ABN 70 250 995 390
180 Thomas Street, Sydney
PO Box A1000 Sydney South
NSW 1235 Australia
T (02) 9284 3000
F (02) 9284 3456

15 October 2026

Kami Kaur
Executive General Manager, Network Regulation
Australian Energy Regulator
MELBOURNE VIC 3000

Submitted by email: capex@aer.gov.au

Dear Ms Kaur,

Transgrid submission to the AER's Draft Network Resilience Guidelines

Transgrid welcomes the opportunity to provide a submission to the Australian Energy Regulator's (AER) draft Network Resilience Guidelines (the Guidelines) and the accompanying Explanatory Statement. Transgrid is the primary Transmission Network Service Provider (TNSP) in NSW and the ACT, responsible for planning, operating and maintaining the high-voltage transmission network that underpins the secure and reliable supply of electricity to consumers across NSW and the ACT.

Transgrid supports Network Resilience Guidelines applying to TNSPs, provided they are appropriately tailored to the role, risk profile and regulatory framework that applies to transmission networks. Appropriately tailored Guidelines would give TNSPs greater certainty about the evidence expected to establish need, demonstrate that a proposed option is prudent and efficient, and explain benefits that may be system-wide, difficult to localise or realised only when a rare event occurs. They would also support greater consistency and transparency in the AER's assessment of comparable proposals over time.

The AER's proposal for the existing guidance on the use of principles is helpful. However, given the importance of power system resilience as the economy electrifies and extreme weather becomes more likely, appropriate Guidelines tailored for TNSP resilience expenditure proposals would provide additional benefit to networks, the AER and ultimately consumers. The remainder of this submission provides initial views on key areas for consideration should specific resilience guidance for TNSPs be developed at a later stage.

Official

Transmission network resilience is critical for consumers and the power system

The core concept of resilience—the capacity of a network and its supporting systems to sustain essential services and recover following disruptive events—is as relevant to transmission as it is to distribution. TNSPs plan, operate and maintain geographically extensive critical infrastructure exposed to severe weather and natural hazards, as well as cyber, physical security and operational technology risks. Just as the draft Guidelines distinguish non-weather risks from resilience expenditure for DNSPs, a transmission framework would need to recognise the full set of risks and obligations relevant to the secure operation of the power system.

The configuration and exposure of Transgrid's network varies considerably. Some assets form part of a highly interconnected meshed network, which can provide alternative pathways for electricity flows when an asset is unavailable, while other assets are located away from the hazards most likely to cause prolonged outages. However, these characteristics do not eliminate resilience risks. In parts of the network with limited redundancy, or where a severe event affects multiple assets or exceeds the network's ability to reroute supply, a transmission outage can interrupt electricity services to consumers in much the same way as an outage on a distribution network. For example, TNSPs such as Transgrid are susceptible to resilience risk in areas of the network that have limited or no geographic redundancy such as radial feeds or multi-circuit lines in close proximity. In these locations, Transgrid is exposed in much the same way as a distributor.

The consequences of a transmission failure can also extend well beyond the immediate location of the affected asset. An outage may affect multiple distribution networks, directly connected industrial customers and generators, constrain inter-regional transfers, disrupt market outcomes, reduce power system security and complicate restoration. Transmission resilience must, therefore, address both the potential for direct impacts on consumers and the wider consequences of low-probability, high-impact events across the power system.

Resilience in the transmission context also depends on the systems, processes, operational capability and technology that enable a TNSP to maintain network services, manage credible contingencies, coordinate an emergency response and restore supply safely and efficiently. Material risks include:

- severe weather and natural hazards, including bushfires, storms and floods. Over the past 17 years, Transgrid has recorded nine events affecting 39 steel towers, predominantly because high-intensity winds exceeded tower capacity. These events have occurred more frequently during the past six years. The 2019–20 bushfire season also illustrated the potential system-wide consequences: approximately 9% of Transgrid's network was affected and outage frequency during the period was 20 times the historical level.
- cyber and physical security threats capable of compromising the availability or operation of critical transmission assets.

TNSPs address these risks through a portfolio of operational and investment measures, including:

- secure operational technology and control systems that support continuous and reliable network operation
- emergency management and restoration capability, supported by coordination with market bodies, emergency services and jurisdictional agencies

Official

- fit-for-purpose redundancy across network and non-network assets
- targeted hardening and asset-resilience investments, including strengthening transmission towers, replacing vulnerable wood-pole structures and upgrading assets exposed to extreme weather and natural disasters.

If you require any further information or clarification on this submission, please feel free to contact Oliver Derum via [redacted]

Yours sincerely

[redacted]

Murray Chandler
General Manager of Asset Management

Official