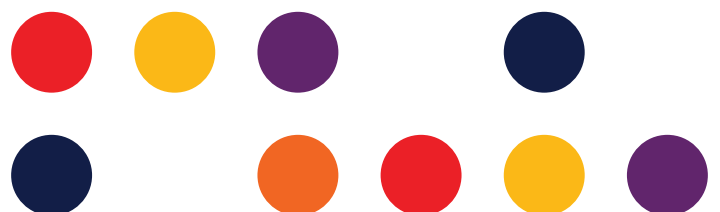# Optus Network Outage

Senate Environment and Communications References Committee

November 17, 2023

Public

Submission

Role of Government in ensuring reliable access to telecommunications technology

Thank you for inviting TPG Telecom to provide a submission to the Committee regarding its inquiry into the Optus network outage. This submission is limited to the matters relevant to the role of Government in ensuring Australians have reliable access to telecommunications technology. TPG Telecom is not in a position to provide any views regarding the remaining elements of the Terms of Reference.

Our investment in a reliable and resilient network

TPG Telecom is a significant network infrastructure owner, operating a national mobile network and metropolitan, regional, inter-capital and international fibre assets. We take our role in connecting Australians very seriously and we invest heavily in ensuring the reliability of our networks.

Our network architecture has been designed to deliver a robust and resilient service for our customers. TPG Telecom's mobile and fixed networks operate on separate core networks that limits the potential for widescale outages such as the one the subject of this inquiry. We proactively conduct testing and failover activities to assess and maintain performance levels across our entire network.

We have a strong incident management framework and culture comprised of various Incident Management teams to ensure a rapid response to any unplanned disruption. Disaster recovery and business continuity plans have been established across all critical systems, business functions and locations.

TPG Telecom also drove the development of industry guidelines that aim to facilitate efficient interactions between the telecommunications industry and relevant Australian Government agencies when events cause major disruptions to telecommunications services.

Existing regulatory obligations

We are currently subject to very stringent obligations under both the Telecommunications Act 1997 and the *Security of Critical Infrastructure* (SOCI) Act 2018.

The Telecommunications Sector Security Reforms (TSSR) of 2018 created a bespoke regulatory framework that includes a range of security and notification obligations. This includes a requirement to protect our networks and facilities from unauthorised access and interference. Under the notification obligation, we are required to notify the Government of any changes to our networks that may have a material adverse effect on our capacity to comply with the security obligation. The Government also has the power to direct carriers to take specific measures or to provide information to agencies.

Our sector is also covered by the SOCI Act, including a declaration that our network is a 'system of national significance'. Currently we are subject to the following obligations:

- Enhanced cyber security obligations that requires the preparation and update of incident response plans
- Government directions in relation to serious cyber security incidents and intervention requests, including information gathering powers and reporting notices
- Obligation to notify data storage and processing service providers when their services relate to our business critical data.

Separate to the SOCI Act, we are also subject to cyber incident notification reporting obligations. In addition, we are required to prepare an inventory of critical infrastructure as part of a register of assets including operational information (such as location of asset) ownership and vendor details.

Reforms to the security obligations

We have been working with the Government on streamlining the various legislative tools overseeing the nation's critical communications infrastructure. Consistent with this approach, our sector has been engaged in constructive discussions with the Departments of Communications and Home Affairs regarding the potential for the TSSR obligations to be brought into the SOCI Act. As part of these reforms, it has been anticipated Government would seek to apply two additional obligations under the SOCI Act including requirements to:

- have a critical infrastructure risk management plan in place – which covers cyber risks, environment risks and hazards, supply chain risk and personnel risk
- provide an annual report to Government (approved at Board level) that sets out all hazards that had a significant impact on critical infrastructure assets, including the effectiveness of the risk management program in mitigating that impact.

The Minister for Home Affairs confirmed the intention to apply the additional SOCI Act obligations to the telecommunications sector on 13 November 2023.

TPG Telecom continues to support sensible reform to strengthen the resilience and redundancy of our networks. While accepting the importance of collaboration between industry and Government agencies on matters of national security, we look forward to working with policy makers to ensure that the reforms promote accountability without duplication and the addition of unnecessary regulatory burdens.

Emergency roaming capability

TPG Telecom also recognises the recent commentary regarding the role that emergency roaming could play in enhancing the resilience of Australia's communications networks.

Together with the other mobile network operators and the Department of Communications, TPG Telecom is participating in a working group to consider how an emergency mobile roaming solution could be practically implemented in the Australian mobile market. Such an

emergency roaming capability is likely to be complex and will require Government funding support. We are committed to continue working with the Government and the broader telecommunications sector to ensure Australians are supported during emergencies.

Mandated domestic roaming

In addition to emergency roaming, TPG Telecom considers there remains a basis for the Government to reconsider avenues to mandate domestic roaming in Australia. Mandated domestic roaming should be considered as a practical option to bring greater choice and connectivity to regional Australia.

This would also create incentives for increased investment in regional areas and reverse the trend of weakened competitive dynamics. A permanent roaming solution would also have the benefit of providing a much higher degree of network resilience for Australians living in regional areas.