



15 July 2024

Nomiky Panayiotakis
Project Lead
Australian Energy Market Commission
Sydney NSW 2000
By online submission

Cyber Security – Consultation Paper

Alinta Energy welcomes the opportunity to provide feedback to the AEMC's consultation paper on Transmission Access Reform.

Alinta Energy acknowledges that AEMO has been a key facilitator of cybersecurity maturity uplift for industry via the development of the Australian Energy Sector Cyber Security Framework (AESCSF) and generally supports further clarification and strengthening of AEMO's role in relation to cybersecurity for the energy sector. In addition to this, formalisation of AEMO's role in cybersecurity should ensure that AEMO carries out this role efficiently and minimises costs in a manner consistent with the standard of a reasonably prudent operator and the national energy objective.

Our responses to the consultation paper's questions are contained in the attachment.

If you would like to discuss this further, please contact me at hugh.ridgway@alintaenergy.com.au.

Yours sincerely,

Hugh Ridgway
Wholesale Regulation Manager

ATTACHMENT

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

AEMO has provided support to participants in the development of the AESCSF and is the appropriate body to coordinate further development of cyber security frameworks and standards across the industry. We support a formalisation of AEMO's role in this respect.

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

Yes. There is also no explicit mention of the cyber security of technologies and assets that support power system security. Existing AEMO responsibilities include maintenance of power system security but does not determine the extent of that role (e.g. does this role include auxiliary functions that may affect the 'technical envelope' such that the power system falls outside the secure operating state?).

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

Policy guidance, or guidance around roles in cyber security as described in the response above would be welcome, however care should be taken to ensure that this does not conflict with the existing role of the Department of Home Affairs under the Security of Critical Infrastructure Act (SoCI) and create confusion and problems of precedence. Where there is overlap, AEMO and the NER should defer to the Department of Home Affairs and SoCI for any cyber security event. Alinta Energy would support the inclusion of definitions of what power system functions fall within the cybersecurity remit (or how those functions may be accurately determined).

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

Yes. Clear and concise guidance would improve certainty for participants and AEMO.

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

It is primarily a power system security issue but network planning could also be impacted by cyber security events and decisions made pursuant to network planning processes may be relevant to cybersecurity as well..

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?

We agree that incident coordination in relation to the power system should be in AEMO's remit regardless of the underlying cause. However, as noted in our response to (3) above, the scope of this role in relation to cybersecurity needs to dovetail with the existing functions of the Department of Home Affairs.

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

The Department of Home Affairs already leads training exercises (such as Trident exercise in May 2024), measuring the outcomes to determine performance gaps, then assuring gap resolution to improve preparedness. AEMO does however have a role in providing advice or guidance to industry on cyber security matters as this does not overlap with existing capability in the Department of Home Affairs.

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?

Alinta Energy supports AEMO in the proposed role of providing advice to government agencies in relation to cybersecurity risks to the power system and continuing to support participants in cybersecurity uplift programs.

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?

Yes, we consider that where AEMO is aware of relevant cyber security information it should disseminate this to market participants as appropriate.

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?

Yes.