Draft National Electricity Amendment (Cyber security roles and responsibilities) Rule 2024

The Australian Energy Market Commission makes the following Rule under the National Electricity Law to the extent applied by:

(a) the *National Electricity (South Australia) Act 1996* of South Australia;
(b) the *Electricity (National Scheme) Act 1997* of the Australian Capital Territory;
(c) the *Electricity - National Scheme (Queensland) Act 1997* of Queensland;
(d) the *National Electricity (New South Wales) Act 1997* of New South Wales;
(e) the *Electricity - National Scheme (Tasmania) Act 1999* of Tasmania;
(f) the *National Electricity (Victoria) Act 2005* of Victoria;
(g) the *National Electricity (Northern Territory) (National Uniform Legislation) Act 2015* of the Northern Territory; and
(h) the *Australian Energy Market Act 2004* of the Commonwealth.

Anna Collyer
Chairperson
Australian Energy Market Commission

Draft National Electricity Amendment (Cyber security roles and responsibilities) Rule 2024

1 Title of Rule

This Rule is the *Draft National Electricity Amendment (Cyber security roles and responsibilities) Rule 2024*.

2 Commencement

This Rule commences operation on [12 December 2024].

3 Amendment to the National Electricity Rules

The National Electricity Rules are amended as set out in Schedule 1.

Schedule 1 Amendment to the National Electricity Rules

(Clause 3)

[1] Rule 4.3Power System Security Responsibilities and Obligations

In rule 4.3, omit all references to "co-ordinate" and substitute "coordinate".

[2] Clause 4.3.1 Responsibility of AEMO for power system security

After clause 4.3.1(c), insert:

(c1) to coordinate and support cyber security preparedness, response and recovery in accordance with the *Cyber security functions*;

[3] Clause 4.3.2A AEMO's cyber security functions

After clause 4.3.2, insert a new clause 4.3.2A as follows:

4.3.2A AEMO's cyber security functions

(a) *AEMO* must use reasonable endeavours to coordinate the response of *Registered Participants* to a cyber incident that adversely affects or could be expected to adversely affect the secure operation of the *power system*. Without limiting the ways in which *AEMO* may coordinate the response, it may do so by:

(1) leading the maintenance and development of an Australian energy sector cyber incident response plan (**AESCIRP**); and

(2) leading the implementation of the AESCIRP, in the manner provided in the AESCIRP, when a cyber incident is occurring.

(b) *AEMO* must use reasonable endeavours to support *Registered Participants* in improving their level of cyber security preparedness and maturity, including in collaboration with relevant government agencies and industry bodies. This may include *AEMO*:

(1) following consultation with *Ministers*, leading the maintenance and development of an Australian energy sector cyber security framework (**AESCSF**) and coordinating annual assessment programs in accordance with the AESCSF;

(2) supporting and undertaking the development and delivery of scenario exercises to test the resilience of the *power system* to cyber threats;

(3) developing and making available to *Registered Participants* guidance materials and tools in relation to cyber security; and

(4) participating in working groups, standards committees and similar bodies relating to cyber security.

(c) *AEMO*:

(1) may, in its role as the *power system* and *market* operator, undertake research and provide advice to a *Minister* 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

(2) must:

(i) at the request of a *Minister*, undertake research and provide advice in relation to cyber security risks to the *power system* and the management or mitigation of those risks; and

(ii) prior to undertaking the research or advice referred to in paragraph (ii), consult with the relevant *Minister* on:

(A) the nature of the research and advice being sought;

(B) *AEMO's* capacity and capability to undertake the research and provide the advice having regard to its role as the *power system* and *market* operator; and

(C) the likely costs that *AEMO* will incur in undertaking the research and advice.

(d) *AEMO* must use reasonable endeavours to facilitate the distribution of critical cyber security information to *participating jurisdictions* and *Registered Participants*. This may include actions such as:

(1) collating and distributing the advice of government agencies and other bodies with respect to cyber security matters relevant to the energy sector;

(2) providing information to *participating jurisdictions* and *Registered Participants* with respect to cyber security threats and vulnerabilities of which *AEMO* becomes aware;

(3) providing information to *participating jurisdictions* and *Registered Participants* with respect to preventative information technology patches and other cyber security management and mitigations of which *AEMO* becomes aware; and

(4) providing public advisory reports, including the preparation of post incident assessments to provide insights into the cause, response, and lessons learned from the incident.

(e) For the avoidance of doubt, the functions outlined in this clause:

(1) do not limit *AEMO's* existing functions that may relate or extend to cyber security; and

(2) do not confer power on *AEMO* to impose mandatory obligations on *Registered Participants*.

[4] Chapter 10 Glossary

In chapter 10, insert the following new definition in alphabetical order:

Cyber security functions

AEMO's cyber security functions outlined in clause 4.3.2A.