AEMC

INFORMATION

Cyber security roles and responsibilities

The Commission has made a final rule that confirms and clarifies the Australian Energy Market Operator's (AEMO's) cyber security responsibilities in the National Electricity Rules (NER). The final rule supports AEMO undertaking preventative cyber security activities that will help reduce potential risks to security and reliability for electricity consumers.

Cyber security was not explicitly addressed in the NER

Under the rules, AEMO is able to respond to an actual cyber incident as it would to any power system security incident (for example by issuing directions to market participants). However, the previous rules did not explicitly define 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.

AEMO had already carried 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 final rule builds on and enhances these activities. It embeds and formalises AEMO's cyber security preparedness role and enables additional resourcing for AEMO to sustain and scale up these functions. The Commission has made the final rule in response to a rule change request from the Honourable Chris Bowen, Minister for Climate Change and Energy.

AEMO has four cyber security functions under the NER

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

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

Function 1: Coordination of cyber security incident response

AEMO can plan and coordinate the NEM-wide response to a cyber incident affecting the energy sector. This involves 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 will lead the incident response according to the plan.

Function 2: Supporting industry cyber security preparedness and uplift

AEMO will continue maintaining the Australian Energy Sector Cyber Security Framework, which is a cyber security self-assessment tool used by market participants. It will 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 can provide cyber security research and advice to governments and may also provide advice to industry. Drawing on AEMO's unique energy expertise, this advice will complement, rather than replace, advice that may be provided by other bodies such as

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

government agencies, research institutes, or industry representatives.

Function 4: Distributing key cyber security information to market participants

AEMO will 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 may include warnings of vulnerabilities or threats, post-cyber incident reports, and preventative patches in commonly used technologies.

The final rule enables cost recovery and liability protection for AEMO

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

AEMO has already been undertaking activities that now form part of its four cyber security functions, but previously, they have been funded by diverting AEMO's internal resources or through one-off Commonwealth, State or Territory funding. The final rule gives AEMO a more sustainable source of funding to continue and scale up this work. The final rule gives AEMO the ability to recover the costs of the cyber security functions through its participant fees, which are subject to an annual consultation process. AEMO has provided updated cost estimates as of 27 November 2024 indicating that the functions would cost approximately between $8 and $10 million per year in years one to three, and between $8.5 million and $9.5 million per year beyond this initial three year period.

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

The final rule commences immediately

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

Mitigating cyber risks supports energy security and reliability

The final rule will 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 allows it access to funding arrangements and liability protection to perform those functions effectively. Effective performance of the functions helps prepare the NEM for such incidents and reduces or mitigates their impact. By carrying out the four functions, AEMO will also support industry participants and governments in enhancing their cyber maturity and incident response.

For information contact:

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

Media enquiries: media@aemc.gov.au

12 December 2024