1 July 2024

Australian Energy Market Commission
Level 15, 60 Castlereagh Street Sydney NSW 2000
Reference: ERC0388

Dear Sir/Madam,

Anchoram Consulting's Response to the rule change request to establish cyber security as one of the Australian Energy Market Operators responsibilities under the National Electricity Rules (NER).

Anchoram Consulting welcomes the opportunity to respond to the AEMC's consultation paper released on 20th June 2024. Anchoram Consulting is a national professional services firm with specific expertise in cyber security within critical infrastructure sectors, and particularly the energy sector.

As an organisation that works continually with energy providers who fall under regulatory purview of the Australian Energy Market Operator, Anchoram is well placed to provide meaningful feedback on how a rule change to the NER may affect providers.

We have reviewed the proposed rule change request and have the following comments:

1. The energy systems that fall under regulatory purview of the NER have multiple layers of technology in play across both sovereign systems, cloud based systems and services provided by third parties. Therefore, these bringing several unique and concurrent risk aspects to operations of the NEM.
2. The interconnected nature of these systems and their associated risks are not fully understood by all NEM participants including AEMO, there are several gaps in understanding the impacts and what an AEMO response would look like in the case of a cyber incident that threatens the broader NEM.
3. The works that AEMO have currently undertaken such as the Australian Energy Sector Cyber Security Framework (AESCSF) and the Australian Energy Sector Cyber Incident Response Plan (AESCIRP) activities are providing participants leadership in improving cyber security maturity and providing incident response collaboration.
4. We support cyber security being explicitly referenced in the NER as it relates to power system security, noting that this should reference the protection of the function of the participants as opposed to general cyber security capabilities.
5. We support the funding and creation of specific cyber security roles and responsibilities that AEMO would perform to assist in enhancing cyber security across the energy system.
6. We support adding cyber security as a function with AEMO's role. As the market operator is in a suitable position to co-ordinate response to any wide ranging cyber incident and provide leadership in enabling collaboration between market participants.
7. We support the sharing of reports, vulnerabilities, and other relevant information from AEMO to market participants and note that both formal and informal forums exist within the industry already such as the Energy Intel Group (EIG) and the Trusted Information Security Network (TISN).
8. We note that the funding requirements are commensurate with the cost of operating these functions and feel that this will provide a return on investment considering the potential cost of an incident that affects the broader NEM.

Consultation Questions and Answers

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

Answer: *Any ad-hoc approaches by definition lack consistency and structure and building on the back of numerous strategic efforts in the energy sector and the proposed changes demonstrate that the Commonwealth understands the risks and is taking steps to address these within the regulatory framework of the NER.*

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

Answer: *The responsibility for direct response should remain with the relevant market participant and their relevant roles, we feel that industry is seeking for an overarching mechanism for collaboration and in some cases direction that relates to the operation of the function of the market participant versus a response that focuses on a cyber response to the technology.*

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

Answer: *Yes, the industry would benefit from "relevant" guidance which focuses on how a response to protecting the function of the market participant as the leading focus, whilst existing initiatives such as AESCSF are valuable to measure maturity, and leaving aside any recent focus on the function it does not mandate the requirements for an operational response capability as it relates to 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?

Answer: *This is problematic, as there is no clear line of sight between a cyber function and the other functions within the NER, clarifying this should provide a linkage to the risk and safety elements of the NER where these relate to a cyber security event.*

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

Answer: *This is a power system security issue, as the threat from a cyber incident impacting the NEM is the worst case scenario. The interconnected nature of energy systems and newer functions such as Distributed and Customer Energy Storage (DER/CER) may have an ability to impact the NEM should be considered holistically as these have technology aspects and large aggregated electrical load which all have the ability to affect energy system stability if maliciously operated.*

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?

Answer: *The benefits that this role would delivery from a collaboration and coordination point particularly focusing on AEMO's current ability to interface with market participant operations control centres would provide a line of sight to an operational response to a cyber incident that may affect the NEM, this would justify the costs for resourcing based on potential improvements and operational responses to any cyber event.*

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?

Answer: *These further cements and builds on the current work that AEMO is doing and ensures that these functions are resourced effectively*.

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?

Answer: *This formalises many informal activities that AEMO and associated industry groups are doing, this focus will further improve and refine these current forums and activities.*

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?

Answer: *This approach will mirror what has been done in other jurisdictions with bodies such as NERC in the United States and aligns AEMO with similar responsibilities within Australia*.

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?

Answer: *These are suitable for assessment criteria noting that Safety is the paramount consideration, it should also be noted that the impacts of a NEM wide cyber event could destabilise large portions of the Nation and as such AEMO's involvement at that time would be critical to response.*

In summary Anchoram welcomes the changes proposed and looks forward to changes in this regulatory framework.

Sincerely,

Glenn Ashe
CEO – Anchoram Consulting Group
Level 1, Suite 3, 16 Napier Close
Deakin, ACT 2600