AGL Energy Limited
T 02 9921 2999
agl.com.au
ABN: 74 115 061 375

Level 24, 200 George St
Sydney NSW 2000
Locked Bag 14120 MCMC
Melbourne VIC 8001

Australian Energy Market Commission

Level 15, 60 Castlereagh St

Sydney NSW 2000

07 November 2024

Dear Sir or Madam,

Draft rule determination – National Electricity Amendment (Cyber security roles and responsibilities) Rule 2024

AGL Energy (**AGL**) welcomes the opportunity to provide responses to the Australian Energy Market Commission's (**AEMC's**) draft determination consultation paper (the **Paper**).

Proudly Australian since 1837, AGL delivers around 4.3 million gas, electricity, and telecommunications services to our residential, small, and large business, and wholesale customers across Australia. We also operate Australia's largest electricity generation portfolio and have the largest renewables and storage portfolio of any ASX-listed company. As one of the largest providers of essential services in Australia, AGL welcomes and embraces the key role it will play in ensuring cyber security is instilled as a strategic national security capability and supporting Australia's ambition of becoming the 'most cyber secure nation' by 2030.

With the increased prevalence of cyber security threats and incidents both domestically and abroad, AGL supports the AEMC's proactive efforts to protect and increase the cyber security resilience of the National Electricity Market (NEM). We recognise that the increased digitisation of the NEM and the interconnected nature of infrastructure networks, exponentially exposes the system to the threat of cyber security incidents. We note that the energy sector – and its potential cyber weaknesses – as emphasised by several stakeholders is not isolated to the NEM/NER and includes gas, WEM, and Consumer Energy Resources (CER). We recognise the AEMC's staged approach to first establish functions dedicated for the NEM, but we encourage a holistic and concerted effort to ensure there is resilience and protection across the entire Australian energy sector.

Our further comments on each of the proposed functions and cost implications are provided below:

Function 1 – Cyber Security Incident Coordinator

AGL supports the formal establishment of a Cyber Security Incident Coordinator role. AEMO plays an important role in coordinating with energy market participants and government agencies to enable effective and timely response to a cyber incident impacting the energy sector. This role should be formalised.

Function 2 – Supporting Cyber Preparedness and Uplift

AGL supports AEMO's proposed function to increase cyber preparedness and uplift. As mentioned in our previous response, AEMO's Energy Markets Cyber Exercise (Trident) delivered earlier this year, was a practical exercise which helped AGL identify several opportunities to enhance capabilities with technology and business partners. We welcome the continued delivery of these types of exercises for industry and government.

To bolster governance, we strongly advocate for the establishment of a working group comprising of energy market participants for the Australian Energy Sector Cyber Security Framework (AESCSF), ensuring a collaborative approach to the stewardship of the framework. Noting the framework is voluntary, involving self-assessment and benchmarking.

We also emphasise the value of advice that aligns the AESCSF with other frameworks like Protective Security Policy Framework (PSPF) and Information Security Manual (ISM), and the need for an aligned refresh cycle for these documents to maintain their relevance and effectiveness.

Function 3 – Examining Risks and Providing Advice

While we recognise AEMO's valuable expertise as the system operator, we believe that cyber security advisory services may be better provided by organisations with broader cyber security knowledge and experience. As mentioned in our previous response, partnerships with institutions like ACSC, CSIRO and ANU who have extensive capabilities and a national perspective that extend beyond the energy market could provide a more comprehensive approach to addressing the diverse and evolving cyber risks faced by the industry. For example, CommsAlliance – an industry representative body for the telecommunications sector – recently worked with ANU to develop the Australian Telecommunications Sector Resilience Profile – a comprehensive report that assesses the resilience of Australia's telecommunications sector. This foundational work demonstrates the benefits of leveraging specialised bodies for such initiatives. We suggest that AEMO's efforts be complemented by insights from specialised organisations to ensure a well-rounded advice.

Function 4 – Facilitating the Distribution of Information

While we appreciate AEMO's efforts in distributing critical cyber security information, we query the incremental value this function brings. As mentioned in our previous response, we believe information provided by the Australian Signals Directorate (ASD) through platforms like the Cyber Threat Intelligence Sharing (CTIS) already offer substantial coverage.

Furthermore, with the recent introduction of the Commonwealth *Cyber Security Bill 2024*, clarity is needed on how this function within AEMO will coordinate or work in conjunction with the National Cyber Incident Response Board (the Board), as both entities would review and produce post-cyber incident reports to Government. Akin to this function within AEMO, at the conclusion of a review, the Board will issue a report detailing its findings and recommendations.

Cost implications

Aligned to the sentiments raised by other stakeholders, AGL expresses concerns regarding the transparency and proportionality of costs associated with establishing AEMO's cyber security functions. We suggest fair cost allocation between industry and government, and proportional costs relative to the benefits provided for both function three and function four.

For example, function three will provide cyber security research and advice primarily to government rather than industry, and therefore should not necessarily be funded through market participant fees. A detailed breakdown and justification of the costs, particularly those outlined in Table 2.1, are essential for all stakeholders to understand the basis of these figures.

We also note that cost estimations for all four initial years are significantly below the $10 million sought through cost recovery measures each year. We strongly advocate for a participant fee structure that is equitable, and welcome AEMO's consultation on fee structure once this rule comes into effect on 12 December 2024.

Thank you for your invitation to comment on this draft determination. If you have any questions in relation to this submission, please contact with Senior Manager, Security Policy Risk & Compliance, Stuart Hay at shay2@agl.com.au.

Yours sincerely,

AGL