THE HON CHRIS BOWEN MP
MINISTER FOR CLIMATE CHANGE AND ENERGY

MS25-001192

Ms Anna Collyer
Chair
Australian Energy Market Commission
Level 15, 60 Castlereagh St
SYDNEY NSW 2000

Anna.collyer@aemc.gov.au

Dear Chair Anna

Please find attached a rule change request to amend the National Gas Rules to confirm and clarify the cyber security roles and responsibilities of the Australian Energy Market Operator in relation to gas markets.

The proposed rule allows the approach affirmed by the recent *National Electricity Amendment (Cyber security roles and responsibilities) Rule 2024 No.23 (Rule 23)* to be reflected in the gas sector. The Victorian Minister for Energy, as part of the Energy and Climate Ministerial Council (ECMC), has agreed to the submission of this rule change request, including any rights, functions or obligations that the request proposes to impose on the ECMC or Ministers. I endorse this rule change request and ask the AEMC to progress with its initiation.

Yours sincerely

CHRIS BOWEN

Enc Rule change request – AEMO – Cyber Security (Gas Sector)

Australian Government
Department of Climate Change, Energy, the Environment and Water

Rule Change Request

Australian Energy Market Operator - Cyber Security (Gas Sector)

October 2025

1. REQUEST TO MAKE A RULE

1.1 Name and address of the person making the request

The Honourable Chris Bowen MP
Minister for Climate Change and Energy
Parliament House CANBERRA
ACT 2600

2. Relevant background

Australia is responding to conditions of heightened cyber security risks. Though there are cyber risks in all sectors, it is a prominent and evolving risk to the energy sector. Disruption of energy supply would threaten serious, cascading consequences to Australia's national interest, community, and economy.

Cyber security is an energy security risk which is inextricably linked with the management of both electricity and gas systems. Consistent with *The National Electricity Amendment (Cyber security roles and responsibilities) Rule 2024 No. 23* (Rule 2024 No23) this rule change proposes to appropriately embed and formalise the Australian Energy Market Operator (AEMO) roles and responsibilities for cyber security under the National Gas Rules. This proposal is made in relation to all jurisdictions where the National Gas Law (NGL) and National Gas Rules (NGR) applies. The submission recognises the application of gas law differs between Western Australia and other participating jurisdictions, which may impact the scope of the final rule.

Recognising AEMO's vital role in the operation of wholesale and retail markets, system monitoring and security, and the potential for cyber security incidents impacting gas market participants to disrupt these functions, Energy Ministers agree a rule to confirm and clarify AEMO's cyber security functions in respect of the gas sector is desirable.

This request proposes new cyber roles and responsibilities for AEMO in relation to the east coast gas system and markets, comparable to those recently affirmed for the National Electricity Market under Rule 2024 No23. The proposal does not seek amendments to AEMO's existing responsibilities for gas system security, reliability, and supply adequacy in the markets it manages.

3. Statement of issue

This rule change request seeks to replicate for the gas market, the four cyber security functions implemented by Rule 2024 No23, harmonising AEMO's role in cyber security across energy sectors.

In making its determination on Rule 2024 No23, the AEMC accepted the need to confirm and clarify AEMO's cyber security role and responsibilities for the National Electricity Market, to ensure a coordinated and strategic approach to efficiently manage increasing

cyber security risks. Embedding and formalising AEMO's cyber security roles and responsibilities in the NGR would further assure participants, industry and AEMO of its role in cyber security uplift and preparedness, supporting a strategic and coordinated approach to cyber security. It also provides certainty over funding and liability protection for AEMO, consistent with the performance of other functions and activities.

3.1 Cyber security in the context of gas security – AEMO's role

Cyber security is inextricably linked with the management of the gas system and markets. However, existing legislation does not explicitly define AEMO's cyber security role, such as preparing for potential incidents, and supporting the day-to-day cyber security uplift of the markets and system.

Under the *National Gas (South Australia) Act 2008*, the National Gas Objective includes the "price, quality, safety, reliability and security of supply" of gas. Under 'Part 6 – Role of AEMO under National Gas Law', AEMO has powers to do "all things necessary or convenient in connection with its statutory function. AEMO's functions include responding to risks or threats to system reliability or adequacy of the supply of gas within the east coast gas system. These functions are expanded in Victoria where AEMO is responsible for maintaining gas system security of the declared transmission system.

Though configured differently than under the NER, AEMO's role has sufficiently similar objectives and outcomes. Significant aspects of AEMO's proposed cyber security role are within the scope of AEMO's statutory functions (s91A(1)) of the NGL. Confirmation and clarification of AEMO's cyber roles and responsibilities in relation to the gas functions would close potential gaps in the coverage of cyber security responsibility across the gas system.

The proposed rule change would ensure AEMO can recover costs in respect of the performance of its statutory functions (s91E NGL), and statutory immunity extends to acts or omissions done in the performance or exercise of its functions and powers, under NGL and NGR s91K(1).

4. Description of the proposed rule

The rule change seeks to;

- Clarify cyber security as a function within AEMO's role in under gas law.
- Create funding certainty and liability protection for AEMO to fulfil these responsibilities.
- Clarify cyber security responsibility under the National Gas Rules to dispel ambiguity.

4.1 Proposed cyber security functions

It is appropriate for AEMO to adopt the roles and responsibilities comparable to those confirmed and clarified in Rule 2024 No23, in relation to the gas functions it performs. Specifically:

- **Function 1** - **Cyber security incident coordinator:**

AEMO plans for and coordinates the system-wide response to a cyber incident affecting the energy sector. AEMO will continue to develop a plan - the Australian Energy Sector Cyber Incident Response Plan (AESCIRP) - outlining how market, state and federal responses to a cyber incident would be coordinated. In the event of a cyber incident AEMO will lead the implementation of the response in the manner set out by the plan.

- **Function 2** - **Supporting cyber preparedness and uplift:**

AEMO will continue to in its stewardship of the Australian Energy Sector Cyber Security Framework (AESCSF), organise testing and scenario training exercises to test the cyber resilience of the gas system, and provide guidance and advice to industry in the form of written materials, digital tools and working groups. AEMO will not create additional mandatory requirements for relevant entities.

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

AEMO will provide cyber security research and advice to governments. This advice will draw on AEMO's unique energy expertise in their position as a system and market operator, and will complement, rather than replace, work undertaken by other cyber security bodies such as the Australian Cyber Security Centre.

- **Function 4 - Facilitating the distribution of critical cyber security information to market participants:**

AEMO will act as a distributor of cyber security information to the energy industry, using its position as a market and system operator and existing communication channels. AEMO can facilitate the distribution of warnings of cyber vulnerabilities of threats, post-cyber incident reports, and preventative information technology patches in commonly used technologies.

These four functions are facilitative and flexible functions and do not enable AEMO to impose mandatory obligations on relevant entities.

4.2 Cyber incident coordinator

The targeted, covert, and rapid escalation of cyber threats against Australia's energy sector warrants early attention and intervention from AEMO and relevant entities.

When a cyber incident has the potential to impact energy supply, AEMO is best placed to coordinate the response of impacted relevant entities and jurisdictions in the event it requires the activation of any emergency protocols.

Establishing and maintaining the processes for coordinating cyber incident response is paramount to security of gas markets and will assist in real time management of threats as they evolve.

The proposed role will enable AEMO's enhanced coordination of the system and markets response to prepare for and respond to cyber risks or incidents which threaten, or have potential to threaten, the security and reliability of the gas system.

For example, establishing this role as a function will allow AEMO to be adequately resourced and equipped to lead the development and stewardship of the AESCIRP and implementing the plan when a cyber incident is occurring.

The AESCIRP sets out the key actions involved in the escalation from an organisational response to a coordinated gas cyber response, and gas operational emergency management responses. The plan establishes unique roles for AEMO including:

- the co-ordination of information during cyber incidents impacting gas markets;
- linking organisation response and management plans with those of the sectoral response plans and the Interruption to Gas Supply Process (ITGSP).
- Engaging with Australian Government arrangements for cyber incident management, including for example the ACSC Cyber Incident Management Arrangements.

This role does not give AEMO the authority or obligation to manage the cyber incident response and recovery for relevant entities. That remains the responsibility of each relevant entity and governments in their respective jurisdictions with support from the Australian Government as required.

4.3 Supporting cyber preparedness and uplift

AEMO's existing responsibility for gas reliability and supply adequacy should also include uplift and cyber maturity efforts led by industry, for example as it has done through:

- Ongoing stewardship of the AESCSF and its regular assessment programs, either by its own initiative or at the request of Energy Ministers;
    - AEMO developed the AESCSF with industry in response to Finkel Review recommendations.
- Supporting or undertaking the development and delivery of scenario exercises to test the cyber resilience of gas markets;
- Participation in Industry Working Groups, standards committees, and in an advisory capacity to government working groups under Energy Ministers.

Further examples of this role include:

- Planning and participating in system resilience and restoration exercises.
- Providing guidance and tools for industry to improve cyber awareness and maturity, including related guidance materials, where appropriate, in partnership with relevant government agencies.

4.4 Examining risks and providing advice to government and industry

AEMO has unique oversight and capability to provide analysis to policy makers on energy and cyber security issues. Providing such advice to government is essential to system security and will allow appropriate and proportionate intervention as required.

To support gas system risk management planning and as part of AEMO's role in the design of Australia's future energy system, AEMO needs to have the capacity to provide, directly or as part of a coordination role, cyber security research and advice to government at all levels, where this relates to risks to the gas system or markets, and AEMO's expertise and capabilities as a system and market operator.

- This role leverages AEMO's understanding of the gas system and markets it monitors and manages and does not replace the cyber security expertise of the ACSC and other subject matter experts and authorities.
- This role would involve – for example – the preparation of specialist reports, independent advice, and/or detailed analysis to support effective and strategic decision-making in government and industry.
- As part of the rule change, a requirement to consider prior consultation with AEMO and costs should be included.

AEMO should also be able to support or undertake the development and ongoing maintenance of cyber security standards and frameworks such as the AESCSF and promote behaviour across markets and systems, as it does for other elements of energy security, to support a stronger and more effective energy system. This should not result in AEMO performing any regulatory responsibilities beyond its existing mandated scope and ability.

4.5 Facilitating the distribution of critical cyber security information to market participants

AEMO routinely issues notices to relevant entities in relation to a wide range of matters, including security-related events, market directions, suspensions and interventions and general notices.

AEMO is well placed to provide – directly or by distributing the advice of other authorities – information to warn relevant entities of cyber security vulnerabilities or threats. For example:

- Public advisory reports, such as advice during or following any significant cyber incidents within the gas system, to provide insight into the cause, response, and lessons from the event for government and industry.
- The ability to provide critical cyber security information and advice to relevant entities through channels deemed most appropriate by AEMO. This includes the notification of urgent vulnerabilities, threats, and preventative patches in commonly used digital or operational technologies to prevent the spread of malicious activity.

Notices inform market participants of circumstances which could impact on gas security, actions AEMO is taking or expects to take in relation to the cyber issue, as well as actions market participants might be asked to take. The benefits of AEMO redistributing cyber security advice are twofold:

- It will support AEMO's ability to maintain gas system reliability and supply adequacy, through the redistribution of advice through channels which industry is familiar with.
- It will assist relevant entities to protect their own systems and take steps necessary to respond to cyber security threats.

AEMO is best placed to perform this communication role as it has an existing relationship and channel of communication with relevant entities. Advice coming from AEMO, even if redistributed from the ACSC or other authorities, will emphasise the importance and urgency of addressing the issues identified to relevant entities, and could reduce the number of different communication channels in play during a cyber incident.

5. Why the current arrangement is insufficient

Cyber security activities are undertaken by AEMO across the energy sector, including gas markets, in a limited capacity, with limited existing resources.

Some of the activities undertaken by AEMO that form part of its cyber security functions were previously funded by diverting AEMO's internal resources, or through one-off Commonwealth, State or Territory funding.

The ad-hoc nature of AEMO's cyber security activity, and lack of dedicated resourcing for the roles described, pose an ongoing risk to system security. As time passes, the risk will increase and the ability of AEMO, government and industry to curtail these risks will become more challenging.

The proposed functions reflect a consensus reached between AEMO and the Department in extensive consultation on Rule 2024 No23, to specify the cyber security functions that are appropriate and necessary.

Incorporating the proposed specific cyber security functions in the National Gas Rules would provide AEMO, relevant entities and government confidence that AEMO will deliver these functions on a consistent basis as part of its gas system responsibilities.

Defining these roles will also reinforce the need for ongoing management of cyber risks and the need for strong collaboration with stakeholders to secure the markets AEMO monitors and manages for gas supply reliability and adequacy.

6. Nature and scope of the proposed rule change

The proposed approach for this rule change request replicates cyber security responsibilities for the gas system, which were affirmed as an AEMO function for the electricity system under Rule 2024 No23.

This would enable AEMO to apply cost recovery fees and charges, and confirm AEMO's immunity from liability for the fulfilment of its functions.

While this request seeks to have the specific roles defined in the rules, it is important that the roles do not limit AEMO's capability or scope to undertake other actions to manage gas system reliability and supply adequacy — whether cyber or by other emerging threat — as this evolves in the future.

6.1 Scope

The proposal seeks roles and responsibilities for AEMO in relation to gas systems which are comparable to those established in the NEM by Rule 2024 No23. This proposal does not propose to extend the scope of these functions.

These functions should be adapted only to the extent necessary to enable them to apply to Australia's various gas markets and the east coast gas system, and enable AEMO to undertake any duties appropriate to deliver the proposed cyber security function in the future, without limiting the ability to adapt to new risks.

The key features of the rule change would provide direction and certainty that it is appropriate for AEMO to:

1) Coordinate the system and market response to cyber incidents that threaten gas system security and/or reliability and supply adequacy, including:
    a. Development, maintenance, and operation of the Australian Energy Sector Cyber Incident Response Plan;
    b. Coordination and delivery of exercises to test relevant incident response plans to improve preparedness and resilience.
2) Support cyber security uplift and cyber maturity efforts led by industry, including:
    a. Providing guidance and tools for industry to improve cyber awareness and maturity, including the oversight of the AESCSF and delivery of its annual assessment program.
3) Provide, directly or as part of a coordination role, cyber security research and advice to government, industry and/or the public where this relates to risks to gas system security, reliability, and/or supply adequacy, and AEMO's expertise and capabilities as a market operator, monitor or manager.
4) Provide, directly and by redistributing advice from third-party authorities (such as from the ACSC), critical cyber security information and advice to relevant entities, where the advice relates to potential impacts to gas system security, reliability, and/or supply.
5) Undertake any other activity in the context of cyber security which is deemed appropriate by AEMO as a market and system operator, monitor or manager to improve and maintain gas system security, reliability, and supply adequacy or any of its other statutory functions.

6.2 Out of scope

The rule change does not propose AEMO undertake any additional regulatory or compliance functions or alter existing provisions relating to AEMO's direction powers.

Any change that could impact AEMO's existing functions that may be relevant to cyber security is out of scope.

These include for example, AEMO's powers to give directions to relevant entities.

The proposed role to support uplift of cyber security would not extend to directly managing the cyber preparedness, response, or recovery outside of AEMO's own technology networks and systems. Primary responsibility for managing cyber security remains with relevant entities, with policy leadership provided by cyber and security agencies at all levels of government.

The rule change would not see AEMO performing any regulatory responsibilities beyond its existing mandated scope and ability. There is no intention to impact the regulating roles of the Australian Energy Regulator or the Department of Home Affairs.

7. How the proposed rule advances the National Gas Objective

Consistent with the National Gas Objective set out in s23 of the National Gas Law, this proposal promotes the safety, security, and reliability of the supply of natural gas, by embedding and formalising AEMO's functions in the NGR. It promotes the NGO by better enabling AEMO to sustainably monitor gas supply with confidence, giving both AEMO and market participants a better understanding of who is responsible for specific cyber security preparedness and incident response functions. This helps enable the secure provision of gas to consumers in the long term, ensuring safety and security outcomes are met.

8. Impact of the proposed rule on affected parties

Incorporating the proposed cyber security functions in the NGR would provide confidence to AEMO, relevant entities and government that AEMO will be able to deliver these functions on a consistent basis, as part of its responsibilities.

The proposal brings the following expected benefits:

- AEMO will be able to continue performing its duties with certainty, sufficient resources, and immunity from liability for delivering these functions.
- Relevant entities, notably industry, would benefit from cyber uplift assistance and clear recovery protocols, including the continued development of the AESCSF and the AESCIRP.
- The improvement of cyber security preparedness across the sector reduces the risks of malicious cyber-attacks which impact energy supply, benefiting customers with improved security of supply.

- AEMO will be sufficiently resourced to advise government and industry on relevant cyber security related issues to continue to ensure gas security, reliability, and supply adequacy.
- Greater clarity provides certainty to industry and government of AEMO's role in cyber security, in the context of changing regulatory arrangements such as the amended SOCI Act 2018 reforms.

With respect to costs, this proposal would harmonise functions clarified by Rule 2024 No23.

To meet the functions described under Rule 2024 No23, AEMO indicated costs of less than $10 million per year (combined). AEMO estimates costs of the gas roles would be in the range of $1.8m-$2.75m per year. If a rule is made, AEMO will engage stakeholders in relation to costs via a public consultation.

9. Stakeholder Engagement

Energy Ministers have noted and agreed to the submission of this rule change request, including rights, functions or obligations that the request proposes to impose on the ECMC or Ministers. This decision recognises that the proposal is further to an extensive body of work undertaken by DCCEEW and AEMO on Rule 2024 No23, and has been developed in consultation with the Energy Security and Resilience Working Group under Energy Ministers.

The public consultation stages within the rule change request process were identified as the best way to engage with industry on the proposed roles, approach, and outcomes.

Attachment A

Proposed approach to drafting the new rule

The Department notes the below approach to these functions, which mirrors the Final Rule adopted by the AEMC in Rule 2024 No23.

To insert into the NGL, appropriately in relation to the responsibility of AEMO for gas system security, and reliability and supply adequacy;

AEMO's cyber security functions

(a) 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 gas 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 (response plan); and

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

(b) 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:

(1) 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;

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

(3) developing and making available to relevant entities 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 may undertake research and provide advice to a Minister and to relevant entities in relation to identified cyber security risks that may impact the gas systems and markets and the management or mitigation of those risks.

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

(e) AEMO must, prior to undertaking the research or advice referred to in paragraph (d), consult with the relevant Minister on:

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

(2) AEMO's capacity and capability to undertake the research and provide the advice having regard to its role in gas systems and markets; and

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

(f) AEMO must use reasonable endeavours to facilitate the distribution of critical cyber security information to participating jurisdictions and relevant entities. 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 relevant entities with respect to cyber security threats and vulnerabilities of which AEMO becomes aware;

(3) 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

(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.

(g) For the avoidance of doubt, the cyber security functions outlined in this clause;

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

(2) do not confer power on AEMO to impose mandatory obligations on relevant entities.

This outlines a draft approach affecting this outcome, however the Department does not prescribe the form proposed and will work with AEMO and the AEMC through the drafting and consultation process to inform the approach.