TELECOM NOTICE OF CONSULTATION
CRTC 2025-226

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

CANADIAN TELECOMMUNICATIONS ASSOCIATION

December 3, 2025

1. Introduction and Executive Summary

1. The Canadian Telecommunications Association (CTA) is pleased to provide its comments regarding Telecom Notice of Consultation CRTC 2025-226 - *Call for comments – Development of a regulatory policy on measures to improve the resiliency of telecommunications networks and the reliability of telecommunications services* (Consultation).

2. CTA is an industry association dedicated to building a better future for Canadians through connectivity. Our members include service providers, equipment manufacturers, and other organizations in the telecommunications ecosystem, that invest in, build, maintain, and operate Canada's world-class telecommunications and broadcasting networks.

3. Through our advocacy initiatives, research, and events, we work to promote the importance of telecommunications to Canada's economic growth and social development, and advocate for policies that foster investment, innovation, and positive outcomes for Canadians who rely on telecommunications and related services. Accordingly, the Association and its members have considerable interest in this Consultation.

4. To the extent that any comments in this submission conflict with a comment of an Association member, the comment of the member shall prevail with respect to that member.

5. CTA agrees that resilient, reliable communications are essential to Canadians' safety, economic participation, and quality of life. The question for this proceeding, however, is not whether resiliency matters, as it unquestionably does, but whether the evidence on record demonstrates the need for new regulatory mandates, and whether such mandates would meaningfully improve outcomes compared to the existing resiliency framework composed of extensive industry practices and voluntary measures already, supplemented by limited and targeted legislative and regulatory measures.

6. CTA submits that it would be premature and unwarranted to impose prescriptive resiliency requirements at this time. Although the Commission raises a wide range of technical, operational, and policy questions in the Notice, the record lacks evidence

of a systemic or widespread resiliency deficit across Canada. Canada's telecommunications service providers (TSPs) already demonstrate strong resiliency performance, supported by a competitive market in which network reliability is a key dimension of customer choice.

7. Furthermore, Canada has a robust and highly collaborative resiliency ecosystem. Through the Canadian Security Telecommunications Advisory Committee (CSTAC) and its network resiliency and cyber protection working groups, multi-carrier emergency coordination agreements, and ongoing engagements with federal, provincial, and territorial authorities, the industry has developed shared frameworks, best practices, and cooperative protocols to strengthen and improve the resiliency of telecommunications networks and services.

8. In rare cases where systemic risks are identified, such as cybersecurity across industries, Parliament responds through targeted legislation like Bill C-8 - *An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts*.

9. International benchmarking provides an equally important perspective. The *Telecommunications Resilience Analysis Benchmarks Report* commissioned by ISED and the Commission shows that Canada's current approach, which relies on market forces, voluntary best practices, and targeted public programs, is closely aligned with international norms. Across the jurisdictions surveyed, legislative and regulatory mandates relating to resiliency are generally limited to universal service, emergency services, cybersecurity, and outage reporting, all of which are well-established in Canada, while operational and technical measures are largely developed through industry collaboration rather than prescriptive rules.

10. Even where countries adopt targeted resiliency initiatives, such as Japan's seismic protections or Australia and New Zealand's government-funded programs in high-risk regions, these measures are grounded in specific national hazards and tailored to the circumstances of the local jurisdiction. The international evidence therefore strongly supports a flexible, principles-based approach in this proceeding rather than broad, prescriptive requirements.

11. Finally, resiliency is not solely a telecommunications problem. The Ofcom *Mobile RAN Power Resilience report*[1] illustrates this clearly. Most mobile service outages in the UK during major events were driven not by telecommunications equipment failures, but by prolonged loss of commercial power. The same is true in Canada where most disruptions arise from events outside TSPs' control, such as general extreme weather, third-party damage, vandalism, or utility failures, while preventative and remedial actions are often constrained or delayed by engineering and permitting restrictions or response times from external agencies and utility providers.

12. Mandating telecom-only measures without considering these dependencies as well as the significant costs associated with imposing telecom-only solutions would assign a disproportionate share of responsibility and costs to TSPs for risks that originate outside of their control. Such an approach would misalign responsibility and divert resources from telecommunications investments that are crucial to meeting the increasing demand for advanced telecommunications across Canada.

13. For these reasons, CTA submits that the Commission should:

    a. Refrain from imposing prescriptive resiliency mandates given the absence of clear evidence demonstrating a systemic resiliency problem in Canada that cannot be addressed through existing industry practices;

    b. Support the work of existing collaborative structures, including CSTAC and its Resiliency and Cyber Protection working groups, that already promote effective information-sharing, best practices, and coordinated preparedness and emergency response;

    c. Continue to support non-prescriptive, principles-based guidance for operational and technical matters, recognizing that TSPs must be able to adopt best practices flexibly and tailor resiliency measures to their network architectures, geographies, and operational capacities;

    d. Acknowledge that resiliency is a shared responsibility across critical-infrastructure sectors, including electricity providers, emergency services, municipalities, and provincial emergency-management organizations, and that

[1] Ofcom, *Mobile RAN power resilience*, February 2025 – (Ofcom Report) https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/272921-resilience-guidance-and-mobile-ran-power-back-up/associated-documents/mobile-ran-power-resilience-technical-report-cfi-update.pdf?v=403602

telecom-only obligations to address vulnerabilities that originate outside TSPs' control would be a disproportionate allocation of responsibility; and

e. Acknowledge that one-size-fits-all or unfunded mandates would divert limited capital from higher-impact resiliency initiatives, undermine competitive differentiation, and reduce the resources available for network modernization and rural and remote deployment.

14. CTA supports a resilient future for Canada's telecommunications networks. The best path toward that objective lies not in prescriptive mandates, but in evidence-based analysis, cross-sector collaboration, and policies that support continued investment and innovation by TSPs.

2. Principles That Should Guide the Regulatory Policy

2.1 Regulation Must Be Based on Demonstrated Need and Reliable Evidence

15. The foundational requirement for any regulatory intervention is clear and reliable evidence that (1) a systemic or widespread problem exists, and (2) it cannot be reasonably addressed through market forces, voluntary measures, or other existing industry practices. Parliament has embedded this principle in both the *Telecommunications Act*, which requires the Commission "to foster increase reliance on market forces for the provision of telecommunications service"[2] and the 2023 Policy Direction, which states that Commission must base it decisions on sound and recent evidence.[3]

16. At present, the record does not demonstrate a systemic resiliency problem in Canada's networks. In its mid-year report, the Commission for Complaints for Telecom-television Services (CCTS) indicates that only 4.2% of the complaints it received pertained to "complete loss of service."[4] Meanwhile, consumers have reported overwhelming satisfaction with reliability with only 9% of respondents in the Commission's Fall of 2024 public opinion survey disagreeing with the statement that they can count on a reliable high-speed network where they live,[5] and the Commission's Wave 4 Report prepared by Ipsos showing that this has fallen to 7% for

---

[2] Paragraph 7(f) – "to foster increased reliance on market forces for the provision of telecommunications services and to ensure that regulation, where required, is efficient and effective"

[3] *Order Issuing a Direction to the CRTC on a Renewed Approach to Telecommunications Policy- SOR/2023-23 (2023 Policy Direction)* - Section 6 – "The Commission should base its decisions on sound and recent evidence and should exercise its powers to obtain necessary evidence".

[4] CCTS, *Mid-Year Report, August 1 2024 – January 31, 2025*, https://pub.ccts-cprst.ca/2024-2025-mid-year-report/.

[5] CRTC, *Canadian Telecommunications Market Report 2025*, https://crtc.gc.ca/pubs/cmr_ctmr_2025-en.pdf p37

high-speed internet and 6% for mobile wireless services.[6] Without clear and convincing evidence of a specific resiliency problem, its cause, and compliance costs, any attempt to mandate specific resiliency measures would be speculative rather than evidence based.

2.2 A Principles-Based Approach Is Superior to Prescriptive Standards

17. Telecommunications networks differ across Canada in geography, climate, topology, customer density, and technological configuration. Measures that are optimal in dense urban cores may not be appropriate or cost-effective in remote areas, and requirements suited to FTTP architecture may not apply to hybrid fibre-coax (HFC), fixed wireless, mobile wireless, or satellite networks. Prescriptive standards risk forcing all providers toward a uniform model that may not reflect their infrastructure, size, and available resources. Prescriptive standards also risk locking in outdated technologies, discouraging network modernization, and creating unnecessary regulatory burden. A principles-based policy encourages innovation, adaptation, and continuous improvement.

18. International examples reinforce this. Gartner's *Telecommunications Resilience Analysis Benchmarks Report* commissioned by the Commission and ISED and discussed further in Section 5 below, indicates that, across the jurisdictions examined, regulatory obligations relating to network resiliency are generally confined to macro-level policy functions, such as universal service obligations, mandated access to emergency services (e.g., 911), and statutory outage or incident-reporting requirements. These obligations form part of the broader public-interest regulatory framework but do not extend into detailed prescriptions governing network architecture, redundancy models, or operational practices.

2.3 Recognition of Shared Responsibility Across Critical-Infrastructure Sectors

19. A telecommunications-only focused view of resiliency overlooks the reality that network continuity is shaped by a much broader set of factors, actors, and infrastructures operating outside the telecommunications sector. International analyses, and Canada's own experience, make clear that improving resiliency requires coordination across multiple critical-infrastructure sectors. The Ofcom Report illustrates this point directly. It found that the ability of mobile networks to operate during major incidents is heavily dependent on the reliability of the electricity grid, and the ability to install and operate power backup, such as generators, depends

---

[6] Ipsos Limited Partnership for the CRTC, *Public opinion research tracker: Wave 4*, POR 022-24, 18 June 2025, https://publications.gc.ca/collections/collection_2025/crtc/BC92-129-4-2025-eng.pdf.

on a range of factors such as municipal permitting, refueling logistics, access routes, and safety considerations. Therefore, a resiliency policy that focuses solely on telecommunications networks, without addressing the underlying dependencies, would be incomplete and ineffective.

20. These findings closely mirror the Canadian context. Many of the most significant service disruptions in Canada originate in external systems: prolonged power outages affecting provincial utilities; access restrictions during wildfires, floods, or winter storms; municipal permitting requirements governing the deployment of generators or fuel storage; and emergency-management directives that can shape restoration timelines. As Ofcom emphasizes, addressing these cross-cutting risks requires a wider, open discussion across relevant stakeholders, because no single sector, including telecommunications, controls the full set of variables that determine resiliency outcomes.

21. In considering any policies aimed at improving telecommunications resiliency, the Commission must recognize shared responsibility across electricity providers, emergency services, municipal authorities, provincial emergency-management organizations, and other stakeholders. Placing exclusive or disproportionate responsibility on TSPs for risks that originate outside their networks not only misdiagnoses the problem, but it also imposes costly administrative and financial burdens on TSPs for factors outside of their control.

2.5 Maintain Strong Incentives for Investment and Competition

22. Canada's telecommunications networks are among the world's best-performing because of sustained private-sector investment. In recent years, the sector has reinvested approximately 18% of revenue, more than its international peers, in network expansion and improvement,[7] which amounts to more than $11 billion in capital investments annually.[8] Service providers are strongly incented to protect these substantial investments by ensuring that networks remain resilient, reliable, and available to customers. This investment directly underpins resiliency through:

    - expanded network deployment,
    - increased wireless capacity,

[7] PwC, Enabling Canada's Economic Independence and Global Competitiveness Through Telecommunications - https://www.pwc.com/ca/en/industries/telecommunications/driving-canada-s-global-competitiveness-through-telecommunications-en.pdf
[8] https://canadatelecoms.ca/industry_data/capital-expenditure/

- enhanced redundancy in backhaul and core networks,
- modernization of legacy equipment, and
- continuous refinement of monitoring and response systems.

23. Prescriptive mandates risk distorting investment priorities by diverting capital toward compliance rather than to improvements that are best suited to individual networks and customer needs. They may also reduce providers' ability to differentiate themselves based on reliability, a key competitive factor. When competitive differentiation is regulated away, competition suffers, and with it, the incentives that have historically driven resiliency improvements.

3. Existing Collaborative Structures Support Resiliency

24. CSTAC and its resiliency and cyber protection working groups, provide an ongoing venue for collaboration between TSPs and federal agencies. Their outputs include best-practice advisories, emergency-coordination protocols, and technical recommendations, such as those included in the 2023 *Telecommunications Network Resiliency in Canada: A Path Forward* report.[9] which included numerous recommendations for TSPs and government.

25. These materials are intentionally non-prescriptive, allowing TSPs to draw on them in a flexible, risk-based manner and apply them where they are most relevant to their network architecture, operating environment, and regional conditions. This enables providers to focus resources on the resiliency measures that deliver the greatest impact, without diverting investment toward recommendations that may be less applicable or provide limited incremental benefit. The result is a framework that supports continuous improvement across the sector while preserving the ability of each TSP to tailor its resiliency practices to the specific characteristics and risks of its own network.

26. TSPs also maintain ongoing collaboration with a broad range of federal, provincial, and local public-sector partners that form part of Canada's critical-infrastructure ecosystem. This includes Public Safety Canada, ISED, provincial emergency management organizations, 9-1-1 authorities, and local first responders. The breadth

[9] https://ised-isde.canada.ca/site/spectrum-management-telecommunications/sites/default/files/attachments/2023/CTNR%20Recommendations%20v1.0%20Final%20%28EN%29.pdf

and regularity of these relationships reflect a mature, well-established coordination framework.

5. International Comparators and Lessons for Canada

27. Gartner's *Telecommunications Resilience Analysis Benchmarks Report*[10] provides a comprehensive review of resiliency practices across nine countries plus Canada. The report shows that each jurisdiction relies on a combination of market forces, government-funded programs, targeted regulatory measures, and voluntary guidance and recommendations to influence and improve network resilience.

28. Regarding regulatory mandates, the report finds that all surveyed countries have adopted some form of universal service obligation and/or emergency service obligation. Most jurisdictions also have a mandatory incident reporting framework. Cybersecurity legislation, such as Canada's pending Bill C-8, is also a common feature in most jurisdictions. Government-funded programs to improve coverage and/or resiliency is also something that most jurisdictions have in common.

29. With respect to developing operating procedures, guidelines, best practices and recommendations such as those referenced in Appendix 1 and 2 of the Consultation, Gartner notes that such guidelines and recommendations are typically developed collaboratively with industry stakeholders and the approach by regulators across jurisdictions is typically a "light touch".[11] Gartner further notes that industry is usually "left to identify and implement best practices within their telecommunications networks."[12]

30. The Gartner report also highlights market forces shaping resiliency across jurisdictions, such as competitive pressure, evolving customer expectations, growing dependence on digital connectivity, and continuous technological innovation, which drive TSPs to invest heavily in strengthening their networks.[13] These drivers operate effectively without regulatory mandates, demonstrating that market dynamics and technological evolution are the principal engines of resiliency improvement.

31. Taken together, the Gartner report demonstrates that Canada's current approach to telecommunications resiliency is broadly aligned with international norms. Across all

[10] https://crtc.gc.ca/eng/publications/reports/gartner2024.htm (Gartner Report)
[11] Ibid, Table 14
[12] Ibid
[13] Ibid, section 3.2.1.2

benchmarked jurisdictions, regulatory mandates are limited to targeted obligations. primarily universal service, emergency services, and incident reporting, supported by government programs to improve network coverage and strength.

32. Importantly for the purposes of this Consultation, Gartner's analysis shows that operational and technical guidance is rarely prescriptive; instead, regulators typically adopt a flexible, principles-based approach that allows operators to determine which practices are most appropriate for their networks, technologies, and operating environments. This model enables TSPs to focus their resources on the measures likely to deliver the greatest resiliency gains, rather than diverting investment toward rigid compliance requirements that may not reflect their specific risk profiles. The international record therefore strongly supports a Canadian framework that continues to rely on voluntary and flexible technical and operational guidance that can be implemented in a manner tailored to each TSP's network and operational capacity.

6. Avoid Regulatory Overlap

33. A further consideration in this proceeding is the need to avoid regulatory overlap, which can create unnecessary complexity, impose conflicting obligations, and divert resources away from the most effective resiliency measures. Bill C-8, the proposed Critical Cyber Systems Protection Act, underscores this risk. The federal government has identified cybersecurity as a priority risk area and is addressing it through a dedicated, issue-specific legislative framework led by Public Safety Canada and other responsible authorities. This targeted approach reflects a deliberate choice: when a systemic risk is clearly defined, Parliament enacts focused legislation tailored to that risk, rather than attempting to regulate every aspect of critical-infrastructure resiliency simultaneously or through multiple regulators.

7. Costs and Impact of Potential Mandated Measures

34. One of the central reasons that operational and technical guidelines must remain flexible and voluntary is that every resiliency measure carries a cost, and all TSPs, regardless of size, operate within finite capital budgets. Decisions about redundancy architecture, site hardening, backup power, and restoration capability must be prioritized based on feasibility and against other competing demands, including rural builds, technology upgrades, customer service improvement, and spectrum investments. If best practices or technical guidelines were transformed into mandatory requirements, even when they may be only marginally relevant to a

provider's geography, network design, or risk profile, the result would be significant unfunded capital obligations that divert resources away from the initiatives likely to deliver the greatest benefit to consumers.

35. International evidence on cybersecurity regulation illustrates these opportunity costs clearly. A recent report, *The Impact of Cybersecurity Regulation on Mobile Operators*,[14] finds that mobile operators globally spend on the order of US$15–19 billion per year on core cybersecurity activities, with this figure expected to rise to approximately US$40–42 billion by 2030 as threats become more sophisticated. Importantly, the study finds that a significant share of this effort is absorbed by regulatory obligations that are "different but not better",[15] requiring operators to change tools or processes, or to satisfy multiple overlapping reporting and audit requirements, without meaningfully enhancing security. In some cases, operators report that most of the cybersecurity operations teams' time is devoted to demonstrating compliance rather than actively detecting and managing threats:

> *"We have to assign people to compliance work which means they are not working on actual security…80% of the year we spend on audits, follow ups and compliance…not on threat mitigation."*[16]

36. Network resiliency investments can be extraordinarily costly. For example, Ofcom's ongoing analysis in the United Kingdom of power resiliency for mobile RAN estimates, at the low end, that providing just one hour of battery backup across all UK mobile RAN sites would cost approximately £1 billion.[17]

37. International experience also shows that when governments desire targeted resiliency upgrades, they often pair those obligations with public funding because such measures serve broad national purposes that go beyond commercial network operations. In Australia, the Mobile Network Hardening Program and related bushfire-resilience initiatives provide substantial government co-funding for site hardening, extended backup power, and coverage improvements in high-risk regions. Similarly, New Zealand's Mobile Black Spots Fund and other network upgrade programs provide government funding help increase the performance and coverage of networks in rural and remote areas. These examples confirm in narrow, hazard-specific

---

[14] https://www.gsma.com/solutions-and-impact/connectivity-for-good/public-policy/wp-content/uploads/2025/11/Impact-of-Cybersecurity-Regulation-on-Mobile-Operators.pdf
[15] Ibid page 20
[16] Ibid page 24
[17] The Ofcom Report

circumstances, governments recognize that the financial burden cannot reasonably rest with providers alone.

38. Imposing significant new resiliency costs without such support would have consequences directly at odds with many of the Commission's policy objectives. Higher network costs could place upward pressure on retail prices and make deployments and expansion in some communities uneconomic. In short, absent public funding, mandatory one-size-fits-all resiliency mandates risk producing outcomes contrary to the very goals the Commission seeks to advance.

39. For these reasons, the Commission should avoid imposing unfunded technical or operational mandates that could distort investment priorities, divert capital from network expansion and undermine the continued modernization of Canada's networks. A flexible, voluntary, and principles-based approach, consistent with international norms and aligned with the findings of the Gartner report, will allow TSPs to allocate resources to the resiliency measures that best suit their networks, operational capacities, and regional risk environments.

8. Conclusion

40. The record in this proceeding does not support introducing new prescriptive resiliency mandates. As outlined in this submission, Canada's telecommunications networks already perform at a high level due to sustained private-sector investment, competitive pressures, and well-established collaborative mechanisms.

41. International benchmarking further confirms that Canada's existing regulatory framework already covers the same areas addressed in other advanced jurisdictions. As the Gartner report shows, regulatory mandates related to resiliency in peer countries are generally confined to universal service, emergency services, cybersecurity, and incident reporting, all of which are already well-established in Canada. Beyond these core elements, operational and technical measures are overwhelmingly developed through voluntary industry best practices and competition-driven investment. In jurisdictions where governments seek additional narrowly tailored, hazard-specific network protections, those measures are typically encouraged and supported through public funding, rather than imposed as unfunded regulatory mandates.

42. Resiliency is also inherently a shared responsibility across critical-infrastructure sectors and other stakeholders. Power-grid failures, access limitations during

emergencies, and municipal permitting constraints often determine restoration timelines and prevention measures. Assigning disproportionate responsibility and cost to TSPs for risks originating in other systems would divert capital from higher-impact investments in modernization and rural deployment, without guaranteeing improved public-safety and resiliency outcomes.

43. CTA therefore encourages the Commission to maintain a proportionate, flexible, and evidence-based approach by relying on principles-based, non-prescriptive guidance; supporting continued collaboration through CSTAC and other forums; and avoiding unfunded, one-size-fits-all mandates that could undermine Canada's strong record of investment, reliability, and innovation.

44. CTA appreciates the opportunity to participate in this proceeding.

** End of Document **