18 July 2024

Ms Anna Collyer
Chair
Australian Energy Market Commission
GPO Box 2603
Sydney NSW 2000

Project Reference Code: ERC0388

Dear Ms Collyer

Cyber security roles and responsibilities

Energy Queensland Limited (Energy Queensland) welcomes the opportunity to provide comment to the Australian Energy Market Commission (AEMC) *Cyber security roles and responsibilities consultation* (the Consultation Paper).

This submission is provided by Energy Queensland, on behalf of its related entities, including:

- Distribution network service providers (DNSPs), Energex Limited (Energex) and Ergon Energy Corporation Limited (Ergon Energy);
- Retailer, Ergon Energy Queensland Pty Ltd (Ergon Energy Retail); and
- Affiliated contestable business, Yurika Pty Ltd and its subsidiaries, including Yurika Metering.

As noted in the Consultation Paper, the *Security of Critical Infrastructure Act 2018* (the SOCI Act) expanded its scope to encompass the energy sector. This legislative update mandated rigorous cyber security standards and incident reporting requirements for energy providers. The SOCI Act requires National Electricity Market (NEM) participants, including the Australian Energy Market Operator (AEMO), to manage their own critical infrastructure in a cyber secure manner. Energy Queensland supports the objective of the rule change provided the final drafting does not create any additional mandatory guidelines that erode, contradict or unnecessarily replicate the SOCI Act mandated cyber security standards for market participants.

Further, it is proposed that an increase of 2% in participant fees will occur to fund the additional activities to be carried out by AEMO. Some participants already incur significant costs to comply with rigorous cyber security standards and incident reporting requirements imposed by the SOCI Act. It is our strong opinion that there needs to be a compelling benefit to justify the increase in participant fees when these participants are already responsible for implementing and managing cyber security (which involve significant administrative costs) under the SOCI Act.

Should AEMC require additional information or wish to discuss any aspect of this response, please contact Laura Males on 0429 954 346 or myself on 0429 394 855.

Yours sincerely,

Alena Chrismas
Manager Regulatory Affairs

Telephone: 0429 394 855
Email: alena.chrismas@energyq.com.au

Encl: *Energy Queensland's responses to the Consultation Paper questions.*

AEMC consultation - Cyber security roles and responsibilities

AEMC consultation Question	Energy Queensland response
Question 1: **Do you agree that the specific cyber security activities being undertaken on an ad hoc basis is problematic?**	Energy Queensland agrees there is a specific risk around the coordination of cyber incident management within the broader operation of the National Electricity Market (NEM) and as such, should be formalised as a responsibility of the Australian Energy Market Operator (AEMO). However, in our view, the fact that AEMO performs several other cyber security functions on an ad hoc basis does not present a fundamental risk to the cyber security of the NEM. The cyber security of the NEM and the cyber risk management activities undertaken by NEM participants is already the focus of a range of other measures including corporate governance requirements. These include but are not limited to the Australian Securities and Investments Commission (ASIC) (for listed entities), licence conditions issued by jurisdictions, legislative obligations (including the *Security of Critical Infrastructure Act 2018* (the SOCI Act) and *The Privacy Act 1988*), cyber insurance requirements and guidance provided by Government security agencies.
Question 2: **Do you consider there is a lack of clarity on the specified roles and responsibilities of cyber security in the NER?**	Energy Queensland views cyber security at a core element of risk management. We suggest responsibility for operational risk management has always been and should remain with NEM participants. As the market operator, AEMO has several established NEM coordination roles, for example the use of emergency powers across jurisdictions, and in this respect Energy Queensland requests further clarification on how cyber management will be aligned to these functions.
Question 3: **Would the industry value more cyber security guidance in the NER, why/why not?** **If yes, what kind of guidance specifically?**	Energy Queensland notes there is a wide range of peer reviewed and progressive cyber security guidance already available from standards organisations (ISO 27000 series, IEC 62443 series), security organisations (Australian Government's Information Security Manual - ISM) and respected research organisations (National Institute of Science and Technology's Cyber Security Framework – NIST CSF). These standards and frameworks are also referenced in the SOCI Act and entities must demonstrate compliance to a particular standard or framework. Additional cyber security guidance in the National Electricity Rules (NER) would at best be duplicative of this requirement and at worst could have negative security outcomes by being restrictive. Therefore, we suggest there is no reason to include additional cyber security guidance in the NER.

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?**	Energy Queensland agrees the rules would benefit from a clarification of AEMO's role in the coordination of cyber management across jurisdictions alongside broader NEM emergency management coordination activities that AEMO performs. In our view, it should mirror AEMO's existing role in managing the Power System Emergency Management Plan (PSEMP), preparing system restart plans, and coordinating system restoration activities.
Question 5: **Do you consider cyber security a power system security issue, a network planning and expansion issue, or neither?** **Why/why not?**	Energy Queensland suggests that cyber security is both a power system security issue and a network planning and expansion issue. We believe it is critical to provide a secure, dynamic and reliable electricity network for a rapidly changing operating environment. Energy Queensland's distribution networks are increasingly dependent on digitally connected components. If these digital grid components are compromised, this could lead to network safety or stability issues. Further, many grid operations and network planning and expansion decisions are increasingly dependent on measurement data derived from digital sources. Should the integrity of this data be compromised, this may adversely impact planning and operational outcomes. In our view, it is vital to maintain critical service provision, support the evolution of the electricity grid and address the increasing volumes of sophisticated and malicious attacks as such, cyber security is both a power system issue and a network planning and expansion issue.
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?**	Energy Queensland agrees there is a benefit for having a cyber management coordination function performed by AEMO. This ensures alignment with NEM emergency management coordination activities that AEMO already performs through the PSEMP.
Question 7: **Do you consider clarifying the**	Energy Queensland suggests this function should not be performed by AEMO. We consider the proposed functions are valuable support activities for industry but would be more effectively performed by existing government

supporting cyber preparedness and uplift as a function in the rules outweigh the costs/risks? **Why/why not?**	services. For example, the Australian Signals Directorate (ASD) already publishes cyber security guidance and conducts testing and training exercises and has significant technical resources to perform these functions. Alternately, this could be performed as a function of the recently established Cyber and Infrastructure Security Centre (CISC). In our view, it would be duplicative for AEMO to perform these activities and the provision of such advice and content is inconsistent with AEMO's function as a market operator. For example, AEMO does not provide guidance to entities on how to manage bushfires or cyclones.
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?**	Energy Queensland suggests this function should not be performed by AEMO. This is inconsistent with AEMO's role as a market operator. We suggest that AEMO does not have insights into the unique operational risks posed by many market participants (for example, AEMO operates no field or operational equipment) and such advice sourced from AEMO may not suitably represent industry risks. Government should instead work to establish better linkages with industry directly, rather than relying on AEMO solely for advice and guidance on risk.
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?**	Energy Queensland suggests this function should not be performed by AEMO. As noted in the response to question 7, this type of information is already published by a range of Australian and international government and commercial organisations, including the ASD. At best, this would become a duplication of these other information sources, creating a challenge for entities. At worst, this may lead organisations to solely rely on the information provided by AEMO, creating a dependency risk. Again, this is inconsistent with AEMO's function as a market operator.
Question 10: **Do you agree with the proposed assessment criteria?** **Are there additional criteria that the**	Energy Queensland agrees the proposed assessment criteria appears fit for purpose. In assessing against the proposed criteria, the AEMC should consider the scope and application of the SOCI Act, the regulatory powers and role of the CISC and the ASD. It is our strong view that much of the proposal duplicates existing cyber security regulations or functions, and therefore, we suggest any duplication is both costly and unnecessary.

Commission should consider or criteria included here that are not relevant?	
Other feedback not provided in responses above	Energy Queensland suggests the proposed solution 1a is problematic as it proposes significant and broad responsibilities for AEMO. As detailed above, participants have their own responsibility to prepare for, respond and recover from cyber security incidents as part of good corporate governance and its obligations. This risk management obligation is also established under the SOCI Act. We do not see why cyber security as a function should sit with AEMO's existing role given a framework already exists.