AEMO
AUSTRALIAN ENERGY MARKET OPERATOR

Level 12
171 Collins Street
Melbourne VIC 3000

Postal address
GPO Box 2008
Melbourne VIC 3001

T 1300 858 724
F 03 9609 8010
E info@aemo.com.au

18 July 2024

Ms Anna Collyer
Chair
Australian Energy Market Commission
Level 15, 60 Castlereagh Street
Sydney NSW 2000

By electronic submission

Dear Ms Collyer,

Cyber Security Roles and Responsibilities Rule Change Consultation Paper

AEMO welcomes the opportunity to respond to the AEMC's Consultation Paper "Cyber security roles and responsibilities" (**Consultation Paper**). The Consultation Paper arises from the rule change request by the Commonwealth Minister for Climate Change and Energy (**Minister**) to amend AEMO's existing functions to include four cyber security roles and responsibilities within the National Electricity Rules (**NER**).

AEMO agrees with the Minister that cyber security is not explicitly referenced in the NER and that AEMO's role in cyber security is not specified in the NER. In the absence of any express reference, the question arises as to whether AEMO is authorised to perform the four cyber security roles within AEMO's existing statutory functions. Excluding AEMO's authority to take actions in response to an immediate or proximate cyber-attack (or a specific threat of cyber-attack) affecting or potentially affecting power system security in the National Electricity Market (**NEM**), AEMO does not believe the National Electricity Law (**NEL**) or the NER authorise ongoing activities in relation to the generalised threat of cyber security incidents.

Given that the four cyber security roles are not currently conferred on AEMO by the NEL or NER, AEMO strongly supports the proposed amendments to the NER to clarify and provide that AEMO's function to maintain and improve power system security:

1. includes an obligation on AEMO to coordinate and support cyber preparedness, response and recovery in accordance with AEMO's cyber security functions; and
2. defines AEMO's cyber security functions (consistent with the Minister's request and as summarised further below).

Expressly conferring these functions within the NER authorises AEMO to perform these new functions, recover the associated costs in accordance with the NEL and NER, and confirms the application of the existing statutory provisions to AEMO's performance of these new functions.

The Consultation Paper outlines the expansion to cyber security governance over the last ten years, including the development of the Australian Energy Sector Cyber Security Framework (AESCSF) following the Finkel Review, the *Security of Critical Infrastructure (SOCI) Act 2018* (Cth) (**SOCI Act**) as well as jurisdictional emergency management arrangements. Under the SOCI Act, AEMO and many market participants (who are responsible entities for critical infrastructure assets) have existing security obligations to their critical infrastructure assets. These include: (i) providing information about their critical infrastructure assets to the Register of Critical Infrastructure Assets, (ii) reporting cyber security incidents that have a significant or

relevant impact on critical infrastructure assets to the Australian Cyber Security Centre, and (iii) establishing, maintaining, and complying with a written critical infrastructure risk management program for critical infrastructure assets that identify and mitigate material risks that could have a relevant impact on critical infrastructure assets. AEMO believes that the four proposed cyber functions have appropriately considered, and are consistent, with these obligations.

Scope

The scope of the four proposed cyber security roles and responsibilities outlined in the Consultation Paper are specific to the NEM. They focus on AEMO coordinating and supporting cyber preparedness, response and recovery in the NEM as follows:

1. Cyber security incident coordinator: clarifying that AEMO would coordinate the response of registered participants to a cyber incident which adversely affects or could be expected to adversely affect the secure operation of the power system, including AEMO leading the: (i) development and maintenance of the Australian Energy Sector Cyber Incident Response Plan (AESCIRP) which sets out how market, state and federal responses are coordinated; and (ii) the implementation of the plan.
2. Supporting cyber preparedness and uplift: AEMO would support registered participants to improve their level of cyber security preparedness and maturity, including in collaboration with relevant government agencies and industry bodies. This may include, following consultation with ministers of participating jurisdictions, leading the maintenance and development of the Australian Energy Sector Cyber Security Framework (AESCSF) and coordinating annual assessment programs in accordance with the AESCSF, supporting and undertaking the development and delivery of scenario exercises to test the resilience of the power system to cyber threats, and developing and distributing cyber security guidance materials and tools to registered participants;
3. Examining risks and providing advice to government and industry: AEMO: (i) may, in its role as the power system and market operator, undertake research and provide advice (to a minister of a participating jurisdiction and to registered participants) in relation to identified cyber security risks that may impact the power system and the management or mitigation of those risks; and (ii) must, at the request of a minister of a participating jurisdiction (following consultation on requested scope, timing and costs), undertake research and provide advice in relation to cyber security risks to the power system and the management or mitigation of those risks.
4. Facilitating the distribution of critical cyber security information to market participants: AEMO would facilitate the distribution of critical cyber security information to participating jurisdictions and registered participants. This may include: (i) collating and distributing the advice of government agencies and other bodies with respect to cyber security matters relevant to the energy sector; (ii) providing information to participating jurisdictions and registered participants of which AEMO becomes aware regarding: (a) cyber security threats and vulnerabilities; (b) preventative patches; and (c) and other cyber security management and mitigations.

As outlined in the Consultation Paper, the four proposed cyber functions do not impose additional mandatory obligations on registered participants. Neither do they confer additional directive powers beyond AEMO's existing authority to take actions in response to an immediate or proximate cyber-attack (or a specific threat of cyber-attack) affecting or potentially affecting power system security in the NEM. The four proposed cyber functions are instead designed to assist in the coordination and adoption of cyber security measures by registered participants in the NEM. Importantly registered participants in the NEM would continue to be responsible for ensuring their own cyber security preparedness and posture, including under the SOCI Act.

Cost Recovery

AEMO considers the estimated costs presented in the rule change request and the Consultation Paper are in the order of magnitude of the required costs to carry out these four cyber roles. In the event a final rule is made that establishes these functions for AEMO under the NER, consultation on the costs will occur through AEMO's annual budget and fee process, with any required changes to AEMO's existing electricity fee structures undertaken in accordance with the NEL and the NER. This may include making this additional set of roles a declared NEM project as per clause 2.11.1 of the NER.

Considerations for Drafting the Rule

AEMO supports the proposed drafting to include the four proposed cyber roles, including their location in Chapter 4 of the NER (which outlines power system security requirements). Given cyber security is rapidly changing and is likely to continue expanding in size and complexity, it is imperative that any responsibilities conferred on AEMO under the NER are clearly stated and consistent with registered participants existing obligations regarding cyber security, including under the SOCI Act. Accordingly, AEMO requests that it be consulted regarding any proposed changes to the submitted drafting.

In summary, AEMO looks forward to a final rule being made that will allow AEMO to perform the four cyber security roles to assist industry by coordinating and supporting cyber preparedness, response and recovery in the NEM. This is a key and discrete element of a broader legislative and regulatory framework to effectively manage cyber security risks in the electricity sector.

Should you wish to discuss any aspects of this submission please contact me or Kevin Ly, General Manager, Reform Development and Insights at kevin.ly@aemo.com.au.

Yours sincerely,

Nicola Falcon
Acting Executive General Manager, Reform Delivery