

7 November 2024

Attn: Nomiky Panayiotakis
Australian Energy Market Commission
GPO Box 2603
SYDNEY NSW 2001

SUBMITTED VIA ONLINE PORTAL

Dear Commissioners,

RE: AEMC Consultation on Cyber Security Rules and Responsibilities

We appreciate the opportunity to provide feedback on the Australian Energy Market Commission's (AEMC) draft determination regarding cyber security rules and responsibilities. We recognise the significant cyber threats facing the industry today and support the proposed measures to enhance security, resilience, and coordination.

Our response focuses on key areas where we see critical alignment with the objectives of the draft determination and offers suggestions to ensure effective implementation.

1. Support for AEMO's Enhanced Role in Cyber Security

We acknowledge the rising cyber security threats across the energy sector, as outlined in the draft determination, and fully support AEMO's enhanced role as a cyber security incident coordinator.

This role is essential for facilitating preparedness and resilience through established frameworks. Importantly, we emphasise the need to align AEMO's functions with our obligations under the Security of Critical Infrastructure (SOCI) Act to ensure comprehensive national energy security.

2. Coordination and Incident Response

We strongly agree with the draft determination's emphasis on a well-coordinated response to cyber security incidents, particularly across the gas and electricity sectors.

Given that the Australian Signals Directorate (ASD) already provides operational assistance during cyber incidents, we encourage AEMO to integrate its activities with existing government response mechanisms to prevent duplication.

Additionally, we support the development of the Australian Energy Sector Cyber Incident Response Plan, which will enhance coordination efforts.

3. Distribution of Critical Information

Further to the above, we support AEMO's role in disseminating timely and relevant cyber security information, including threat intelligence, incident reports, and preventive measures, through established channels.

This function complements the existing work by ASD and is essential for enhancing sector resilience. Given the restrictions under the SOCI Act, we encourage AEMO to align with existing SOCI regulations to ensure compliance when receiving information from market participants which may be classified as protected information under that Act.

4. Cyber Preparedness and Uplift Function

As mandated by the SOCI Act, Epic Energy is committed to maintaining robust cyber resilience measures. We value AEMO's stewardship of the Australian Energy Sector Cyber Security Framework (AESCSF) and suggest aligning these efforts with SOCI Act reporting requirements, particularly the Critical Infrastructure Risk Management Program (CIRMP).

This alignment would help to streamline industry compliance activities and avoid duplication of efforts.

5. Cost Recovery and Liability Protection

We appreciate the draft rule's inclusion of cost recovery provisions and liability protection for AEMO's cyber security functions.

These measures provide clarity regarding financial and legal expectations for AEMO and industry participants, including pipeline operators.

We would welcome additional clarity on how costs associated with these initiatives will be apportioned across participants.

6. Clarification of Roles and Responsibilities

We commend this rule change's proactive stance on cyber security. However, we strongly urge the AEMC to distinctly delineate these responsibilities to prevent overlap with other governmental bodies, such as ASD (and DHA). It is also crucial to avoid redundancy with mandates under the SOCI Act. Clear and precise roles and responsibilities will ensure an efficient and streamlined approach to cyber security governance across the energy sector.

We also urge the AEMC to consider what Cyber Security reporting will be mandated and ensure that that this is aligned with other reporting requirements from state and federal departments (particular the proposed Cyber Security Bill and SOCI Act).

We also urge AEMO to consider the additional burden that having multiple reporting lines can cause and work with other departments to streamline this process via their procedures wherever possible. AEMC and AEMO must also considered the restrictions that many energy organisations have in sharing information under the SOCI Act and ensure that any obligations are in line with this.

We look forward to continued engagement on this important topic and remain committed to contributing to a secure and resilient energy sector. If you have any questions or queries with respect to this feedback, please don't hesitate to contact me via email (Jordan.dodd@epic.com.au) or telephone (0473 562 947).

Kind Regards,



Jordan Dodd
Regulatory Advisor