Draft National Gas Amendment (Gas cyber security roles and responsibilities for AEMO) Rule 2026

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

(a) the *National Gas (South Australia) Act 2008* of South Australia;
(b) the *National Gas (ACT) Act 2008* of the Australian Capital Territory;
(c) the *National Gas (New South Wales) Act 2008* of New South Wales;
(d) the *National Gas (Queensland) Act 2008* of Queensland;
(e) the *National Gas (Tasmania) Act 2008* of Tasmania;
(f) the *National Gas (Victoria) Act 2008* of Victoria;
(g) the *National Gas (Northern Territory) Act 2008* of the Northern Territory;
(h) the *Australian Energy Market Act 2004* of the Commonwealth.

Anna Collyer
Chairperson
Australian Energy Market Commission

Draft National Gas Amendment (Gas cyber security roles and responsibilities for AEMO) Rule 2026

1 Title of Rule

This Rule is the *Draft National Gas Amendment (Gas cyber security roles and responsibilities for AEMO) Rule 2026.*

2 Commencement

Schedule 1 of this Rule commences operation on 30 July 2026.

3 Amendment to the National Gas Rules

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

Schedule 1 Amendment to the National Gas Rules

(Clause 3)

[1] Part 28 AEMO cyber security functions

After rule 715 in Part 27, insert new Part 28:

Part 28 AEMO cyber security functions

716 AEMO cyber security functions

(1) AEMO must use reasonable endeavours to coordinate the responses of relevant entities to a cyber incident that adversely affects or could be expected to adversely affect the secure operation of the east coast gas system. Without limiting the ways in which AEMO may coordinate the response, it may do so by:

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

(b) leading the implementation of the response plan, in the manner provided in the response plan, when a cyber incident is occurring.

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

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

(b) supporting and undertaking the development and delivery of scenario exercises to test the resilience of the east coast gas system to cyber threats;

(c) developing and making available to relevant entities guidance materials and tools in relation to cyber security; and

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

(3) AEMO may undertake research and provide advice to a Minister and to relevant entities in relation to identified cyber security risks that may impact the east coast gas system and the management or mitigation of those risks.

(4) AEMO must, at the request of a Minister, undertake research and provide advice in relation to cyber security risks to the east coast gas system and the management or mitigation of those risks.

(5) AEMO must, prior to undertaking the research or advice referred to in subrule (4), 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 in the east coast gas system; and

(c) the likely costs that AEMO will incur in undertaking the research and providing the advice.

(6) AEMO must use reasonable endeavours to facilitate the distribution of critical cyber security information to participating jurisdictions and relevant entities in the east coast gas system. This may include actions such as:

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

(b) providing information to participating jurisdictions and relevant entities with respect to cyber security threats and vulnerabilities of which AEMO becomes aware;

(c) providing information to participating jurisdictions and relevant entities with respect to preventative information technology patches and other cyber security management and mitigations of which AEMO becomes aware; and

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

(7) For the avoidance of doubt, the cyber security functions outlined in this rule:

(a) do not limit AEMO’s other functions that may relate or extend to cyber security; and

(b) do not confer powers on AEMO to impose mandatory obligations on relevant entities.

(8) In this rule:

Minister means a Minister of an east coast jurisdiction.

relevant entity has the same meaning as in section 91AF(8) of the *NGL*.