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

Tuesday, 4 March 2025

Australian Energy Market Operator

Lodged via email: reformdevelopmentandinsights@aemo.com.au

## AEMO's New cyber security roles and responsibilities

Transgrid welcomes the opportunity to respond to the Australian Energy Market Operator's (**AEMO**) New cyber security roles and responsibilities consultation paper, which was published on 4 February 2025. The consultation paper is seeking feedback on the determination of the AEMO cyber security roles and responsibilities described in the National Electricity Amendment (Cyber security roles and responsibilities) Rule 2024 as a declared National Electricity Market (**NEM**) project and if so the fee structure.

As the NSW Transmission Network Service Provider (**TNSP**), Transgrid supports AEMO's role in protecting electricity and gas systems from cyber security threats and attack. AEMO's role as the energy market operator places them in an ideal position to ensure they provide expert advice and analysis to government and registered participants on current and emerging cyber security issues for the energy sector.

Transgrid is supportive of AEMO's role in ensuring cyber-readiness. Specifically, we support continued collaboration with industry and government stakeholders, including AEMO, Australian Cyber Security Centre (**ACSC**), Australian Signals Directorate (**ASD**), Cyber and Infrastructure Security Centre (**CISC**), and representatives from Australian energy organisations.

Transgrid has participated in two AEMO cyber security related activities over the past year. These include:

1. Energy Market Cyber Security group - this forum facilitated greater collaboration with energy sector cyber security leaders and discuss common challenges and solutions.
2. Trident cyber security exercise - Transgrid participated in the Trident cyber security exercise organised by AEMO in May 2024. The exercise was well run and was useful for the Transgrid team as we were able to hone AEMO's cyber security incident response processes and procedures as well as collaborate with other energy sector cyber security teams.

These forums provide an opportunity for the industry to come together and share insights and learnings. We encourage AEMO to continue to provide these sessions to the industry given their value add and their ability to enhance collaboration between key government and industry stakeholders.

In addition, it is vital that consumers are kept informed through transparent costs breakdown and collaboration with industry.

**Fee structure**

AEMO is consulting on how their expanded cyber security roles and responsibilities should be treated and the associated cost recovery. Options being considered include:

1. Be considered as a declared NEM projects and the fee structure associated with this, or
2. Expanding the scope of one of AEMO's existing NEM Participant fee structures (e.g. NEM Core fee), or
3. Establishing an additional separate fee structure (i.e. an additional separate cyber security roles and responsibilities related Participant fee).

Transgrid does not consider that the new roles and responsibilities qualify as a declared NEM project, and we therefore support the expansion of AEMO's existing NEM Participant fee structure (Option 2 above).

AEMO has listed the type of projects, consistent with NER clause 2.11.1(ba), that would be considered a declared NEM project. These include major reform or major changes to functions and/or systems. While Transgrid supports AEMO's expanded cyber security role we do not consider it to be a 'major' development or change in functions and/or systems as per the definitions outlined in the AEMO consultation paper.

As outlined in the AEMC's final rule[1], AEMO had previously carried out some security preparedness activities, including developing and maintaining the Australian Energy Sector Cyber Security Framework. The final rule therefore builds on and enhances these activities rather than introducing a new and significant function. Essentially it embeds and formalises AEMO's existing cyber security preparedness role and enables additional resourcing for AEMO to sustain and scale up these functions. Given this, we do not consider this to be a major change, but rather the maturing and strengthening of existing responsibilities.

We also note that the anticipated costs associated with the new cyber security work program are not particularly large relative to AEMO's overall costs, AEMO already has significant expertise in the field, and the new function can be reasonably easily incorporated into their existing organisational structure.

We therefore support AEMO including the efficient costs associated with these important activities within the NEM Core fee, rather than introducing a separate, additional fee structure.

**Activities and role transparency**

As AEMO continues to develop the work program to comply with its new cyber security obligations, we encourage them to collaborate closely with industry and other stakeholders to ensure it is delivered as efficiently as possible, avoiding duplication and at the lowest cost to energy consumers. For example:

[1] AEMC's National Electricity Amendment (Cyber security roles and responsibilities) Rule 2024 published 12 December 2024.

- Clarifying cyber security roles and responsibilities with other agencies including the ASD, ACSC and Home Affairs (SoNS program).
- Providing further clarification on the Critical Infrastructure Uplift Program (**CI-UP**). This may involve close collaboration with the ASD which currently offers a program similar to what AEMO is proposing in Function 2 for the Energy Sector.
- Streamlining cyber security incidents coordination. It may be beneficial to consolidate Cyber security Incident Coordinator across AEMO, ASD and Home Affairs. This will minimise duplication of tasks and enable coordination of incidents leading to better real-time responses and lower costs. This will also allow TNSPs to efficiently address queries and requests from different government bodies in a coordinated way, without unnecessary duplication.

**Cost transparency**

Transgrid believes that it is essential for consumers to have transparency and visibility of costs given these costs will be passed on to them by TNSPs in network charges. We believe increased transparency will build trust between consumers, regulators and market participants. As such, we encourage AEMO to:

1. Consult with stakeholders (including TNSPs) on proposed work plans, including providing forward visibility of costs, proposed activities and benefits.
2. Provide fixed forward budgets for at least five years (likely seven years) to enable TNSPs to accurately account for associated costs when preparing revenue proposals for future revenue periods and support full cost-recovery. This should include detailed cost breakdowns, including escalation assumptions and supporting information that can be used to explain new fees to consumers (who ultimately bear their cost).

The AEMC's 2022 Rule Change on *Recovering the cost of AEMO's participant fees* concluded that (following a transitional period) AEMO fees for TNSPs are to be managed through the incentive-based revenue determination framework for rather than as a direct passthrough to consumers. It is therefore essential that project-related fees over the outlook period are provided on a firm basis (i.e. capped) as TNSPs would have no mechanisms available to recover unanticipated cost increases once revenue determinations are completed (expenditure would need to be reduced elsewhere on the network to accommodate them, e.g. on maintenance programs). While the costs associated with the new cyber security responsibilities are not, in themselves, especially large, they form part of a broader range of new and expanded costs that can be large and volatile and will be passed on to consumers with considerable cumulative impact on energy bills and cost of living pressures.

In addition, the final AEMC rule introduced four expanded functions. This includes Function 3 which involves providing cyber security research and advice to governments including requests by the Minister to proceed with a particular research or advice task. We support AEMO leading this role, however, consider these costs should be recovered from the government via an agreement rather than from energy consumers.

Transgrid looks forward to engaging with AEMO in appropriate forums on an ongoing basis to assist with the efficient delivery of its new responsibilities and management of associated costs via the Financial Consultation Committee.

We appreciate the opportunity to provide a submission to the consultation and look forward to continuing to work with AEMO and industry to ensure the electricity system is protected from cyber security threats. If you would like to discuss this submission, please feel free to contact Zainab Dirani, Policy and Advocacy Manager at zainab.dirani@transgrid.com.au.

Yours faithfully

Fiona Orton
General Manager of Innovation and Energy Transition