Australian Energy Market Commission

AEMC
Australian Energy Market Commission

RULE

Draft rule determination

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

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

7 May 2026

Enquiries

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, Draft rule determination, 7 May 2026

Summary

1 The Australian Energy Market Commission (the Commission or AEMC) has decided to make a draft gas rule, to embed and formalise the Australian Energy Market Operator's (AEMO) cyber security roles and responsibilities in the National Gas Rules (NGR), in response to a rule change request submitted by the Honourable Chris Bowen MP, Minister for Climate Change and Energy (the Minister or proponent). By embedding and formalising AEMO's cyber security role and responsibilities in the NGR we are ensuring participants, industry, and AEMO have greater clarity on AEMO's role in cyber security uplift and preparedness across the East Coast Gas System (ECGS), supporting a strategic and coordinated approach to cyber security. This would also harmonise AEMO's cyber security functions with its functions for electricity and provide certainty over cost recovery and liability protection for AEMO.

2 Cyber security is of critical importance in Australia. While it impacts all sectors, it is a particularly prominent issue in energy security given the increasing digitisation and connectivity between the gas and electricity systems. Digitisation can bring a range of benefits, including new opportunities for innovation and increased transparency at both a sector-wide and individual customer basis. While the gas sector's digital transformation has not been as significant as in the electricity system, it still introduces new challenges and vulnerabilities, namely, cyber security threats.

3 A cyber security incident in the gas sector could have far-reaching implications from outages, to economic disruptions, breaches of sensitive data, and threats to national security. While the benefits of increased digitisation and connectivity are worth pursuing, it also requires enhanced capabilities to mitigate threats from any malicious cyber activity.

4 The Independent Review into the Future of the National Electricity Market[1] emphasised the importance of cyber security in the energy sector and underscored the necessity of resilient and secure energy infrastructure. Since then, cyber security measures across the energy sector have been progressively introduced, including through an AEMC rule change in 2024 that clarified AEMO's roles and responsibilities for the electricity sector.

5 We are seeking feedback on our draft determination and rule by 18 June 2026.

Our draft rule would formalise and embed cyber security as part of AEMO's NGR roles and responsibilities

6 The draft rule would formalise and embed cyber security as part of AEMO's roles and responsibilities in the NGR. Currently, the NGR does not address cyber security, so AEMO does not have a clear role or confirmed responsibilities in this area for the gas sector. The draft rule would clarify this by establishing specific cyber security prevention and preparedness functions for AEMO across the ECGS.

7 Importantly, this rule change request does not place additional requirements on gas participants but rather, clarifies AEMO's role in providing prevention and preparedness functions to facilitate cyber security measures across the gas sector. Infrastructure owners would remain responsible for managing the cyber security of their own assets.

AEMO's cyber security functions would be consistent across the energy sector

8 The draft rule would harmonise AEMO's cyber security roles and responsibilities with the electricity sector to ensure a coordinated and strategic approach to cyber security across the

1 Independent Review into the Future of the National Electricity Market, June 2017, Dr Alan Finkle AO.

energy sector.

9 While AEMO performs some cyber security activities for the gas sector, the lack of defined functions in the NGR could create inconsistencies and gaps in the application of AEMO's cyber security preparedness and uplift measures across the energy sector.

10 The Commission recognises that the gas sector differs in operational characteristics, physical infrastructure, and governance arrangements from the electricity sector.

11 More specifically, the electricity sector operates as a real-time system that instantaneously balances supply and demand using centralised and digitally integrated platforms. By contrast, the gas sector operates with longer scheduling periods and long term contracts and relies more heavily on individually owned and operated physical assets. These differences create a risk asymmetry because the pathways through which cyber risks materialise, and the speed at which impacts propagate, differ. In the gas sector, the ownership, structure and operational characteristics of the gas sector mean that dedicated cyber security preparedness and response arrangements are required to reflect the specific operational and physical interventions that may be required to restore operations.

12 Despite these differences the Commission considers that harmonising AEMO's cyber security functions with its functions for the electricity sector is appropriate because they are broad and flexible functions that do not impose specific activities on AEMO or operational obligations on gas sector participants. This means AEMO would:

- have flexibility to apply the proposed functions in a way that is tailored to gas market arrangements across the ECGS
- where appropriate, maintain a consistent energy system-wide approach to identifying emerging risks, supporting uplift activities and coordinating responses when required, e.g. through the Australian Energy Sector Cyber Security Framework (AESCSF) or the Australian Energy Sector Cyber Incident Response Plan (AESCIRP).

AEMO would be able to recover costs and have liability protection for cyber security activities

13 The draft rule would provide certainty on how AEMO would recover fees and charges for conducting cyber security activities under its functions as well as provide AEMO with immunity from liability in performing these functions.

14 This would allow AEMO to properly establish and undertake cyber security activities on a well defined and permanent basis for the ECGS and scale up its incident response preparation. For example, by updating the Australian Energy Sector Cyber Incident Response Plan more frequently or establishing tools and technologies to support it.

15 Additionally, market participants would be able to confidently rely on AEMO to perform specific preparedness, uplift and responsiveness activities.

The draft rule would embed four cyber security functions into the NGR

16 The draft rule would embed a set of four cyber security functions in the NGR clarifying AEMO's roles and responsibilities for cyber security across the ECGS:

- **Function 1: Cyber security incident 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 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. 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 in its stewardship of the Australian Energy Sector Cyber Security Framework.[2] 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. It would also 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. AEMO supporting uplift of cyber security would not extend to directly managing cyber preparedness, responses, or recovery outside of AEMO's own technology networks and systems.
- **Function 3: Examining cyber risks and providing advice to government and industry:** Drawing on AEMO's unique energy expertise in market operations, monitoring and forecasting for the ECGS, 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 the gas sector:** In its position as a market operator and system coordinator and using existing communication channels, 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.

17 AEMO would recover the costs of performing the functions through participant fees. AEMO estimates that the functions would likely cost between $1.8 million and $2.75 million per year depending on whether there were any cyber incidents. The Commission also understands that this factors in the efficiency gains for the cyber security work already underway. Stakeholders generally agreed that the expected costs are justified, and that the benefits of the proposed solution would outweigh the potential cost of a cyber incident.

18 The Commission considers that the costs of the four functions are outweighed by the benefits of reducing cyber security risks across the ECGS. More specifically, the proposed cyber security functions would improve cyber preparedness and response arrangements and reduce the likelihood and impacts of cyber incidents that could affect gas supply.

19 The draft rule would enable AEMO to recover cyber security costs from gas participants through AEMO's existing cost recovery process which involves a standard consultative procedure. AEMO has noted that cost recovery will likely be on the same basis as the Gas Statement of Opportunities (GSOO) fees because cyber security fees would benefit the same group of participants. This would help ensure the proposed cyber security functions are adequately and sustainably funded.

2 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.

The Commission has considered stakeholder feedback in making its decision

20 Stakeholders in their submissions to the consultation paper agreed that the NGR lacks clarity on cyber security and that it is problematic for AEMO to undertake cyber security tasks without certainty. Stakeholders agreed that confirming and clarifying AEMO's cyber security role and responsibilities in the NGR would provide greater clarity and guidance to industry. Stakeholders also agreed that harmonising AEMO's cyber security gas functions with the functions it has for the electricity sector is important. This is because it could streamline processes, avoid duplication, and reduce costs.

21 The key stakeholder observations that the Commission considered in shaping the draft rule included:

- Acknowledgement that there is a lack of clarity on AEMO's cyber security roles and responsibilities in the NGR[3]
- Support for harmonising AEMO's cyber security functions across electricity and gas to help ensure a coordinated and strategic approach to efficiently manage cyber security risks[4]
- AEMO's inability to recover costs and lack of liability protection for performing cyber security activities in the gas sector needs to be addressed[5]
- Overall support for the four functions,[6] however, while still supportive, two stakeholders questioned whether AEMO is best placed to provide research and advice (function three), recommending it remains limited in scope[7]
- That the benefits of the four functions outweigh the costs,[8] with one stakeholder requesting further information around the projected costs of the functions.[9]

22 The Commission has considered these issues and is of the view that:

- Confirming and clarifying AEMO's cyber security role for the gas sector is important because the consequences of a cyber incident could impact the operation of the sector, and in turn the supply of gas to industry and consumers. See section 3.1.
- Harmonising AEMO's cyber security functions with its functions for the electricity sector is appropriate because they are broad and flexible functions that do not impose specific activities on AEMO or operational obligations on gas sector participants. See section 3.1.1.
- Certainty about cost recovery and liability protection would enable AEMO to continue and scale up its incident response preparation, for example by updating the Australian Energy Sector Cyber Incident Response Plan more frequently or establishing tools and technologies to support it. See section 3.1.2.
- AEMO's unique position and expertise across the ECGS would enable them to provide valuable research and advice on cyber security risks to government and industry. See section 3.2.3.
- The benefits of embedding and formalising AEMO's cyber security functions for the gas sector, far outweigh the cost of performing the proposed functions. See section 3.3.

3 Submissions to the consultation paper: Alinta Energy, p.1; APA, p.1; APGA, p.1; AGL, p.1; Marissa McCauley, p.1.
4 Submissions to the consultation paper: Alinta Energy, p.1; APGA, p.1; Marissa McCauley, pp.1-2; AGL, p.1.
5 Submission to the consultation paper, Marissa McCauley, p.2.
6 Submissions to the consultation paper: Alinta Energy, pp.1-2; APA, p.2; APGA, p.1; Marissa McCauley, p.2.
7 Submissions to the consultation paper: Alinta Energy, pp.1-2; AGL. p.1.
8 Submissions to the consultation paper: APGA, p.1; Marissa McCauley, p.2; Alinta Energy, p.2.
9 Submission to the consultation paper, AGL, p.1.

We assessed our draft rule against three assessment criteria considering stakeholder feedback

23 The Commission has considered the National Gas Objective (NGO)[10] and the issues raised in the rule change request and assessed the draft rule against three assessment criteria outlined below. We gathered and analysed stakeholder feedback in relation to these criteria.

24 The draft rule would contribute to the achievement of the NGO by:

- **Promoting safety, security, and reliability:** by embedding and formalising AEMO's functions in the NGR and harmonising these with the electricity sector, the draft rule would promote safety, security, and reliability outcomes which would benefit consumers. The draft rule would better enable AEMO to manage and operate a secure system, giving both AEMO and market participants a better understanding of who is responsible for specific cyber security preparedness and incident response functions. This would help enable the secure provision of gas to consumers in the long term, ensuring safety and security outcomes are met. See section 2.3.1.
- **Aligning with principles of good regulatory practice:** the draft rule would align with good regulatory practice by seeking to improve predictability, stability, and transparency of cyber security in an increasingly digitised and interconnected gas sector. The draft rule also considers broader cyber security reforms to support harmonisation of AEMO's role across the energy sector, and to avoid unnecessary duplication of activities. AEMO would have predictability and stability because by introducing these functions under the NGR, they would be able to recover fees and charges and have liability protection under the NGL in performing these functions. This would allow for resourcing certainty to properly establish and undertake cyber security activities on a more well-defined and permanent basis. This would enable AEMO to continue and scale up its cyber security activities. Additionally, market participants would be able to confidently rely on AEMO to perform specific preparedness, uplift and responsiveness activities in the gas sector, and consistently throughout the energy system. Under the draft rule, AEMO would not be unduly limited in the cyber security activities it can undertake. Additionally, there are no overly prescriptive requirements for industry because AEMO would not have the ability to impose mandatory obligations on participants. See section 2.3.2.
- **Taking into account implementation considerations:** the draft rule accounts for cost implications, governance arrangements, timing considerations, and relevant jurisdictional conditions. The Commission considers that the overall cost of formalising cyber preparedness and incident response functions in the gas system is low compared to the benefits and the magnitude of any potential cyber incident, especially where it could have been prevented by clarifying roles and responsibilities and upscaling AEMO's preparedness activities. Any complexities in cyber security governance would become more transparent and simplified for industry participants as the draft rule would formally establish functions for AEMO in the gas sector to support consistent cyber security coordination across the energy sector. The impact on AEMO and other participants would be manageable because AEMO is already performing these activities in the electricity sector and for the gas sector, meaning that existing processes could be built on. See section 2.3.3.

The draft rule would commence on 30 July 2026

25 The Commission's final determination and final rule (if made) is scheduled to be published on 30

10 Section 23 of the NGL.

July 2026. The commencement date of the rule is proposed to be the same day as publication. Immediate commencement is possible because AEMO is already performing these functions within the electricity sector and some activities under the functions for the gas sector.

26 An earlier commencement date would ensure AEMO has protection from liability and be able to recover costs for the performance or exercise of these cyber security functions as soon as possible. This in turn would mean the benefits for consumers are realised more quickly.

27 AEMO would need to determine and consult on the participant fee structure and the period for cost recovery. In addition, AEMO would need to carry out work to establish or ramp up some aspects of the cyber security functions. However, the Commission considers that AEMO could do this work before 30 July 2026 because the functions are facilitative and flexible. Further, AEMO would not need to make any updates to procedures, guidelines, or settlement systems before the rule takes effect.

How to make a submission

We encourage you to make a submission

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

How to make a written submission

Due date: Written submissions responding to this draft determination and rule must be lodged with Commission by 18 June 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.[11]

Tips for making submissions on rule change requests are available on our website.[12]

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).[13]

Next steps and opportunities for engagement

There are other opportunities for you to engage with us, such as one-on-one discussions or industry briefing sessions. You can also request the Commission to hold a public hearing in relation to this draft rule determination.[14]

Due date: Requests for a hearing must be lodged with the Commission by 14 May 2026.

How to request a hearing: 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. Specify in the comment field that you are requesting a hearing rather than making a submission.[15]

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

11 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

12 See: https://www.aemc.gov.au/our-work/changing-energy-rules-unique-process/making-rule-change-request/our-work-3

13 Further information about publication of submissions and our privacy policy can be found here: https://www.aemc.gov.au/contact-us/lodge-submission

14 Section 310(2) of the NGL.

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

Contents

1 The Commission has made a draft determination 1
1.1 Our draft rule would confirm and clarify AEMO's gas sector roles and responsibilities for cyber security 1
1.2 Currently the NGR does not address AEMO's cyber security role 2
1.3 Stakeholder input and support for AEMO's cyber security role helped shape our draft rule 3
1.4 Our determination would support a strategic and coordinated approach to cyber security 4

2 The rule would contribute to the energy objectives 6
2.1 The Commission must act in the long-term interests of gas consumers 6
2.2 We have considered how the draft rule may apply in Western Australia 6
2.3 Our draft rule to clarify and confirm AEMO's cyber security functions in the gas sector would contribute to the achievement of the NGO 7

3 Our draft rule would confirm and clarify AEMO's cyber security functions in the NGR 12
3.1 Cyber security is a growing and prevalent concern in the gas sector 12
3.2 The draft rule would embed four functions into the NGR 19
3.3 The four functions are likely to significantly reduce cyber security risks and costs 23
3.4 The draft rule would commence on 30 July 2026 26

Appendices

A Rule making process and background to the rule change request 28
A.1 Cyber security is a growing and prevalent issue 28
A.2 The process to date 30

B Legal requirements to make a rule 31
B.1 Draft rule determination and draft rule 31
B.2 Power to make the rule 31
B.3 Commission's considerations 31
B.4 Making gas rules in Western Australia 32
B.5 Civil penalty provisions and conduct provisions 32

Abbreviations and defined terms 33

Tables

Table 3.1: Structure of gas participant fees for the GSOO 25
Table A.1: Australian government bodies playing a role in cyber security 29

Figures

Figure 1.1: Timeline of cyber security reforms and frameworks 4
Figure 3.1: The market differences between the gas sector and electricity sector 15
Figure 3.2: The physical and facility differences between the gas sector and electricity sector 16
Figure 3.3: The governance differences between the gas sector and electricity sector 17

1 The Commission has made a draft determination

The Australian Energy Market Commission (the Commission or AEMC) has decided to make a draft gas rule, to embed and formalise the Australian Energy Market Operator's (AEMO) cyber security role and responsibilities in the National Gas Rules (NGR), in response to a rule change request submitted by the Honourable Chris Bowen MP, Minister for Climate Change and Energy (the Minister or proponent).

This chapter provides an overview of the Commission's draft rule and rationale.

- Section 1.1 outlines the draft determination and draft rule to make the rule proposed by the Minister
- Section 1.2 outlines the proposed rule change to embed and formalise AEMO's cyber security roles and responsibilities in the NGR
- Section 1.3 outlines the input from stakeholders that shaped our draft determination
- Section 1.4 explains how our determination would support a strategic and coordinated approach to cyber security

1.1 Our draft rule would confirm and clarify AEMO's gas sector roles and responsibilities for cyber security

The draft rule is consistent with the rule change request (see section 1.2) and addresses the lack of clarity around AEMO's cyber security role and responsibilities in the gas sector by confirming AEMO's cyber security functions in the NGR.

In doing so, this would also harmonise AEMO's cyber security functions with its functions in the electricity sector to ensure a coordinated and strategic approach to cyber security across the energy sector. See section 3.1.1 for more information.

Importantly, the draft rule would allow AEMO to recover fees and charges and confirms its immunity from liability, consistent with the performance of AEMO's other powers and functions under the NGL and NGR, to deliver these cyber security functions. See section 1.2 and 3.1.2 for more information on liability protection and section 3.3 for more information on costs.

Specifically, the draft rule would insert four functions for AEMO in the NGR:

- **Function 1: Cyber security incident 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 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.
- **Function 2: Supporting cyber preparedness and uplift:** AEMO would continue in its stewardship of the Australian Energy Sector Cyber Security Framework.[16] 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, and operate in an advisory capacity to government working groups.
- **Function 3: Examining cyber 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), AEMO would provide cyber security research and advice to

16 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.

governments. 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 the gas sector:** In its position as a market operator and system coordinator and using existing communication channels, AEMO would act as a distributor of cyber security information to industry.

These four functions would be facilitative and flexible and would not enable AEMO to impose mandatory obligations on market participants. See section 3.2 for more information on the functions.

1.2 Currently the NGR does not address AEMO's cyber security role

Currently, the NGR does not explicitly define or address cyber security, so AEMO's role in cyber security for the gas sector is unclear. There is a need to confirm and clarify what AEMO's role and responsibilities are in relation to cyber security to ensure a coordinated and strategic approach is implemented to efficiently manage potential cyber security risks to the gas sector.

1.2.1 The Minister proposed a rule to confirm and clarify AEMO's role in cyber security functions for the gas sector

The proponent stated that while they consider the proposed cyber security role and responsibilities for AEMO are within AEMO's statutory functions in the NGL, confirming and clarifying AEMO's cyber security functions in the NGR would provide clarity for cyber security responsibilities across the gas system.

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.[17] This would enable AEMO to recover fees and charges it incurs in carrying out these functions, and ensures AEMO does not incur civil monetary liability in performing these functions under the NGR.[18]

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.

1.2.2 The Minister identified two broad issues with the lack of explicit reference to cyber security in the NGR

Issue 1 - AEMO's cyber security role is not explicitly referenced 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.

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 national electricity system.

17 AEMO's statutory functions include any other functions conferred under the NGR or Procedures. See section 91A(1)(l) of the NGL.

18 For more information see sections 91E and 91K of the NGL.

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

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.

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. See section 3.1.2.

1.3 Stakeholder input and support for AEMO's cyber security role helped shape our draft rule

Stakeholders in their submissions to the consultation paper agreed that the NGR lacks clarity on cyber security and that it is problematic for AEMO to undertake cyber security tasks without certainty. Stakeholders agreed that confirming and clarifying AEMO's cyber security role and responsibilities in the NGR would provide greater clarity and guidance to industry.[19] Stakeholders also agreed that harmonising AEMO's cyber security gas functions with the functions it has for the electricity sector is important because it could streamline processes, avoid duplication, and reduce costs.[20]

The key stakeholder observations that shaped the draft rule included:

- Acknowledgement that there is a lack of clarity on AEMO's cyber security roles and responsibilities in the NGR[21]
- Support for harmonising AEMO's cyber security functions across electricity and gas to help ensure a coordinated and strategic approach to efficiently manage cyber security risks[22]
- AEMO's inability to recover costs and lack of liability protection for performing cyber security activities in the gas sector needs to be addressed[23]
- Overall support for the four functions,[24] however, while still supportive, two stakeholders questioned whether AEMO is best placed to provide research and advice (function three), recommending it remains limited in scope[25]
- That the benefits of the four functions outweigh the costs,[26] with one stakeholder requesting further information around the projected costs of the functions[27]

19 Submissions to the consultation paper: (Q.1).
20 Submissions to the consultation paper: (Q.2).
21 Submissions to the consultation paper: Alinta Energy, p.1; APA, p.1; APGA, p.1; AGL, p.1; Marissa McCauley, p.1.
22 Submissions to the consultation paper: Alinta Energy, p.1; APGA, p.1; Marissa McCauley, pp.1-2; AGL. p.1.
23 Submission to the consultation paper, Marissa McCauley, p.2.
24 Submissions to the consultation paper: Alinta Energy, pp.1-2; APA, p.2; APGA, p.1; Marissa McCauley, p.2.
25 Submissions to the consultation paper: Alinta Energy, pp.1-2; AGL, p.1.
26 Submissions to the consultation paper: APGA, p.1; Marissa McCauley; p.2; Alinta Energy, p.2.
27 Submission to the consultation paper, AGL, p.1.

The Commission has considered these issues and is of the view that:

- Confirming and clarifying AEMO's cyber security role for the gas sector is important because the consequences of a cyber incident could impact the operation of the sector, and in turn the supply of gas to industry and consumers. See section 3.1.
- Harmonising AEMO's cyber security functions with its functions for the electricity sector is appropriate because they are broad and flexible functions that do not impose specific activities on AEMO or operational obligations on gas sector participants. See section 3.1.1.
- Cost recovery and liability protection would enable AEMO to continue and scale up its incident response preparation, for example by updating the Australian Energy Sector Cyber Incident Response Plan more frequently or establishing tools and technologies to support it. See section 3.1.2.
- AEMO's unique position and expertise across the ECGS would enable them to provide valuable research and advice on cyber security risks to government and industry. See section 3.2.3.
- The benefits of embedding and formalising AEMO's cyber security functions for the gas sector, far outweigh the cost of performing the proposed functions. See section 3.3.

See section 3.2 for further detail around the four proposed cyber security functions.

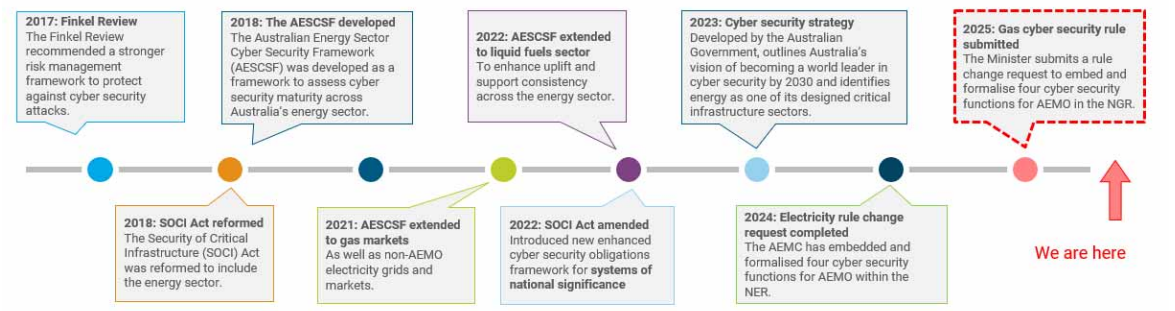
1.4 Our determination would support a strategic and coordinated approach to cyber security

Cyber security is of critical importance in Australia. While it impacts all sectors, it is a particularly prominent issue in energy security given the increasing digitisation and connectivity between the gas and electricity systems. Digitisation can bring a range of benefits, including new opportunities for innovation and increased transparency at both a sector-wide and individual customer basis. While the gas sector's digital transformation has not been as significant as in the electricity system, it still introduces new challenges and vulnerabilities, namely, cyber security threats.

A cyber security incident in the gas sector could have far-reaching implications from outages, to economic disruptions, breaches of sensitive data, and threats to national security. While the benefits of increased digitisation and connectivity are worth pursuing, it also requires enhanced capabilities to mitigate threats from any malicious cyber activity.

Cyber security reforms and frameworks in Australia, particularly within the energy sector, have evolved over the past decade. **Figure 1.1** below provides an overview of cyber security reforms and frameworks in Australia.

Figure 1.1: Timeline of cyber security reforms and frameworks



Source: AEMC.

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 energy sector. Its recommendations underscored the necessity for resilient and secure energy infrastructure. Following these recommendations the Australian Energy Sector Cyber Security Framework was developed. Specifically, the Independent Review into the Future Security of the National Electricity Market recommended that AEMO should have a cyber security role. As seen in Figure 1.1 above, in 2024 the AEMC completed a rule change that embedded and formalised four cyber security functions that AEMO performs for the electricity sector,[28] with this rule change seeking to do the same for the gas sector.

By formalising AEMO's cyber security role and responsibilities in the NGR we are ensuring participants, industry, and AEMO have greater clarity on its role in cyber governance, supporting a strategic, coordinated and harmonised approach to cyber security across the energy system.

See Appendix A for more information on the history and broader context for cyber security measures in the energy system.

28 Cyber security roles and responsibilities.

2 The rule would contribute to the energy objectives

This chapter sets out how our draft rule promotes the NGO. It explains how our draft rule promotes the safety, security and reliability of the gas sector. This includes how it is aligned with principles of good regulatory practice, while also taking implementation considerations into account.

In this chapter:

- Section 2.1 outlines the NGO test that the Commission must apply to make a draft rule
- Section 2.2 considers how the rule may apply in Western Australia
- Section 2.3 explains how our draft rule contributes to the NGO

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

The Commission can only make a rule if it is satisfied that the rule will or is likely to contribute to the achievement of the relevant energy objectives.[29] For this rule change, the relevant energy objective is the NGO.

The NGO is:[30]

> 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.[31]

2.2 We have considered how the draft rule may apply in Western Australia

In developing the draft rule, the Commission has considered how it may apply to Western Australia according to the following questions:

- Does the AEMC have a relevant rule-making power? No, the draft rule does not fall within the subject matters about which the Commission may make rules under the *National Gas Access (WA) Act 2009*.
- Is the AEMC amending parts of the NGR that currently apply in Western Australia? No, the draft rule will create a new Part in the NGR.

Therefore, the draft rule will not apply in Western Australia. See Appendix A for more detail on the legal requirements for this decision.

29 291(1) of the NGL.
30 Section 23 of the NGL.
31 72A(5) of the NGL.

2.3 Our draft rule to clarify and confirm AEMO's cyber security functions in the gas sector would contribute to the achievement of the NGO

The Commission must consider how to address the absence of defined cyber security functions for AEMO in the gas sector. It must also consider how to harmonise these functions with those it has for the electricity sector, to support a strategic and coordinated approach to cyber security in the energy system.

The Commission has identified the following **three** criteria to assess whether the proposed rule change would contribute to achieving the NGO:

- **Safety, security and reliability:** we have considered whether confirming and clarifying AEMO's cyber security functions in the gas sector would enable the reliable, safe and secure provision of gas to consumers over the long term.
- **Principles of good regulatory practice:** we have considered whether the proposed solution would promote predictability, stability, and transparency around AEMO's cyber security roles and responsibilities in the gas sector, without placing new obligations on industry participants or limiting AEMO's current functions.
- **Implementation considerations:** we have assessed relevant implementation considerations, including the cost of the proposed solution, the timing of the rule change, and its success as a market wide solution for the gas sector.

These assessment criteria reflect the key potential impacts – costs and benefits – of the rule change request within the scope of the NGO. Our reasons for choosing these criteria are set out in section 4.2 of the consultation paper.

Following stakeholder feedback to the consultation paper, the Commission is satisfied that the assessment criteria are fit for purpose. One stakeholder, while supporting the proposed assessment criteria, suggested including systemic resilience.[32]

The Commission does not propose including this criterion because we consider that resilience can be assessed indirectly through the criteria of safety, security and reliability outcomes. This is because an energy system that enables the secure and safe provision of gas across the system and the energy sector more broadly, would also enable a resilient energy sector. Thus, we will consider systemic resilience through this lens.

The rest of this section explains why the draft rule best promotes the long-term interest of consumers when compared to other options and assessed against the criteria.

2.3.1 The draft rule would promote safety, security, and reliability

The Commission considers that by embedding and formalising AEMO's functions in the NGR and harmonising these with the electricity sector, the draft rule would promote safety, security, and reliability outcomes by securing the long-term supply of gas, which would also benefit consumers.

Cyber security is important to the security and reliability of the gas sector because a cyber 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. Stakeholders agree that there is a lack of clarity around AEMO's gas sector cyber security responsibilities and a need to formalise its role[33] to ensure that security and reliability outcomes for consumers are maintained.[34]

32 Submission to the consultation paper, Marissa McCauley, p.2.

33 Submissions to the consultation paper: Alinta Energy, p.1; APA, p.2; APGA, p.1; Marissa McCauley, p.1; AGL, p.1.

The draft rule would promote safety, security, and reliability in the gas sector by better enabling AEMO to manage and operate a secure system, giving both AEMO and market participants a better understanding of who is responsible for specific cyber security preparedness and incident response functions. This would help the secure supply of gas to consumers in the long term, ensuring safety and security outcomes are met.

At present, the lack of confirmation on AEMO's cyber security roles and responsibilities in the NGR means that AEMO is not properly resourced to undertake cyber security activities in the gas sector. This creates ongoing security risks because it contributes to a lack of coordination and responsiveness among gas sector participants. As such, the Commission considers that the safety, security and reliability benefits of the draft rule would outweigh the potential costs of leaving AEMO's roles and responsibilities for cyber security unclarified.

As a market and system operator, AEMO is well-placed to support the gas sector with preparedness, learning and uplift activities. The four functions under the draft rule would give AEMO the ability to be properly resourced to undertake more proactive preparedness, learning and uplift activities across the ECGS. Specifically, the four functions contribute to proactive measures as AEMO could:

- Have a cyber security framework that can help prevent security incidents, which helps industry participants keep their precautionary measures current. See section 3.2.2.
- Examine risks and provide proactive cyber security advice to government and industry. See section 3.2.3.
- Disseminate critical cyber security information, such as preventative patches in commonly used technologies. See section 3.2.4.

In considering stakeholder feedback, the Commission is of the view that confirming and clarifying AEMO's cyber security functions in the NGR and harmonising them with the electricity sector would result in improved safety, security, and reliability outcomes. Specifically, stakeholders agree that harmonising AEMO's cyber security functions across electricity and gas would be beneficial, with Alinta Energy noting that it would "streamline processes, avoid duplication and reduce costs".[35]

If a final rule is made, the proponent states that AEMO has estimated the costs of the functions to be in the range of $1.8 million to $2.75 million per year.[36] The Commission understands that cost recovery for these functions would likely be on the same basis as the GSOO fees because cyber security fees will benefit the same group of participants. See section 3.3 for more information on the forecast costs of the proposed solution and the expected consultation process for recovering participant fees which is expected to take place from 1 July 2027.

By confirming these four functions in AEMO's cyber security roles and responsibilities and harmonising these functions with the electricity sector, the draft rule would further support AEMO's ability to manage and operate a safe, secure, and reliable gas system at a time when cyber security concerns are increasingly prevalent.

2.3.2 The draft rule would align with principles of good regulatory practice

The Commission considers that the draft rule would be aligned with principles of good regulatory practice. This is because it is seeking to improve predictability, stability and transparency of cyber

34 Submission to the consultation paper, Marissa McCauley, p.3.
35 Submissions to the consultation paper: Alinta Energy, p.1; APA, p.2; APGA, p.1; Marissa McCauley, pp.1-2; AGL, p.1.
36 Rule change request, p.11.

security in an increasingly digitised and interconnected gas sector. The draft rule also considers broader cyber security reforms to support harmonisation of AEMO's role across the energy sector, and to avoid unnecessary duplication of activities.

By introducing these cyber security functions under the national gas framework, AEMO would be able to recover fees and charges in the performance or exercise of its functions and have immunity from liability. This would provide predictability and stability for AEMO and participants because it would allow for resourcing certainty to properly establish and undertake cyber security activities on a more well-defined and permanent basis. Cost recovery and liability protection would enable AEMO to continue and scale up its cyber security activities. Additionally, market participants would be able to confidently rely on AEMO to perform specific preparedness, uplift and responsiveness activities in the gas sector, and consistently throughout the energy system. Under the draft rule, AEMO is not conferred powers to impose mandatory obligations on participants. However, it does provide AEMO with sufficient flexibility by not limiting their ability to perform other activities that may relate to cyber security.

It follows that AEMO, government, and gas market participants would then have transparency around activities and the cost of AEMO's cyber security roles and responsibilities. To ensure transparency in the gas sector, AEMO is required to consult on its proposed fee structure in accordance with the standard consultative procedure. See section 3.3 for more detail.

Cyber security is a particularly prominent issue in energy security given the gas sector's increasing digitisation, connectivity, and interconnection with the electricity system. Bearing this in mind, broader cyber security reforms have been taken into consideration. Specifically, by including the four functions for AEMO in the NGR, the draft rule extends to the gas sector a recommendation from the Independent Review into the Future of the National Electricity Market that AEMO should have a cyber security role. While AEMO has begun performing some of the activities for the gas sector under the functions, such as overseeing the Australian Energy Sector Cyber Security Framework,[37] because of the lack of certainty under the statutory framework regarding their ability to recover costs and protection from liability, AEMO have not been able to upscale and adapt to circumstances as need arises.

Further, the Commission acknowledges that the gas sector differs from the electricity sector (see section 3.1.1). Despite these differences, the Commission considers that harmonising AEMO's cyber security functions with its functions for the electricity sector aligns with principles of good regulatory practice. This is because they are broad and flexible functions that do not impose specific activities on AEMO or operational obligations on gas sector participants. More specifically, harmonising AEMO's cyber security functions across the energy sector will promote predictability and stability in the regulatory framework, as well as simplicity and transparency for stakeholders. Harmonising AEMO's cyber security functions also interacts constructively with the broader direction of cyber security reform in the energy sector.

Importantly, the proposed functions would complement, rather than duplicate, the role of other agencies such as the ACSC and frameworks such as the SoCI Act. This is because they have a different focus and because of the unique insight AEMO provides as a market and a system operator which is not provided by other entities or bodies.

In considering stakeholder feedback, the Commission is of the view that confirming and clarifying AEMO's functions in the NGR and harmonising these with the electricity sector would be aligned with principles of good regulatory practice. Specifically, stakeholders agreed that it is problematic

37 Rule change request, p.6; AEMO, Australian Energy Sector Cyber Security Framework.

that AEMO's cyber security functions remain unclear, and that the lack of harmonisation in AEMO's cyber security functions across the energy sector limits predictability, stability and transparency in the gas sector.[38]

2.3.3 We have taken implementation considerations into account for the draft rule

The Commission has considered cost implications, governance arrangements, timing impacts and relevant jurisdictional conditions in making this draft rule.

The Commission considers that the overall cost of formalising AEMO's cyber preparedness and incident response functions in the gas system is low compared to the benefits and the magnitude of a potential cyber incident, particularly where incidents could be prevented through clarified roles and responsibilities and by upscaling AEMO's preparedness activities. The Commission therefore considers the costs are justified because much of this work is already underway and benefiting participants, for example, through AEMO's electricity cyber security functions that are already underway. This reflects the reality that the cyber threat environment has changed considerably, making formalisation and additional resourcing increasingly important for the gas sector. The draft rule would support participants to improve cyber preparedness and maturity without introducing additional mandatory obligations. This would help to reduce associated costs and provides confidence that benefits will be realised and AEMO's cost estimates are likely to be accurate. See section 3.3 for more information about the benefits of the four functions outweighing the costs.

The Commission considers that any complexities in cyber security governance would become more transparent and simplified for industry participants as the draft rule would formally establish functions for AEMO in the gas sector to support consistent cyber security coordination across the energy sector.

Further, the cyber security functions in the draft rule build on the activities that AEMO is already undertaking. Accordingly, the Commission considers that a commencement date of 30 July 2026, meaning the rule would take effect immediately, is appropriate. See section 3.4 for more detail. We welcome stakeholder feedback on this proposed implementation plan.

The impact on AEMO and other participants would be manageable because AEMO is already performing these activities in the electricity sector and for the gas sector, meaning that existing processes could be built on. While the draft rule proposes to establish four functions, AEMO is not limited in its activities under the functions, meaning it is well placed to adapt to the cyber security needs of the gas sector. The draft rule does not provide AEMO with the ability to impose additional mandatory obligations on market participants, meaning the compliance costs for participants would be low. AEMO's four functions should assist participants in managing cyber security risks because they would support cyber preparedness and uplift, examine cyber risks and provide advice, and facilitate the distribution of critical information which would help participants manage cyber security risks before they eventuate into an incident. See section 3.2 for more information on AEMO's proposed functions.

Additionally, the draft rule takes into consideration relevant jurisdictional and market conditions across the gas sector. Cyber security incidents across the gas sector could affect individual assets, with potential flow on effects to the electricity system and the NEM. In addition to the SoCI Act, which places an obligation on AEMO and entities to look after their own assets from a

38 Submissions to consultation paper: Alinta Energy, p.1; APA, p.2; APGA, p.1; Marissa McCauley, pp.1-2; AGL, p.1.

national security perspective, clarifying and confirming the proposed functions in the draft rule would help ensure that sector-wide risks between participants and AEMO are being addressed.

3 Our draft rule would confirm and clarify AEMO's cyber security functions in the NGR

This chapter provides an overview of the draft rule which takes into account stakeholder feedback provided in submissions to the consultation paper.

- **Section 3.1** explains that the draft rule would define AEMO's cyber security roles and responsibilities in the NGR.
- **Section 3.2** outlines the four proposed functions and addresses stakeholder feedback on those functions.
- **Section 3.3** outlines the expected costs of the functions and why they are justified.
- **Section 3.4** explains the proposed timing for commencement of the draft rule.

3.1 Cyber security is a growing and prevalent concern in the gas sector

Box 1: Cyber security roles and responsibilities would be established for AEMO for the gas sector

The draft rule would:

- formalise and embed cyber security as part of AEMO's roles and responsibilities in the NGR across the ECGS
- harmonise AEMO's cyber security roles and responsibilities with the electricity sector to ensure a coordinated and strategic approach to cyber security across the energy sector
- provide more certainty on cost recovery and liability protection for AEMO in performing these functions. This would allow AEMO to properly establish and undertake cyber security activities on a well defined and permanent basis for the gas sector.

The draft rule would formalise and embed cyber security as part of AEMO's roles and responsibilities in the NGR across the ECGS.[39]

Currently, the NGR does not address cyber security, so AEMO does not have a clear role or confirmed responsibilities in this area for the gas sector. The draft rule would clarify this by establishing specific cyber security prevention and preparedness functions for AEMO in the NGR for the ECGS.

The Independent Review into the Future of the National Electricity Market emphasised the importance of cyber security in the energy sector and underscored the necessity of resilient and secure energy infrastructure.[40] Since then, cyber security measures across the energy sector have been progressively introduced, including clarifying AEMO's roles and responsibilities for the electricity sector.[41] See chapter 1 for more information.

The draft rule would also harmonise AEMO's gas sector cyber security functions with its electricity sector functions. This would allow AEMO to deliver a strategic and coordinated approach to cyber security across the energy sector. See section 3.1.1 below.

39 Draft rule, 716.
40 Independent Review into the Future of the National Electricity Market, p.67.
41 Cyber security roles and responsibilities.

Importantly, the draft rule does not place additional requirements on gas participants but rather, clarifies AEMO's role in providing prevention and preparedness functions to facilitate cyber security measures across the gas sector. Infrastructure owners would remain responsible for managing the cyber security of their own assets.

Stakeholders support formalising AEMO's cyber security role for the gas sector

Stakeholders agree with the definition of the problem set out in the consultation paper. Stakeholder submissions recognised the importance of embedding and formalising AEMO's cyber security functions in the gas sector and harmonising these with the electricity sector.[42] Stakeholders believe that this is especially important given the increasing digitisation and the interconnected nature of infrastructure networks.[43]

The Commission agrees and considers that confirming and clarifying AEMO's cyber security role for the gas sector is important because the consequences of a cyber incident could impact the operation of the sector, and in turn the supply of gas to industry and consumers. We also note that the interconnectivity between Gas Powered Generation (GPG) and the electricity sector means a cyber incident affecting gas supply or gas market operations could have flow on impacts for the electricity system.

3.1.1 AEMO's cyber security functions would be consistent across the energy sector

The draft rule would harmonise AEMO's cyber security roles and responsibilities across the energy sector.[44] It would do so by replicating AEMO's electricity cyber security functions for electricity in the gas sector, thereby supporting a coordinated and strategic approach to cyber security.[45]

While AEMO performs cyber security activities for the gas sector, the lack of defined functions in the NGR could create inconsistencies and gaps in the application of AEMO's cyber security preparedness and uplift measures across the energy sector.

Stakeholders agree that it would be beneficial to harmonise AEMO's cyber security functions across the gas and electricity sector, explicitly supporting a consistent approach to AEMO's cyber security functions across the energy sector.[46] Stakeholders believe that harmonising AEMO's gas and electricity cyber security functions would:

- reduce duplicated compliance efforts and costs.[47]
- support a consistent regulatory approach across the energy sector.[48]
- better manage sector-wide cyber security risks in interconnected operations.[49]

Operational characteristics, physical infrastructure, and governance arrangements differ across gas and electricity

The Commission recognises that the gas sector differs in operational characteristics, physical infrastructure, and governance arrangements from the electricity sector.

More specifically, the electricity sector operates as a real-time system that instantaneously balances supply and demand using a centralised market and digitally integrated platforms. By

42 Submissions to the consultation paper: Alinta Energy, p.1; APA, p.2; APGA, p.1; Marissa McCauley, p.1; AGL, p.1.
43 Submission to the consultation paper, AGL, p.1.
44 Draft rule, 716.
45 Cyber security roles and responsibilities.
46 Submissions to the consultation paper: Alinta Energy, p.1; APGA, p.1; Marissa McCauley, p.1; AGL, p.1.
47 Submission to the consultation paper, Alinta Energy, p.1.
48 Submission to the consultation paper, AGL, p.1.
49 Submission to the consultation paper, Marissa McCauley, pp.1-2.

contrast, the gas sector operates with longer scheduling periods (predominantly through long-term contracts) and relies less on centralised platforms.

These differences create a risk asymmetry because the pathways through which cyber risks materialise, and the speed at which impacts propagate, differ. For example, in the electricity sector, a cyber incident affecting market and dispatch systems may produce immediate, system-wide impacts on market outcomes. Comparably, in the gas sector, the ownership, structure and operational characteristics of the gas sector mean that dedicated cyber security preparedness and response arrangements are required to reflect the specific operational and physical interventions that may be required to restore operations. Gas sector cyber incidents can also impact the supply of electricity when GPG is affected.

Importantly, while the NER provides formalised cyber security functions for AEMO, the NGR lacks comparable system-level cyber security responsibilities for AEMO in the gas sector. AEMO's lack of embedded and formalised functions for gas sector wide coordination on cyber security preparedness and response measures creates the potential for delayed detection and response times. This could increase the risk of localised disruptions escalating into broader supply and economic impacts (see table 3.3).

The comparative analysis suggests that, while the gas and electricity sectors differ, the underlying rationale for formalising AEMO's system level cyber security functions is common to both.

See table 3.1, 3.2, and 3.3 below for a comparative analysis of these differences.

Figure 3.1: The market differences between the gas sector and electricity sector

		Gas Sector					Electricity Sector
Market		**Declared Wholesale Gas Market (DWGM)**	**Short Term Trading Market (STTM)**	**Gas Supply Hub (GSH)**	**Day Ahead Auction (DAA)**	**Capacity Trading Platform (CTP)**	**National Electricity Market (NEM)**
Location		Victorian Declared Transmission System (DTM) (Victoria)	Brisbane, Sydney, and Adelaide	Wallumbilla, Moomba, Culcairn, Sydney, Longford, Iona	Most east coast pipelines	Most east coast pipelines	Queensland, New South Wales (including the Australian Capital Territory), Victoria, South Australia, and Tasmania
Type		Commodity	Commodity	Commodity	Capacity	Capacity	Commodity
Mandatory or Voluntary		Mandatory (Gross)	Mandatory (Gross)	Voluntary (Net)	Voluntary (Auction) (Mandatory for capacity to be made available)	Voluntary (Net)	Mandatory
Market operator		AEMO operated	AEMO operated (but does not operate the physical pipeline or network assets)	AEMO operated	AEMO operated	AEMO operated	AEMO operated
Operational differences	**Timing & dispatch**	Trading occurs well ahead of physical delivery (days, months, or years in advance). Short term gas markets clear around a defined gas day.					Operates continuously in real time, with central dispatch every 5 minutes. Supply and demand must balance.
	Role of physical constraints	Physical delivery of gas depends on pipeline capacity, compression and storage. Constraints are often contractual and locational, and congestion can persist over time.					Power flows instantaneously across the network and is constrained by system security limits. Constraints can change rapidly.
	Market participation & contracts	Strong reliance on contracts for supply and capacity.					Energy volumes are primarily determined through the central spot market.
	Operational role of AEMO	AEMO operates the markets but generally does not operate the physical pipelines (with the exception of the Victorian Declared Transmission System). Producers and shippers retain greater responsibility for delivery feasibility.					AEMO has a direct operational role in real-time system operation, including dispatch, frequency control and system security.
	Flexibility & storage	Flexibility is provided through storage, line pack and contract flexibility.					Historically limited storage; flexibility is provided through dispatchable generation and increasing battery storage and demand response.

Source: AEMC.

Note: While the ECGS operates markets, the majority of wholesale gas is traded through bilateral agreements including Gas Transportation Agreements (GTA) and Gas Supply Agreements (GSA). Participants generally use spot markets to manage imbalances in contract positions, peak day, and short term supply.

Figure 3.2: The physical and facility differences between the gas sector and electricity sector

	Gas sector			Electricity Sector		
	Production	**Transmission**	**Distribution**	**Production**	**Distribution**	**Transmission**
What happens?	Extraction of gas from underground reservoirs.	Bulk transport of gas over long distances.	Delivery of gas to end-users.	Conversion of primary energy into electricity.	Transport of electricity from generators to load centers.	Delivery of electricity to end-users.
Key components	Gas fields and wells.	High-pressure transmission pipelines	Distribution pipelines (lower pressure)	Power stations (coal, gas, hydro)	High-voltage transmission lines	Low voltage Poles and wires
	Wellheads and gathering systems.	Compressor stations	Pressure reduction stations	Renewable generators (wind farms, solar PV, solar thermal)	Substations and transformers	Zone and distribution substations
	Gas processing plants.	Metering stations	Customer meters and regulators	Inverters (for inverter-based resources)	Switchgear, protection systems	Distribution transformers
	Liquification facilities.	Storage facilities and line pack (gas retained in pipelines)				Customer connections and meters
						Customer Energy Resources: EVs, Rooftop PV and batteries
Characteristics	Production is geographically fixed and often remote from demand centers. Output is generally stable but ramping production is slow.	Gas flows are controllable and directional but slow to change. Capacity is constrained by pipeline ratings and compression. Gas can be stored within the system	Flows are predictable and demand changes slowly. Limited operational intervention required in real time.	Generation can be dispatchable or variable. Output can change rapidly (especially for thermal plant and batteries).	Electricity flows instantaneously and follows physical laws, not contracts. No inherent storage in the network. Subject to tight thermal and system security limits.	Increasingly two-way due to rooftop PV, batteries and EVs. Actively managed for voltage, congestion and reliability.

Source: AEMC.

Figure 3.3: The governance differences between the gas sector and electricity sector

	Gas	Electricity

System Operation	• AEMO operates gas markets and performs system-level functions such as scheduling, balancing and information provision.
	• Physical pipelines are generally operated by pipeline owners/operators, not AEMO.
	• Exception: Victoria, where AEMO operates the Declared Transmission System (DTS) and has a more direct operational role.
		• AEMO is the central system operator, with direct responsibility for:
		  • Real-time dispatch
		  • Frequency control
		  • Power system security and reliability
		• AEMO actively manages system conditions continuously and in real time.

Production & Generation Assets	• Producers own and operate gas fields, wells and processing facilities. • Decisions about production levels are primarily commercial, subject to contractual and regulatory constraints. • Limited real-time operational direction from AEMO.	• Generators own and operate power stations and renewable plants. • Generation output is centrally coordinated through AEMO dispatch instructions. • Compliance with technical performance and security standards is critical.

Transmission networks	• Transmission pipelines are owned and operated by private or state-owned pipeline businesses.
	• Pipeline access and capacity are governed by:
	  • Bilateral contracts
	  • Economic regulation (where applicable)
	• AEMO generally does not control pipeline flows directly.
		• Transmission Network Service Providers (TNSPs) own and maintain high-voltage networks.
		• AEMO determines how the transmission system is used in real time through dispatch and constraint management.
		• Strong coordination between AEMO and TNSPs is required for system security.

Distribution networks	• Gas distributors own and operate low-pressure distribution networks.
	• Operations are relatively stable and predictable.
	• Limited interaction with central system operation once gas enters distribution networks.
		• Distribution Network Service Providers (DNSPs) own and operate poles-and-wires networks. Increasing operational complexity due to:
		  • Distributed energy resources (rooftop PV, batteries, EVs)
		  • Two-way power flows
		• Stronger interaction with AEMO, especially for security and reliability.

Market governance & regulation	• Multiple markets with different governance arrangements (DWGM, STTM, GSH, DAA, CTP). Greater reliance on:
	  • Contractual arrangements
	  • Self-scheduling by participants
	  • Regulatory oversight varies by market and jurisdiction.
		• A single, integrated national market (NEM). Clear separation of roles:
		  • AEMO – operator
		  • AER – economic regulation and compliance
		  • AEMC – rule-making
		• Strong emphasis on system security and reliability outcomes.

Source: AEMC.

Despite these differences the Commission considers that harmonising AEMO's cyber security functions in the gas sector with its functions for the electricity sector is appropriate because they are broad and flexible functions that do not impose specific activities on AEMO or operational obligations on gas sector participants. This means AEMO would:

- have flexibility to apply the proposed functions in a way that is tailored to gas market arrangements across the ECGS
- where appropriate, maintain a consistent energy system-wide approach to identifying emerging risks, supporting uplift activities and coordinating responses when required, e.g. through the Australian Energy Sector Cyber Security Framework or the Australian Energy Sector Cyber Incident Response Plan.

The Commission is of the view that harmonising the functions would allow for a consistent and coordinated approach and understanding around AEMO's cyber security role and responsibilities while retaining AEMO's flexibility to determine the specific activities it undertakes under the functions. It is important that AEMO has the flexibility to adapt these functions to enable it to undertake preparedness and uplift activities across the energy sector, without unduly limiting the activities it can perform if new risks emerge.[50] See section 3.2 for more information on how the functions would work.

3.1.2 AEMO would be able to recover costs and have immunity from liability for cyber security activities in the gas sector

By clarifying and confirming AEMO's cyber security functions in the NGR, the draft rule would provide certainty on how AEMO would recover fees and charges for conducting cyber security activities under its function.[51] It would also allow AEMO to have immunity from liability when conducting its proposed cyber security functions in the gas sector.[52] This would allow AEMO to properly establish and undertake cyber security activities on a well defined and permanent basis for the gas sector. Additionally, market participants would be able to confidently rely on AEMO to perform specific preparedness, uplift and responsiveness activities.

One stakeholder explicitly agreed that AEMO should be able to recover costs and have liability protection, noting that:

- cost recovery builds and maintains capability over the long term[53]
- liability protection would minimise AEMO's risk of litigation, allowing AEMO to act more decisively.[54]

The Commission believes that cost recovery and liability protection would enable AEMO to continue and scale up its incident response preparation, for example by updating the Australian Energy Sector Cyber Incident Response Plan more frequently or establishing tools and technologies to support it. Additionally, market participants would be able to confidently rely on AEMO to perform specific preparedness, uplift and responsiveness activities. Importantly, the draft rule would not give AEMO the ability to manage participants' or other bodies' responses to a cyber incident. See section 3.2.1 for more information on AEMO's incident coordinator role, and section 2.3.2 for more information on how this promotes principles of good regulatory practice.

50 Draft rule, 716(7a).
51 Draft rule, 716.
52 Rule change request, p.4.
53 Submission to the consultation paper, Marissa McCauley, p.2.
54 Submission to the consultation paper, Marissa McCauley, p.2.

3.2 The draft rule would embed four functions into the NGR

Box 2: Cyber security functions in the NGR

The draft rule would establish four 'cyber security functions' to be performed by AEMO. The four functions are:

1. Acting as cyber security incident coordinator
2. Supporting cyber security preparedness and uplift
3. Examining risks and providing research and advice to government and industry
4. Facilitating the distribution of critical cyber security information to the gas sector

Stakeholders were broadly supportive of all four functions, with some questioning AEMO's suitability to perform some of the functions and raising concerns about duplication with other bodies' roles.

The Commission's draft determination is that the four functions would have benefits for gas consumers and participants. We consider that AEMO is the appropriate body to carry out these functions, noting AEMO's unique position and expertise in the gas sector. Making the draft rule to embed and formalise these functions would enable AEMO to scale up and consistently perform a cyber security role, supported by appropriate cost recovery arrangements and protection from liability.

3.2.1 Function 1: Cyber security incident coordinator

As the cyber security incident coordinator AEMO would plan for and coordinate the response of relevant entities to a cyber incident that adversely affects the secure operation of the ECGS.[55] The draft rule would ensure AEMO is adequately resourced and equipped to undertake this function using reasonable endeavours.[56] AEMO may coordinate the energy-sector wide response by continuing to develop the Australian Energy Sector Cyber Incident Response Plan outlining how market, state and federal responses to a cyber incident would be coordinated.

The Australian Energy Sector Cyber Incident Response Plan 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:[57]

- the coordination 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 Australian Cyber Security Centre Cyber Incident Management Arrangements.

Stakeholders expressed support for AEMO's proposed cyber incident coordinator function.[58] Stakeholders noted support for:

- infrastructure owners retaining primary responsibility for their assets, with AEMO playing a coordination role which would help reduce the duration and severity of a cyber incident.[59]

55 Rule change request, p.4.
56 Draft rule, 716(1).
57 Rule change request, p.5.
58 Submissions to the consultation paper: Alinta Energy, p.1; APA, p.2; APGA, p.1; Marissa McCauley, p.2; AGL, p.1.
59 Submission to the consultation paper, Marissa McCauley, p.6.

- ongoing industry exercises and improved industry governance.[60]

Considering stakeholder feedback and the rule change request, the Commission believes that clarifying AEMO's coordinating role is especially important for the gas sector, since AEMO is not the system operator across the board, there is a need to ensure AEMO's role is clearly understood by participants. This would also help protect gas consumers and participants from the potential consequences of a cyber incident because, in the event of a cyber incident, gas consumers and participants would have consistent guidance on how to respond and, if necessary, guidance on how to follow emergency protocols.

3.2.2 Function 2: Supporting cyber preparedness and uplift

The industry uplift function in the draft rule would require AEMO to continue to help industry participants improve their cyber security preparedness and maturity.[61] This function could include, but would not be limited to:[62]

- **Ongoing stewardship of the Australian Energy Sector Cyber Security Framework** | AEMO could continue to apply the Australian Energy Sector Cyber Security Framework to the gas sector as needed. This function would also include continuing to oversee Australian Energy Sector Cyber Security Framework self-assessments for the gas industry. See section 3.1.2.
- **Provision of guidance and tools for industry** | As part of this function, AEMO could participate in Industry Working Groups, standards committees, and in an advisory capacity to government working groups under Energy Ministers. AEMO could also provide guidance and tools for industry to improve cyber awareness and maturity, including related guidance materials, where appropriate, in partnership with relevant government agencies.
- **Organisation of testing and training exercises** | As part of this function, AEMO could support or undertake the development and delivery of scenario exercises to test the cyber resilience of the ECGS.

Stakeholders support AEMO's proposed function for cyber preparedness and uplift. Stakeholders noted that ongoing industry exercises and stronger collaborative governance, for example through an Australian Energy Sector Cyber Security Framework working group, can support sector-wide uplift.[63]

In considering stakeholder feedback and the rule change request, the Commission is of the view that AEMO is well placed to support cyber security uplift for the gas sector. While AEMO is not a system operator in the same way as the NEM, see section 3.1.1, unlike other participants they play a broader role in the ECGS by undertaking market operations, operating the DTS, operating the Gas Bulletin Board, and providing gas planning and forecasting reports[64] which gives them a system-wide lens and capabilities across the gas sector distinct from other participants.

Given the diversity of system and infrastructure operators and their more limited role, compared to AEMO, the gas sector would benefit from AEMO having clear authority to provide guidance, tools, testing and training for cyber security uplift and preparedness activities where appropriate.

60 Submission to the consultation paper, AGL, p.1.
61 Draft rule, 716(2).
62 Rule change request, pp.5-6.
63 Submissions to the consultation paper: AGL, p.1; Marissa McCauley, p.6.
64 AEMO, About the East Coast Gas System.

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

Under this function, AEMO would draw on its unique energy expertise in market operations, monitoring and forecasting for the ECGS, to provide cyber security research and advice to governments and industry in relation to identified cyber security risks that may impact the ECGS and the management or mitigation of those risks.[65] This function would complement, rather than replace, work undertaken by other cyber security bodies such as the Australian Cyber Security Centre.[66]

This research and advice function would enhance cyber security maturity for AEMO, governments, and industry participants. By further enabling AEMO to build up and share its cyber security expertise, this function would help governments and industry to prepare for and respond to cyber incidents to limit the impact on consumers.

AEMO has unique oversight and capability to provide analysis to policy makers on energy and cyber security issues. AEMO providing this advice to government would:

- allow for appropriate and proportionate intervention from government as required[67]
- support gas system risk management planning and as part of AEMO's role in the design of Australia's future energy system[68]
- include, for example, the preparation of specialist reports, independent advice, and detailed analysis to support effective and strategic decision-making in government and industry.[69]

The intention is that AEMO can initiate advice when it identifies an issue and would also be obliged to prepare advice if requested by a relevant Minister, subject to consultation on the nature and extent of the research or advice. Additionally, AEMO could collate and distribute the advice of government agencies and other bodies to provide information on cyber security measures. As part of this function, AEMO could also, at its discretion, provide similar information to gas sector participants.

The function would be advisory only and would not result in AEMO performing any regulatory responsibilities beyond its existing mandated scope and ability.

The majority of stakeholders supported this function.[70] Specifically, one stakeholder noted that AEMO was best placed to examine risks and provide advice to government and industry because of their system-level visibility across the gas sector that individual gas participants do not have.[71]

However, two stakeholders questioned whether AEMO was best placed to provide advice and carry out research on cyber security risks. The stakeholders believe that the proposed research and advisory function would be better provided by organisations with more specialised cyber security expertise beyond AEMO's operational focus on the ECGS.[72] However, one of these stakeholders, while questioning this function, also expressed preferential support for a consistent regulatory approach across the gas and electricity sector, supporting the intent of this function to operate as proposed.[73]

65 Draft rule, 716(3)(4)(5).
66 Rule change request, p.4.
67 Rule change request, p.6.
68 Rule change request, p.6.
69 Rule change request, p.6.
70 Submissions to the consultation paper: APA, p.2; APGA, p.1; Marissa McCauley, p.2.
71 Submission to consultation paper, Marissa McCauley, p.6.
72 Submissions to the consultation paper: Alinta Energy, p.1; AGL, p.1.
73 Submission to consultation paper, AGL, p.1.

In considering stakeholder feedback and the rule change request, the Commission considers that AEMO's unique position and expertise in the gas sector means it would be well placed to provide valuable research and advice on cyber security risks to government and industry. The Commission notes that the draft rule would not make AEMO the sole provider of cyber security advice and would not replace other channels by which governments and industry may seek advice, including government agencies such as the Australian Cyber Security Centre. AEMO would also have the flexibility to seek input from other bodies or from industry when carrying out this function.

3.2.4 Function 4: Facilitating the distribution of critical cyber security information to the gas sector

In its position as a market and system operator and using existing communication channels, AEMO would act as a distributor of cyber security information to industry.[74] Under the draft rule, this would include facilitating the distribution of:[75]

- information with respect to cyber security 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.

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 matters, including security-related events, market directions, suspensions and interventions and general notices.[76]

Stakeholders generally support this function. Specifically, stakeholders identify the need for timely information to be distributed, believing AEMO is best placed to do this.[77]

However, AGL questioned the added value of AEMO distributing cyber threat information, noting the existence of ASD platforms, and requested clarity on how this function aligns with new national cyber security governance structures.[78] Despite this, as noted above, AGL expressed preferential support for a consistent regulatory approach across the gas and electricity sector, supporting the intent of this function to operate as proposed.[79]

In considering this feedback, and the rule change request, the Commission believes that the benefits of this function include:

- supporting AEMO's and participant's ability to maintain gas system security, through the redistribution of advice through channels which industry is familiar with
- assisting relevant entities to protect their own systems and take steps necessary to respond to cyber security threats
- ensuring advice coming from AEMO, even if redistributed from the Australian Cyber Security Centre or other authorities, will emphasise the importance and urgency of addressing the issues identified to relevant entities. This could reduce the number of different communication channels in play during a cyber incident.

74 Rule change request, p.4.
75 Draft rule, 716(6).
76 Rule change request, pp.6-7.
77 Submissions to the consultation paper: Marissa McCauley, p.7; APGA, p.1.
78 Submission to the consultation paper, AGL, p.1.
79 Submission to consultation paper, AGL, p.1.

The Commission understands that some industry participants may receive cyber security information from sources, such as the ASD. However, we note that the dissemination of information by AEMO is likely to be more useful to smaller participants which may not have the resources to keep track of cyber security information from multiple sources. In these cases AEMO could provide a valuable service by gathering pertinent cyber security information in one place.

3.3 The four functions are likely to significantly reduce cyber security risks and costs

Box 3: The benefits of the cyber security functions outweigh the costs

The Commission considers that the costs of the four functions are outweighed by the benefits of reducing cyber security risks in the gas sector. More specifically, the proposed cyber security functions would improve cyber preparedness and response arrangements and reduce the likelihood and impacts of cyber incidents that could affect gas supply.

AEMO would recover the costs of performing the functions through participant fees. AEMO estimates that the functions would likely cost between $1.8 million and $2.75 million per year. Stakeholders generally agreed that the expected costs are justified, and that the benefits of the proposed solution would outweigh the potential cost of a cyber incident. One stakeholder requested that the scope of the proposed rule change should be reduced where the benefits are uncertain.

The draft rule would enable AEMO to recover cyber security costs from gas participants through AEMO's existing cost recovery process which involves a standard consultative procedure (outlined in Box 4). AEMO has noted 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 3.4). This would help ensure the proposed cyber security functions are adequately and sustainably funded.

As outlined in section 3.1.2, the draft rule would provide certainty on how AEMO would recover fees and charges for conducting the four proposed functions.[80]

The proponent states that AEMO has estimated the costs of the functions to be in the range of $1.8 million to $2.75 million per year.[81] The Commission understands that the cost estimate:

- factors in the efficiency gains for the cyber security work already underway, accounting for the lower value than quoted for the NEM.[82]
- 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.

Due to the evolving cyber threat landscape and the resources required by AEMO to manage new and emerging threats over time, ensuring cost recovery for AEMO would provide stability and predictability to industry. See section 3.1.2 and section 2.3.2. It would allow these specific

80 Draft rule, 716.

81 Rule change request, p.9.

82 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.

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

Several stakeholders explicitly agreed that the benefits of the proposed functions would outweigh the costs.[83] That is, the expected cost would be low compared to the potential benefits in avoiding or mitigating the impact of cyber security incidents. One stakeholder explicitly agreed that the cost of a cyber security incident far outweighs the cost of the proposed solution, stating that AEMO's projected annual costs for the functions are negligible compared to the cost of infrastructure downtime in the event of a cyber incident.[84]

One stakeholder, while supportive, requested:

- that the scope of the proposed rule change should be reduced where the benefits are uncertain to avoid duplicated effort.[85]

While the Commission appreciates this feedback, the Commission does not consider that the scope of the functions should be reduced to avoid duplication. The functions are intentionally broad enough to allow AEMO to tailor the cyber security activities provided under the functions to reflect system, market, government and industry needs under an evolving threat environment. Importantly, the draft rule would not enable AEMO to create new obligations on participants, as such there would be no mandatory compliance costs for industry participants.[86]

Considering stakeholder feedback, and the rule change request, the Commission considers that the benefits of embedding and formalising AEMO's cyber security functions for the gas sector outweigh the cost of performing the proposed functions. Specifically, benefits would include:

- harmonising AEMO's cyber security functions with those it has for the electricity system
- AEMO would be able to continue performing cyber security activities with certainty, sufficient resources, and immunity from liability for delivering these functions. This reflects the reality that while AEMO has been performing some of these activities the environment has changed considerably, with cyber preparedness and uplift becoming increasingly more important for the gas sector. More specifically, the digitisation of the gas sector, while beneficial, has introduced new challenges and vulnerabilities to systems, namely cyber security threats
- 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
- relevant entities, notably industry, would benefit from cyber uplift assistance and clear recovery protocols, including the continued development of the Australian Energy Sector Cyber Security Framework and the Australian Energy Sector Cyber Incident Response Plan
- the improvement of cyber security preparedness across the sector, which would reduce the risks of malicious cyber-attacks which impact energy supply, benefiting customers with improved security of supply
- AEMO would be sufficiently resourced to advise government and industry on relevant cyber security related issues to continue to ensure gas security
- greater clarity and 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.

83 Submissions to the consultation paper: APGA, p.1; Marissa McCauley, p.2.

84 Submission to the consultation paper, Marissa McCauley, p.2 notes that the "estimated $1.8M-$2.75M annual cost is negligible compared to the $1.2M-$3.8M per hour cost of infrastructure downtime". Sources: Splunk Australia & ANZ Research, Downtime: a rising challenge for ANZ organisations; Oxford Economics Global Partnership, The hidden costs of downtime: The $400B problem facing the global 2000.

85 Submission to the consultation paper, Alinta Energy, p.2.

86 Draft rule, 716(7b).

AEMO would recover costs from gas participants

AEMO recovers gas participant fees from liable registered participants for the:[87]

- 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 would likely be on the same basis as the GSOO fees because cyber security fees will benefit the same group of participants. See table 3.4 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 forecast costs of performing cyber security functions would be incorporated into AEMO's annual budget and fee process.[88] AEMO consults on its proposed fee structure for gas participant fees in accordance with the standard consultative process, See Box 4 below. The next consultation for general determination of gas participant fees would be from 1 July 2027.[89]

Box 4: 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

87 AEMO, Structure of Gas Participant Fees, December 2023.

88 Rule change request, p.9.

89 The fee structure term is for a three-year period from 1 July 2024 to 1 July 2027. AEMO, Structure of Gas Participant Fees, December 2023.

- 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 5.

Box 5: 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 ECGS 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 4.
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.

3.4 The draft rule would commence on 30 July 2026

The Commission's final determination and final rule (if made) is scheduled to be published on 30 July 2026. The commencement date of the rule is proposed to be the same day as publication. Immediate commencement is possible because AEMO is already performing these functions within the electricity sector and some activities under the functions, without having a cyber security role established in the NGR, for the gas sector.

An early commencement date would ensure AEMO has protection from liability for the cyber security functions as soon as possible. Additionally, it would not delay the process for AEMO to be able to cost recover for the performance or exercise of these cyber security functions as soon as possible. AEMO will only be able to plan to recover costs, and sufficiently commit resources to these four functions, from the commencement of the final rule. Benefits for consumers would be realised more quickly in turn.

As outlined above in section 3.3 AEMO would need to determine and consult on the participant fee structure and the period for cost recovery.

In addition, AEMO would need to carry out work to establish or ramp up some aspects of the cyber security functions. However, the Commission considers that AEMO could do this work before 30 July 2026 because the functions are facilitative and flexible.

AEMO would not need to make any updates to procedures, guidelines, or settlement systems before the draft rule takes effect in order to be compliant with the rule.

A Rule making process and background to the rule change request

A standard rule change request includes the following stages:

- a proponent submits a rule change request
- the Commission initiates 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).

You can find more information on the rule change process on our website.[90]

A.1 Cyber security is a growing and prevalent issue

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 NEM would be essential for maintaining Australia's growth and prosperity in an increasingly global economy.[91] The review recommended:[92]

> 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 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, the Critical Infrastructure Security Centre, 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

90 See our website for more information on the rule change process: https://www.aemc.gov.au/our-work/changing-energy-rules.
91 Independent review into the Future of the National Electricity Market, p.67.
92 Independent review into the Future of the National Electricity Market, p.69.

cyber security capability and maturity. Participants can use the results to inform and prioritise investment to improve cyber security posture.

In addition, the Security of Critical Infrastructure Act 2018 (the SoCI Act) outlines the legal obligations you have if you own, operate or have direct interests in critical infrastructure assets. It also outlines how the government can support you if an incident occurs that impacts your critical infrastructure asset. The SoCI Act was amended in 2021 to expand its scope to include the energy sector, acknowledging its vital role in national security. This resulted in more rigorous cyber security standards and incident reporting requirements for the responsible entity for a critical electricity and gas asset. Under the SoCI Act, AEMO is primarily responsible for maintaining the cyber security of its own assets.[93]

The AESCSF can be used by owners and operators to meet SoCI Act requirements.[94]

See table A.1 below for a description of Australian government bodies who play a role in cybersecurity.

Table A.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 cybersecurity, 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

93 Security of Critical Infrastructure Act 2018.

94 The AESCSF framework and resources, AEMO.

Body name	Description
	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 requires specific NEM and gas market entities, including AEMO, to manage their own critical infrastructure as it relates to cyber security. This rule change request does not place requirements on industry 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.[95] 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.[96]

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.[97] 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.[98] 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. This could also be performed by AEMO under the proposed ECGS cyber security functions.[99]

A.2 The process to date

On 29 January 2026, the Commission published a notice advising of the initiation of the rule making process and consultation in respect of the rule change request.[100] A consultation paper identifying specific issues for consultation was also published. Submissions closed on 26 February 2026. The Commission received five submissions as part of the first round of consultation. The Commission considered all issues raised by stakeholders in submissions. Issues raised in submissions are discussed and responded to throughout this draft rule determination.

95 Final determination, Cyber security roles and responsibilities.

96 Rule change request, p.3.

97 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.

98 '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.

99 Rule change request, p.1.

100 This notice was published under section 303 of the NGL.

B Legal requirements to make a rule

This appendix sets out the relevant legal requirements under the NGL for the Commission to make a draft rule determination.

B.1 Draft rule determination and draft rule

In accordance with section 308 of the NGL, the Commission has made this draft rule determination in relation to the rule proposed by the Honourable Chris Bowen MP, Minister for Climate Change and Energy.

The Commission's reasons for making this draft rule determination are set out in chapters two and three.

A copy of the draft rule is attached to and published with this draft determination. Its key features are described in chapter three.

B.2 Power to make the rule

The Commission is satisfied that the draft rule falls within the subject matter about which the Commission may make rules.

The draft rule falls within section 74 of the NGL as it relates to:

- regulating the activities of Registered participants, users, end users and other persons in a regulated gas market;[101] and
- rules made by the AEMC in accordance with this Law and the Regulations may confer functions or powers on, or leave any matter or thing to be decided or determined by AEMO.[102]

B.3 Commission's considerations

In assessing the rule change request the Commission considered:

- its powers under the NGL to make the draft rule
- the rule change request
- submissions received during first round consultation
- the Commission's analysis as to the ways in which the draft rule would or is likely to contribute to the achievement of the NGO
- the application of the draft rule to Western Australia.

There is no relevant Ministerial Council on Energy (MCE) statement of policy principles for this rule change request.[103]

The Commission may only make a rule that has effect with respect to an adoptive jurisdiction (relevantly, Victoria) if satisfied that the proposed rule is compatible with the proper performance of AEMO's declared system functions in that jurisdiction.[104] The draft gas rule is compatible with AEMO's declared system functions because it would not affect those functions.

---

101 Section 74(1)(a)(vi) of the NGL.

102 Section 74(3)(c)(i) of the NGL.

103 Under s. 33 of the NEL and s. 73 of the NGL the AEMC must have regard to any relevant MCE statement of policy principles in making a rule. The MCE is referenced in the AEMC's governing legislation and is a legally enduring body comprising the Federal, State and Territory Ministers responsible for energy.

104 Section 295(4) of the NGL.

B.4 Making gas rules in Western Australia

Under the *National Gas Access (WA) Act 2009* (WA Gas Act), a modified version of the NGL was adopted, known as the National Gas Access (Western Australia) Law (WA Gas Law). Under the WA Gas Law, the NGR applying in Western Australia is version 1 of the NGR, as amended by rules made by the South Australian Minister for Energy[105] and rules made by the AEMC in accordance with its rule making powers under section 74 and 313 of the WA Gas Law.[106] As a result, the Commission's power to make rules for Western Australia differs from its rule-making power under the NGL. 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. Therefore, the draft rule does not fall within the subject matters about which the Commission may make rules under the WA Gas Law. Additionally, the draft rule does not amend a Part of the NGR that applies in the Western Australia version of the NGR. Accordingly, the draft rule will not apply in Western Australia.

B.5 Civil penalty provisions and conduct provisions

The Commission cannot create new civil penalty provisions or conduct provisions. However, it may recommend to the energy ministers' that new or existing provisions of the NGR be classified as civil penalty provisions or conduct provisions.

The draft rule does not amend any clauses that are currently classified as civil penalty provisions or conduct provisions under the National Gas (South Australia) Regulations or National Gas (Victoria) (Declared System Provisions) Regulations. The Commission does not propose to recommend to energy ministers' or the Victorian Minister for Energy, Environment and Climate Change that any of the amendments made by the draft rule be classified as civil penalty provisions or conduct provisions.

105 The Statutes Amendment (National Energy Laws) (Binding Rate of Return Instrument) Act 2018 and the National Gas (South Australia (Pipelines Access—Arbitration) Amendment Act 2017.

106 See our website for further information at https://www.aemc.gov.au/regulation/energy-rules/national-gas-rules/western-australia.

Abbreviations and defined terms

ACSC	Australian Cyber Security Centre
AEMC	Australian Energy Market Commission
AEMO	Australian Energy Market Operator
AESCIRP	Australian Energy Sector Cyber Incident Response Plan
AESCSF	Australian Energy Sector Cyber Security Framework
AER	Australian Energy Regulator
ASD	Australian Signals Directorate
CTP	Capacity Trading Platform
Commission	See AEMC
DAA	Day Ahead Auction
DNSP	Distribution Network Service Provider
DTS	Declared Transmission System
DWGM	Declared Wholesale Gas Market
ECGS	East Coast Gas System
EV	Electric Vehicle
GPG	Gas Powered Generation
GSA	Gas Supply Agreements
GSH	Gas Supply Hub
GSOO	Gas Statement of Opportunities
GTA	Gas Transportation Agreements
ITGSP	Interruption to Gas Supply Process
MCE	Ministerial Council on Energy
NEM	National Electricity Market
NGL	National Gas Law
NGO	National Gas Objective
NGR	National Gas Rules
NT Act	*National Electricity (Northern Territory) (National Uniform Legislation) Act 2015*
Proponent	The individual / organisation who submitted the rule change request to the Commission
Rooftop PV	Rooftop photovoltaic
SoCI Act	*Security of Critical Infrastructure Act 2018*
STTM	Short Term Trading Market
TNSP	Transmission Network Service Provider