AEMC

INFORMATION

Cyber security roles and responsibilities

The Commission has made a draft rule that would confirm and clarify the Australian Energy Market Operator's (AEMO's) cyber security responsibilities in the National Electricity Rules (NER). The draft rule would support AEMO to undertake preventative cyber security activities that would reduce potential risks to security and reliability for electricity consumers.

Cyber security has not been explicitly addressed in the NER

Under the current rules, AEMO can respond to an actual cyber incident as it would to any power system security incident (for example by issuing directions to market participants). However, AEMO's role in preparing for potential incidents and maintaining the cyber security of the National Electricity Market (NEM) on a day-to-day basis is not explicitly defined in the NER.

AEMO already carries out some security preparedness activities, including developing and maintaining the Australian Energy Sector Cyber Security Framework, in line with the recommendations of the 2017 Finkel review. The draft rule would build on and enhance these existing powers and activities. It would embed and formalise AEMO's cyber security preparedness role and enable additional resourcing for AEMO to sustain and scale up these functions. The Commission has made the draft rule in response to a rule change request from the Honourable Chris Bowen, Minister for Climate Change and Energy.

AEMO would be responsible for four cyber security functions under the NER

The draft rule would explicitly establish cyber security as one of AEMO's power system security responsibilities in Chapter 4 of the NER. AEMO's role would be to coordinate and support cyber security preparedness, response and recovery by carrying out the four cyber security functions described below.

AEMO would not be able to impose mandatory obligations on market participants. AEMO's cyber security role would be power-system specific and would not duplicate the role of the Department of Home Affairs or government cyber security agencies.

Function 1: Coordination of cyber security incident response

AEMO would plan and coordinate the NEM-wide response to a cyber incident affecting the energy sector. This would involve further developing the Australian Energy Sector Cyber Incident Response Plan outlining the coordination of market, state, and federal responses. In a cyber security event, AEMO would lead the incident response according to the plan.

Function 2: Supporting industry cyber security preparedness and uplift

AEMO would continue maintaining the Australian Energy Sector Cyber Security Framework, which is a cyber security self-assessment tool used by market participants. It would also be able to organise testing and scenario training exercises to test the cyber resilience of the power system, and provide guidance and advice to industry in the form of written materials, digital tools and working groups.

Function 3: Examining cyber risks and providing advice to government and industry

AEMO would provide cyber security research and advice to governments and could also provide advice to industry. Drawing on AEMO's unique energy expertise, this advice would complement, rather than replace, advice that may be provided by other bodies such as government agencies, research institutes, or industry representatives.

AUSTRALIAN ENERGY MARKET COMMISSION LEVEL 15, 60 CASTLEREAGH STREET SYDNEY NSW 2000
T: 02 8296 7800 E: AEMC@AEMC.GOV.AU W: WWW.AEMC.GOV.AU

Function 4: Distributing key cyber security information to market participants

AEMO would facilitate the distribution of critical cyber security information to the energy industry, using its position as the system operator and its existing communication channels. Key pieces of information could include warnings of vulnerabilities or threats, post-cyber incident reports, and preventative patches in commonly used technologies.

The draft rule would enable cost recovery and liability protection for AEMO

Confirming and clarifying AEMO's cyber security responsibilities would allow it to recover the costs of fulfilling those responsibilities through its usual cost recovery processes. It would also mean that AEMO is protected from liability for performing the cyber security functions, consistent with its other statutory functions.

AEMO is already undertaking activities that would form part of the cyber security functions, but this has been funded by diverting AEMO's internal resources or through one-off Commonwealth, State or Territory funding. A more sustainable source of funding is required for AEMO to continue and scale up this work. If the draft rule is made, AEMO would recover the costs of the cyber security functions through its participant fees, which are subject to an annual consultation process. AEMO has estimated the costs to be less than $10 million per year, or approximately 2 per cent of current participant fees.

By formalising cyber security as part of AEMO's statutory functions, it would have liability protection under the National Electricity Law (NEL) for the performance of the cyber security functions. This would enable AEMO to take on appropriate risks to carry out the functions (including by supporting AEMO's access to insurance arrangements).

The draft rule would commence on 12 December 2024

To enable cost recovery and liability protection as soon as possible, the draft rule would commence on 12 December 2024. AEMO would consult with industry, as per the Rules consultation procedures, to set participant fees for cyber security cost recovery.

Mitigating cyber risks would support energy security and reliability

The draft rule would benefit consumers by supporting AEMO and industry to address cyber security risks that may impact energy supply. A cyber incident affecting the electricity sector could cause power outages, which would translate to negative security and reliability outcomes for consumers. Cyber incidents in the electricity industry could also have broader consequences including economic disruptions, breaches of sensitive data, and threats to national security.

Establishing clear functions for AEMO in the NER would allow it access funding arrangements and liability protection to perform those functions effectively. Effective performance of the functions would help prepare the NEM for such incidents and reduce or mitigate their impact. By carrying out the four functions, AEMO would also support industry participants and governments in enhancing their cyber maturity and incident response.

We are seeking stakeholder feedback on the draft rule

The AEMC requests submissions to the draft determination by 7 November 2024. We will publish the final determination for the rule change on 12 December 2024.

For information contact:

Senior Adviser, **Nomiky Panayiotakis** (02) 8296 7810

Direction, **Kate Degen** (02) 8296 7812

Media enquiries: media@aemc.gov.au

26 September 2024