall reliability and resiliency of the corresponding end-to-end 3rd party internet services.
ISI-07	To the extent practicable, CTSPs should consider establishing a mutually agreed operating framework (including maintenance planning, capacity planning and outage notification procedures) with each interconnection partner to minimize unexpected traffic behaviour or traffic overload situations.
ISI-08	To the extent practicable, CTSPs should consider planning and documenting interconnection failure scenarios such that CDN/cache, Internet peering, Internet transit and any other form of interconnection capacity are sufficient to maintain overall reliability and resiliency of the Internet services, in the event that one of the forms of interconnection capacity becomes degraded or unavailable.
ISI-09	To the extent practicable, CTSPs should consider maintaining adequate reserved network capacity to handle extraordinary load and events on their internet services infrastructure servers.
ISI-10	To the extent practicable, CTSPs should consider deploying appropriate platforms and measures to protect their DNS servers, Email servers, and other critical Internet Infrastructure servers against Distributed Denial of Service (DDOS) cyber-attacks and to ensure continuous operations of these infrastructure servers.

6. Access Networks

In this report, the term “access networks” refers to connections between network aggregation points and the customer. This definition includes mobile backhaul to the cell site or tower as well as “last mile” connections between aggregation points or cell sites and the customer (both wireline and wireless).

Various approaches to reliability and survivability are described in this section, but it is important to note that the level of effort employed in this portion of the network varies by location and density. For example, a mobile network in urban areas is built for traffic density with significant overlap between cell sites. As such, a single or even multiple site outage in these areas rarely results in complete coverage failure. On the other hand, rural areas tend to provide unique coverage from a given site without much overlap with its neighbour. Therefore, the importance of power or backhaul circuit recovery in these

areas is typically higher than for similar limited site outages in urban zones.

ACC-01	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.
ACC-02	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.
ACC-03	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.
ACC-04	Where practical and feasible, sites without overlapping coverage from other locations should have backup battery power.
ACC-05	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.
ACC-06	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, as noted above in Section 1.2 action #2, would be required to enable the expeditious implementation of this recommendation in any particular severe network outage event.
ACC-07	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.

7. Processes

CTSP processes are a key component of ensuring telecommunications networks continue to run smoothly, and to enable quick identification and responses to major events. This section focuses on the processes that are most critical for maintaining high quality networks, along with well managed and timely responses that are required if or when major failures occur.

7.1. Emergency Management and Service Continuity Planning

EMC-01	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.
EMC-02	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.
EMC-03	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).
EMC-04	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.
EMC-05	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.
EMC-06	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.
EMC-07	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.
EMC-08	CTSPs should consider making use of multiple alternative communication devices, systems and service providers for use by their critical staff during emergencies.
EMC-09	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.
EMC-10	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.
EMC-11	CTSPs should consider creating a remote system access strategy for use during emergencies recovery.
EMC-12	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.
EMC-13	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.
EMC-14	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.
EMC-15	Recommendations pertaining to emergency roaming are covered under the September 9, 2022 CSTAC Memorandum of Understanding (MOU).

7.2. Process Requirements for Resilient Telecom Networks

PRR-01	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
PRR-02	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.
PRR-03	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.
PRR-04	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.
PRR-05	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.
PRR-06	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.
PRR-07	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.
PRR-08	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.
PRR-09	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.
PRR-10	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. 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.

PRR-11	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.
PRR-12	CTSPs should, as appropriate, run preventative maintenance programs for network site support systems including emergency generators, UPS, DC plant, HV, and fire suppression systems.
PRR-13	Overall, resilience of the network and services should be delivered through an appropriate combination of resilient equipment, redundancy, restoration, repair and review.

8. Next Steps

The CSTAC, the overarching committee to the CTNR-WG, is committed to the continuous improvement of their members' networks' resiliency, availability, and reliability. As the number of telecommunications subscribers increases with population growth, so too will the number of devices and services that will come online due to the evolution and emergence of new technologies. These factors will put added pressure on the availability of CTSPs' networks and supporting infrastructure. CTSPs are adjusting for this growth and are actively implementing measures to accommodate the increased demand.

The CSTAC will continue to address issues and exchange information about the rapidly evolving telecommunications industry within Canada. Providing secure and reliable telecommunications services to Canadians will remain a focus for all industry participants.

9. Conclusion

The wide-ranging recommendations within this report were developed through an open, honest and collaborative information exchange from all of the working group members. The foundation on which these recommendations are built is the unwavering commitment of CTSPs to provide resilient and reliable services, coupled with rapid recovery mechanisms, for the benefit of their customers.

The CTNR-WG looks ahead to the future of Canada's telecommunications industry with a clear vision to provide world-leading network resiliency, availability, and reliability for all Canadians.

10. Glossary

CRTC	Canadian Radio-television and Telecommunications Commission
CTSP	Canadian Telecommunications Service Providers
CSTAC	Canadian Security Telecommunications Advisory Committee
CTNR WG	Canadian Telecom Network Resiliency Working Group
DNS	Domain Name System
MFA	Multi-Factor Authentication
SS7	Signaling System No. 7

11. References

[1] 18 U.S. Code § 1362 – Communication lines, stations or systems:
Whoever willfully or maliciously injures or destroys any of the works, property, or material of any radio, telegraph, telephone or cable, line, station, or system, or other means of communication, operated or controlled by the United States, or used or intended to be used for military or civil defense functions of the United States, whether constructed or in process of construction, or willfully or maliciously interferes in any way with the working or use of any such line, or system, or willfully or maliciously obstructs, hinders, or delays the transmission of any communication over any such line, or system, or attempts or conspires to do such an act, shall be fined under this title or imprisoned not more than ten years, or both.

In the case of any works, property, or material, not operated or controlled by the United States, this section shall not apply to any lawful strike activity, or other lawful concerted activities for the purposes of collective bargaining or other mutual aid and protection which do not injure or destroy any line or system used or intended to be used for the military or civil defense functions of the United States.
https://www.govinfo.gov/app/details/USCODE-2021-title18/USCODE-2021-title18-partI-chap65-sec1362/summary

[2] Memorandum of Understanding on Telecommunications Reliability (July, 11, 2022)
https://ised-isde.canada.ca/site/mobile-plans/en/memorandum-understanding-telecommunications-reliability

[3] Ontario Underground Infrastructure Notification System Act, 2012, S.O. 2012, c. 4
https://www.ontario.ca/laws/statute/12o04#BK1

[4] *Telecommunications Act*: https://laws-lois.justice.gc.ca/eng/acts/t-3.4/
Radiocommunication Act: https://laws-lois.justice.gc.ca/eng/acts/r-2/

[5] EC-RRG Resilience Guidelines for Providers of Critical National Telecommunications Infrastructure (June 2021)
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1020214/EC-RRG_Resilience_Guidelines_v3.1__2021_.pdf

[6] ITU-T Focus Group on Disaster Relief Systems, Network Resilience and Recovery: Requirements for Network Resilience and Recovery (May 2014)
https://www.itu.int/dms_pub/itu-t/opb/fg/T-FG-DRNRR-2014-6-PDF-E.pdf

[7] Security Best Practice Policy for Canadian Telecommunications Service Providers (CTSPs) V1.1 (January 20, 2020)
https://ised-isde.canada.ca/site/spectrum-management-telecommunications/sites/default/files/attachments/2022/CSTAC_CCCSTsecuritybestpractices2020_01EN.pdf

[8] Critical Infrastructure Protection Standard for Canadian Telecommunications Service Providers (CTSPs) V1.1 (January 20, 2020)
https://ised-isde.canada.ca/site/spectrum-management-telecommunications/sites/default/files/attachments/2022/CSTAC_CCCSTcriticalInfrastructureProtection2020_01EN.pdf

[9] Domain Name Service (DNS) tampering - ITSAP.40.021 (August 2022)
https://cyber.gc.ca/en/guidance/domain-name-service-dns-tampering-itsap40021

[10] Implementation guidance: email domain protection (ITSP.40.065 v1.1) (August 2021)
https://cyber.gc.ca/en/guidance/implementation-guidance-email-domain-protection

12. Appendix

CTNR-WG Industry Membership	
Bell	Nick Payant, VP, Operations Services and Core Network
	Erone Quek, Technical Director, Network
Cogeco	Michel Blais, VP, Network, Operation, Technology Delivery
	Zouheir Mansourati, SVP and Chief Technology Officer
Eastlink	Pierre Guynot de Boismenu, Director, Network Engineering Wireline
Rogers	Bryce Mitchell, VP, Wireless Network Engineering
	Asit Tandon, VP, Network Operations
SaskTel	David Harley, Senior Director, Strategy, Planning and Development
Shaw	Brian O'Shaughnessy, SVP, Wireless and 5G Technology
	Cynthia Rathwell, Vice President, Legislative Policy & Strategy
TbayTel	Jamie Hays, VP, Operations and Outside Plant Engineering
	Tuomas Minor, Director, Network Operations
Telesat	Roger Korus, Director, Engineering
TELUS	Brian Lakey, VP, Reliability Centre of Excellence
	Alexandra Day, Sr Strategy Manager, Reliability Centre of Excellence
Vidéotron	Juan Ramos, VP, Network Engineering
Xplore	Nick Dewar, VP, Network Strategy
Zayo	Ron Hoseman, Sr Director, Service Operations
	Jeff Brown, Head of Canadian Operations