AUSTRALIAN ENERGY REGULATOR

Level 17, Casselden
2 Lonsdale Street
Melbourne Vic 3000

GPO Box 3131
Canberra ACT 2601

tel: (03) 9290 1800

www.aer.gov.au

Our Ref: 17429114
Your Ref: ERC0388
Contact Officer: George Huang
Contact Phone: (02) 9230 3856

15 November 2024

Anna Collyer
Chair
Australian Energy Market Commission
GPO Box 2603
SYDNEY NSW 2001

Dear Ms Collyer

Re: Cyber security roles and responsibilities - draft determination

The Australian Energy Regulator (**AER**) welcomes the opportunity to provide this submission in response to the Australian Energy Market Commission's (**AEMC**) draft determination on Cyber security roles and responsibilities.

The AER supports the rule change's intent to embed and formalise the Australian Energy Market Operator's (**AEMO's**) cyber security responsibilities in the National Electricity Rules (**NER**). The increasing digitisation and connectivity of the National Electricity Market (**NEM**), along with the high take-up of consumer energy resources and distributed energy resources, necessitates greater role clarity and a strategic and coordinated approach to cyber security. Whilst there has been no publicly reported large-scale cyber attack on Australia's power system, it is important that AEMO's role in maintaining the cyber security of the NEM is clear. This is to reduce potential risks a cyber security incident could pose to Australia's energy security and power system reliability for electricity consumers.

The AER supports the draft rule's approach to providing greater clarity on and embedding AEMO's role in cyber security uplift and preparedness into the NER framework by establishing four new, specific cyber security prevention and preparedness functions. The AER agrees with the draft determination's assessment that clarifying AEMO's cyber security role in this regard is appropriate, particularly because of the unique insight AEMO provides as the system operator. Cyber incidents in the electricity sector could have far-reaching consequences including widespread outages, other economic disruptions, breaches of sensitive data and threats to national security. Preparation and planning for their occurrence will assist in minimising any impact to power system security and help ensure the secure provision of electricity in the long term.

This rule change may result in an incremental impact on the AER's role reviewing and assessing network revenue determination proposals. However, we do not anticipate any significant resourcing impacts for the AER arising from this rule change. The AER assesses network expenditure proposals from both transmission and distribution network service providers, which include cyber security components. Incremental impacts could occur if AEMO seeks to recover the costs of its new cyber security responsibilities by increasing participant fees for network service businesses. Network service businesses may also seek to recover additional costs from their participation in testing and training exercises and response to any identified deficiencies. To the extent cost recovery is sought for any costs not currently incurred, the AER would consider these costs as part of its revenue determination assessments. As the draft rule does not allow AEMO to create new obligations on participants, no mandatory compliance costs are expected from this rule change.

The AER appreciates the opportunity to provide this submission and if needed, can be available to discuss the contents of our submission further.

Yours sincerely

Stephanie Jolly
Executive General Manager
Consumers, Policy & Markets
Australian Energy Regulator

Sent by email on: 15.11.2024