24 July 2024

Nomiky Panayiotakis

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

Submitted via email: aemc@aemc.gov.au

Ausgrid
24-28 Campbell St
Sydney NSW 2000
All mail to
GPO Box 4009
Sydney NSW 2001
T +61 2 131 525
ausgrid.com.au

Ausgrid submission to the AEMC Cyber security roles and responsibilities consultation paper.

Ausgrid is pleased to provide this submission to the *Cyber security roles and responsibilities consultation paper*.

Ausgrid operates the electricity distribution network that powers the homes and businesses of more than 4 million Australians living and working in an area that covers over 22,000 square kilometres from the Sydney CBD to the Upper Hunter in New South Wales.

Our submission responds to the questions from the Consultation Paper, as set out in detail in Attachment A.

We support the proposed rule change. It is appropriate for the Australian Energy Market Operator (**AEMO**) to take on a leadership role in coordinating cyber security activities across the energy sector, particularly in light of growing concerns around cyber security risks. We recognise that there will be compliance costs for industry participants from this rule change, but further detail will be needed to understand and quantify these impacts and consider how these costs will be recovered.

AEMO's governance of cyber security should seek to align industry best practice and drive a more consistent and comprehensive adoption of applicable standards. A stable and consistent approach to cyber security governance allows AEMO to appropriately match each industry participant's required cyber security capability to its function within the National Electricity Market (**NEM)**, ensuring that those whose risk is highest have commensurate cyber security measures in place. However, the proposed rule change could be strengthened by also clarifying the responsibilities of system participants (including Ausgrid) to AEMO relative to the Commonwealth Department of Home Affairs and other existing cyber security authorities.

We look forward to the opportunity to provide further feedback on the proposed rule change. For further information please contact Simon Moore, Senior Policy Advisor at simon.moore@ausgrid.com.au

Yours sincerely,

Junayd Hollis,
Group Executive - Customer, Assets and Digital

Attachment A: Ausgrid responses to questions

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

Agree. Ausgrid supports a systematised approach to AEMO's cyber security activities. The ad hoc approach employed to date leads to inconsistencies and risks a lack of follow-through on important activities. AEMO governance of cyber security should seek to align industry best practice and drive a more consistent and comprehensive adoption of applicable standards (such as NERC-CIP, IEC 62443, IEC 62351, relevant NIST SP800 documents and others) with respect to the operation of the power system.

With adequate oversight, AEMO should be able to provide assurance of the power system's cyber security preparedness, similar to the approach taken for other hazards such as high demand, instability in load, frequency, natural disasters and extreme weather. A stable and consistent approach to cyber security governance allows AEMO to appropriately match each industry participant's required cyber security capability to its function within the NEM, ensuring that those whose risk to the NEM operations is highest have commensurate cyber security measures in place.

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

Agree. While Ausgrid believes that primary responsibility for each system participant's cyber security is theirs to manage, it is appropriate that a central coordinator have responsibility for overall security architecture. If balanced by appropriate accountability for costs, the market operator could be the natural authority to establish, baseline and maintain systemwide security architecture, and to ensure that market participants are meeting their responsibilities.

With respect to cyber security threat identification and incident response, there is merit in having the rules provide greater clarity as to how AEMO could function as a central point of contact and direction. AEMO is also suitably positioned to act as an interface with the multiple government bodies (at state and federal levels) and other critical infrastructure operators with whom the energy system shares various dependencies. In this regard Ausgrid supports the rule changes as proposed. However, the proposed rule change could be strengthened by also clarifying the responsibilities of system participants (including Ausgrid) to AEMO relative to the Commonwealth Department of Home Affairs and other existing cyber security authorities.

By establishing clear roles and responsibilities, AEMO and the broader market can develop a position that supports a more secure and resilient power system overall.

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

Yes.

Ausgrid considers it beneficial for all participants to apply a risk led approach to cyber security such that the security controls and countermeasures are commensurate with the consequences and impacts related to those identified risks. IEC 62443 (the international series of standards that address cybersecurity for operational technology in automation and control systems) provides guidance on how those risks identified are managed. AEMO is well placed to disseminate what controls it might expect to see as a baseline for the various operators. This would bring alignment between the maturity level of cyber practices of the Australian Energy Sector Cyber Security Framework (**AESCSF**) and expected controls considerate of their function and criticality to NEM operations.

Examples of where Ausgrid views additional cyber security guidance as being valuable include:

- Providing standards where specific outcomes relevant to the market and operational systems are needed, and act as part of the control systems for the applicable industry

standards (such as NERC-CIP, IEC 62443, IEC 62351, relevant NIST SP800 documents and others);
- Integration architectures and their associated security;
- Guidance to reduce participants sharing telecommunications or compute infrastructure or common third-party services; and
- Training that goes beyond cyber incident responses, to also cover cyber security for systems concerned with the power system and its ancillary supporting services.

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?

Agree. The AESCSF has been supported and promoted by AEMO, however there has otherwise been a limited approach to cyber security programs or driving cyber maturity within the electricity sector. This is due in part to the absence of any rules relating to cyber security functions, like those currently under consideration. A lack of clarity in relation to cyber security functions has been exacerbated in the past by vague guidance associated with the *Security of Critical Infrastructure Act 2018* (**SOCI Act)**, although this has recently been made clearer by the adoption of material risk rules.

Providing AEMO with the ability to assume these cyber security functions and have appropriate powers will not only clarify the cyber security of the power system, but also provide consideration to the broader supporting systems used by each participant.

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

Cyber security is both a power system security issue and a network planning and expansion issue. Power system security is the primary operational function of the NEM. The cyber security risks associated with the technologies now in service must be managed. Moving forward, the growing role played by consumer energy resources (**CER**) and distribution system operators (**DSO**), increases the importance of considering cyber security at each step.

It is imperative to ensure that new technologies and devices do not create weaknesses in the overall cyber security of interlinked systems in the electricity sector. Planning in relation to CER must take into account, and mitigate as far as possible, any vulnerabilities resulting from the increasing online connectedness of CER assets. In particular, we want to ensure that the core aged assets responsible for managing the bulk generation, transmission and distribution supply duties are not threatened by new connected CER with a variety of support and maintenance models.

Assigning a greater role to AEMO in considering these issues will be important in managing the overarching cyber security framework.

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?

Ausgrid considers that the benefits of the proposed change significantly outweigh anticipated costs. Even a minor cyber security incident impactful to the NEM operations has the potential to impose significant financial impacts, not just on NEM participants but on energy consumers and the wider societies economy. Depending on the scenario, there are other potential detriments to energy consumers, such as, for example, if safety imperatives cannot be met when there is uncontrolled loss of supply.

By simplifying messaging through the market operator, other entities and stakeholders can work on their own incident response with the confidence that AEMO is able use their position to direct and instruct the market and work towards restoration and recovery of the power system after any incident. The forecast cost of developing the capabilities outlined in the proposed rules is insignificant when compared to the costs of a cyber incident that could be avoided by a well-orchestrated and cohesive incident response.

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?

Yes. In line with the response to Question 6, the National Electricity Rules (**NER**) were originally developed to establish the market operator to ensure the stability of the power system and support its resilience. As a result, the NER contain exhaustive guidance as to the outcomes registered participants must support in the operation of their assets but rarely prescribe how those outcomes should be achieved.

With cyber security now being included as part of our all-hazards approach to security, the first four proposed functions described in the rule change proposal (plus a potential fifth relating to baseline architectures) will establish the foundation for further rule changes to build out the rigour operators should exercise to protect the power system.

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?

Yes. As the market operator for the electricity market, AEMO is best positioned to provide coordinated, aggregated advice to government on behalf of all energy market participants. The SOCI Act is an instrument that remains industry agnostic by design and is therefore unable to draw focus to particular security outcomes that might be considered more industry specific.

Given the essential nature of electricity supply on the livelihoods of our communities, and the potential impacts to lives and livelihoods, and other critical infrastructure, should there be major interruptions to the power system due to cyber incidents, the NER should empower AEMO to advocate for the industry. There should also be sufficient resourcing internally within AEMO to collect and understand market participants' views, so that the views and advice being provided by AEMO represent the industry and are not simply those held by AEMO.

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?

Yes. There is benefit in centralising the dissemination of threat intelligence and reporting of incidents that may be relevant to the respective functions within the energy market. This establishes a baseline of threat intelligence that should be actionable, and facilitates a response by each participant that goes to mitigating or defeating the threats. AEMO and the AEMC may wish to consider future rule changes to establish the ability to request that certain intelligence is acted on by specified market participants.

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?

We recognise that there will be compliance costs for industry participants from this rule change, but further detail will be needed to understand and quantify these impacts and consider how they will be recovered.

Ausgrid would support AEMO being provided with the authority to prescribe to market participants certain patterns or architectures and their associated solution architectures. These patterns and architectures need to be industry aligned and carefully developed in collaboration between AEMO, TNPs, DNSPs and other key market participants. Prescribed technical engineered controls or minimum standards may help buy time for market participants whose cyber capabilities are still maturing, but who need to keep pace with an escalating threat environment.

Given the timeframes needed for the industry to increase its cyber security capability, effective technical controls provide a way to protect the power system in the short-term while market participants implement longer term, more mature solutions.