

Rule determination

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

Proponent

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

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

This work is copyright. The Copyright Act 1968 (Cth) permits fair dealing for study, research, news reporting, criticism and review. You may reproduce selected passages, tables or diagrams for these purposes provided you acknowledge the source.

Citation

To cite this document, please use the following:

AEMC, Gas cyber security roles and responsibilities for AEMO, Rule determination, 30 July 2026

Summary

- 1 The Australian Energy Market Commission (the Commission or AEMC) has decided to make a final 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 roles 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). This supports a strategic and coordinated approach to cyber security. This also harmonises AEMO's cyber security functions with its functions for electricity and provides certainty over AEMO's ability to recover fees and charges 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 Market¹ 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 cyber security roles and responsibilities for the electricity sector.

Our final rule formalises and embeds cyber security as part of AEMO's NGR roles and responsibilities

- 5 The final rule formalises and embeds cyber security as part of AEMO's roles and responsibilities in the NGR. Previously, the NGR did not address cyber security, so AEMO did not have a clear role or confirmed responsibilities in this area for the gas sector. The final rule clarifies this by establishing specific cyber security prevention and preparedness functions for AEMO across the ECGS.
- 6 Importantly, this rule does not place additional prescriptive 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 remain responsible for managing the cyber security of their own assets.

AEMO's cyber security functions are consistent across the energy sector

- 7 The final rule harmonises 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.
- 8 While AEMO performs some cyber security activities for the gas sector, the previous lack of defined functions in the NGR created inconsistencies and gaps in the application of AEMO's cyber

¹ [Independent Review into the Future of the National Electricity Market](#), June 2017, Dr Alan Finkle AO.

security preparedness and uplift measures across the energy sector.

- 9 The Commission recognises that the gas sector differs in operational characteristics, physical infrastructure, and governance arrangements from the electricity sector. However, the Commission considers that harmonising AEMO's gas cyber security functions with the electricity sector is appropriate because the functions are broad and flexible and do not impose specific activities on AEMO or operational obligations on gas sector participants.

AEMO can recover costs and have liability protection for cyber security activities

- 10 The final rule provides certainty on how AEMO recovers fees and charges for conducting cyber security activities under its functions. It also provides AEMO with immunity from liability in performing these functions.
- 11 This allows 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.
- 12 Additionally, market participants can confidently rely on AEMO to perform specific preparedness, uplift and responsiveness activities.

The final rule embeds four cyber security functions into the NGR

- 13 The final rule embeds 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 can plan for and coordinate the gas and energy sector-wide response to a cyber incident. AEMO continues to develop the Australian Energy Sector Cyber Incident Response Plan outlining how market, state and federal responses to a cyber incident are coordinated. In the event of a cyber incident, AEMO leads the implementation of the response in the manner set out by the plan. Importantly, this role does not give AEMO the authority or obligation to manage cyber incident responses for relevant entities. Extending this activity to the gas sector enables AEMO to have harmonised energy sector and jurisdiction wide roles and responsibilities.
 - **Function 2 - Supporting cyber preparedness and uplift:** AEMO continues in its stewardship of the Australian Energy Sector Cyber Security Framework.² It also organises testing and scenario training exercises to test the cyber resilience of the gas system, and participates in industry working groups and standards committees. It also operates in an advisory capacity to government working groups under Energy Ministers, and provides guidance and advice to industry in the form of written materials, digital tools and working groups. AEMO supporting uplift of cyber security does 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 may provide cyber security research and advice to governments. This function complements, rather than replaces, work undertaken by other cyber security bodies such as the Australian Cyber Security Centre (ACSC). This includes, for example, the preparation of specialist reports, independent advice, and detailed analysis to support effective and strategic decision-making in government and industry.

² The Australian Energy Sector Cyber Security Framework program provides a tool for assessing cyber security maturity across Australia's energy sector. It was developed through collaboration with industry and government.

- **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 acts as a distributor of cyber security information to industry. This includes facilitating the distribution of:
 - warnings of cyber vulnerabilities or threats, post-cyber incident reports, such as advice during or following any significant cyber incidents within the gas system, to provide insight into the cause, response, and lessons from the event for government and industry; and
 - preventative information technology patches in commonly used digital or operational technologies to prevent the spread of malicious activity.

- 14 AEMO recovers the costs of performing the functions through participant fees. AEMO estimates that the functions will likely cost between \$1.8 million and \$2.75 million per year depending on whether there are any cyber incidents. The Commission also understands that this estimate factors in the efficiency gains from the cyber security work already underway. Stakeholders generally agreed that the expected costs are justified, and that the benefits of the proposed solution outweigh the potential cost of a cyber incident.
- 15 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 improve cyber preparedness and response arrangements and reduce the likelihood and impacts of cyber incidents that could affect gas supply.
- 16 The final rule enables AEMO to recover cyber security fees and charges 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 benefit the same group of participants. This helps ensure AEMO's cyber security functions are adequately and sustainably funded.

The Commission has considered stakeholder feedback in making its decision

- 17 In submissions to the consultation paper and draft determination, stakeholders agreed that the NGR previously lacked clarity on cyber security and that it is problematic for AEMO to undertake cyber security activities without certainty. Stakeholders agreed that confirming and clarifying AEMO's cyber security roles and responsibilities in the NGR provides greater clarity and guidance to industry.³ Stakeholders also agreed that harmonising AEMO's gas cyber security functions with the functions it has for the electricity sector is important because it streamlines processes, avoids duplication, and reduces costs.⁴
- 18 The key stakeholder support that shaped the final rule included:
 - Acknowledgement that there was previously a lack of clarity on AEMO's cyber security roles and responsibilities in the NGR⁵
 - 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 risks⁶

3 Submissions to the [consultation paper](#): Alinta Energy, p.1; APA, p.2; APGA, p.1; Marissa McCauley, p.1; AGL, p.1. Submission to the draft determination: AGL, p.1.

4 Submissions to the [consultation paper](#): Alinta Energy, p.1; APGA, p.1; Marissa McCauley, p.2; AGL, p.1. Submissions to the draft determination: AGL, p.1; Alinta Energy, p.1.

5 Submissions to the [consultation paper](#): Alinta Energy, p.1; APA, p.2; APGA, p.1; Marissa McCauley, p.1; AGL, p.1.

6 Submissions to the [consultation paper](#): Alinta Energy, p.1; APGA, p.1; Marissa McCauley, p.2; AGL, p.1. Submissions to the draft determination: AGL, p.1; Alinta Energy, p.1.

- Certainty on cost recovery and liability protection for performing cyber security activities in the gas sector allows AEMO to properly establish and undertake cyber security activities on a well-defined and permanent basis for the gas sector⁷

However, stakeholders also raised minor concerns, including:

- Overall support for the four functions, however, while still supportive, one stakeholder questioned whether AEMO is best placed to distribute cyber security information, and considered gas participants should not bear the costs of AEMO providing research and advice. Another stakeholder suggested that participants should be required to undertake external assessments under the Australian Energy Sector Cyber Security Framework⁸
- That the benefits of the four functions outweigh the cost, however, one stakeholder considers the monetary costs of AEMO providing research and advice do not outweigh the benefits of it providing this function, and argues that gas participants should not bear the costs of this function.⁹

The Commission has considered these issues against the assessment criteria under the National Gas Objective (NGO) 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. It could also have broader flow on effects across the energy sector. 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.
- The ability to recover fees and charges and have liability protection enables 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 enables it to distribute valuable research and advice on cyber security risks to government and industry. See section 3.2.3.
- It is out of scope of the rule change request to mandate external cyber security maturity assessments under the Australian Energy Sector Cyber Security Framework. The functions are intentionally designed to be facilitative, without imposing mandatory obligations on participants. See section 3.2.2
- 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.

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

- 19 The Commission has considered the NGO¹⁰ and the issues raised in the rule change request and assessed the final rule against three assessment criteria outlined below. We gathered and analysed stakeholder feedback in relation to these criteria.

⁷ Submission to the [consultation paper](#): Marissa McCauley, p.2.

⁸ Submissions to the draft determination: AGL, pp.1-2; Alinta Energy, p.1.

⁹ Submissions to the draft determination: AGL, pp.1-2; Alinta Energy, p.1.

¹⁰ Section 23 of the NGL.

20 The final rule contributes to achieving 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 final rule promotes safety, security, and reliability outcomes which benefit consumers. The final rule better enables 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 helps 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 final rule aligns with good regulatory practice by seeking to improve predictability, stability, and transparency of cyber security in an increasingly digitised and interconnected gas sector. The final 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 has predictability and stability because by introducing these functions under the NGR, it can recover fees and charges and have liability protection under the NGL when performing these functions. This allows for resourcing certainty to properly establish and undertake cyber security activities on a more well-defined and permanent basis. This enables AEMO to continue and scale up its cyber security activities. Additionally, market participants can confidently rely on AEMO to perform specific preparedness, uplift and responsiveness activities in the gas sector, and consistently throughout the energy system. Under the final rule, AEMO is not unduly limited in the cyber security activities it can undertake. Additionally, there are no overly prescriptive requirements for industry because AEMO does not have the ability to impose mandatory obligations on participants. See section 2.3.2.
- **Taking into account implementation considerations:** the final 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 will become more transparent and simplified for industry participants as the final rule formally establishes functions for AEMO in the gas sector to support consistent cyber security coordination across the energy sector. The impact on AEMO and other participants is manageable because AEMO is already performing these activities in the electricity sector and for the gas sector, meaning that existing processes can be built on. See section 2.3.3.

The final rule commences on 30 July 2026

- 21 The final rule commences on publication of this determination on 30 July 2026. Immediate commencement is possible because AEMO is already performing these functions in the electricity sector and some activities under the functions without having a cyber security role established in the NGR, for the gas sector.
- 22 An immediate commencement date allows AEMO to recover fees and charges and provides protection from liability for the cyber security functions as soon as possible. Additionally, this does not delay the process for AEMO to be able to recover costs for the performance or exercise of these cyber security functions. This way, benefits for consumers will be realised more quickly because AEMO is only able to recover costs and sufficiently commit resources to these four functions from the commencement of the final rule.

- 23 AEMO has indicated that it does not need to make any updates to procedures, guidelines, or settlement systems before the final rule takes effect in order to be compliant with the rule.

Contents

1	The Commission has made a final determination	1
1.1	Our final rule confirms and clarifies AEMO's gas sector roles and responsibilities for cyber security	1
1.2	Stakeholder input and support for AEMO's cyber security role helped shape our final rule	2
1.3	Our final rule supports a strategic and coordinated approach to cyber security	3
2	The rule contributes to the energy objectives	5
2.1	The Commission must act in the long-term interests of gas consumers	5
2.2	We have considered how the rule applies in Western Australia	5
2.3	Our final rule to clarify and confirm AEMO's cyber security functions in the gas sector contributes to the achievement of the NGR	6
3	Our final rule confirms and clarifies AEMO's cyber security functions in the NGR	11
3.1	The final rule formalises AEMO's cyber security role in the gas sector	11
3.2	The final rule embeds four functions into the NGR	13
3.3	The four functions are likely to significantly reduce cyber security risks and costs	18
3.4	The rule commences on 30 July 2026	20

Appendices

A	Rule making process and background to the rule change request	21
A.1	Cyber security governance in Australia	21
A.2	Previously the NGR did not explicitly address AEMO's cyber security role	23
A.3	Gas and electricity sector differences reinforce the need for formalised gas cyber security functions	25
A.4	The process to date	29
B	Legal requirements to make a rule	30
B.1	Final rule determination and final rule	30
B.2	Power to make the rule	30
B.3	Commission's considerations	30
B.4	Making gas rules in Western Australia	31
B.5	Civil penalty provisions and conduct provisions	31

Abbreviations and defined terms	32
--	-----------

Tables

Table 3.1:	Structure of gas participant fees for the GSOO	19
Table A.1:	Australian government bodies playing a role in cyber security	22

Figures

Figure 1.1:	Timeline of cyber security reforms and frameworks	4
Figure A.1:	The market differences between the gas sector and electricity sector	26
Figure A.2:	The physical and facility differences between the gas sector and electricity sector	27
Figure A.3:	The governance differences between the gas sector and electricity sector	28

1 The Commission has made a final determination

The Australian Energy Market Commission (the Commission or AEMC) has decided to make a final 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 final rule and rationale.

- **Section 1.1** outlines the final determination and final rule, which makes the rule proposed by the Minister
- **Section 1.2** outlines the input from stakeholders that shaped our final determination
- **Section 1.3** explains how our determination supports a strategic and coordinated approach to cyber security

1.1 Our final rule confirms and clarifies AEMO's gas sector roles and responsibilities for cyber security

The final rule is consistent with the proponent's rule change request, see appendix A, and addresses the previous lack of clarity around AEMO's cyber security roles and responsibilities in the gas sector by confirming AEMO's cyber security functions in the NGR.

In doing so, this also harmonises 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.

Importantly, the final rule allows 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 National Gas Law (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 final rule inserts four functions for AEMO in the NGR:

- **Function 1 - Cyber security incident coordinator:** AEMO can plan for and coordinate the gas and energy sector wide response to a cyber incident. AEMO continues to develop the Australian Energy Sector Cyber Incident Response Plan outlining how market, state and federal responses to a cyber incident are coordinated. In the event of a cyber incident, AEMO leads the implementation of the response in the manner set out by the plan.
- **Function 2 - Supporting cyber preparedness and uplift:** AEMO continues in its stewardship of the Australian Energy Sector Cyber Security Framework. It also organises testing and scenario training exercises to test the cyber resilience of the gas system, participates in industry working groups and standards committees, and operates 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 is able to provide cyber security research and advice to governments. This could 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 acts as a distributor of cyber security information to industry.

These four functions are facilitative and flexible and do not enable AEMO to impose mandatory obligations on market participants. See section 3.2 for more information on how the functions will operate.

1.2 Stakeholder input and support for AEMO's cyber security role helped shape our final rule

In submissions to the consultation paper and draft determination, stakeholders agreed that the NGR previously lacked clarity on cyber security and that it is problematic for AEMO to undertake cyber security tasks without certainty.¹¹

Stakeholders agreed that confirming and clarifying AEMO's cyber security roles and responsibilities in the NGR provides greater clarity and guidance to industry.¹² Stakeholders also agreed that harmonising AEMO's gas cyber security functions with the functions it has for the electricity sector is important because it streamlines processes, avoids duplication, and reduces costs.¹³

The key stakeholder support that shaped the final rule included:

- Acknowledgement that there was previously a lack of clarity on AEMO's cyber security roles and responsibilities in the NGR¹⁴
- Support for harmonising AEMO's cyber security functions across the electricity and gas sectors to help ensure a coordinated and strategic approach to efficiently manage cyber security risks¹⁵
- Certainty on cost recovery and liability protection for performing cyber security activities in the gas sector allows AEMO to properly establish and undertake cyber security activities on a well-defined and permanent basis for the gas sector.¹⁶

However, stakeholders also raised minor concerns, including:

- Overall support for the four functions, however, while still supportive, one stakeholder questioned whether AEMO is best placed to distribute cyber security information, and considered gas participants should not bear the costs of AEMO providing research and advice.¹⁷ Another stakeholder suggested that participants should be required to undertake external assessments under the Australian Energy Sector Cyber Security Framework¹⁸
- That the benefits of the four functions outweigh the cost, however, as detailed above, one stakeholder considers the monetary costs of AEMO providing research and advice do not

11 Submissions to the [consultation paper](#): Alinta Energy, p.1; APA, p.2; APGA, p.1; Marissa McCauley, p.1; AGL, p.1. Submission to the determination: AGL, p.1.

12 Submissions to the [consultation paper](#): Alinta Energy, p.1; APA, p.2; APGA, p.1; Marissa McCauley, p.1; AGL, p.1. Submission to the draft determination: AGL, p.1.

13 Submissions to the [consultation paper](#): Alinta Energy, p.1; APGA, p.1; Marissa McCauley, p.2; AGL, p.1. Submissions to the draft determination: AGL, p.1; Alinta Energy, p.1.

14 Submissions to the [consultation paper](#): Alinta Energy, p.1; APA, p.2; APGA, p.1; Marissa McCauley, p.1; AGL, p.1.

15 Submissions to the [consultation paper](#): Alinta Energy, p.1; APGA, p.1; Marissa McCauley, p.2; AGL, p.1. Submissions to the draft determination: AGL, p.1; Alinta Energy, p.1.

16 Submission to the [consultation paper](#): Marissa McCauley, p.2.

17 Submission to the draft determination: AGL, pp.1-2.

18 Submissions to the draft determination: Alinta Energy, p.1.

outweigh the benefits of it providing this function, and argues that gas participants should not bear the costs of this function.¹⁹

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. It could also have broader flow on effects across the energy sector. 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.
- The ability to recover fees and charges and have liability protection enables 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 enables it to distribute valuable research and advice on cyber security risks to government and industry. See section 3.2.3.
- It is out of scope of the rule change request to mandate external cyber security maturity assessments under the AESCSF. The functions are intentionally designed to be facilitative, without imposing mandatory obligations on participants. See section 3.2.2
- 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 information on how the four cyber security functions operate.

1.3 Our final rule supports a strategic and coordinated approach to cyber security

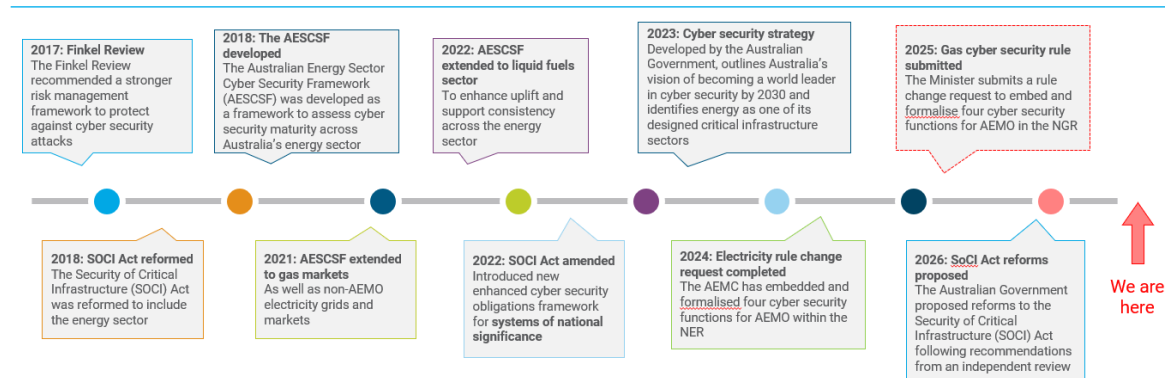
Cyber security is of critical importance in Australia. While it impacts all sectors, it is a particularly prominent issue in energy security given the increasing digitisation and connectivity between the gas and electricity systems. Digitisation can bring a range of benefits, including new opportunities 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.

¹⁹ Submissions to the draft determination: AGL, pp.1-2; Alinta Energy, p.1.

Figure 1.1: Timeline of cyber security reforms and frameworks



Source: AEMC.

The Independent Review into the Future of the National Electricity Market,²⁰ 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, with this rule change seeking to do the same for the gas sector.

The Commission also notes that the Australian Government is currently undertaking consultation on reforms to the Security of Critical Infrastructure Act 2018 (SoCI Act) in response to recommendations provided by an Independent Review.²¹ The proposed reforms seek to reduce unnecessary complexity and regulatory duplication, modernise and refine sector and asset coverage, clarify legislative expectations, assurance mechanisms, and governance arrangements, and better assess whether security and resilience outcomes are being achieved.²²

The Commission considers that the proposed reforms to the SoCI Act would complement the cyber security activities AEMO performs for the gas sector under the final rule. This is because the SoCI Act focus on the obligations of critical infrastructure owners and operators to manage the cyber security of their own assets, while the Commission's final rule clarifies AEMO's sector-wide preparedness and coordinator cyber security roles and responsibilities. Together, these frameworks support both individual asset resilience and a coordinated approach to cyber security risks across the gas and energy sectors. The Commission acknowledges that the consultation period for these proposed reforms closes on 31 July 2026.

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.

²⁰ [Independent Review into the Future of the National Electricity Market](#).

²¹ [Streamlining and modernising the Security of Critical Infrastructure Act, consultation paper](#). Independent Review into the Security of Critical Infrastructure Act 2018, Dr Jill Slay AM, 31 January 2026.

²² [Streamlining and modernising the Security of Critical Infrastructure Act, consultation paper](#).

2 The rule contributes to the energy objectives

This chapter sets out how our final rule promotes the National Gas Objective (NGO). It explains how our final 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 final rule.
- **Section 2.2** considers how the rule will apply in Western Australia.
- **Section 2.3** explains how our final 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.²³ For this rule change, the relevant energy objective is the NGO.

The NGO is:²⁴

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.²⁵

There are also a number of relevant legal requirements for the Commission to consider under the NGL to make a final determination. These are set out in appendix B.

2.2 We have considered how the rule applies in Western Australia

In developing the final rule, the Commission has considered how the rule should apply in Western Australia according to the following questions:

- **Does the AEMC have a relevant rule-making power?** No, the final 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 final rule creates a new Part in the NGR.

Therefore, the final rule will not apply in Western Australia. See appendix B for more detail on the legal requirements for this decision.

²³ 291(1) of the NGL.

²⁴ Section 23 of the NGL.

²⁵ Section 72A(5) of the NGL.

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

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

For this rule change process, we have applied the following **three** criteria to assess whether the final rule better contributes to achieving the NGO compared to the status quo:

- **Safety, security and reliability:** we have considered whether confirming and clarifying AEMO's cyber security functions in the gas sector will 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 solution will 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 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, for impacts within the scope of the NGO. Our reasons for choosing these criteria are set out in section 4.2 of the [consultation paper](#).

The Commission has incorporated stakeholder feedback into its analysis and is satisfied that the assessment criteria are fit for purpose.

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

2.3.1 The final rule promotes safety, security, and reliability

The Commission considers that embedding and formalising AEMO's functions in the NGR and harmonising these with the electricity sector promotes safety, security, and reliability outcomes by securing the long-term supply of gas, which also benefits 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. In feedback to the draft determination, AGL explicitly stated that digitisation of the energy system and the interconnected nature of infrastructure networks expose the gas sector to a heightened risk of cyber security incidents.²⁶

The final rule promotes 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 helps ensure the secure supply of gas to consumers in the long term and supports the achievement of safety and security outcomes.

²⁶ Submission to the draft determination: AGL, p.1.

Prior to this rule, the lack of clarity on AEMO's cyber security roles and responsibilities in the NGR meant that AEMO was unable to recover fees and charges and had no liability protection if undertaking cyber security activities in the gas sector. This created ongoing security risks by contributing 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 final rule outweigh the potential costs of leaving AEMO's roles and responsibilities for cyber security unclear. See section 3.3 for more information on the benefits of the final rule outweighing the costs.

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 final rule 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.

AEMO estimates the costs of the functions to be in the range of \$1.8 million to \$2.75 million per year. The Commission understands that cost recovery for these functions will likely be on the same basis as the Gas Statement of Opportunities (GSOO) fees because cyber security fees will benefit the same group of participants. AGL supported the clarification of AEMO's cost recovery process and the projected costs of the functions.²⁷ In feedback to the [consultation paper](#), stakeholders explicitly agreed that the benefits of clarifying AEMO's cyber security functions in the gas sector outweigh the potential costs of a cyber security incident.²⁸ See section 3.3 of the draft determination for more information and stakeholder feedback on the forecast costs of the four functions and the cost recovery process.

The Commission has incorporated stakeholder feedback into its analysis and is of the view that by confirming AEMO's four cyber functions in the NGR, the final rule supports AEMO's ability to manage and operate a safe, secure, and reliable system at a time when cyber security concerns are increasingly prevalent.

2.3.2 The final rule is aligned to principles of good regulatory practice

The Commission considers that the final rule aligns with principles of good regulatory practice because it improves the predictability, stability and transparency of cyber security in an increasingly digitised and interconnected energy sector. The final rule supports broader cyber security reforms to support the harmonisation of AEMO's role across the energy sector and avoid unnecessary duplication of cyber security activities.

By introducing these provisions relating to cyber security functions into the NGR, AEMO is able to recover fees and charges in the performance or exercise of its functions and has immunity from liability. This provides predictability and stability for AEMO and participants because it allows for resourcing certainty to properly establish and undertake cyber security activities on a more well-

²⁷ Submission to the draft determination: AGL, p.1.

²⁸ Submissions to the [consultation paper](#): Alinta Energy, p.2; APGA, p.1; Marissa McCauley, p.2.

defined and permanent basis. Certainty around cost recovery and liability protection also allows AEMO to continue and scale up cyber security activities. Additionally, market participants are able to confidently rely on AEMO to perform specific preparedness, uplift, and responsiveness activities in the gas sector, and consistently throughout the energy system. Importantly, the final rule does not give AEMO powers to impose mandatory obligations on participants.

The final rule also provides AEMO with sufficient flexibility by not limiting the activities it may undertake in performing its cyber security functions. Rather than prescribing specific activities, the final rule allows AEMO to adapt its approach as cyber risks and industry needs evolve, including through activities such as information distribution, preparedness initiatives, and sector-wide cyber security uplift activities. This flexibility supports the ongoing effectiveness of AEMO's functions.

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

Cyber security is a particularly prominent issue in energy security given the gas sector's increasing digitisation, connectivity, and interconnection with the electricity system. By including the four functions for AEMO in the NGR, the final 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.²⁹ While AEMO previously performed some of the activities for the gas sector under the functions, such as overseeing the Australian Energy Sector Cyber Security Framework, because of the lack of certainty under the statutory framework regarding their ability to cost recover and protection from liability, AEMO was not able to scale up and adapt to circumstances as needed.

Further, while the Commission acknowledges the differences between the gas and electricity sector, the Commission considers that harmonising AEMO's cyber security functions with its functions for the electricity sector aligns with principles of good regulatory practice 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 promotes predictability and stability in the regulatory framework, simplicity and transparency for stakeholders, and interacts constructively with the broader direction of cyber security reform in the energy sector. See section 3.1.1 and appendix A for more information.

Importantly, the four functions complement, rather than duplicate, the role of other agencies such as the Australian Cyber Security Centre (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. Stakeholders broadly agree that the four functions are fit for purpose, with AGL explicitly agreeing that functions one and two should be embedded in the NGR. However, AGL raised minor concerns regarding AEMO's role in distributing cyber security information to industry and AEMO recovering the costs of providing research and advice from gas participants.³⁰ See section 3.2 for more information on stakeholder feedback to AEMO's four functions.

²⁹ Rule change request, p.6; [Independent Review into the Future of the National Electricity Market](#), p.67.

³⁰ Submissions to the draft determination: AGL, pp.1-2 and Alinta Energy, p.1.

The Commission has incorporated stakeholder feedback into its analysis and is of the view that confirming and clarifying AEMO's functions in the NGR and harmonising these with the electricity sector aligns with principles of good regulatory practice.

2.3.3 The final rule accounts for implementation considerations

The Commission considers that by embedding and formalising AEMO's cyber functions in the NGR, the final rule takes into account implementation considerations including cost implications, governance arrangements, timing impacts, and relevant jurisdictional conditions.

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 an incident could have been prevented by clarifying AEMO's cyber security functions and upscaling preparedness activities. The Commission therefore considers that the costs are justified because much of this work is already underway and benefiting participants, for example, through AEMO's cyber security functions in the electricity sector.³¹

The final rule will also support participants to improve cyber preparedness and maturity without giving AEMO the ability to impose additional mandatory obligations on market participants. This will help to reduce associated costs and provide confidence that benefits will be realised and AEMO's cost estimates are likely to be accurate. See section 3.3 for more information on the benefits of the four functions outweighing the costs.

The Commission considers that cyber security governance will become more transparent and simplified for industry participants because the final rule establishes functions for AEMO to support consistent cyber security coordination across the energy sector.

Further, the cyber security functions in the final rule build on the activities that AEMO is already undertaking. Accordingly, the Commission considers it appropriate for the final rule to take effect immediately, with a commencement date of 30 July 2026. See section 3.4 for more detail on the implementation plan.

The impact on AEMO and other participants will be manageable because AEMO is already performing these activities in the electricity sector and for the gas sector, meaning that existing processes will be built on. While the final rule establishes four functions, AEMO is not limited in its activities under the functions and is well placed to adapt to the cyber security needs of the gas sector. AEMO's four functions assist participants in managing cyber security risks because they support cyber preparedness and uplift, examine cyber risks and provide advice, and facilitate the distribution of critical information, which will help participants manage cyber security risks before they eventuate into an incident. See section 3.2 for more information on how AEMO's cyber security functions will operate.

Additionally, the final 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 National Electricity Market (NEM). In addition to the SoCI Act, which places an obligation on AEMO and entities to look after their own assets from a national security perspective, clarifying and confirming the functions in the final rule ensures that sector-wide risks between participants and AEMO are being addressed. AGL noted that embedding and formalising AEMO's gas sector cyber security functions is especially important given the increasing digitisation and interconnected nature of infrastructure

31 [Cyber security roles and responsibilities](#).

networks.³² In feedback to the [consultation paper](#), all stakeholders supported the clarification of AEMO's cyber security roles and responsibilities in the gas sector.³³

The Commission has incorporated stakeholder feedback into its analysis and considers that by embedding and formalising AEMO's cyber functions in the NGR, the final rule adequately accounts for implementation considerations.

³² Submission to the draft determination: AGL, p.1.

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

3 Our final rule confirms and clarifies AEMO's cyber security functions in the NGR

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

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

3.1 The final rule formalises AEMO's cyber security role in the gas sector

Box 1: AEMO's cyber security roles and responsibilities in the gas sector

The final rule:

- formalises and embeds cyber security as part of AEMO's roles and responsibilities in the NGR across the ECGS
- harmonises 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
- provides more certainty on cost recovery and liability protection for AEMO in performing these functions. This allows AEMO to properly establish and undertake cyber security activities on a well-defined and permanent basis for the gas sector.

The final rule formalises and embeds cyber security as part of AEMO's roles and responsibilities in the NGR across the ECGS.³⁴

Prior to this final rule, the NGR did not address cyber security, so AEMO did not have a clear role or confirmed responsibilities in this area for the gas sector. The final rule clarifies this by establishing four cyber security prevention and preparedness functions for AEMO.

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.³⁵ Since then, cyber security measures across the energy sector have been progressively introduced, including clarifying AEMO's roles and responsibilities for the electricity sector.³⁶

The final rule harmonises AEMO's gas sector cyber security functions with its electricity sector functions, therefore allowing AEMO to deliver a strategic and coordinated approach to cyber security across the energy sector. See section 3.1.1 below.

Importantly, the final rule does not place additional requirements on gas participants but rather, clarifies AEMO's role in providing prevention and preparedness functions to facilitate cyber

³⁴ Rule, 716.

³⁵ [Independent Review into the Future of the National Electricity Market](#), p.67.

³⁶ [Cyber security roles and responsibilities](#).

security measures across the gas sector. Infrastructure owners remain responsible for managing the cyber security of their own assets.

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

In feedback to the draft determination, AGL noted that embedding and formalising AEMO's gas sector cyber security functions is especially important given the increasing digitisation and interconnected nature of infrastructure networks.³⁷

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 are consistent across the energy sector

The final rule harmonises AEMO's cyber security roles and responsibilities across the energy sector by replicating AEMO's electricity cyber security functions in the gas sector.³⁸ This supports a coordinated and strategic approach to cyber security by addressing inconsistencies and gaps in the application of AEMO's cyber security preparedness and uplift measures across the energy sector.

Stakeholders explicitly agreed that it is beneficial to harmonise AEMO's cyber security functions across the gas and electricity sector, and expressed support for a consistent approach to AEMO's cyber security functions across the energy sector.³⁹ Specifically, Alinta Energy considered that harmonising AEMO's gas sector cyber security functions with the electricity sector will reduce duplicated compliance efforts and costs.⁴⁰

The Commission considers that harmonising AEMO's functions across the gas and electricity sector will support a consistent and coordinated approach to cyber security. At the same time, it allows AEMO to retain the flexibility to determine the specific activities it undertakes. It is important that AEMO has the flexibility to adapt these functions as it sees fit when performing preparedness and uplift activities across the energy sector, without unduly limiting the activities it can perform if new risks emerge. See section 3.2 for more information on how the functions work.

Importantly, the Commission recognises that the gas sector differs from the electricity sector. However, the Commission maintains that harmonising AEMO's gas cyber security functions with its functions in 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:

- has flexibility to apply the four functions in a way that is tailored to gas market arrangements across the ECGS
- where appropriate, has 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.

³⁷ Submission to the draft determination: AGL, p.1.

³⁸ Rule, 716.

³⁹ Submissions to the draft determination: AGL, p.1; Alinta Energy, p.1.

⁴⁰ Submission to the draft determination: Alinta Energy, p.1.

See section 3.1.1 of the [draft determination](#) for more information, and appendix A for a comparative analysis of the gas and electricity sectors.

3.1.2 **AEMO is able to recover costs and has immunity from liability for cyber security activities in the gas sector**

By clarifying and confirming AEMO's cyber security functions in the NGR, the final rule provides certainty on how AEMO recovers fees and charges for conducting cyber security activities under its functions. It also provides AEMO with immunity from liability when conducting cyber security functions in the gas sector. This allows AEMO to properly establish and undertake cyber security activities on a well-defined and permanent basis for the gas sector. This means market participants can now confidently rely on AEMO to perform specific preparedness, uplift and responsiveness activities.

In feedback to the [consultation paper](#), one stakeholder explicitly agreed that AEMO should be able to recover fees and charges and have liability protection for conducting cyber security activities in the gas sector.⁴¹ Stakeholders provided no further comments on this matter in feedback to the draft determination.

As such, the Commission is of the view that providing certainty around recovering fees and charges and liability protection allows 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. Market participants will also be able to confidently rely on AEMO to perform specific preparedness, uplift and responsiveness activities. Importantly, the final rule does 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.

3.2 The final rule embeds four functions into the NGR

Box 2: Cyber security functions in the NGR

The final rule establishes four new 'cyber security functions' for 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 as proposed in the draft rule. However, one stakeholder questioned AEMO's suitability to distribute cyber security information and raised concerns about cost recovery arrangements for AEMO providing research and advice. Another stakeholder recommended external cyber security maturity assessments should be required under the Australian Energy Sector Cyber Security Framework.

The Commission's final determination is that the four functions are fit for purpose, and will deliver benefits to gas consumers and participants. Following stakeholder feedback, we consider that AEMO is the appropriate body to carry out these functions, noting AEMO's unique position and expertise in the gas sector. We also consider that mandating external cyber security maturity

⁴¹ Submission to the [consultation paper](#): Marissa McCauley, p.2.

assessments is outside the scope of the rule because AEMO's functions are intended to be facilitative, without imposing mandatory obligations on participants. Making the final rule to embed and formalise these functions allows 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 plans for and coordinates the response of relevant entities to a cyber incident that could adversely affect the secure operation of the ECGS. The final rule ensures AEMO is adequately resourced and equipped to undertake this function using reasonable endeavours.⁴² 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 are coordinated.

If a cyber incident occurs, the Australian Energy Sector Cyber Incident Response Plan sets out the key actions involved in a response, including an organisational response, coordinated gas cyber response, and gas operational emergency management responses. The plan establishes unique roles for AEMO including:

- 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.

AGL expressed explicit support for AEMO's cyber incident coordinator function.⁴³

The Commission has incorporated stakeholder feedback and the rule change request into its analysis and is of the view that clarifying AEMO's coordinating role is especially important for the gas sector since AEMO is not the system operator across the board, meaning there is a need to ensure AEMO's role is clearly understood by participants. This also helps 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 will 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 requires AEMO to continue to help industry participants improve their cyber security preparedness and maturity.⁴⁴ This function may include, but is not limited to, the following:

- **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 may also include continuing to oversee the Australian Energy Sector Cyber Security Framework self-assessments for the gas industry.
- **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

⁴² Final rule, 716(1).

⁴³ Submission to the draft determination: AGL, p.1.

⁴⁴ Rule, 716(2).

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.

AEMO is well placed to support cyber security uplift in the energy industry due to its expertise and unique position in the gas sector. Improving participants' preparedness for a cyber incident helps mitigate the risk of such incidents and flow on consequences for consumers.

AGL explicitly agreed that AEMO's cyber preparedness and uplift function should be embedded in the NGR.⁴⁵ However, while supportive, Alinta Energy recommended that as part of AEMO's ongoing stewardship of the Australian Energy Sector Cyber Security Framework, AEMO should require gas sector participants to undertake external assessments of their cyber security maturity. Alinta Energy considers this would support a more consistent assessment of cyber security maturity among participants than the self-assessments alone.⁴⁶

The Commission is of the view that mandating external assessments under the Australian Energy Sector Cyber Security Framework is out of scope because the functions are intentionally designed to formalise AEMO's facilitative role in supporting cyber security preparedness and uplift, without imposing mandatory obligations on market participants. The Commission also notes that introducing a requirement for external assessments could impose additional compliance costs on participants. However, the Commission notes there is nothing preventing AEMO from considering these external assessments in its administration of the Australian Energy Sector Cyber Security Framework.

The Commission has incorporated stakeholder feedback and the rule change request into its analysis and is of the view that AEMO is well placed to support cyber security preparedness and uplift for the gas sector. While AEMO is not a system operator in the same way it is in the NEM, unlike other participants, it plays a broader role in the ECGS by undertaking market operations, operating the Declared Transmission System (DTS) and the Gas Bulletin Board, and providing gas planning and forecasting reports. This gives AEMO a system wide view 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 will benefit from AEMO having clear authority to provide guidance, tools, testing, and training for cyber security uplift and preparedness activities where appropriate.

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

Under this function, AEMO draws 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. This function complements, rather than replaces, work undertaken by other cyber security bodies such as the ACSC.

This research and advice function contributes towards enhancing cyber security maturity for AEMO, governments, and industry participants. By further enabling AEMO to build up and share its

⁴⁵ Submission to the draft determination: AGL, p.1.

⁴⁶ Submission to the draft determination: Alinta Energy, p.1.

cyber security expertise, this function helps 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:

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

This allows AEMO to initiate advice when it identifies an issue and 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 is advisory only and does not result in AEMO performing any regulatory responsibilities beyond its existing mandated scope and ability.

Stakeholders broadly supported this function. However, AGL questioned whether AEMO is best placed to distribute critical cyber security information to the gas sector, noting the risk of duplicated and inconsistent information.⁴⁷ AGL also considered that gas sector participants should not bear the costs of function three because research and advice provided to government does not directly benefit those participants. However, AGL also expressed preferential support for a consistent regulatory approach across the gas and electricity sector, thereby supporting the intent of this function to operate as proposed.⁴⁸

The Commission has incorporated stakeholder feedback and the rule change request into its analysis and considers that AEMO's unique position and expertise in the gas sector means it is well placed to distribute critical cyber security information to government and industry, especially for smaller gas sector participants who may not have the resources to access other information distribution channels. The Commission also notes that the final rule does not make AEMO the sole provider of cyber security advice and does not replace the information distributed by other channels through which governments and industry may seek advice. Advice provided by AEMO is not intended to duplicate information provided by other agencies, such as the ACSC, because AEMO holds unique operational knowledge and oversight of the ECGS. AEMO also has the flexibility to seek input from other bodies or from industry when carrying out this function.

Additionally, the Commission considers it is appropriate that gas sector participants bear the costs of AEMO providing research and advice. This function benefits participants by supporting improved preparedness and risk management outcomes, even where the outputs are not always delivered directly to individual entities.

Enabling AEMO to provide the government with specialist reports, independent advice, and detailed analysis, facilitates effective and strategic decision making, which supports risk management planning and can potentially mitigate the impacts of a cyber security incident. The Commission considers that limiting or separating funding for research and advisory functions

⁴⁷ Submission to the [consultation paper](#): AGL, p.1. Submission to the [cyber security roles and responsibilities draft determination](#): AGL, p.2.

⁴⁸ Submission to the draft determination: AGL, p.1.

could undermine AEMO's ability to deliver a coordinated and effective cyber security capability across the energy sector. See section 3.3 for more information on AEMO's cost recovery process.

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 will act as a distributor of cyber security information to industry. Under the final rule, this includes facilitating the distribution of:⁴⁹

- information with respect to cyber security vulnerabilities or threats
- post-cyber incident reports, such as advice during or following any significant cyber incident 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 either 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 on a wide range of matters, including security-related events, market directions, suspensions and interventions, and general notices.⁵⁰

As noted above, AGL questioned the value of AEMO distributing cyber threat information, noting the risk of AEMO distributing duplicated or inconsistent cyber security information. However, AGL also expressed preferential support for a consistent regulatory approach across the gas and electricity sector, thereby supporting the intent of this function to operate as proposed.⁵¹ See section 3.2.3 for more information on AGL's feedback.

The Commission has incorporated this feedback and the rule change request into its analysis and believes that the benefits of this function include:

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

The Commission understands that some industry participants may receive cyber security information from sources, such as the Australian Signals Directorate (ASD). However, the Commission notes that the dissemination of information by AEMO is likely to be more useful to smaller participants who 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. Additionally, as detailed in section 3.2.3, the Commission considers that AEMO's unique role and expertise in the gas sector make it the appropriate body to collect and distribute critical cyber security information to the gas sector.

⁴⁹ Rule, 716(6).

⁵⁰ Rule change request, pp.6-7.

⁵¹ Submission to the draft determination: AGL, p.1.

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 cost of the four functions is low compared to the benefits of reducing cyber security risks in the gas sector. More specifically, the cyber security functions improve cyber preparedness and response arrangements, and reduce the likelihood and impacts of cyber incidents that could affect gas supply.

AEMO is able to 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 benefits of the four functions outweigh the potential cost of a cyber incident. However, AGL considers the cost of research and advice should not be borne by gas sector participants, given AEMO's activities under this function will not directly benefit those participants.

The final rule allows 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 GSOO fees because cyber security benefits the same group of participants. This helps ensure the cyber security functions are adequately and sustainably funded.

As outlined in section 3.1.2, the final rule provides certainty on how AEMO recovers fees and charges for conducting the four proposed functions.⁵²

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.⁵³ 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 NEM⁵⁴
- 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 AEMO is able to recover fees and charges provides stability and predictability to industry. See section 3.1.2 for more information on AEMO's cost recovery and section 2.3.2 for more information on how AEMO's cyber security functions provide predictability and stability to the gas sector. This allows the functions to be sufficiently resourced and could, for example, enable long-term initiatives, investment in essential resources, and upskill personnel.

In feedback to the draft determination, stakeholders broadly agreed that the benefits of the four functions outweigh the costs.⁵⁵ That is, the expected costs are low compared to the potential

⁵² Rule 135CC and 135CF.

⁵³ Rule change request, p.9.

⁵⁴ 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.

⁵⁵ Submissions to the draft determination: AGL, pp.1-2; Alinta Energy, p.1.

benefits in avoiding or mitigating the impact of cyber security incidents. However, while noting that AEMO's cost recovery process is now clear, as discussed above, AGL considered that gas sector participants should not bear the costs of AEMO providing research and advice to government because this function does not directly benefit participants. AGL recommends that these costs should instead be covered by government. However, AGL also expressed preferential support for a harmonised approach across the gas and electricity sector.⁵⁶ Alinta Energy also reiterated that this approach should focus on limiting unnecessary scope and reducing costs where possible.⁵⁷

The Commission considers that AEMO providing research and advice supports sector-wide cyber security preparedness and risk management. For this reason, the Commission considers that gas sector participants are best placed to cover the costs of AEMO providing this function. These cost recovery arrangements are also consistent with the electricity framework and help ensure AEMO can deliver an effective cyber security capability, rather than fragmenting complementary functions through separate funding arrangements.⁵⁸

The Commission has incorporated stakeholder feedback and the rule change request into its analysis and is of the view that the benefits of embedding and formalising AEMO's cyber security functions for the gas sector outweigh the cost of performing the proposed functions. See section 3.3 of the draft determination for more information on the benefits of the four functions.⁵⁹

AEMO will recover costs from gas participants

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

- Declared Wholesale Gas Market (DWGM)
- Short Term Trading Market (STTM)
- Retail markets (Victoria, New South Wales/Australian Capital Territory, Queensland, South Australia)
- Gas Bulletin Board
- GS00
- Energy Consumers Australia fees

The Commission understands from AEMO that cost recovery will likely be on the same basis as the GS00 fees because cyber security fees will benefit the same group of participants. See table 3.1 below.

Table 3.1: Structure of gas participant fees for the GS00

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 GS00 costs)
Retailer fee	\$ / customer supply point (to allocate 70% of GS00 costs)

56 Submission to the draft determination: AGL, p.1.

57 Submission to the draft determination: Alinta Energy, p.1. Submission to the [consultation paper](#): Alinta Energy, p.1.

58 [Cyber security roles and responsibilities](#).

59 [Draft determination](#), p.24.

Liabe registered participants	Fee structure
Each retail gas market participant participating in the registrable capacity of market participant–retailer in Vic or retailer in NSW/ACT, Qld and SA.	

Source: AEMO, Structure of Gas Participant Fees, December 2023, [Final Report and Determination](#).

The forecast costs of performing cyber security functions will be incorporated into AEMO’s annual budget and fee process. AEMO consults on its proposed fee structure for gas participant fees in accordance with the standard consultative process. The next consultation for general determination of gas participant fees will be from 1 July 2027.

Further, if AEMO consults on and determines that the cyber security functions are to be declared a major gas project, it allows 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 section 3.3 of the [draft determination](#) for more information on AEMO’s cost recovery process.

3.4 The rule commences on 30 July 2026

The final rule commences on publication of this determination on 30 July 2026. Immediate commencement is possible because AEMO is already performing these functions in the electricity sector and some activities under the functions for the gas sector without having a cyber security role established in the NGR.

An immediate commencement date allows AEMO to access protection from liability for the cyber security functions as soon as possible. Additionally, this does not delay the process for AEMO to be able to cost recover for the performance or exercise of these cyber security functions. This way, benefits for consumers will be realised more quickly because AEMO is only able to recover costs and sufficiently commit resources to these four functions from the commencement of the final rule.

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

AEMO has indicated that it does not need to make any updates to procedures, guidelines, or settlement systems before the final 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.⁶⁰

A.1 Cyber security governance in Australia

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 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.⁶¹ The review recommended:⁶²

- 1 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 (CISC), and representatives from Australian energy organisations. It is both a framework and an annual voluntary assessment program, enabling participants to undertake assessments of their own

⁶⁰ See our website for more information on the rule change process: <https://www.aemc.gov.au/our-work/changing-energy-rules>

⁶¹ [Independent review into the Future of the National Electricity Market](#), p.67.

⁶² [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 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.⁶³

The Commission also notes that the Australian Government is currently undertaking consultation on reforms to the SoCI Act in response to recommendations provided by an Independent Review.⁶⁴ The proposed reforms seek to reduce unnecessary complexity and regulatory duplication, modernise and refine sector and asset coverage, clarify legislative expectations, assurance mechanisms, and governance arrangements, and better assess whether security and resilience outcomes are being achieved. The Commission considers that the proposed reforms to the SoCI Act would complement the cyber security activities AEMO performs for the gas sector under the final rule. See section 1.3 for more information on the proposed reforms to the SoCI Act.

The Australian Energy Sector Cyber Security Framework can be used by owners and operators to meet SoCI Act requirements.⁶⁵

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

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 cyber security, providing materials and advice for consumers, small and large businesses, and government.
Department of Home Affairs	Among other functions: • Supports the development and implementation of national cyber security policy. • Manages all types of threats to critical infrastructure, in partnership with industry and the broader community through the CISC.

⁶³ [Security of Critical Infrastructure Act 2018](#).

⁶⁴ [Streamlining and modernising the Security of Critical Infrastructure Act, consultation paper](#). Independent Review into the Security of Critical Infrastructure Act 2018, Dr Jill Slay AM, 31 January 2026.

⁶⁵ [The Australian Energy Sector Cyber Security Framework resources](#), AEMO.

Body name	Description
Critical Infrastructure Security Centre (CISC)	Assists critical infrastructure owners and operators in understanding risk and meeting regulatory requirements. Reports to the Department of Home Affairs.
State and territory cyber security units	Various jurisdictions have cyber security agencies or units that support government (and sometimes public sector) cyber security initiatives. They may also be responsible for leading jurisdictional government responses to cyber incidents.

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

As noted above, the SoCI Act requires specific NEM and gas market entities, including AEMO, to manage their own critical infrastructure as it relates to cyber security. The final rule 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.⁶⁶ The proponent believed that there was a similar need to confirm and clarify these functions for the gas sector to facilitate cohesive cyber security practices across the energy sector.⁶⁷

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.⁶⁸ 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.⁶⁹ 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, which could include developing a cyber incident response plan. This could also be performed by AEMO in the gas sector under the ECGS cyber security functions.⁷⁰

A.2 Previously the NGR did not explicitly address AEMO's cyber security role

Previously, the NGR did not explicitly define or address cyber security, so AEMO's role in cyber security for the gas sector was unclear. There was a need to confirm and clarify what AEMO's role

⁶⁶ Final determination, [Cyber security roles and responsibilities](#).

⁶⁷ Rule change request, p.3.

⁶⁸ 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>.

⁶⁹ '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.

⁷⁰ Rule change request, p.1.

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.

A.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 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 provides clarity for cyber security responsibilities across the gas system.

The proponent proposed 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 proposed to do this by adding cyber security as a function in the NGR, which identifies cyber security as a statutory function for the purpose of the NGL.⁷¹ This enables 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.⁷²

The proponent proposed 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.

A.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 was not explicitly referenced in the gas rules

The proponent stated that cyber security is inextricably linked with the management of the gas system and markets. However, previously, existing legislation did 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 NEM. 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 was a lack of funding certainty and liability protection for cyber security activities across the gas sector

The request considered that while AEMO has performed some cyber security activities in gas using existing resources, the lack of certainty for cost recovery and liability protection prior to this rule change, 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 stated 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 posed an ongoing risk to system security. The proponent asserts that as time passed, the risk would have increased, and the ability of AEMO, government, and industry to curtail these risks would have become more challenging. See section 3.1.2.

⁷¹ AEMO's statutory functions include any other functions conferred under the NGR or Procedures. See section 91A(1)(l) of the NGL.

⁷² For more information see sections 91E and 91K of the NGL.

A.3 Gas and electricity sector differences reinforce the need for formalised gas cyber security functions

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 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 National Electricity Rules (NER) provide formalised cyber security functions for AEMO, the NGR previously lacked 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 created the potential for delayed detection and response times. This could have increased the risk of localised disruptions escalating into broader supply and economic impacts (see Figure A.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 figures A.1, A.2, and A.3 below for a comparative analysis of these differences.

Figure A.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 A.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
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 A.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:

- has the flexibility to apply the proposed functions in a way that is tailored to gas market arrangements across the ECGS
- where appropriate, maintains 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 allows 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.⁷³ See section 3.2 for more information on how the functions would work.

A.4 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.⁷⁴ 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 the draft rule determination.

On 7 May 2026, the Commission published a draft rule determination including a draft rule. The Commission received two submissions on the draft rule determination. Issues raised in submissions are discussed and responded to throughout this final rule determination.

⁷³ Rule, 716(7a).

⁷⁴ 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 final rule determination.

B.1 Final rule determination and final rule

In accordance with section 311 of the NGL, the Commission has made this final 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 final rule determination are set out in chapters two and three.

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

B.2 Power to make the rule

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

The final 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;⁷⁵ 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.

B.3 Commission's considerations

In assessing the rule change request the Commission considered:

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

There is no relevant Ministerial Council on Energy (MCE) statement of policy principles for this rule change request.⁷⁶

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.⁷⁷ The final gas rule is compatible with AEMO's declared system functions because it would not affect those functions.

⁷⁵ Section 74(1)(a)(vi) of the NGL.

⁷⁶ 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.

⁷⁷ 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 Energy⁷⁸ and rules made by the AEMC in accordance with its rule making powers under section 74 and 313 of the WA Gas Law.⁷⁹ 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.

The final rule does not fall within the subject matters about which the Commission may make rules under the WA Gas Act.

The final rule creates a new Part in the NGR that does not apply in the Western Australian version of the NGR.

Accordingly, the final 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 final 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 final rule be classified as civil penalty provisions or conduct provisions.

⁷⁸ 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.

⁷⁹ 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
AER	Australian Energy Regulator
AESCIRP	Australian Energy Sector Cyber Incident Response Plan
AESCSF	Australian Energy Sector Cyber Security Framework
ASD	Australian Signals Directorate
CISC	Critical Infrastructure Security Centre
Commission	See AEMC
CTP	Cyber Training Platform
DAA	Day Ahead Auction
DNSP	Distribution Network Service Provider
DTS	Declared Transmission System
DWGM	Declared Wholesale Gas Market
ECGS	East Coast Gas System
EVs	Electric Vehicles
GPG	Gas Powered Generation
GSA	Gas Supply Agreement
GSH	Gas Supply Hub
GSOO	Gas Statement of Opportunities
GTA	Gas Transportation Agreement
ITGSP	Interruption to Gas Supply Process
MCE	Ministerial Council on Energy
NEM	National Electricity Market
NER	National Electricity Rules
NGL	National Gas Law
NGO	National Gas Objective
NGR	National Gas Rules
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