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

18 July 2024

Dear Sir or Madam,

Cyber security preparedness role and responsibilities that the Australian Energy Market Operator (AEMO)

AGL Energy (**AGL**) welcomes the opportunity to provide responses to the consultation questions posed by the Australian Energy Market Commission (**AEMC**) in response to the abovementioned 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, particularly over the last few years in Australia, AGL supports the AEMC's proactive efforts to protect and increase the cyber security resilience of energy's critical infrastructure and operation. Where relevant, we have indicated our support for proposed solutions, however, we also believe that the proposed rule change could be strengthened by providing more information on how these proposed functions complement and differentiate from existing cyber security roles, entities, and guidance within the energy sector. Additionally, there is an opportunity to clarify how these proposed functions are distinct from each other, as some appear to overlap in their cyber related activities. More information on the costings for each role would also be beneficial.

AGL's detailed responses to the consultation questions are set out within **Appendix A**.

If you have any questions in relation to this submission, please contact with Senior Manager, Policy Risk & Compliance Manager, Stuart Hay at shay2@agl.com.au.

Yours sincerely,

AGL

Appendix A – AGL's Responses to Consultation Questions

Question 1: Do you agree that the specific cyber security activities being undertaken on an ad hoc basis is problematic?

Yes – AGL agrees that undertaking cyber security activities on an ad hoc basis, rather than a coordinated approach is not best practice. The *2023 – 2030 Australian Cyber Security Strategy* postures Australia as a world leader in cyber security by 2030. This objective cannot be achieved if the cyber security activities which support the resilience of the energy sector are carried out on an ad hoc basis.

However, AGL would like to recognise the existing cyber security activities that have been effective in improving cyber security preparedness in the energy sector. For example, in May, AGL participated in the AEMO Energy Markets Cyber Exercise (codenamed Trident), which aimed to prepare AEMO, energy market participants and government agencies to jointly respond to a sector-wide cyber incident. Each participant engaged in their own detailed investigation and response activities and reported back to the AEMO Cyber Incident Response Forum (CIRF) on the findings and actions taken to investigate, respond to, and contain the threat actor, as well as engaging relevant partners and government entities. AEMO and the Australian Signals Directorate (ASD) considered the participant briefings and provided feedback and recommendations where appropriate. This practical exercise was beneficial to AGL, as we were able to identify several opportunities to enhance capabilities with technology and business partners. We support these types of efforts in creating cyber uplift across the sector and advocate for continued, coordinated efforts in keeping these cyber security exercises occurring on an ongoing basis.

Question 2: Do you consider there is a lack of clarity on the specified roles and responsibilities of cyber security in the NER?

Generally, yes, AGL considers there to be a lack of clarity on the specified roles and responsibilities of cyber as it relates to the National Electricity Rules (the NER/Rules) as there is currently no explicit reference to cyber security in Rules. AGL recognises that the increased digitisation of the National Energy Market (NEM) and the interconnected nature of infrastructure networks, exponentially exposes the system to the threat of cyber security incidents. But we note that the energy sector – and its potential cyber weaknesses – are not isolated to the NEM/NER and includes gas as a significant portion of the sector. We also emphasise the interrelated nature of gas and electricity markets, which is driven in part by gas providing a significant fuel source for electricity generation. This interconnected nature is further supported by rule change requests currently being considered by the AEMC involving amendments to the NER and the National Gas Rules (NGR) which, among other things, would explicitly require AEMO, in developing its Integrated System Plan (ISP), to explicitly consider gas market conditions, including the cost and feasibility of gas projects and supply issues.

As touched on in the consultation paper, AGL suggests that the scope of the cyber security roles and responsibilities, if implemented, should go beyond the NER and cover the NGR and the Wholesale Energy Market (WEM) in Western Australia to create coherent governance. Lack of clarity on the specified roles and responsibilities and how these functions span across the energy sector may increase the risk of governance alignment challenges in the future, as well as generate inconsistent application of cyber related activities across gas and electricity markets.

Question 3: Would the industry value more cyber security guidance in the NER, why/why not? If yes, what kind of guidance specifically?

No – AGL believes that industry does not need more cyber security guidance in the NER. We believe that there is existing and sufficient guidance in place via the Australian Energy Sector Cyber Security Framework (AESCSF) as well as the Critical Infrastructure Risk Management Program (CIRMP) under the Security of

Critical Infrastructure Act 2018. Both frameworks allow for participants to complete assessments to measure their own cyber security capability and maturity, as well as to allow for targeted, individualised response plans for the energy sector.

We believe that rather than creating new guidance material, more effort could be directed towards harmonising existing pieces of information into the one source of guidance and/or ensure alignment across existing forms of information. As creating new guidance on top of existing materials may further complicate the landscape of information and confuse energy market participants on their obligations.

Question 4: Do you agree that the lack of clarity regarding the identified cyber security functions in the Rules is problematic? Why or why not?

Similar to our answer to question 2, yes, AGL agrees that a lack of clarity regarding AEMO's identified cyber security functions in the NER can be problematic as this can lead to duplicated efforts, poorly coordinated response to cyber security incidents, and ineffective use of existing cyber related resources across the energy sector. Although we recognise that there is a general lack of specified cyber security roles and responsibilities in the NER, we also believe that the four proposed roles under this rule change require more specificity. AGL would benefit from more information, particularly as it relates to how each role is distinct from one another, and how their application will fit in with existing activities carried out by external entities.

For example, the consultation paper outlines function 1 'Cyber Security Incident Coordinator' to be responsible for [planning and coordinating] the NEM-wide response to a cyber incident affecting the energy sector (p 12)'. However, this overlaps with the fourth proposed function which would '[facilitate] the distribution of critical cyber security information to market participants' via activities such as 'warnings of cyber vulnerability and threats' or 'post cyber incident reports' (p 13). Furthermore, function 2 'supporting cyber preparedness and uplift' through activities such as the ongoing stewardship of the AESCSF and providing guidance and advice to industry (p ii), also overlaps with the 'examining risks and providing advice to government and industry' activities outlined within function 3 (p ii).

As mentioned below, AGL believes that the activities outlined under function 4 can be subsumed under the activities undertaken through the 'Cyber Security Incident Coordinator' (function 1), and that function 2 and 3 could be consolidated or simplified so that they are not duplicating efforts. In the absence of clarity of how these functions are distinct in what they provide to NEM participants, AGL reserves its position to fully support the introduction of these roles within the NER or broader.

Question 5: Do you consider cyber security a power system security issue, a network planning and expansion issue, or neither? Why/why not?

AGL considers cyber security to intersect with both power systems security and network planning and expansion, with the first impacting the latter. Cyber security is integral to both domains to safeguard the operation of modern power grids.

Power system security requires cyber security measures to protect critical infrastructure such as power plants, substations, and control systems from cyber-attacks. As interruption to power generation, transmission, or distribution can cause a significant disruption to daily life (as we have seen with major natural hazards). Additionally, with power systems increasingly utilising digital technologies, cyber security has become integral to network planning and expansion. For example:

- new technologies such as the rollout of the digital smart meters, and renewable energy sources (such as CER and DER) now connected to the grid all introduce further interfaces and require a considered approach to help ensure any potential points of cyber vulnerability are appropriately mitigated and consumers are appropriately protected.

- as new technologies and infrastructure are added to the grid, cybersecurity needs to be integrated into the planning and design phases to ensure resilience against cyber threats.
- The adoption of smart grid technologies and Internet of Things (IoT) devices in the energy sector increases the attack surface. Planning for these technologies requires robust cybersecurity measures to protect against vulnerabilities.
- network planning and expansion must adhere to cybersecurity regulations and standards, ensuring that new infrastructure meets security requirements from the outset.
- cybersecurity considerations in network planning help future-proof the energy infrastructure against evolving cyber threats, ensuring long-term security and reliability.

Question 6: Do you consider that the benefits for clarifying the cyber security incident coordinator as a function for AEMO in the Rules outweigh the costs/risks? Why/why not?

In principle, we believe that clarifying a cyber security incident coordinator as a function within AEMO is valuable in providing a single, credible source of truth during critical cyber security incidents. But we believe this role has already been somewhat established within AEMO via the AEMO Cyber Duty Manager role (CDM) within AEMO's Australian Energy Sector Cyber Incident Response Plan (AESCIRP).

It is unclear to AGL how the function of the cyber security incident coordinator would provide coordination activities beyond what has been established through AEMO CDM and/or whether the proposed function would replace the CDM. In the second iteration of the AESCIRP, which was released in May 2023, the AEMO CDM is listed as one of the 5 specified roles in the plan who 'acts as the primary AEMO contact for cyber incidents, and is the interface point between the cyber forum and the operational emergency forums' (p 7). The AESCIRP also further outlines this role as responsible for 'continuously correlating and triaging active cyber incidents affecting NEM participants that they are notified of, this plan and, in doing so, trigger a coordinate response' (p 9). This is highly correlated to the proposed function 1 in this consultation paper.

As mentioned in our answer to question 2, the practical application of function 1 (cyber security incident coordinator) seems to overlap with the responsibilities outlined in function 4 (facilitating the distribution of critical cyber security information to market participants). We suggest that these functions could be consolidated.

Furthermore, as the greatest estimated cost out of all proposed cyber functions (requiring $4.25 million to establish, and then $4.25 million in year 1), industry would benefit with more information around the key responsibilities and actions that would be completed under this function to be able to discern if the benefits outweigh the costs/risks. We also recognise that there could be potential risks associated with codifying this function – and others – in the Rules, as prescriptive wording may lead to rigid application. We acknowledge that the drafted wording will need to strike a balance between the need to provide AEMO with sufficient flexibility to be responsive during cyber incidents, whilst not be too vague to so that the scope of such roles is too broad.

Question 7: Do you consider clarifying the supporting cyber preparedness and uplift as a function in the Rules outweigh the costs/risks? Why/why not?

In principle, yes, we do consider clarifying the cyber preparedness and uplift function in the Rules to be beneficial. However, we also recognise that AEMO already supports cyber preparedness and uplift through existing activities, despite these not presently codified in the Rules.

Notably, the supporting activities under this function mentioned in the consultation paper – (1) stewardship of the AESCSF, (2) organisation of testing and training exercises, and (3) provision of guidance and advice to the industry – already are activities already carried out by AEMO at varying degrees. For example, in our response to question 1 we mentioned AEMO's Energy Markets Cyber Exercise which AGL and other market participants engaged in as a training exercise to understand where there were organisational and system weaknesses which would fall within the 'organisation testing and training exercises' section. We also query how the 'provision of

guidance and advice to industry' within this function is different to function 3 'Examining risks and providing advice to government and industry'.

Notably, the estimated costing for this role is significantly higher in year 1 ($2.06 million) compared to the establishment year ($1.56 million). As NEM participants will be absorbing the costs associated with these activities through participation fees, AGL would be interested to understand further break down of how these costs have been calculated. Furthermore, to the extent that AEMO is already performing some of these functions today, it would be beneficial to clarify whether the above costing factors in pre-existing activities/funding. This would support AGL's ability to discern whether the proposed function in the Rules would outweigh the costs and associated risks.

Question 8: Do you consider the benefits of clarifying the examining risks and providing advice to government and industry as a function in the Rules outweigh the costs/risks? Why/why not?

The consultation paper places greater emphasis on the specialised advisory services that AEMO could provide directly to government, with advice to NEM registered participants considered as a discretionary and supplementary activity within this function. AGL recognises that AEMO providing cyber security research and advice to Energy Ministers on request may be beneficial to government as they are uniquely placed to provide expertise as the system operator. On the other hand, we question whether AEMO is best positioned to lead this research function compared to organisations such as the CSIRO, and instead, may be better suited to provide industry-specific subject matter expertise to research organisations to support the broader cybersecurity research and thought leadership agenda. It is also worth noting that given the nature of such advice to government would likely be confidential, it may not be a benefit that directly translates or supports industry participants.

The consultation paper estimates this function to cost $0 in the establishment year, and then $775 K in year 1, and then $400 K in year 2 and 3. AGL would be interested to understand the rationale behind such costings, and why establishment costs are considered nil. This function also has the possibility to have the highest variability, year on year, in terms of costs, as the consultation paper touches on a 'advice on request' model. We recognise that there are some cyber related activities that will better support government over industry and encourage AEMC to consider whether the funding should reflect fair and proportioned costs across industry and government.

Question 9: Do you consider the benefits of clarifying the facilitating the distribution of cyber security information to market participants as a function in the Rules outweigh the costs/risks? Why/why not

As mentioned in our answer to question 4, 6 and 7, AGL considers this function as similar to function 1 (cyber security incident coordinator) and thinks that better consolidation and distinction of responsibilities could be devised. We also consider there to be overlaps with the existing AEMO Cyber Duty Manager role (CDM) within AEMO's Australian Energy Sector Cyber Incident Response Plan (AESCIRP) (please refer to answer to question 6).

We also note that AGL already receives critical cyber security threat reports from Australian Signals Directorate's (ASD's) Cyber Threat Intelligence Sharing (CTIS) platform which enables government and industry partners to quickly receive and share information about malicious cyber activity. We query how this information would differ from, or go beyond the distribution of cyber information, or whether it is needed, noting the addition of another information-sharing channel may risk adding unnecessary cost and complexity. This function would perhaps be a greater benefit to smaller NEM registered participants that are not a part of the ASD's partnership in the CTIS platform.

Question 10: Do you agree with the proposed assessment criteria? Are there additional criteria that the Commission should consider, or criteria included here that are not relevant?

AGL agrees with the proposed assessment criteria for the Commission's regulatory impact analysis of the proposed rule change which includes: (1) Safety, security and reliability, (2) Principles of good regulatory practice and (3) implementation considerations.

Within the third criteria, in relation to implementation considerations, we encourage this section to focus beyond the direct and indirect costs for the solution, but to also evaluate:

- Feasibility and practicality - i.e. what guidance, advisory services, frameworks, communication channels and expertise already exist within cyber security for the energy sector and whether there is a genuine need for the proposed solution. Or how the proposed solution would complement existing functions. This type of assessment is briefly touched on in the consultation paper but could be broadened and emphasised. For example, the paper notes consideration of the timing of the proposed rule and the costs and benefits which will be supported by analysis of 'interactions with other reforms, including outside the AEMC' (p 16),
- Risks and unintended consequences of the proposed function - i.e. is the proposed solution creating more complexity in the system, and/or creating more regulatory burden for NEM participants.

We also note that heading 4.2 sites four criteria (p 15), and subsection 4.2.2 outlines three separate criteria (p 15 - 16). We query whether this is a typo in heading 4.2 or if this there is a fourth criteria that has not been added to the consultation paper.

Additional considerations to note – cost estimation

We note that the estimated costs for the proposed cyber security roles and responsibilities have an estimated establishment cost of $6.46 million in the first year, $7.4 million in year 1, and subsequent years with estimated costs significantly below $10 million. We query whether funding for the proposed AEMO functions will be sought through a retainer fee of $10 million each year through increased participation fees, or whether cost will be recovered on an ad hoc basis. As a AEMO participant member, we would also benefit from further break down of how these costs have been calculated, and the rationale behind the costings. This would provide a better indication as to whether costs are likely to increase or stay stable.

Furthermore, as we previously mentioned, for activities that provide a direct benefit to government rather than industry participants, we suggest that funding sought is apportioned fairly across government and industry. We also suggest that there is a review mechanism instated at the end of the initial implementation period to evaluate the effectiveness of the proposed cyber security roles and responsibilities in achieving the intended outcomes, and to assess whether on-going funding should be considered or approved.