AUSTRALIAN ENERGY REGULATOR

Level 17, Casselden
2 Lonsdale Street
Melbourne Vic 3000

GPO Box 520
Melbourne Vic 3001

tel: (03) 9290 1800

www.aer.gov.au

13 January 2025

Andrew Pirie
Australian Energy Market Commission
Level 15, 60 Castlereagh Street
Sydney NSW 2000

Sent via email: 13 January 2025

Dear Andrew

Supplementary submission in response to the AEMC's consultation paper – National Electricity Amendment (including distribution network resilience in the National Electricity Rules) Rule

We welcome the opportunity to respond further to the AEMC's consultation paper on the Victorian Minister for Energy and Resources' rule change request to explicitly include network resilience in the National Electricity Rules (NER) for Distribution Network Service Providers (DNSPs) and to require the AER to develop and publish a network resilience guideline.

This submission is further feedback on the AEMC's consultation paper and should be considered as a supplement to the AER's submission of 7 November 2024.

As noted in our submission of 7 November 2024, the AER welcomes consideration of whether the current regulatory framework accommodates and incentivises efficient levels of expenditure in network resilience for extreme weather. Despite the positive outcomes achieved already in the area of network resilience, we appreciate that there may be value in including network resilience as an explicit factor to consider when assessing expenditure proposals to address long duration outages from extreme weather events.

This supplementary submission is to raise our concerns about the broader scope of the rule change request. While the Minister's rule change request is predominately focused on addressing risks from extreme weather events that may result in long duration outages, we understand that the proposed rule change is also intended to cover risks from "other catastrophic events such as cyber-security events and terrorist attacks on critical infrastructure".[1]

[1] AEMC, *National Electricity Amendment (including distribution network resilience in the national electricity rules) Rule – Consultation Paper*, 3 October 2024, p. 14.

We do not consider there is currently a need to amend the National Electricity Rules (NER) beyond the scope of weather-related events. Therefore, in response to Question 3 (b) in the AEMC's Consultation Paper, where the AEMC asks: [2]

> *Should the resilience expenditure factors cover severe weather events and other catastrophic events that may result in long-duration outages?*

Our response is that we do not consider that the resilience expenditure factors should cover "other catastrophic events such as cyber-security events and terrorist attacks". We set out our concerns below including implementation issues that need to be considered further.

The rule change request does not provide compelling evidence on the policy problem to be addressed

There is limited explanation as to the policy problem to be addressed by broadening the scope of the resilience expenditure factor to include cyber-security events and terrorist attacks. The Minister's rule change request focuses on the recent impacts from climate change and weather-related events, with data and evidence presented in the request relating only to the impact from extreme weather events[3] The Minister's rule change request makes very minor references to cyber-security and terrorism events.[4]

Further, we note that there is no evidence presented in the Minister's rule change request or the AEMC's consultation paper that:

- Cyber security and terrorism events have or will cause prolonged outages. This is in contrast to long duration outages as a result of extreme weather events.
- there are impediments to, or a lack of guidance on, or disincentives for DNSPs to seek ex-ante funding in areas such as cyber security and terrorism.
- additional ex-ante funding and investment in these areas would be in the long-term interests of consumers, including consideration of potential price impacts and the appropriate balance of risks to be borne by consumers and the DNSP.

From an implementation perspective, we note that amendments to include the broader scope of cyber security and terrorism in the resilience expenditure factor requires consideration of the interaction with the existing prescribed and nominated pass through events in the NER and revenue determinations that seek to address the risk from similar catastrophic events.

The proposed rule change does not appear to consider the existing provisions and arrangements to deal with "other catastrophic events"

The rule change request does not discuss the existing legislative provisions and arrangements that already place obligations on DNSPs to address the risk of cyber security and terrorism events on electricity networks.

The NEO and NER capex and opex objectives already include specific references that the AER is required to approve expenditure to "maintain security of supply and safety".

---

[2] AEMC, *National Electricity Amendment (including distribution network resilience in the national electricity rules) Rule – Consultation Paper*, 3 October 2024, p. 15.

[3] Hon. Lily D'Ambrosio MP, *Rule Change Request to account for resilience in the National Electricity Rules capital and operating expenditure factors*, 30 July 2024.

[4] Hon. Lily D'Ambrosio MP, *Rule Change Request to account for resilience in the National Electricity Rules capital and operating expenditure factors*, 30 July 2024.

Proposed expenditure to address cyber security and terrorism risks and threats would relate to these objectives. In contrast, for expenditure related to addressing the risk from extreme weather-related events, we appreciate that there may be some degree of ambiguity as to whether the proposed expenditure for resilience purposes would be covered under the objective of "maintaining reliability".

Under the Security of Critical Infrastructure Act (SOCI Act), regulatory obligations are already placed on DNSPs to undertake risk-based planning, management, reporting and oversight to address potential physical and cyber threats. More specifically, on 2 April 2022, a new obligation under the SOCI Act was placed on entities responsible for critical infrastructure assets such as DNSPs to create and maintain a critical infrastructure risk management program (CIRMP). The purpose of the CIRMP is to identify each hazard where there is a material risk that of an impact on the asset if the hazard occurred, and as far as reasonably practicable to minimise the material risk of such a hazard occurring and mitigate the relevant impact on the asset.

The CIRMP must identify hazards relating to:[5]

- physical security – including unauthorised access to, interference with, or control of critical infrastructure assets, to compromise the proper function of the asset or cause significant damage to the asset.
- cyber and information security – including improper access or misuse of information or systems related to the asset, or use of a computer system to obtain unauthorised control of or access to the asset that might impair its proper functioning.
- natural events – including fire, flood, cyclone, storm, heatwave, earthquake, tsunami, space weather or biological health hazard (such as a pandemic)
- personnel – including where a critical worker acts, through malice or negligence, to compromise the proper function of the asset or cause significant damage to the asset.
- supply chains – including malicious people both internal and external exploiting, misusing, accessing or disrupting the supply chain, and over-reliance on particular suppliers.

As can be seen by the description of the hazards required to be identified in a DNSP's CIRMP, the rule change request is likely to overlap with a DNSP's requirement to maintain a CIRMP under the SOCI Act. We consider it would be prudent for the AEMC to engage with the Department of Home Affairs and AEMO (who establishes the cyber security framework that must be adhered to) on the implementation issues, such as duplication and inconsistencies and consequentially the regulatory burden placed on DNSPs if the rule change is to be broader in scope beyond weather-related events.

We note that the AER has approved efficient costs for NSPs to address their obligations under the SOCI Act in all revenue determinations since these obligations have come into place. It is unclear that the economic regulatory framework should be funding NSPs to a greater extent than already required to comply with the explicit regulatory obligations set by the Department of Home Affairs and AEMO.

[5] Department of Home Affairs, Cyber and Infrastructure Security Centre, *Guidance for the Critical Infrastructure Risk Management Program*, January 2024.

The broader scope of network resilience to include "other catastrophic events' would limit the efficacy of the proposed AER guidelines for network resilience

We note that there are very different drivers, risks, data and information requirements that would inform the assessment of expenditure for 'other catastrophic events', compared to severe weather-related events. While there is likely to be linkages between cyber security and terrorism risk such as there may be similar data and information requirements, these requirements would be significantly different from the factors we would have regard to when assessing network resilience expenditure like incident response for weather-related events. We therefore do not see any synergies in combining the information/data requirements for assessing expenditure to address the risk from extreme weather events and 'other catastrophic events'.

Further, a guideline that sought to address all 'other catastrophic events' would necessarily be at a very high and broad principles level given the different drivers and risks associated with cyber security and terrorism. This may not be useful to stakeholders who are seeking more specific guidance on network resilience expenditure for weather-related events.

We welcome any further dialogue with the AEMC on the contents of this submission or related matters.

If you would like to discuss any of the issues raised above or have any questions or queries please do not hesitate to contact Kim Huynh on (03) 9290 1960 or 0413 732 430.

Yours sincerely

Dr Kris Funston
Executive General Manager (Network Regulation)
AER

Sent by email on: 13.01.2025