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

Thursday, 7 November 2024

Ms Anna Collyer
Chair
Australian Energy Market Commission

Lodged online: www.aemc.gov.au

Project Ref: ERC0388

Dear Anna,

AEMC's Cyber security roles and responsibilities

Transgrid welcomes the opportunity to respond to the Australian Energy Market Commission's (**AEMC**) draft decision on Cyber security roles and responsibilities. The AEMC's draft decision explicitly establishes cyber security as one of Australian Energy Market Operator's (**AEMO**) power system security responsibilities in Chapter 4 of the National Electricity Rules (**NER, Rules**).

As the NSW Transmission Network Service Provider (**TNSP**), Transgrid is obligated to protect the integrity of data from increasingly sophisticated and numerous cyber-threats. Emerging technologies will be required to securely and effectively manage cyber roles and responsibilities and also manage increasing data volumes expected in the business.

Transgrid broadly supports the AEMC's draft decision including:

- Maintaining AEMO's current role and responsibility in some security preparedness activities, including developing and maintaining the Australian Energy Sector Cyber Security Framework.

- AEMO's role to coordinate and support cyber security preparedness, response and recovery.

However, we have a few concerns that warrant further considerations. These include:

- Transgrid currently has direct engagement with Department of Home Affairs in relation to cyber threat briefings and preparedness. We understand the draft decision has proposed this will now be done via AEMO. We support this for Operational Technology (including SCADA) related cyber threats. However, this model would likely delay and risk our response to a Transgrid specific cyber threat that is not related to our Operational Technology systems.

    - We recommend the AEMC clarify that this is only applicable to Operational Technology cyber security incident rather than incidents that are isolated to a corporate impact.

- Under Function 1, the AEMC has proposed that AEMO would be able to plan and coordinate the NEM-wide response to a cyber incident affecting the energy sector.
    - Transgrid understand this is related to NEM-wide cyber security incidents, however we would appreciate further clarification on the level and type of involvement. For example, if Transgrid experienced a cyber security incident, we would expect AEMO to co-ordinate the response in coordination with Transgrid. Essentially, we expect the response to be an integrated response between the NSP and AEMO.
- In Table B.1[1], the AEMC have outlined the increase in participant fees to be less than $10 million. This takes into consideration AEMO estimates.
    - Transgrid would encourage the AEMC to provide further clarity on these costs. We would recommend more accurate costing and ensure AEMO provides 7-year rolling budgets so that TNSPs are able to anticipate costs and incorporate these costs into their 5-year regulatory period.

We look forward to working with the AEMC to continue to ensure that any proposed reform is fit-for-purpose and has no unintended consequences. If you or your staff require any further information or clarification on this submission, please contact Zainab Dirani, Policy and Advocacy Manager at zainab.dirani@transgrid.com.au.

Yours faithfully

Monika Moutos
General Manager of Regulation, Policy and Governance

[1] AEMC Cyber security roles and responsibilities Draft determination | page 37