Jason Ball
Vice President, Legal

Rogers Communications
One Mount Pleasant Road, 4th Floor
Toronto, Ontario M4Y 3A1
jason.ball@rci.rogers.com

January 17, 2024

Filed via GCKey

Leila Wright
Canadian Radio-television and Telecommunications Commission (the “Commission”)
Executive Director, Telecommunications Sector
1 Promenade du Portage, Ottawa, ON K1A 0N2
leila.wright@crtc.gc.ca

Dear Ms. Wright:

RE: Response to Assessment of Rogers Networks for Resiliency and Reliability Following the 8 July 2022 Outage

Rogers Communications Canada Inc. (“Rogers”) is in receipt of your letter dated December 22, 2023, and the accompanying Assessment of Rogers Networks for Resiliency and Reliability Following the 8 July 2022 Outage report (the “Report”). Rogers appreciates the opportunity to provide a response to the Report (the “Response”). Attached please find our Response.

Pursuant to Rogers’ commitment throughout this process to participate in an open and transparent manner, we are confirming that Rogers is not seeking confidentiality protections (pursuant to subsection 20(1)(b) of the *Access to Information Act*, and sections 38 and 39 of the *Telecommunications Act*) over any portion of the Response.

Sincerely,

ROGERS COMMUNICATIONS

Jason Ball
Vice President, Legal

c.c.: Noah Moser, CRTC, noah.moser@crtc.gc.ca

Attach. (1)

Response to the Assessment of Rogers Networks for Resiliency and Reliability

By Rogers Communications

Rogers appreciates the opportunity to respond to the "Rogers Networks for Resiliency and Reliability Following the 8 July 2022 Outage" independent report (the "Report") and demonstrate to the Commission, the Government of Canada and Canadians our continued commitment to be Canada's most reliable network.

We know how much Canadians rely on our networks and understand the impact of the outage. Rogers is focused on delivering the highest level of network reliability to Canadians, committing $20 billion over five years in our networks. We completed a full review of our networks to optimize resiliency and through this work we introduced several additional safeguards, including the recommendations listed in the Report. We agree with the Report's conclusion that "*the combination of measures that Rogers undertook after the July 2022 outage are satisfactory to improve Rogers' network resiliency and reliability as well as to address the root cause of the July 2022 outage*", and as network technology and telecom platforms evolve, we will keep strengthening our processes and investing in our networks to ensure our customers continue to have networks they can rely on.

Separation of Network IP Cores

Rogers is in agreement with the Report's conclusion that:

> "*The Rogers network is a national Tier 1 network and is architecturally designed for reliability; it is typical of what would be expected of such a Tier 1 service provider network. The July 2022 outage was not the result of a design flaw in the Rogers core network architecture*."

Rogers continues to pursue the separation of our wireless and wireline IP cores to further strengthen the measures we have already introduced by enhancing the overall resiliency of our networks.

Improvement Efforts

Rogers' efforts to improve the reliability and resiliency of our networks have been focused on the factors that led to this outage. Rogers agrees with the Report's identification and characterization of the areas in which Rogers has already undertaken network improvements, including:

- Configuration and Back-up Changes
    - Implemented additional safeguards in the configuration of the routers in its core network to prevent the flooding of IP routing data, thus preventing a similar outage from happening in the future.
    - Implemented a separate physical and logical management network to access network elements for troubleshooting and root cause analysis.
    - Deployed backup connectivity from third party service providers to its network operation centre and other critical remote infrastructure sites.
    - Invested in additional tools that would help validate router configuration changes.

- Improving Change Management
  - Implemented new risk assessment algorithms.
  - Implemented organizational changes to improve collaboration between network operations and engineering teams.
  - Enhanced the process for introducing new equipment and technology.
  - Improved the process for implementing network changes such as introducing automation to streamline the change management process.
  - Implemented additional lab testing of planned network configuration changes.

- Improving Incident Management
  - Bolstered incident management guidelines to encompass additional outage scenarios.
  - Streamlined incident response with well-defined leadership roles.
  - Implemented a solution for prioritization of alarms during outage.
  - Enhanced automated rollbacks to previous configurations when needed.
  - Implemented additional measures to improve its communication protocols.
  - Equipped all incident response and crisis management team members with backup communications from third-party service providers to maintain communication capabilities during outages.

Report Recommendations

Rogers has responded below to each of the Report’s recommendations for additional measures that could be undertaken by Rogers to further improve network resiliency. All of these recommendations were previously identified as part of Rogers’ earlier review and we welcome the opportunity to provide an update. Each of the proposed recommendations has been implemented.

1. **Test emergency roaming with other mobile network operators and expand it to include a more comprehensive set of test scenarios. Rogers has signed the Memorandum of Understanding on Telecommunications Reliability which includes emergency roaming with other mobile network operators to enable Rogers’ customers to access emergency services (e.g., 9-1-1 calls) during a major outage. This additional testing would ensure that emergency roaming is feasible under different network failure scenarios, specifically the scenario observed during the July 2022 outage (where the radio network is up and the core network is down).**

   Status: Completed (with continuous testing ongoing)

   Implementation: Rogers has implemented this recommendation pursuant to the Memorandum of Understanding on Telecommunications Reliability (MOU), with involvement from the Canadian Telecommunications Network Resiliency Working Group (CTNR) of the Canadian Security Telecommunications Advisory Committee, and other Canadian operators.

   Rogers will continue to actively test emergency roaming with the other MOU-party mobile network operators for whom Rogers has overlapping wireless network coverage. Through the

CTNR, the operators have aligned on a bi-annual testing schedule. Rogers is also fully committed to working with our roaming partners to support and develop additional testing use cases related to core network failures in order to enhance the level of network resilience. Rogers is monitoring, and will incorporate into our testing regime, regular evolutions and industry best practices that will support a more robust and adaptable emergency roaming testing regime.

2. **Develop a detailed root cause analysis for future major outages as this would benefit the process of assessing an outage and its impact, and identifying the appropriate mitigation measures.**

   Status: Completed.

   Implementation: As part of our incident management, Rogers has strengthened its Root Cause Analysis (RCA) process for all major incidents. The RCAs include all relevant details about the incident, timelines, impacts, resolution steps and causal factors, with all actions, owners and due dates assigned and tracked through to resolution. This RCA process is supported by a dedicated team who performs the analysis, tracks the progress and implements available improvement opportunities across people, process and technology. RCAs are shared across the technology teams and centrally stored in a searchable database, for a broader application of learning.

3. **Ensure wide coverage and rigor in testing configuration changes. This would help avoid errors leading to potential outages. Rogers would need to leverage new test tools for modeling test scenarios that replicate the production network, and to address the evolution of networking technologies.**

   Status: Completed

   Implementation: Rogers has reinforced our configuration and change testing process with further lab validation and testing to simulate our production environment as accurately as possible. Load testing and network simulation tools are utilized to confirm validation of changes prior to deployment. We also have a team of technical peers that review each proposed change based on the criticality scale before the change proceeds into production.

4. **Expand the scope of incident management drills. This would enhance staff and the network's emergency preparedness and proactively uncovers weaknesses.**

   Status: Completed

   Implementation: Rogers expanded and enhanced our existing incident response processes. We will continue to build on this practice to ensure staff readiness for the safe, rapid recovery, and support of our customers.

5. **Institutionalize learning from own and other service providers' network failures to implement preventive actions, minimize the impact of network outages and enhance quality of service.**

   Status: Completed

   Implementation: Rogers reviewed and enhanced our incident management process (including the components supporting internal learning) and formalized the sharing of network failure information with vendors and other operators. A governance regime has been implemented to ensure that there is an opportunity for regular touchpoints with vendors and operators.

6. **Inform customers how to reach 9-1-1 services during an outage.**

   Status: Completed

   Implementation: Rogers has included this information on our websites at: https://www.rogers.com/support/mobility/911-emergency-service. Pursuant to our incident management process, Rogers will evaluate and activate further communication channels when needed.

7. **Share outage root cause and mitigation strategies with the broader Internet community represented by bodies such as the North American Network Operator's Group, to help other telecom network operators prevent similar network failures.**

   Status: Completed

   Implementation: Rogers has shared details of the outage root cause and learnings with vendors and industry groups and committed to this principle by implementing processes to institutionalize this practise. In addition, Rogers' engineering and operations teams have regular debrief and information exchange sessions with other operators. This process allows for the exchange of experiences, information, and implementations to ensure that all Canadians have access to the best and most resilient networks.

Rogers looks forward to continuing our collaboration with governmental agencies and operator peers to further strengthen the industry's ability to deliver the highest level of network reliability to Canadians.