Australian Energy Market Commission

AEMC
Australian Energy Market Commission

RULE

Consultation paper

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

Proponent
The Honourable Chris Bowen MP, Minister for Climate Change and Energy

29 January 2026

Inquiries

Australian Energy Market Commission
Level 15, 60 Castlereagh Street
Sydney NSW 2000

E aemc@aemc.gov.au
T (02) 8296 7800

Reference: GRC0091

About the AEMC

The AEMC reports to the energy ministers. We have two functions. We make and amend the national electricity, gas and energy retail rules and conduct independent reviews for the energy ministers.

Acknowledgement of Country

The AEMC acknowledges and shows respect for the Traditional Custodians of the many different lands across Australia on which we live and work. The AEMC office is located on the land of the Gadigal people of the Eora nation. We pay respect to all Elders past and present, and to the enduring connection of Aboriginal and Torres Strait Islander peoples to Country.

Copyright

Citation

To cite this document, please use the following:
AEMC, Gas cyber security roles and responsibilities for AEMO, Consultation paper, 29 January 2026

Summary

1 Cyber security is a critical concern globally and within Australia. While it impacts all sectors, it is a particularly prominent issue in energy given the energy system's increasing digitisation and connectivity. Digitisation can bring a range of benefits, including new opportunities for innovation and increased transparency at both a sector-wide and individual customer basis. However, the gas sector's digital transformation introduces new challenges and vulnerabilities to systems, namely cyber security threats.

2 On 28 October 2025, the Australian Energy Market Commission (AEMC or the Commission) received a rule change request from the Honourable Chris Bowen MP, Minister for Climate Change and Energy (the 'proponent'). The rule change request seeks to embed and formalise the Australian Energy Market Operator's (AEMO) roles and responsibilities in cyber security uplift and preparedness for the gas sector. The rule change seeks to harmonise AEMO's roles and responsibilities with those it has for the electricity sector, supporting a strategic and coordinated approach to cyber security in the energy system.

3 The proponent proposes that as energy systems become increasingly interconnected and reliant on digital technologies, the potential impact of a cyber breach amplifies. The proponent identifies the following issues relating to the current cyber security arrangements in the National Gas Rules (NGR or rules):

- cyber security is not explicitly referenced in the gas rules
- specific cyber security roles and responsibilities that AEMO would perform to assist in enhancing cyber security across the gas system are not specified in the rules.

4 The AEMC has commenced its consideration of the request, and this consultation paper is the first stage.

The rule change request identifies issues with the lack of explicit reference to cyber security in the NGR

5 We are seeking stakeholder views on the following issues raised in the rule change request.

Issue 1 - AEMO's cyber security role is not explicitly referenced in the gas rules:

6 The proponent states that 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 for the gas sector, such as preparing for potential incidents, and supporting the day-to-day cyber security uplift of the markets and system.

7 As of December 2024 AEMO's cyber security functions were embedded and formalised to confirm AEMO's roles and responsibilities for cyber security as it relates to the electricity system. The proponent considers not having a harmonised approach for cyber security across the electricity and gas sector risks the energy sector's ability to manage increasing cyber security risks.

Issue 2 - There is a lack of funding certainty and liability protection for cyber security activities across the gas sector

8 The request considers that while AEMO has performed some cyber security activities in gas using existing resources, the lack of funding certainty and liability protection, due to cyber security not being specified in the NGR, for the delivery of these functions could lead to gaps in the management of cyber security. The proponent states that some of the activities undertaken by AEMO were previously funded by diverting AEMO's internal resources, or through one-off

Commonwealth, State or Territory funding.

9 The proponent believes that the informal nature of AEMO's cyber security activities poses an ongoing risk to system security. The proponent asserts that as time passes, the risk would increase, and the ability of AEMO, government, and industry to curtail these risks would become more challenging.[1]

The request seeks to establish cyber security as a function for AEMO in the NGR

10 The proponent states that while they believe the proposed cyber security role and responsibilities for AEMO are within AEMO's statutory functions in the National Gas Law (NGL), confirming and clarifying AEMO's cyber security functions in the NGR would provide clarity for cyber security responsibilities across the gas system.

11 The proponent proposes to explicitly reference cyber security within the NGR and to clarify AEMO's role in relation to cyber security threats and coordinating the response to any cyber security incidents by adding four new functions in the rules. The proponent proposes to do this by adding cyber security as a function in the NGR, which would identify cyber security as a statutory function for the purpose of the NGL. This would enable AEMO to recover fees and charges it incurs in carrying out these functions, and ensure statutory immunity.

12 The proponent proposes that the four functions should be harmonised with AEMO's cyber security functions for the electricity system to ensure a consistent approach across the energy sector, i.e. both electricity and gas frameworks.

13 The proposed four functions are:[2]

- **Function 1 - Cyber security incidents coordinator:** AEMO would plan for and coordinate the energy sector-wide response to a cyber incident. AEMO would continue to develop 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 would lead the implementation of the response in the manner set out by the plan. Importantly, this role would not give AEMO the authority or obligation to manage cyber incident responses for relevant entities. The proponent considers that extending this activity to the gas sector would enable AEMO to have harmonised energy sector and jurisdiction wide roles and responsibilities.
- **Function 2 - Supporting cyber preparedness and uplift:** AEMO would continue to, in its stewardship of the Australian Energy Sector Cyber Security Framework.[3] It would also organise testing and scenario training exercises to test the cyber resilience of the gas system, participate in industry working groups, and standards committees,. As well as operate in an advisory capacity to government working groups under Energy Ministers, and provide guidance and advice to industry in the form of written materials, digital tools and working groups. The proposed role to support uplift of cyber security would not extend to directly managing cyber preparedness, responses, or recovery outside of AEMO's own technology networks and systems.

1 Rule change request, p 7.
2 Rule change request, p 5.
3 The AESCSF program provides a tool for assessing cyber security maturity across Australia's energy sector. It was developed through collaboration with industry and government.

- **Function 3 - Examining risks and providing advice to government and industry:** Drawing on AEMO's unique energy expertise in market operations, monitoring and forecasting for the East Coast Gas System (ECGS), the proponent proposes that AEMO would provide cyber security research and advice to governments. This function would complement, rather than replace, work undertaken by other cyber security bodies such as the Australian Cyber Security Centre (ACSC). This would include, for example, the preparation of specialist reports, independent advice, and detailed analysis to support effective and strategic decision-making in government and industry.
- **Function 4 - Facilitating the distribution of critical cyber security information to market participants:** In its position as a market and system operator and using existing communication channels, the proponent proposes AEMO would act as a distributor of cyber security information to industry. This would include facilitating the distribution of: warnings of cyber vulnerabilities or threats, post-cyber incident 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, and preventative information technology patches in commonly used digital or operational technologies to prevent the spread of malicious activity.

14 The proponent states that AEMO estimates the cost of the functions for the gas sector would be in the range of $1.8 million to $2.75 million per year. The Commission understands that this estimate factors in the efficiency gains for the cyber security work underway. In comparison, AEMO's costs to meet the functions for the electricity system, were estimated to be between $8 million and $10 million per year for establishment and business per usual costs in year one to three, and ongoing costs beyond this period between $8.5 million and $9.5 million.

15 The proponent notes that if a rule is made, AEMO will engage stakeholders in relation to costs via a public consultation. AEMO consults on its proposed fee structure for gas participants in accordance with the standard consultative process. The Commission understands from AEMO that cost recovery will likely be on the same basis as the Gas Statement of Opportunities (GSOO) fees because cyber security will benefit the same group of participants. The next consultation for general determination of gas participant fees would be from 1 July 2027.

We consider that there are three assessment criteria that are most relevant to this rule change request

16 Considering the National Gas Objective (NGO)[4] and the issues raised in the rule change request, the Commission proposes to assess the rule change request against three assessment criteria. These are the same criteria used to assess the National Electricity Market (NEM) rule change request.

17 Please provide feedback on our proposal to assess the request against:

- **Safety, security, and reliability:** We selected this criterion because safety and security outcomes for consumers are the end goal of the proposed rule change. Cyber security incidents present an energy sector risk that could have significant consumer impacts. The rule change request notes that AEMO's role and responsibilities for cyber security in the gas sector are currently informal in nature, which could lead to gaps in the management of cyber security. This assessment criterion will be used to assess how any changes made to AEMO's cyber security role and responsibilities will support AEMO's ability to manage and operate the ECGS,

4 Section 23 of the NGL.

including in Victoria where AEMO is responsible for maintaining gas system security of the declared transmission system.

- **Principles of good regulatory practice:** The proposed solution seeks to promote predictability and stability in cyber security for the gas sector by embedding and formalising responsibilities on AEMO. The rule change request seeks to improve transparency around AEMO's cyber security role for all stakeholders, including governments and industry. Simplicity in implementing the rule change will help to minimise the administrative burden on AEMO and reduce costs for industry participants. The rule change proposal also aims to outline key functions that are facilitative and flexible without being overly prescriptive and imposing mandatory obligations. This assessment criterion will be used to assess how any changes made to the rules enable AEMO to play a clear role in cyber security, without unduly limiting AEMO's cyber security work, or placing new obligations on other industry participants.
- **Implementation considerations:** This criterion will be used to assess the cost of the proposed solution, both directly and indirectly. It will also assess whether now is the right time for the rule change based on the expected costs and benefits (see chapter 3 for more information on the expected costs). Relevant factors will include the level of cyber security risk and interactions with other broader cyber security reforms including the functions embedded and formalised for AEMO for the electricity system. This assessment criterion will also focus on whether the proposed solution is a sector-wide solution that is effective for the ECGS. This is especially true given that, unlike the electricity system, AEMO does not operate the ECGS as a centralised market. We will consider both federal cyber security initiatives as well as any jurisdictional differences.

We have previously engaged with stakeholders about AEMO's cyber security functions

18 During the Commission's consultation on AEMO's cyber security functions for the electricity system, stakeholders highlighted that cyber vulnerabilities in energy are prevalent not only in the electricity sector but also in the gas sector, especially when considering the interconnected nature of our energy system.[5]

19 During that consultation, stakeholders indicated that they supported the cyber security functions extending to the gas sector, highlighting that a lack of clarity on AEMO's specified roles and responsibilities and how these functions span across the energy sector may increase the risk of governance misalignment, as well as produce inconsistent cyber related activities across gas and electricity sectors. We are interested in how these views may or may not have changed since that time, as well as any differences to how we should consider gas in the gas sector, as opposed to the electricity sector.

Submissions are due by 26 February 2026 with other engagement opportunities to follow

20 There are multiple options to provide your feedback throughout the rule change process.

21 Written submissions responding to this consultation paper must be lodged with the Commission by 26 February 2026 via the Commission's website, www.aemc.gov.au.

22 There are other opportunities for you to engage with us, such as one-on-one discussions or industry briefing sessions. See the section of this paper about "How to engage with us" for further

5 AEMC, Cyber security roles and responsibilities, Rule determination, 12 December 2024.

instructions and contact details for the project leader.

Full list of consultation questions

Question 1:

Do you consider there is a lack of clarity on the specified cyber security roles and responsibilities for AEMO in the NGR? If so, why?

Question 2:

Would harmonising AEMO's cyber security functions across the electricity and gas sector help to ensure a coordinated and strategic approach to cyber security risks? If so, why?

Question 3:

Do you agree that the lack of funding certainty and liability protection for AEMO needs to be addressed? If so, why?

Question 4:

Would harmonising AEMO's cyber security functions across the electricity and gas sector help to ensure a coordinated and strategic approach to efficiently manage cyber security risks? Is so, why?

Question 5:

Do you consider that these four functions are fit for purpose for the gas sector? Do they require any adapting to enable them to apply to Australia's various gas markets and the ECGS? If so, how?

Question 6:

Do you consider that the benefits will outweigh the costs of the proposed solution? Is there anything the Commission could do in designing the rule that would help to minimise the costs and maximise the benefits, e.g. transparency or reporting requirements? If so, how?

Question 7: Assessment framework

Do you agree with the proposed assessment criteria? Are there additional criteria that the Commission should consider or criteria included here that are not relevant?

How to make a submission

We encourage you to make a submission

Stakeholders can help shape the solutions by participating in the rule change process. Engaging with stakeholders helps us understand the potential impacts of our decisions and, in so doing, contributes to well-informed, high quality rule changes.

We have included questions in each chapter to guide feedback, and the full list of questions is above. However, you are welcome to provide feedback on any additional matters that may assist the Commission in making its decision.

How to make a written submission

Due date: Written submissions responding to this consultation paper must be lodged with Commission by 26 February 2026.

How to make a submission: Go to the Commission's website, www.aemc.gov.au, find the "lodge a submission" function under the "Contact Us" tab, and select the project reference code GRC0091.[6]

You may, but are not required to, use the stakeholder submission form published with this consultation paper.

Tips for making submissions are available on our website.[7]

Publication: The Commission publishes submissions on its website. However, we will not publish parts of a submission that we agree are confidential, or that we consider inappropriate (for example offensive, defamatory, vexatious or irrelevant content, or content that is likely to infringe intellectual property rights).[8]

Other opportunities for engagement

There are other opportunities for you to engage with us, such as one-on-one discussions or industry briefing sessions. Please contact the project leader to request a meeting.

For more information, you can contact us

Please contact us with questions or feedback at any stage, noting the project code.

Email:	aemc@aemc.gov.au
Telephone:	(02) 8296 7800

6 If you are not able to lodge a submission online, please contact us and we will provide instructions for alternative methods to lodge the submission.

7 See: https://www.aemc.gov.au/our-work/changing-energy-rules-unique-process/making-rule-change-request/submission-tips.

8 Further information is available here: https://www.aemc.gov.au/contact-us/lodge-submission.

Contents

Tables

1 The context for this rule change request

On 28 October 2025, the Australian Energy Market Commission (AEMC or the Commission) received a rule change request from the Honourable Chris Bowen MP, Minister for Climate Change and Energy (the 'proponent'). The rule change request seeks to embed and formalise AEMO's roles and responsibilities in cyber security uplift and preparedness for the gas sector. The rule change seeks to harmonise roles and responsibilities with the electricity sector supporting a strategic and coordinated approach to cyber security in the energy system.

This section provides an overview of Minister Bowen's rule change request along with relevant context and background:

- Section 1.1 Cyber security is a growing and prevalent issue
- Section 1.2 Over the last decade cyber security governance has expanded in the energy sector
- Section 1.3 The proponent proposes to harmonise and formalise AEMO's role in cyber security for the gas sector
- Section 1.4 We have previously engaged with stakeholders about AEMO's cyber security functions
- Section 1.5 We have started the rule change process

1.1 Cyber security is a growing and prevalent issue

Cyber security is a critical concern globally and within Australia. While it impacts all sectors, it is a particularly prominent issue in energy security given the energy system's increasing digitisation and connectivity. Digitisation can bring a range of benefits, including new opportunities for innovation and increased transparency at both a sector-wide and individual customer basis. However, the gas sector's digital transformation introduces new challenges and vulnerabilities to systems, namely cyber security threats.

The Australian Government defines cyber security as measures used to protect the confidentiality, integrity and availability of systems and information. A cyber incident is an unwanted or unexpected cyber security event, or a series of such events, that have a significant probability of compromising business operations.[9] A cyber security incident in the gas sector could have far-reaching implications, from widespread outages, to economic disruptions, breach of sensitive data, and threats to national security. Cyber attacks could cause prolonged operational outages and critical information losses which could impact on the safety, security, reliability, and supply adequacy of the East Coast Gas System (ECGS) and have flow on impacts to the electricity system.

The cyber attack on Colonial Pipeline in the United States in May 2021 demonstrates how an attack on a pipeline, and not having a plan for malicious cyber activities, can cause a state of emergency. The attack affected over 8000km's of pipeline causing major economic problems, leading the government to declare a state of emergency.[10] This incident clearly demonstrates how vulnerable essential services, like energy infrastructure, are to cyber attacks.

While there has been no publicly reported large-scale cyber attack on Australia's gas sector or energy system, there has been a growing number of reported incidents on major corporations. These incidents highlight the growing prevalence of cyber security in the Australian context and

9 Australian Cyber Security Centre, 'Glossary'.
10 Queensland Government, case studies, Colonial Pipeline cyber incident.

the need for capabilities to mitigate threats as our gas system becomes increasingly connected and digitised.

1.2 Over the last decade cyber security governance has expanded in the energy sector

Cyber security governance in Australia, particularly within the energy sector, has evolved over the past decade. One of the key milestones in the history of cyber security governance in Australia was the establishment of the Australian Cyber Security Centre (ACSC) in 2014. The ACSC serves as the central hub for cyber security coordination and information sharing between government, industry, and academia. It plays a crucial role in helping organisations within the energy sector enhance their cyber security capabilities and respond effectively to cyber incidents.

Subsequently, the Independent Review into the Future of the National Electricity Market, commissioned in response to the 2016 South Australian blackout, emphasised the importance of cyber security within the electricity sector. Its recommendations underscored the necessity for resilient and secure energy infrastructure, with the report highlighting the increasing dependence on gas-fired generation to provide a reliable, low emissions substitute for ageing coal-fired generation and that strong cyber security measures for the National Electricity Market (NEM) would be essential for maintaining Australia's growth and prosperity in an increasingly global economy.[11] The review recommended:[12]

> an annual report into the cyber security preparedness of the National Electricity Market should be developed by the Energy Security Board, in consultation with the Australian Cyber Security Centre and the Secretary of the Commonwealth Department of the Environment and Energy

Building upon this recommendation, the Australian Energy Sector Cyber Security Framework (AESCSF) was developed as a framework to assess cyber security maturity across Australia's energy sector, including gas and electricity. It was developed through collaboration with industry and government stakeholders, including AEMO, ACSC, Critical Infrastructure Security Centre (CISC), and representatives from Australian energy organisations. It is both a framework and an annual voluntary assessment program, enabling participants to undertake assessments of their own cyber security capability and maturity. Participants can use the results to inform and prioritise investment to improve cyber security posture.

In addition, the amended *Security of Critical Infrastructure Act 2018* (the SoCI Act) expanded its scope to encompass the energy sector, acknowledging its vital role in national security. This legislative update mandated rigorous cyber security standards and incident reporting requirements for energy providers, elevating the industry's cyber security capabilities to align with contemporary threats. It outlines the legal obligations you have if you own, operate, or have direct interests in critical infrastructure assets. The SoCI Act also outlines how the government can support you if an incident occurs that impacts your critical infrastructure asset. Under the SoCI Act, it is AEMO's primary responsibility to maintain the cyber security of its own assets.

The SoCI Act places cyber security obligations on owners and operators of critical infrastructure, including electricity and gas infrastructure.[13] The AESCSF can be used by owners and operators to meet SoCI Act requirements.[14]

11 Independent Review into the Future of the National Electricity Market, p 67.
12 Independent Review into the Future of the National Electricity Market, p 69.
13 Security of Critical Infrastructure Act 2018.

See table 1.1 below for a description of Australian government bodies who play a role in cyber security.

Table 1.1: Australian government bodies playing a role in cyber security

Body name	Description
Australian Signals Directorate (ASD)	A statutory agency within the Defence Portfolio that collects and communicates foreign signals intelligence, provides cyber security advice, and aims to protect Australia from cyber threats.
Australian Cyber Security Centre (ACSC)	An agency of the ASD that acts as the federal government's technical authority on cyber security, providing materials and advice for consumers, small and large businesses, and government.
Department of Home Affairs	Among other functions: • Supports the development and implementation of national cyber security policy. • Manages all types of threats to critical infrastructure, in partnership with industry and the broader community through the CISC.
Critical Infrastructure Security Centre (CISC)	Assists critical infrastructure owners and operators in understanding risk and meeting regulatory requirements. Reports to the Department of Home Affairs.
State and territory cyber security units	Various jurisdictions have cyber security agencies or units that support government (and sometimes public sector) cyber security initiatives. They may also be responsible for leading jurisdictional government responses to cyber incidents.

Source: ASD; ACSC; Department of Home Affairs - 'Cyber security', 'Critical infrastructure security'; CISC; QLD Government - 'About the Cyber Security Unit'; NSW Government - 'Cyber Security NSW'; VIC Government - 'About the Cyber Security Unit'; Government of WA - 'Cyber Security Unit'.

As noted above, the SoCI Act effectively requires NEM and gas participants, including AEMO, to manage their own critical infrastructure as it relates to cyber security. This rule change request does not place requirements on gas participants but rather aims to confirm AEMO's cyber security role in the gas sector to facilitate cohesive cyber security practices across the energy sector. In 2024, the AEMC embedded and formalised four cyber security functions that AEMO performs for the electricity sector.[15] The proponent believes that there is a similar need to confirm and clarify these functions for the gas sector to facilitate cohesive cyber security practices across the energy sector.[16]

14 AESCSF framework and resources, AEMO.
15 Cyber security roles and responsibilities.

For example, one such activity is the cyber incident response plan for the energy sector. Each state or territory has an emergency management plan developed by a government agency that would apply in a significant cyber or energy supply incident.[17] Many states also have specialised sub-plans for a loss of electricity supply or a potential severe energy shortage, but they do not specifically consider cyber events as a potential cause of such emergencies.[18] Similarly, many jurisdictions have a sub-plan for a serious cyber incident, but these do not specifically address a cyber incident impacting the energy sector. As of 2024 AEMO has a cyber security incident coordinator function for the electricity system, this could include developing a cyber incident response plan. There may be a need for this activity to be extended to the gas sector[19] which would enable AEMO to have a harmonised energy sector and jurisdiction wide cyber incident response plan in place.

1.3 The proponent proposes to harmonise and formalise AEMO's role in cyber security for the gas sector

This rule change request seeks to replicate for the gas market the four cyber security functions implemented in 2024 for the electricity system, which would harmonise AEMO's role in cyber security across the energy sector.[20] The proponent states that cyber security risks in the energy sector are evolving, and a disruption of energy supply would have serious consequences for Australia's national security and economy.[21]

The proponent identifies several issues relating to the current cyber security arrangements in the National Gas Rules (NGR):

- cyber security is not explicitly referenced in the gas rules
- specific cyber security roles and responsibilities that AEMO would perform to assist in enhancing cyber security across the gas system are not specified in the rules.

The proponent considers that the lack of resourcing for AEMO's cyber security activities poses an ongoing risk to the security of the gas sector.[22] To resolve this, the proponent seeks to confirm and formalise AEMO's cyber security role by adding four new preventative functions for AEMO in the NGR to perform to assist in maintaining the safety, security, reliability, and supply adequacy of the ECGS. Additionally, the proponent proposes that the four functions should be harmonised with AEMO's cyber security functions for the electricity system to ensure a consistent approach across the energy sector. These changes would enable AEMO to recover the costs it incurs in carrying out these functions for the gas sector and confirm AEMO's immunity from liability for the delivery of these functions.

The rule change request can be found on the project page.

16 Rule change request, p 3.

17 NSW Government, https://www.nsw.gov.au/rescue-and-emergency-management/state-emergency-management-plan-emplan; Emergency Management Victoria, https://www.emv.vic.gov.au/responsibilities/state-emergency-management-plan-semp;Queensland Government Disaster Management, https://www.disaster.qld.gov.au/plans; Government of South Australia Department of the Premier and Cabinet, https://www.dpc.sa.gov.au/responsibilities/security-emergency-and-recoverymanagement/state-emergency-management-plan; TAS State Emergency Service, https://www.ses.tas.gov.au/emergency-management-2/tasmanian-emergency-management-arrangements-tema/; ACT Emergency Services Agency, https://esa.act.gov.au/be-emergency-ready/emergency-arrangements.

18 'Sub plan' is the term used for a hazard-specific plan which is subordinate to the overall emergency management plan, and details the arrangements for preventing, preparing for, and responding to an emergency of that type.

19 Rule change request, p 1.

20 Rule change request, p 2.

21 Rule change request, p 2.

22 Rule change request, p 7.

1.4 We have previously engaged with stakeholders about AEMO's cyber security functions

During the Commission's consultation on AEMO's cyber security functions for the NEM, stakeholders highlighted that cyber vulnerabilities in energy are prevalent not only in the electricity sector but also in the gas sector, especially when considering the interconnected nature of our energy system.[23] At this stage, stakeholders indicated that they supported the cyber security functions extending into the gas sector, highlighting that a lack of clarity on AEMO's specified roles and responsibilities and how these functions span across the energy sector may increase the risk of governance misalignment, as well as produce inconsistent cyber related activities across gas and electricity sectors.[24] We are interested in how these views may or may not have changed since that time, as well as any differences to how we should consider cyber security in the gas sector, as opposed to the electricity sector.

As detailed in the initial rule change request, the proponent indicated that they would look to address cyber security in the Wholesale Electricity Market, Western Australia gas market, and ECGS through separate processes.[25] This rule change request addresses cyber security for the ECGS, which includes gas markets, gas industry facilities, and stakeholders participating within the east coast jurisdiction, which includes all states and territories except for Western Australia.[26]

1.5 We have started the rule change process

This paper is the first stage of our consultation process. The Commission invites stakeholders to make submissions on the stated problem and the proposed solutions.

A standard rule change request includes the following formal stages:

- a proponent submits a rule change request
- the Commission commences the rule change process by publishing a consultation paper and seeking stakeholder feedback
- stakeholders lodge submissions on the consultation paper and engage through other channels to make their views known to the AEMC project team
- the Commission publishes a draft determination and draft rule (if relevant)
- stakeholders lodge submissions on the draft determination and engage through other channels to make their views known to the AEMC project team
- the Commission publishes a final determination and final rule (if relevant).

Information on how to provide your submission and other opportunities for engagement is set out at the front of this document.

You can find more information on the rule change process on our website.[27]

To make a decision on this proposal, we seek stakeholder feedback on how we propose to assess the request, the stated problem and the proposed solutions.

23 AGL submission to cyber roles and responsibilities consultation paper, p 2.

24 AGL submission to cyber roles and responsibilities consultation paper, March 2024, p 2; Epic Energy submission to cyber roles and responsibilities draft determination, March 2024, p 1.

25 Rule change request, Cyber Security Role, March 2024, Minister Bowen, p. 4.

26 AEMO, About the East Coast Gas System (ECGS).

27 See our website: https://www.aemc.gov.au/our-work/changing-energy-rules.

2 The problem raised in the rule change request

This chapter seeks stakeholder feedback on the problem identified in the rule change request - whether it is or will soon become a problem and if so, the scale and impact of the problem.

The rule change request notes that AEMO's role and responsibilities for cyber security in the gas sector are currently informal in nature, which could lead to gaps in the management of cyber security. Additionally, this is inconsistent with its functions for the power system. The rule change request also suggests that by replicating the four cyber security functions implemented for the electricity system, for gas, the rule change would harmonise AEMO's role in cyber security across the energy sector.[28] This would provide confidence that AEMO will deliver these functions on a consistent basis.

This section summarises the issues raised in the rule change request including:

- Section 2.1 - Cyber security is not explicitly referenced in the gas rules
- Section 2.2 - There is a lack of funding certainty and liability protection for cyber security activities in the gas sector

2.1 Issue 1 - AEMO's cyber security role is not specifically defined in the gas rules

The proponent states that 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 for the gas sector, such as preparing for potential incidents, and supporting the day-to-day cyber security uplift of the markets and system.[29]

The proponent states that while they believe the proposed cyber security role and responsibilities for AEMO are within AEMO's statutory functions in the National Gas Law (NGL),[30] confirming and clarifying AEMO's cyber security functions in the NGR would close potential gaps, such as the preparation of energy sector wide incident response plans, in the coverage of cyber responsibility across the gas system.[31]

Additionally, the proponent states that incorporating the four proposed cyber security functions in the NGR would provide AEMO, relevant entities, and government confidence that AEMO would deliver these functions on a consistent basis as part of its gas system responsibilities. Defining these roles would 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.[32]

2.1.1 AEMO's cyber security functions are inconsistent across the energy sector

The proponent states that cyber security is an energy security risk that is inextricably linked with the management of both electricity and gas systems. As outlined in section 1.2, cyber security governance of the energy system has evolved over the last decade. This has resulted in legislative structures being developed at the federal level, including the SoCI Act 2018, as well as cross-organisational frameworks such as the Australian Energy Sector Cyber Security Framework.[33]

28 Rule change request, p 2.
29 Rule change request, p 3.
30 Section 91A(1) of the NGL.
31 Rule change request, p 3.
32 Rule change request, p 7.
33 Rule change request, p 2.

As of December 2024 AEMO's cyber security functions for the electricity sector were embedded and formalised to confirm AEMO's roles and responsibilities for cyber security.[34] Confirming AEMO's cyber security role in the National Electricity Rules (NER) has helped ensure a coordinated and strategic approach to efficiently manage the increasing cyber security risk to the electricity system. Importantly, at the time, the proponent indicated that clarifying AEMO's cyber security roles and responsibilities in the gas sector would be considered through a separate rule change process, which is the subject of this consultation paper.[35]

The proponent views harmonising AEMO's cyber security functions (see section 3.2) for the gas sector with its electricity system functions are important to continue to enhance a coordinated and strategic approach to manage increasing cyber security risks across the energy sector. Additionally, the proponent believes that this would further assure participants, industry, and AEMO of its role in cyber security uplift and preparedness.[36] The proponent believes that although AEMO's role is configured differently than under the NER, AEMO's role has sufficiently similar objectives and outcomes.[37]

The Commission recognises that inconsistent and unclear policies relating to AEMO's cyber security role and responsibilities across the energy system could create confusion and inefficiencies. There is also the risk of inconsistent implementation and falling short of cyber security standards. The Commission is seeking feedback on whether stakeholders consider that the lack of harmonisation between cyber security functions in the electricity and gas sector poses an energy sector risk.

Question 1:

Do you consider there is a lack of clarity on the specified cyber security roles and responsibilities for AEMO in the NGR? If so, why?

Question 2:

Would harmonising AEMO's cyber security functions across the electricity and gas sector help to ensure a coordinated and strategic approach to cyber security risks? If so, why?

2.2 Issue 2 - There is a lack of funding certainty and liability protection for cyber security activities in the gas sector

The proponent considers that while AEMO has performed some cyber security activities this has been done using existing resources.[38] The proponent considers the lack of funding certainty and liability protection, due to cyber security not being specified in the NGR, for the delivery of these functions has led to AEMO performing cyber security activities without sufficient resources. The proponent states that some of the activities undertaken by AEMO were previously funded by diverting AEMO's internal resources, or through one-off Commonwealth, State or Territory funding.[39]

34 AEMC, Cyber security roles and responsibilities, Rule determination, 12 December 2024.
35 Rule change request to the AEMC, March 2024, Minister Bowen, p 4.
36 Rule change request, p 2-3.
37 Rule change request, p 3.
38 Rule change request, p 7.

The proponent believes that the lack of dedicated resourcing around AEMO's cyber security activities poses an ongoing risk to system security. The proponent asserts that as time passes, the risk will increase and the ability of AEMO, government, and industry to curtail these risks will become more challenging.[40]

By clarifying AEMO's cyber security roles and responsibilities in the NGR, the proponent believes this would provide certainty over funding and liability protection for AEMO, consistent with the performance of its other statutory functions and activities.[41]

Question 3:

Do you agree that the lack of funding certainty and liability protection for AEMO needs to be addressed? If so, why?

39 Rule change request, p 7.
40 Rule change request, p 7.
41 Rule change request, p 3.

3 The proposed solution and implementation

The proponent proposes to explicitly reference cyber security within the NGR and to clarify AEMO's role in relation to cyber security threats and coordinating the response to any cyber security incidents by adding four new functions in the rules. The proponent proposes to do this by adding cyber security as a function in the NGR, which would identify cyber security as a statutory function for the purpose of the NGL. This would enable AEMO to recover fees and charges, and confirm AEMO's immunity from liability for the delivery of these services.

For the purposes of facilitating stakeholder consultation, we have grouped the proposed changes into two broad categories that relate to the two key issues identified in the rule change request:

- Change 1: Cyber security would be explicitly referenced in the gas rules
- Change 2: A strategic and coordinated approach to efficiently manage cyber security across the energy sector

3.1 Change 1: Cyber security would be explicitly referenced in the gas rules

The proponent seeks to embed and formalise AEMO's cyber roles and responsibilities for the gas sector in the NGR in order to clarify and confirm AEMO's statutory functions under the NGL[42] as they relate to the National Gas Objective (NGO) by reference to "price, quality, safety, reliability and security of supply of covered gas."[43] However, the proponent does not explicitly suggest which area of the NGR AEMO's cyber security role could belong to.

AEMO's cyber security functions for the electricity system fall within AEMO's responsibilities for system security[44] however the NGR does not have a similar system security chapter as it is not a centrally operated market like the NEM. As such, the Commission considers that if a rule were to be made to include this AEMO's gas security roles and responsibilities in the Rules, then this would be done by creating a *new* Part of the rules, rather than including it in any other area. This would reflect that the proposed functions would apply across all geographical jurisdictions in the ECGS, including the three facilitated markets.

3.2 Change 2: A strategic and coordinated approach to efficiently manage cyber security across the energy sector

The proponent considers that it is appropriate for AEMO to adopt the cyber security roles and responsibilities comparable to those embedded and formalised for the electricity system to ensure a coordinated and strategic approach to cyber security across the energy sector.[45]

Adopting these four functions would enable AEMO to apply cost recovery fees and charges (see section 3.3) from gas participants, 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 security, reliability, and supply adequacy.[46]

42 Section 91A(1) of the NGL.

43 Section 23(a) of the NGL.

44 This was the result of the Commission's Recent Rule determination: National Electricity Market Amendment (Cyber security roles and responsibilities) Rule 2024; Clause 4.3.1(c1) of the NER.

45 Rule change request, p 1-3.

46 Rule change request, p 7-8.

The proponent intends that the four functions are facilitative and flexible, and would not enable AEMO to impose mandatory obligations on relevant entities. The rule change would not see AEMO performing any regulatory responsibilities beyond its existing mandated scope and ability. Additionally, there is no intention to impact the regulating roles of the Australian Energy Regulator (AER) or the Department of Home Affairs.[47] 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.[48]

At present, AEMO only has certainty over funding and liability protection around these four functions for the electricity sector. This could cause inconsistencies and gaps in the application of cyber security activities across the energy sector. The proponent considers harmonising AEMO's cyber security functions with the gas sector would mitigate this risk.[49]

The proponent also considers that 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 AEMO's ability to adapt to new risks.[50]

The four proposed functions are outlined below.

3.2.1 Function 1: Cyber security incident coordinator

As the cyber security incidents coordinator AEMO would plan for and coordinate the energy sector-wide response to a cyber incident. AEMO will continue to develop 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 would lead the implementation of the response in the manner set out by the plan.[51]

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:[52]

- 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.

3.2.2 Function 2: Supporting cyber preparedness and uplift

To support cyber preparedness and uplift, the proponent proposes that AEMO would[53]:

- continue to in its stewardship of the Australian Energy Sector Cyber Security Framework,
- organise testing and scenario training exercises to test the cyber resilience of the gas system,
- participate in industry working groups, standards committees, and in an advisory capacity to government working groups under Energy Ministers, and

47 Rule change request, p 4.
48 Rule change request, p 8.
49 Rule change request, p 1.
50 Rule change request, p 8.
51 Rule change request, p 4.
52 Rule change request, p 5.
53 Rule change request, p 4-5.

- provide guidance and advice to industry in the form of written materials, digital tools and working groups.

The proposed role to support uplift of cyber security would not extend to directly managing cyber preparedness, responses, or recovery outside of AEMO's own technology networks and systems. Primary responsibility for managing cyber security would remain with relevant entities, with policy leadership provided by cyber and security agencies at all levels of government.[54] Importantly this function would not allow AEMO to impose any additional mandatory requirements for relevant entities.[55]

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

Drawing on AEMO's unique energy expertise in market operations, monitoring and forecasting for the ECGS, the proponent proposes that AEMO would provide cyber security research and advice to governments. This function would complement, rather than replace, work undertaken by other cyber security bodies such as the Australian Cyber Security Centre.[56]

AEMO has unique oversight and capability to provide analysis to policy makers on energy and cyber security issues. The proponent believes that AEMO providing this advice to government is essential to the security of the gas sector and will allow appropriate and proportionate intervention as required.[57]

To support gas system risk management planning and as part of AEMO's role in the design of Australia's future energy system, the proponent believes 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 would include, for example, the preparation of specialist reports, independent advice, and detailed analysis to support effective and strategic decision-making in government and industry.[58]

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

In its position as a market and system operator and using existing communication channels, the proponent proposes AEMO would act as a distributor of cyber security information to industry.[59] This would include facilitating the distribution of:

- warnings of cyber vulnerabilities or threats
- post-cyber incident 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
- preventative information technology patches in commonly used digital or operational technologies to prevent the spread of malicious activity.

The proponent considers that 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. AEMO routinely issues notices to relevant entities in relation to a wide range of

54 Rule change request, p 8.
55 Rule change request, p 5.
56 Rule change request, p 4.
57 Rule change request, p 6.
58 Rule change request, p 6.
59 Rule change request, p 4.

matters, including security-related events, market directions, suspensions and interventions and general notices.[60]

The proponent believes that the benefits of AEMO redistributing cyber security advice are that this would:[61]

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

Question 4:

Would harmonising AEMO's cyber security functions across the electricity and gas sector help to ensure a coordinated and strategic approach to efficiently manage cyber security risks? Is so, why?

Question 5:

Do you consider that these four functions are fit for purpose for the gas sector? Do they require any adapting to enable them to apply to Australia's various gas markets and the ECGS? If so, how?

3.3 What are the costs and benefits of the proposed solution?

As noted in section 2.2 this rule change request seeks to increase funding certainty for AEMO to perform the four proposed functions in relation to cyber security monitoring, adaptation, and innovation to stay ahead of malicious actors.

The proponent states that AEMO estimates the cost of the functions for the gas sector would be in the range of $1.8 million to $2.75 million per year. The Commission understands that these costs are specific to gas related elements of the activities under the functions, such as:

- specific guidance and advice in the Australian Energy Sector Cyber Security Framework
- customisations of the Australian Energy Sector Cyber Incident Response Plan specific to the gas emergency management arrangements
- other activities specific to gas.

As such the Commission also understands that the cost estimate factors in the efficiency gains for the cyber security work underway, accounting for the lower value than quoted for the NEM.[62]

While the estimated costs depend on the evolving cyber threat landscape and the resources required by AEMO to manage new and emerging threats over time, ensuring funding certainty would provide stability and predictability to industry. It would allow these specific functions to be

60 Rule change request, p 6-7.

61 Rule change request, p 7.

62 Rule change request, p 9; In comparison, AEMO's costs to meet the functions for the electricity system were estimated to be between $8 and $10 million per year for establishment and business as usual costs in years one to three, and ongoing costs beyond this period between $8.5 million and $9.5 million, see AEMC, Cyber Security roles and responsibilities, Rule determination, 12 December 2024.

sufficiently resourced and could, for example, enable long-term initiatives, investment in essential resources, and upskill personnel.

AEMO would recover costs from gas participants

AEMO recovers gas participant fees from liable registered participants for the:

- Declared Wholesale Gas Market (DWGM)
- Short Term Trading Market (STTM)
- Retail markets (Victoria, New South Wales/Australian Capital Territory, Queensland, South Australia)
- Gas Bulletin Board
- Gas Statement of Opportunities (GSOO)
- Energy Consumers Australia fees

The Commission understands from AEMO that cost recovery will likely be on the same basis as the GSOO fees because cyber security fees will benefit the same group of participants. See table 3.1 below.

Table 3.1: Structure of gas participant fees for the GSOO

Liable registered participants	Fee structure
Producer fee Each Bulletin Board facility operator registered as the Bulletin Board reporting entity for a Bulletin Board production facility.	$ / GJ produced (to allocate 30% of GSOO costs)
Retailer fee Each retail gas market participant participating in the registrable capacity of market participant –retailer in Vic or retailer in NSW/ACT, Qld and SA.	$ / customer supply point (to allocate 70% of GSOO costs)

Source: AEMO, Structure of Gas Participant Fees, December 2023, Final Report and Determination, https://www.aemo.com.au/-/media/files/stakeholder_consultation/consultations/gas_consultations/2023/structure-of-gas-participant-fees/final-report-gas-fee-structures.pdf?la=en

The proponent notes that if a rule is made, AEMO would engage stakeholders in relation to costs.[63] AEMO consults on its proposed fee structure for gas participant fees in accordance with the standard consultative process, See Box 1 below. The next consultation for general determination of gas participant fees would be from 1 July 2027.[64]

Box 1: How AEMO recovers fees from gas participants

AEMO must consult on its proposed fee structure for gas participants in accordance with the standard consultative procedure. Under this procedure, AEMO is required to:

- Publish a notice on its website, describing the proposal and inviting written submissions within 15 business days of the date of the notice

63 Rule change request, p 9.

64 The fee structure term is for a three-year period from 1 July 2024 to 1 July 2027.

- Consider relevant submissions and make a draft decision, including identifying any changes to the proposal within 15 business days
- Make a final decision within 20 business days after the end of the period for making submissions to the draft decision.

Source: Rule 135CA, Development of participant fee structure, of the NGR; Rule 8, Standard consultative procedure, of the NGR

Further, if AEMO consults on and determines that the cyber security functions are to be declared a major gas project, it would allow AEMO to consult and determine a participant fee structure to recover the costs of the project until the next general determination of participant fees, See Box 2.

Box 2: How AEMO recovers fees for a major gas project 1. AEMO may determine any of the following projects to be major gas projects:

- a major reform or development
- a major change to any of AEMO's functions, responsibilities, obligations, or powers under the rules or the Procedures
- a major change to any of the computer software or systems that AEMO uses in the performance of its functions, responsibilities, obligations, or powers under the rules or the Procedures
- the exercise or performance of an east coast gas system reliability and supply adequacy function

2. AEMO must consult on a determination of a major gas project in accordance with the standard consultative procedure, see Box 1.

3. AEMO may consult on a determination of a major gas project in accordance with the expedited consultative procedure.

4. When AEMO determines a project to be a major gas project, it must also determine the start date and period of cost recovery.

5. AEMO must determine a participant fee to be used for cost recovery until the next general determination of participant fees.

Source: Rule 135CB, Major gas project, of the NGR.

AEMO consulted on and determined for the electricity system that the functions were a 'declared NEM project'.[65] This allows AEMO to recover costs associated with the functions, with the fee structure in place until the next general determination of NEM participant fees is made for the period commencing 1 July 2026.

The proponent considers that the changes sought would bring the following expected benefits:[66]

- It would harmonise AEMO's cyber security functions with those it has for the electricity system
- AEMO would be able to continue performing its duties with certainty, sufficient resources, and immunity from liability for delivering these functions

65 New cyber security roles and responsibilities for AEMO -Declared NEM project.

66 Rule change request, p 8-9.

- 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[67]
- 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.

Question 6:
Do you consider that the benefits will outweigh the costs of the proposed solution? Is there anything the Commission could do in designing the rule that would help to minimise the costs and maximise the benefits, e.g. transparency or reporting requirements? If so, how?

67 Rule change request, p 8.

4 Making our decision

When considering a rule change proposal, the Commission considers a range of factors.

This chapter outlines:

- issues the Commission must take into account
- the proposed assessment framework
- decisions the Commission can make

We would like your feedback on the proposed assessment framework.

4.1 The Commission must act in the long-term interests of consumers

The Commission is bound by the National Gas Law (NGL) to only make a rule if it is satisfied that the rule will, or is likely to, contribute to the achievement of the national gas objective.[68]

The NGO is:[69]

> to promote efficient investment in, and efficient operation and use of, covered gas services for the long term interests of consumers of covered gas with respect to—
>
> (a) price, quality, safety, reliability and security of supply of covered gas; and
>
> (b) the achievement of targets set by a participating jurisdiction—
>
> (i) for reducing Australia's greenhouse gas emissions; or
>
> (ii) that are likely to contribute to reducing Australia's greenhouse gas emissions.

The targets statement, available on the AEMC website, lists the emissions reduction targets to be considered, as a minimum, in having regard to the NGO.[70]

4.2 We propose to assess the rule change using these three criteria

4.2.1 Our methods to analyse the proposed rule

Considering the NGO and the issues raised in the rule change request, the Commission proposes to assess this rule change request against the set of criteria outlined below. These assessment criteria reflect the key potential impacts – costs and benefits – of the rule change request. We consider these impacts within the framework of the NGO.

The Commission's analysis may use qualitative and/or quantitative methodologies. The depth of analysis will be commensurate with the potential impacts of the proposed rule change. We may refine these methodologies as this rule change progresses, including in response to stakeholder submissions.

Consistent with good regulatory practice, we also assess other viable policy options - including not making the proposed rule (a business-as-usual scenario) and making a more preferable rule - using the same set of assessment criteria and impact analysis methodology where feasible.

68 Section 291 of the NGL.
69 Section 23 of the NGL.
70 Section 72A(5) of the NGL.

4.2.2 Assessment criteria and rationale

The proposed assessment criteria, which are the same criteria used to assess the NEM rule change request, and rationale for each is as follows:

- **Safety, security, and reliability**

  We selected this criterion because safety and security outcomes for consumers are the end goal of the proposed rule change. Cyber security incidents present an energy sector risk that could have significant consumer impacts. The rule change request notes that AEMO's role and responsibilities for cyber security in the gas sector are currently informal in nature, which could lead to gaps in the management of cyber security. The proponent proposes that the lack of dedicated funding poses an ongoing security risk to the gas sector. The proposal seeks to embed and formalise AEMO's cyber security functions for the gas sector, bringing them into line with the electricity sector, which could help enable the secure provision of energy to end customers over the long term. This assessment criterion will be used to assess how any changes made to AEMO's cyber security role and responsibilities will support AEMO's ability to manage and operate the ECGS, including in Victoria where AEMO is responsible for maintaining gas system security of the declared transmission system.

- **Principles of good regulatory practice**

  The issues in this proposed rule change request relate to the problem of the rules not being fit for purpose by not specifically identifying AEMO's role and responsibilities in relation to cyber security under the NGR. Principles of good regulatory practice will be critical to selecting the best solution for this rule change request. The proposed solution seeks to promote predictability and stability in cyber security (for the gas sector) by embedding and formalising well-defined responsibilities on AEMO.

  The rule change request seeks to improve transparency around AEMO's cyber security role for all stakeholders, including governments and industry. Simplicity in implementing the rule change will help to minimise the administrative burden on AEMO and reduce costs for industry participants. The rule change proposal also aims to outline key functions that are facilitative and flexible without being overly prescriptive and imposing mandatory obligations.

  This assessment criterion will be used to assess how any changes made to the rules enable AEMO to play a clear role in cyber security, without unduly limiting AEMO's cyber security work, or placing new obligations on other industry participants. It will also assess how the design of the solution needs to consider this broader direction of reform to leverage AEMO's electricity cyber security systems and activities, broader cyber security initiatives, and avoid duplication.

- **Implementation considerations**

  Implementation considerations will be critical to considering a solution for this rule change request. This assessment criterion will be used to assess the cost of the proposed solution, both directly and indirectly.

  It will also assess whether now is the right time for the rule change based on the expected costs and benefits (see chapter 3 for more information on the expected costs). Relevant factors will include the level of cyber security risk and interactions with other broader cyber security reforms including the functions embedded and formalised for AEMO in the NER.

  Although the rule change focuses on AEMO's responsibilities, all industry participants have a role to play in cyber security. In addition, there are cyber security risks to businesses in the gas sector. Therefore, impact analysis for all stakeholders will be key to the rule change process.

This assessment criterion will also focus on whether the proposed solution is a sector-wide solution that is effective for the ECGS. This is especially true given that, unlike the electricity market, AEMO does not operate the ECGS as a centralised market. We will consider both federal cyber security initiatives as well as any jurisdictional differences.

Question 7: Assessment framework

Do you agree with the proposed assessment criteria? Are there additional criteria that the Commission should consider or criteria included here that are not relevant?

4.3 We have three options when making our decision

After using the assessment framework to consider the rule change request, the Commission may decide:

- to make the rule as proposed by the proponent[71]
- to make a rule that is different to the proposed rule (a more preferable rule), as discussed below, or
- not to make a rule.

The Commission may make a more preferable rule (which may be materially different to the proposed rule) if it is satisfied that, having regard to the issue or issues raised in the rule change request, the more preferable rule is likely to better contribute to the achievement of the NGO.[72]

4.4 Making gas rules in Western Australia

The versions of the NGL and NGR that apply in Western Australia differ from the NGL and NGR as they apply in other participating jurisdictions.[73]As a result the Commission's power to make rules for Western Australia differs from its rule-making power under the NGL.[74] For example, there is no express head of power for the Commission to make gas rules for or with respect to regulating AEMO's functions or conferring functions or powers on AEMO as they have a limited role in the Western Australian gas markets.

While it may be unlikely, the Commission will consider whether any proposed rules may be made in Western Australia under other heads of power that do apply in that jurisdiction, and the extent that any proposed rules should apply.

71 The proponent describes its proposed rule in Attachment A of the rule change request.

72 Section 296 of the NGL.

73 Under the *National Gas Access (WA) Act 2009* (WA Gas Act), a modified version of the NGL, known as the National Gas Access (Western Australia) Law (WA Gas Law), was adopted. Under the WA Gas Law, the National Gas Rules applying in Western Australia are version 1 of the uniform NGR as amended by the SA Minister under an adoption of amendments order made by the WA Minister for Energy and by the AEMC in accordance with its rule making power under section 74 and 313 of the WA Gas Law. See the AEMC website for further information, https://www.aemc.gov.au/regulation/energy-rules/national-gas-rules/western-australia.

74 See section 74 and Schedule 1 of the WA Gas Law for the subject matters for the AEMC's rule making power in Western Australia.

Abbreviations and defined terms

ACSC	Australian Cyber Security Centre
AEMC	Australian Energy Market Commission
AEMO	Australian Energy Market Operator
AER	Australian Energy Regulator
AESCIRP	Australian Energy Sector Cyber Incident Response Plan
AESCSF	Australian Energy Sector Cyber Security Framework
CISC	Critical Infrastructure Security Centre
Commission	See AEMC
DWGM	Declared Wholesale Gas Market
ECGS	East Coast Gas System
GSOO	Gas Statement of Opportunities
ITGSP	Interruption to Gas Supply Process
NEM	National Electricity Market
NER	National Electricity Rules
NGL	National Gas Law
NGO	National Gas Objective
NGR	National Gas Rules
Proponent	The proponent of the rule change request
SoCI Act	Security of Critical Infrastructure Act 2018
STTM	Short Term Trading Market