AUSTRALIAN ENERGY MARKET COMMISSION

RULE

Draft rule determination

National Electricity Amendment (Cyber security roles and responsibilities) Rule 2024

Proponent

The Honourable Chris Bowen, Minister for Climate Change and Energy

26 September 2024

Inquiries

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

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

Reference: ERC0388

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 all live and work. We pay respect to all Elders past and present and the continuing connection of Aboriginal and Torres Strait Islander peoples to Country. The AEMC office is located on the land traditionally owned by the Gadigal people of the Eora nation.

Copyright

Citation

To cite this document, please use the following:
AEMC, Cyber security roles and responsibilities, Draft rule determination, 26 September 2024

Summary

1 The Australian Energy Market Commission (AEMC or Commission) has decided to make a draft rule to confirm and clarify the Australian Energy Market Operator's (AEMO) cyber security role and responsibilities in the National Electricity Rules (NER). In response to the rule change request submitted by Minister for Climate Change and Energy, the Hon. Chris Bowen MP, the draft rule will insert four new cyber security functions into Chapter 4 of the NER. As the system operator, AEMO currently has existing emergency powers to respond to actual cyber incidents that are impacting or have the potential to impact system security. By embedding and formalising AEMO's cyber security role and responsibilities in the NER we are ensuring participants, industry, and AEMO have greater clarity on its role in cyber security uplift and preparedness, supporting a strategic and coordinated approach to cyber security. This will also provide certainty over funding and liability protection, consistent with the performance of other functions and activities, for AEMO.

2 Cyber security is of critical importance. While there are cyber risks in all sectors, it is a particularly prominent issue in energy security given the National Electricity Market's (NEM) increasing digitisation and connectivity. This includes real-time data of critical power system components, supervisory control and data acquisition (SCADA) systems, smart grids, smart meters and smart appliances connected to open networks. Additionally, the NEM's high take-up of consumer energy resources (CER) and distributed energy resources (DER), such as neighbourhood batteries, amplifies the risks.

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

4 The Finkel Review, 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 co-developed between the Commonwealth Government, industry, and AEMO.

5 Following the Finkel Review's recommendation AEMO worked with the relevant agencies to increase cyber protections, reporting to Energy Ministers. In December 2022 Energy Ministers endorsed the development of a rule change request to embed and formalise AEMO's roles and responsibilities by establishing cyber functions in the NER.

6 We are seeking feedback on our draft determination and rule by 7 November 2024.

Our draft rule would allow AEMO to recover costs and confirm immunity from liability to perform prevention and preparedness functions

7 Currently, the NER does not explicitly address cyber security, so there are opportunities to confirm and clarify AEMO's role and responsibilities in this area. While under the existing rules AEMO has directions powers and the contingency event framework for responding to an actual or pending cyber security incident if the security of the power system is compromised or likely to be compromised, the draft rule would establish specific cyber security prevention and preparedness functions for AEMO in the NER.

8 The draft rule would allow AEMO to recover costs and confirm immunity from liability, consistent with the performance of AEMO's other activities and functions, to deliver these cyber security

functions. This will provide certainty to AEMO and participants about recovery of costs and liability arrangements for certain cyber security roles and responsibilities they undertake. This clarity will help strengthen the management of cyber risks across the power system from individual participants to whole-of-system considerations.

9 The Commission considers that the costs of the four functions are outweighed by the benefits of reducing cyber security risks. The draft rule would enable AEMO to recover cyber security costs through their normal cost recovery process. Going forward, this would help ensure the cyber security functions are adequately and sustainably funded. See **section 2.3** for more information.

The draft rule would add a set of four cyber security functions to AEMO's power system security responsibilities

10 The draft rule would add a set of four cyber security functions to AEMO's power system security responsibilities in Chapter 4 of the NER.

11 Specifically, the draft rule would insert four new functions for AEMO into the NER:

- **Function 1: Cyber security incident coordinator:** AEMO would be able to plan and coordinate the NEM-wide response to a cyber incident affecting the energy sector. AEMO would continue to develop a plan, the Australian Energy Sector Cyber Incident Response Plan, outlining how market, state, and federal responses to a cyber incident would be coordinated. In the event of a cyber incident AEMO would lead the implementation of the response in the manner set out by the plan. In supporting the plan, AEMO would lead and organise testing and scenario training exercises to test the cyber resilience of the power system.
- **Function 2: Supporting cyber preparedness and uplift:** AEMO would continue to have stewardship of the Australian Energy Sector Cyber Security Framework, organise testing and scenario training exercises to test the cyber resilience of the power system, and provide guidance and advice to industry in the form of written materials, digital tools and working groups. AEMO would not create additional mandatory requirements for registered participants.
- **Function 3: Examining cyber risks and providing advice to government and industry:** AEMO would provide cyber security research and advice to governments. This advice would draw on AEMO's unique energy expertise in their position as system operator, and would complement, rather than replace, work undertaken by other cyber security bodies such as the Australian Cyber Security Centre (ACSC).
- **Function 4: Facilitating the distribution of critical cyber security information to market participants:** AEMO would act as a distributor of cyber security information to the energy industry, using their position as system operator and existing communication channels. AEMO would facilitate the distribution of warnings of cyber vulnerabilities of threats, post-cyber incident reports, and preventative information technology patches in commonly used technologies.

12 These four functions would be facilitative and flexible and would not enable AEMO to impose mandatory obligations on market participants. The Commission considers that the costs of the four functions are outweighed by the benefits of reducing cyber security risks. Specifically, the costs represent only around 2% of participant fees and the Commission is satisfied that further resourcing is required to undertake more cyber security activities under the functions. For these reasons the Commission considers that the costs are appropriate and not duplicative, with the benefits significantly outweighing the costs. See **section 2.3** for more information.

13 Importantly, AEMO's existing statutory function under the National Electricity Law (NEL) to "maintain and improve power system security" inherently extends to cyber incidents impacting power system security. The NER references AEMO's authority to issue power system security directions, prepare a system restart plan for managing and coordinating system restoration during a major disruption, and coordinate the protection of power system equipment. This draft rule will build on the existing statutory functions to provide greater clarity on and embed AEMO's role in cyber security uplift and preparedness into the NER framework.

The Commission has considered stakeholder feedback in making its decision

14 A clear majority of stakeholders agreed that the NER lacks clarity on cyber security roles and responsibilities and acknowledged that it is problematic for AEMO to undertake cyber security tasks without certainty. Stakeholders generally agreed that confirming and clarifying AEMO's cyber security role and responsibilities in the NER would provide greater clarity and guidance to industry.

15 The key stakeholder observations that shaped the draft rule included:

- Support for the need to confirm and clarify, in the NER, what AEMO's role and responsibilities are in relation to cyber security. Stakeholders considered this was important for ensuring a coordinated and strategic approach is implemented to efficiently manage the increasing cyber security risk to power system security.
- Support the four functions, and broad agreement that the benefits would likely justify the costs. However, some stakeholders:
  - asked for clarification around costs
  - cautioned against duplication of roles with other agencies and within functions
  - did not agree that certain functions were consistent with AEMO's role as market operator
  - requested further detail in the case of function and requested advice is proactive rather than reactive
  - requested compliance with consultation procedures.

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

- the costs of embedding and formalising the functions are justified because it will ensure ongoing benefits from AEMO performing cyber security activities. The costs are relatively low for a set of functions that will become increasingly important due to cyber risks. In this context, ensuring certainty of funding and liability protection will allow AEMO to upscale and further resource these activities.
- the roles are not duplicative because AEMO's responsibilities under the functions are different from those of other agencies.
- the functions are consistent with AEMO's role as market operator and they are appropriate for AEMO to perform because of its unique expertise and perspective as the operator of the power system.
- there is sufficient flexibility under the draft rule for government's to seek cyber security advice from other bodies, in addition to AEMO. Further detail on each function is provided in **section 2.2**.

17 Stakeholders also raised other cyber security issues that are important but are outside the scope of this particular rule change process because they relate to broader matters, which are under consideration by other bodies through other reform processes. These include the work being undertaken by the CER Taskforce and the Energy and Climate Change Ministerial Council,

Standards Australia and the Energy Security and Resilience Working Group, and the Department of Home Affairs. See **section 1.4** and **section 2.5** for more information.

We assessed our draft rule against three assessment criteria using regulatory impact analysis and stakeholder feedback

18 The Commission has considered the National Electrcity Objective (NEO)[1] and the issues raised in the rule change request and assessed the draft rule against three assessment criteria outlined below.

19 The draft rule would contribute to achieving the NEO by:

- **Promoting safety, security and reliability:** by embedding and formalising AEMO's functions in the NER the draft rule would help enable the secure provision of electricity in the long term. The draft rule would promote power system safety, security, and reliability by better enabling AEMO to manage and operate a secure system, giving both AEMO and market participants a better understanding of who is responsible for specific cyber security preparedness and incident response functions. This would help enable the secure provision of electricity to consumers in the long term, ensuring safety and security outcomes are met. See **section 3.3.2** for a more detailed analysis.
- **Aligning with principles of good regulatory practice:** the proposed draft rule would be aligned with principles of good regulatory practice because it is seeking to improve predictability, stability and transparency of cyber security where the power system is increasingly digitised, and considers broader reforms while avoiding duplication. By formalising the functions AEMO would have clarity over funding and liability protection arrangements (consistent with the performance of AEMO's other activities and functions), which would allow for resourcing certainty to properly establish and undertake cyber security activities on more well-defined and permanent basis. This would enable AEMO to continue and scale up its cyber security activities which appropriately reflects that the environment has changed considerably with cyber preparedness and uplift becoming increasingly more important for the NEM, requiring more resourcing. It follows that AEMO, governments, and market participants would then have **transparency** around activities and the cost of AEMO's cyber security role and responsibilities. See **section 3.3.3** for a more detailed analysis.
- **Taking into account implementation considerations:** the draft rule would take implementation considerations into account by considering cost implications, governance complexities, timing considerations, and relevant jurisdictional conditions. The additional **cost** of embedding and formalising cyber preparedness and incident response functions is low compared to the risks posed by a potential cyber incident, especially where it could have been prevented by clarifying roles and responsibilities and upscaling AEMO's preparedness activities. The Commission considers that any existing **complexities in cyber security governance** would become more transparent and simplified as the draft rule would formally establish functions for AEMO, which would make cyber security governance more transparent for industry. The draft rule would clarify any **uncertainty and timing** considerations by providing more certainty around cyber security in the NER. The **impact** on AEMO and other participants would be manageable because AEMO is already performing some of the activities under the new proposed functions, meaning that some processes are in place that can be built on. Additionally, the draft rule takes into consideration **relevant jurisdictional conditions** across the NEM. Cyber security incidents across the NEM could affect individual assets or the system

1 Section 7 of the NEL.

as a whole, and since the NEM is interconnected between regions, a cyber security incident can have a system-wide effect, meaning that necessarily a rule to manage system wide risks should apply to all NEM jurisdictions. See **section 3.3.4** for a more detailed analysis.

The draft rule would commence on 12 December 2024

20 The Commission's draft determination is that the draft rule should commence as early as possible. AEMO does not require an implementation period before commencement. The draft rule would come into effect as soon as the final determination is published on 12 December 2024.

21 This would mean that AEMO could cost recover from the commencement date of the final rule. Cost recovery arrangements would be determined in accordance with the existing rules and consultation processes that govern this.

22 If AEMO sought to determine the cyber security functions as a declared NEM project, as per clause 2.11.1 of the NER,[2] it would need to follow the Rules consultation procedures in making this determination.[3] AEMO will consider the timing of consultation on fees and structure, and the NEM declared project, if it elects to do so.

2 AEMO submission to the consultation paper, p. 3.

3 Clause 2.11.1(bc) of the NER.

How to make a submission

We encourage you to make a submission

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

How to make a written submission

Due date: Written submissions responding to this draft determination and rule must be lodged with Commission by **7 November 2024**.

How to make a submission: Go to the Commission's website, www.aemc.gov.au, find the "lodge a submission" function under the "Contact Us" tab, and select the project reference code **ERC0388**. [4]

Tips for making submissions on rule change requests are available on our website.[5]

Publication: The Commission publishes submissions on its website. However, we will not publish parts of a submission that we agree are confidential, or that we consider inappropriate (for example offensive or defamatory content, or content that is likely to infringe intellectual property rights).[6]

Next steps and opportunities for engagement

There are other opportunities for you to engage with us, such as one-on-one discussions.

You can also request the Commission to hold a public hearing in relation to this draft rule determination.[7]

Due date: Requests for a hearing must be lodged with the Commission by 3 October 2024.

How to request a hearing: Go to the Commission's website, www.aemc.gov.au, find the "lodge a submission" function under the "Contact Us" tab, and select the project reference code **ERC0388.** Specify in the comment field that you are requesting a hearing rather than making a submission.[8]

For more information, you can contact us

Please contact the project leader with questions or feedback at any stage.

Project leader:	Nomiky Panayiotakis
Email:	nomiky.panayiotakis@aemc.gov.au

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

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

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

7 Section 101(1a) of the NEL.

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

Contents

Tables

Figures

1 The Commission has made a draft determination

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

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

- **Section 1.1** outlines the draft determination and draft rule to make the rule proposed by the Minister.
- **Section 1.2** outlines AEMO's powers under the current the National Electricity Rules (NER) for managing cyber security.
- **Section 1.3** outlines the input from stakeholders that shaped our draft determination.
- **Section 1.4** explains how our determination would support a strategic and coordinated approach to cyber security.

1.1 Our draft rule would confirm and clarify AEMO's role and responsibilities for cyber security

The draft rule is consistent with the rule change request (see **appendix A**) and explicitly addresses cyber security in the NER as it relates to power system security. It confirms AEMO's roles and responsibilities for cyber security. It does this by building on AEMO's existing powers to maintain power system security in response to certain events through the directions powers and contingency event mechanisms by specifying in the NER the roles and responsibilities that AEMO would perform to assist in enhancing cyber security across the energy system. Importantly, the draft rule would allow AEMO to recover costs and confirm immunity from liability, consistent with the performance of AEMO's other activities and functions, to deliver these cyber security functions. See **section 1.2** for more information on liability protection and **section 2.3** for more information on cost recovery.

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

- **Function 1: Cyber security incident coordinator:** AEMO would be able to plan and coordinate the response, across the whole National Electricity Market (NEM), to a cyber incident affecting the energy sector. AEMO would continue to develop a plan, the Australian Energy Sector Cyber Incident Response Plan (AESCIRP), outlining how market, state, and federal responses to a cyber incident would be coordinated. In the event of a cyber incident AEMO would lead the implementation of the response in the manner set out by the plan.
- **Function 2: Supporting cyber preparedness and uplift:** AEMO would continue to have stewardship of the Australian Energy Sector Cyber Security Framework (AESCSF), organise testing and scenario training exercises to test the cyber resilience of the power system, and provide guidance and advice to industry in the form of written materials, digital tools and working groups. AEMO would not create additional mandatory guidelines on cyber security.
- **Function 3: Examining cyber risks and providing advice to government and industry:** AEMO would provide cyber security research and advice to governments. This advice would draw on AEMO's unique energy expertise in their position as system operator, and would complement, rather than replace, work undertaken by other cyber security bodies such as the Australian Cyber Security Centre (ACSC).

- **Function 4: Facilitating the distribution of critical cyber security information to market participants:** AEMO would act as a distributor of cyber security information to the energy industry, using their position as system operator and existing communication channels. AEMO would facilitate the distribution of warnings of cyber vulnerabilities of threats, post-cyber incident reports, and preventative patches in commonly used technologies.

These four functions would be facilitative and flexible and would not enable AEMO to impose mandatory obligations on market participants. See **section 2.2** for more information.

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

Currently, the NER does not explicitly define or explicitly address cyber security, so AEMO's role in cyber security is less well understood when compared to its traditional role in maintaining a secure technical envelope for the power system. There is a need to confirm and clarify, in the NER, what AEMO's role and responsibilities are in relation to cyber security to ensure a coordinated and strategic approach is implemented to efficiently manage the increasing cyber security risk to power system security.

It is worth noting that while not specifically referenced, AEMO's existing statutory function under the National Electricity Law (NEL) to "maintain and improve power system security" inherently extends to cyber incidents impacting power system security. In this context, the NER further references AEMO's authority to issue power system security directions, prepare a system restart plan for managing and coordinating system restoration during a major disruption, and coordinate the protection of power system equipment.

The absence of an explicit reference to cyber security in the NER has the potential to create uncertainty about funding and liability protection for the cyber security functions AEMO performs. The uncertainty about funding and liability protection for the delivery of cyber security functions could lead AEMO to perform these functions without sufficient resources and certainty. This has the potential to harm the power system, as it weakens the management of cyber risks across the power system from individual participants to whole-of-system considerations.

While AEMO can respond to an actual cyber incident as it would to any power system security incident (such as by issuing directions), it lacks clear authority to undertake preventative work. The draft rule seeks to embed and formalise an existing practice that is working well, that is AEMO's cyber security incident and preparedness work, as well as formalising the four new functions.

Following the Finkel Review,[9] which recommended AEMO should have an explicit cyber security role, AEMO has adopted some cyber security roles and responsibilities. However, because cyber security is not explicitly referenced in the NER it does not have the ability to recover costs and it does not have liability protection. Importantly by embedding and formalising these functions in the NER:

- AEMO would be clearly accountable and responsible for activities under the four functions pertaining to cyber security which will help clarify their role and responsibilities for participants and ensure this work is undertaken. Market participants will benefit by knowing who is responsible for certain cyber security preparedness functions and who is responsible in a crisis.

9 The Finkel Review was commissioned in response to the 2016 South Australian blackout. It emphasised the importance of cyber security within the energy sector. Its recommendations underscored the necessity for resilient and secure energy infrastructure, with the report noting "strong cyber security measures for the NEM will be essential for maintaining Australia's growth and prosperity in an increasingly global economy".

- AEMO would be able to recover costs from participants ensuring adequate resourcing, allowing it to upscale and further expand these activities. While AEMO has been performing some of these activities to date, the environment and operating realities of the power system have changed considerably, with cyber security and uplift becoming increasingly more important for the NEM. This would ensure AEMO can undertake activities which will benefit market participants and consumers by ensuring the security and reliability of the power system.
- AEMO would have liability protection for the performance of these functions, consistent with its other functions. As a not-for-profit, liability protection under the NEL is a key consideration in determining AEMO's access to appropriate insurance arrangements and limiting corporate costs. Liability protection would enable AEMO to take on the appropriate amount of risk to perform the functions effectively. The effective performance of these functions is important for the security of the power system, which is ultimately in the long term interests of consumers.[10]
- Participants will be supported to improve their level of cyber security preparedness and maturity as they would be able to access the latest information about risks, learnings, and preparedness which will help minimise the risk of a cyber incident, which in turn will mitigate the cost of cyber security incidents on participants, while not imposing any mandatory obligations or costs.

See **appendix A** for more information.

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

A clear majority of stakeholders in their submissions to the consultation paper agreed that the NER lacks clarity on cyber security and that it is problematic for AEMO to undertake cyber security tasks without certainty. Stakeholders generally agreed that confirming and clarifying AEMO's cyber security role and responsibilities in the NER would provide greater clarity and guidance to industry.

The key stakeholder observations that shaped the draft rule included:

- support for the need to confirm and clarify, in the NER, what AEMO's role and responsibilities are in relation to cyber security. Stakeholders considered this was important for ensuring a coordinated and strategic approach is implemented to efficiently manage the increasing cyber security risk to power system security.
- general support for the four functions, and broad agreement that the benefits would likely justify the costs. However, some stakeholders:
  - Asked for clarification around the costs proposed[11]
  - Cautioned against duplication of roles with other agencies and within function[12]
  - Did not agree that certain functions were consistent with AEMO's role as market operator[13]

10 It is noted that liability protection is especially relevant to where AEMO's exercising of the Australian Energy Sector Cyber Incident Response Plan (AESCIRP) which involves interactions with market participant's systems to test the robustness of the plan.

11 Submissions to the consultation paper: Energy Queensland, p. 1; AGL, pp. 4-5; Splunk, p. 4; SAPN, p. 2.

12 Submissions to the consultation paper: Alinta Energy, p. 2; AGL, p. 3; Energy Queensland, pp. 3-5; TasNetworks, p. 1.

13 Energy Queensland submission to the consultation paper, pp. 3-5.

- Requested further detail in the case of function 3, which relates to providing advice to governments,[14]and requested advice is proactive rather than reactive[15]
- Requested compliance with consultation procedures.[16]

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

- The costs are justified because participants are already benefiting from AEMO performing some cyber security activities, and ensuring certainty of funding and liability protection will ensure AEMO can continue and bolster their cyber security roles are responsibilities for the power system. This reflects the reality that while AEMO has been performing these activities the environment has changed considerably with cyber preparedness and uplift becoming increasingly more important for the NEM, requiring more resourcing. See **section 2.3**.
- Roles are not duplicative because AEMO's responsibilities under the functions are different from those of other agencies.
- The functions are consistent with AEMO's role as market operator, and they are appropriate for AEMO to perform because of its unique expertise and perspective as the operator of the power system.
- There is sufficient flexibility under the draft rule for governments to seek cyber security advice from other bodies, in addition to AEMO. See **section 2.2.3**.

Further detail on each function is provided in **section 3.2**.

Stakeholders also raised other cyber security issues that are important and related to cyber security but are outside the scope of this particular rule change process. These include:

- Who is responsible for governance arrangements for cyber security in the NEM[17]
- A national strategy for cyber security and consumer energy resources (CER)[18]
- Clarity on who provides guidelines, standards, or mandatory obligations for market participants, including original equipment manufacturers (OEMs)[19]
- Clarity around the role of networks[20]

We consider the above issues that are outside of the scope of this particular rule change process are being considered and complemented through other reform processes, including the work being undertaken by:

- The AEMC around Accelerating smart meter deployment[21] and Integrating price-responsive resources into the NEM.[22]
- The CER Taskforce and the Energy and Climate Change Ministerial Council, who recently released the National Consumer Energy Resources Roadmap which includes a workstream to define the roles and responsibilities in a high CER world, including with respect to cyber security, of distribution network service providers (DNSPs)/distribution system operators (DSOs) by 2026. It is important to note that the DSO workstream relating to roles and responsibilities is evolving and as models for implementation are developed, this may result in

14 Splunk submission to the consultation paper, p. 9.
15 SAPN submission to the consultation paper, p. 2.
16 TasNetworks submission to the consultation paper, p.3.
17 Submissions to the consultation paper: SMA, p. 4; Splunk, pp. 6-7.
18 Submissions to the consultation paper: SEC, pp. 1-2; Fronius, p. 2.
19 Submissions to the consultation paper: Vestas, pp. 1-2; CEC, p. 2.
20 Submissions to the consultation paper: SMA, p. 3; SEC, pp. 1-2; Fronius, pp. 1-2; ENA, p. 3; CEC, pp. 1-2.
21 AEMC, Accelerating smart meter deployment, https://www.aemc.gov.au/rule-changes/accelerating-smart-meter-deployment.
22 AEMC, Integrating price-responsive resources into the NEM, https://www.aemc.gov.au/rule-changes/integrating-price-responsive-resources-nem.

multiple options for where cyber security roles are allocated. The Roadmap also indicates that voluntary CER cyber standards and technical specifications will be available in 2027.[23]

- Standards Australia and the Energy Security and Resilience Working Group who are implementing the *Roadmap for CER Cyber Security,* which includes proposals to adopt some standards and develop technical specifications for CER cyber security specific to Australian technologies and markets.[24]
- The Department of Home Affairs' consultation on potential legislative reforms to support the Government's cyber security strategy for 2023-2030, which also includes proposed new cyber security legislation and changes to the Security of Critical Infrastructure Act 2018 (SOCI Act).[25]

See **appendix D** for more information.

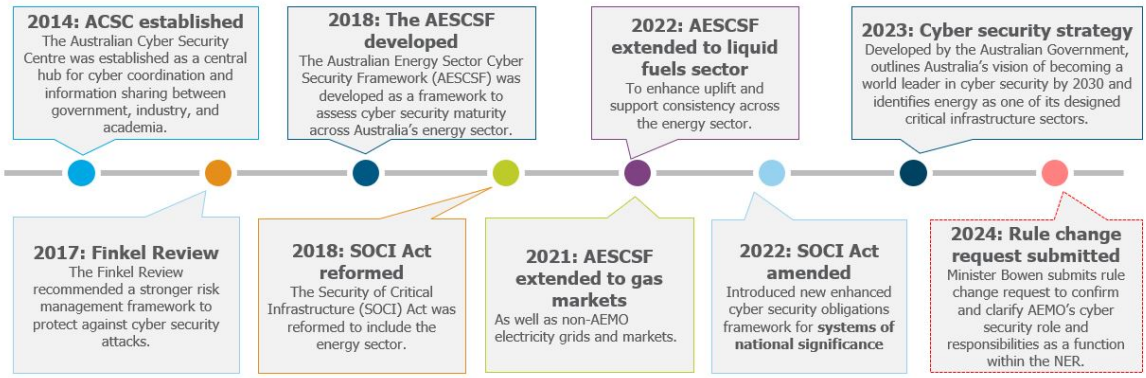
1.4 Our determination would support a strategic and coordinated approach to cyber security

Cyber security is of critical importance in Australia. While it impacts all sectors, it is a particularly prominent issue in energy security given the NEM's increasing digitisation and connectivity. This includes real-time data of critical power system components, supervisory control and data acquisition (SCADA) systems, smart grids, smart meters and smart appliances connected to open networks. Additionally, the NEM's high take-up of CER and distributed energy resources (DER), such as neighbourhood batteries, further amplifies the issue.

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

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

Figure 1.1: Timeline of cyber security reforms and frameworks



Source: AEMC.

23 National Consumer Energy Resources Roadmap, https://www.energy.gov.au/sites/default/files/2024-07/national-consumer-energy-resources-roadmap.pdf, p43.

24 Roadmap for CER cybersecurity, https://www.standards.org.au/news/securing-the-future—-a-cybersecurity-roadmap-for-consumer-energy-resources.

25 Australian Government Department of Home Affairs, Cyber security legislative reofrms, https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/cyber-legislative-reforms.

The Finkel Review, 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 Finkel Review recommended that AEMO should have a cyber security role**.** As seen in **Figure 1.1** above this rule change seeks to embed and formalise the cyber security functions AEMO performs.

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

See **appendix A** for more information on the history and broader context for cyber security in the NEM.

2 Our draft rule would confirm and clarify AEMO's cyber security functions in the NER

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

- **Section 2.1** explains why the draft rule would define cyber security responsibilities in Chapter 4 of the NER.
- **Section 2.2** outlines the four proposed functions and addresses stakeholder feedback on those functions.
- **Section 2.3** outlines the expected costs of the functions and why they are justified.
- **Section 2.4** explains the proposed timing for commencement of the draft rule.
- **Section 2.5** notes that some key issues raised by stakeholders need to be addressed through other processes.

2.1 Cyber security is a power system security concern

Box 1: Cyber security would be established as a power system security responsibility

The draft rule would add a set of specific cyber security functions to AEMO's power system security responsibilities in Chapter 4 of the NER. These functions largely reflect activities already undertaken by AEMO, but without a rules-based obligation. This would allow AEMO and participants to have clarity over funding and liability arrangements.

Our consultation paper asked stakeholders whether cyber security should be considered a power system security issue (Chapter 4 of the NER) or a network planning and expansion issue (Chapter 5 Part D of the NER). Stakeholders broadly agreed that cyber security was part of power system security, but many noted it was also relevant to network planning and expansion as well as other aspects of the energy system.

The draft rule would add a set of four cyber security functions to AEMO's power system security responsibilities in Chapter 4 of the NER.

Currently, the NER does not specifically address cyber security, so AEMO does not have a clear role or confirmed responsibilities in this area. While under the existing rules AEMO can respond to a cyber security incident if the security of the power system is compromised, for example by issuing directions to market participants, the draft rule would establish specific cyber security prevention and preparedness functions for AEMO in the NER.

The 2017 Finkel Review emphasised the importance of cyber security in the energy sector. The review recommended that the former Energy Security Board (ESB) should complete an annual report on the cyber security preparedness of the NEM. While the annual report did not eventuate, this recommendation led to the development of the Australian Energy Sector Cyber Security Framework, a cyber security self-assessment tool for industry (**see section 2.2.2**).

The Finkel Review also noted a number of other actions that could be accelerated to improve the cyber security of the NEM, including:

- Enhanced collection, speed and automation of threat intelligence sharing amongst local industry, Australian government and international energy peers.
- Greater clarity on roles, responsibilities and protocols in responding to a nationally significant cyber attack, and increased scale and tempo of exercises to test and improve response capability at an industry and national level.

Following the review, AEMO began undertaking some cyber security preparedness work in line with the actions above. The proposed functions for inclusion in the NER reflect this. For example, function 4 (distribution of information) supports sharing of threat intelligence amongst local industry, government, and international bodies. Function 1 (incident coordinator) would clarify roles and protocols in responding to a cyber incident and function 2 (industry uplift) would involve more extensive and frequent testing and training exercises.

2.1.1 The Commission considers it appropriate to include cyber security in Chapter 4

The draft rule would make these cyber security activities part of AEMO's power system security responsibilities in the NER. Cyber security functions would be added to AEMO's power system security responsibilities in NER clause 4.3.1. The specific functions would be set out in a new clause 4.3.2A as outlined in the remainder of this section. NER 4.3.2A would also state, for the avoidance of doubt, that these functions do not limit AEMO's existing functions and do not impose mandatory obligations on other participants. See the draft rule available on the project page.[26]

We consider it is appropriate to include cyber security in Chapter 4 of the NER because cyber security incidents can pose a threat to power system security. While not specifically referenced, AEMO's existing statutory function under the National Electricity Law (NEL) to "maintain and improve power system security" inherently extends to cyber incidents impacting power system security. In this context, the NER further references AEMO's authority to issue power system security directions, prepare a system restart plan for managing and coordinating system restoration during a major disruption, and coordinate the protection of power system equipment.

However, in spite of this, there is merit in making clear AEMO's roles and responsibilities in relation to cyber security in the NER. Including this in Chapter 4 makes sense, given that the other mechanisms AEMO has to respond to a cyber security incident that has occurred, directions and the contingency event framework, are also included in this Chapter. Alternatively, the rule change request also contemplated placing the functions in Chapter 5 Part D (network planning and expansion), but following stakeholder feedback we consider Chapter 4 more appropriate.

Stakeholders agreed that cyber security is a power system security issue

Stakeholders broadly agreed that cyber security is a power system security issue and that cyber security roles and responsibilities should be confirmed and clarified in the NER. AEMO explicitly supported the legal drafting that was suggested in the rule change request, including the placement in Chapter 4.

Among those other stakeholders who discussed the classification of cyber security, a majority agreed it should be considered a power system security issue.[27] The Clean Energy Council (CEC)

26 AEMC, Cyber security roles and responsibilities rule change, https://www.aemc.gov.au/rule-changes/cyber-security-roles-and-responsibilities.

27 Submissions to the consultation paper: Anchoram Consulting, p. 2; TasNetworks, p. 1; Alinta Energy, p. 2; SMA, p. 5; Snowy Hydro, p. 1; CEC, p. 1; AEMO, p. 3; Splunk, p. 7; Fronius, p. 2.

reasoned that the consequences of a cyber incident could extend to a "system-wide disruption".[28] Energy Queensland (EQL) explained that its "distribution networks are increasingly dependent on digitally connected components. If these digital grid components are compromised, this could lead to network safety or stability issues."[29] This reasoning could easily be applied to most of the NEM's infrastructure, not only distribution networks.

Several stakeholders said that cyber security is as important to network planning and expansion as it is to power system security.[30] Ausgrid noted the "importance of considering cyber security at each step".[31] Energy Queensland noted that network planning and expansion decisions depend on digitally derived data which could be compromised by a cyber incident.[32] Although cyber security is indeed relevant to many aspects of energy system planning and operation, we did not receive any feedback suggesting it should not be considered a power system security issue.

The Commission's draft determination is to make the new rule in Chapter 4. In line with stakeholder feedback, we consider that cyber security is most closely linked to power system security because the consequences of a cyber incident could impact the secure operation of the system, and in turn the supply of electricity to consumers. We note that embedding and formalising cyber security roles and responsibilities for AEMO would have positive impacts in all areas of the energy market and networks and not just power system security.

2.2 The draft rule consists of four proposed functions

Box 2: Cyber security functions in the NER

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

1. Acting as cyber security incident coordinator and maintaining a cyber incident response plan
2. Supporting industry participants in 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 market participants

Stakeholders were broadly supportive of all four functions, with some raising concerns about the proposed costs, duplication with other bodies' roles, AEMO's suitability to perform some of these functions, how the functions were defined, and consultation procedures.

The Commission's draft determination is that each of the four functions would have benefits for electricity consumers and industry. We consider that AEMO is the appropriate body to perform the functions, noting that it is already carrying out some of this cyber security work without a specific responsibility in the NER. Making the draft rule to embed and formalise these functions would enable AEMO to scale up and consistently perform a cyber security role, supported by appropriate cost recovery arrangements and protection from liability.

28 CEC submission to the consultation paper, p. 1.
29 EQL submission to the consultation paper, p. 4.
30 Submissions to the consultation paper: EQL, p. 4; Vestas, p. 3; AGL, p. 3; SEC, p. 3; Origin Energy, p. 1; Ausgrid, p. 3.
31 Ausgrid submission to the consultation paper, p. 3.
32 EQL submission to the consultation paper, p. 4.

2.2.1 Function 1: Cyber security incident coordinator

The cyber security incident coordinator function would involve AEMO developing and maintaining a NEM cyber incident response plan and coordinating the industry's response in the event of a cyber incident.

The Commission understands AEMO has already developed a version of this plan, which is referred to as the Australian Energy Sector Cyber Incident Response Plan. The Australian Energy Sector Cyber Incident Response Plan outlines how market, state and federal responses to a cyber incident affecting the NEM would be coordinated. If a cyber incident occurs, AEMO would lead the implementation of the response in the manner set out by the plan.

Creating an incident response plan enables AEMO and market participants to respond more quickly and effectively to a cyber incident in order to prevent or mitigate impacts on the energy system. The plan would achieve this by allocating clear roles and responsibilities in a cyber incident, including AEMO's coordinating role. This would help protect consumers from the potential consequences of a cyber incident including negative impacts on reliability or system security.

The proposed function 1 could also involve activities that support a timely and effective incident response, such as maintaining sector and jurisdictional contact lists, monitoring the cyber risk landscape, and triaging cyber events.

The draft rule is designed to ensure resourcing and protection from liability for AEMO to keep the Australian Energy Sector Cyber Incident Response Plan up to date and perform the incident coordinator role. Funding certainty and liability protection would enable AEMO to continue and scale up its incident response preparation, for example by updating the Australian Energy Sector Cyber Incident Response Plan more frequently or establishing tools and technologies to support it (see **Table 2.2**). Importantly, the draft rule would not give AEMO the ability to manage market participants' or other bodies' responses to a cyber incident.

Stakeholders supported the cyber incident coordinator role for AEMO

There was strong stakeholder support for the cyber incident coordinator function, with some recognising how it aligns with the work AEMO currently undertakes. The majority of submissions to the consultation paper supported the proposed rule as a whole.[33]

Stakeholders considered that this function would benefit market participants by:

- providing "clear direction when following cyber security procedures",[34]
- "[providing] defined responsibility, [improving] coordination during incidents, [strengthening] sector preparedness, and [ensuring] compliance with regulations",[35]
- "enhancing and better equipping capabilities supporting the [Australian Energy Sector Cyber Incident Response Plan]",[36]
- acting as a "single, credible source of truth during critical cyber security incidents",[37]
- "simplifying messaging through the market operator" and enabling a "well-orchestrated and cohesive incident response",[38]

33 Submissions to the consultation paper: Anchoram Consulting, p. 1; SAPN, p. 1; TasNetworks, p. 1; Alinta Energy, pp. 1-3; SMA, pp. 3-6; Snowy Hydro, p. 1; CEC, p. 1; AEMO, p. 1; Vestas, p. 1; Splunk, p. 3; AGL, p. 1; SEC, p. 1; Origin Energy, p.1; Fronius, pp. 2-3; ENA, p. 2; Ausgrid, p. 1.

34 CEC submission to the consultation paper, p. 1.

35 Vestas submission to the consultation paper, p. 4.

36 Splunk submission to the consultation paper, p. 8.

37 AGL submission to the consultation paper, p. 4.

38 Ausgrid submission to the consultation paper, p. 3.

Some stakeholders noted that the costs of developing and maintaining the Australian Energy Sector Cyber Incident Response Plan would likely be much lower than the potential costs of responding to a cyber incident without a coordination plan, and that the costs would therefore be well justified.[39] See **section 2.3** for more information on costs.

AEMO's incident coordinator function would build on its existing emergency management role

Alinta Energy considered that the cyber incident coordinator function should "dovetail" with the role of the Department of Home Affairs but should not duplicate or conflict with it. The Department of Home Affairs' role is in national security while AEMO would be focused on cyber incidents affecting the NEM specifically. Acknowledging that some cyber risks could affect both the energy system and national security, we consider there is a need for AEMO to have a clearly defined power system-specific role which will complement Home Affairs' role where relevant.

Energy Queensland supported the proposed function 1, noting it should align with AEMO's existing NEM emergency management responsibilities under the Power System Emergency Management Plan (PSEMP).[40] The Australian Energy Sector Cyber Incident Response Plan is (and under the draft rule, would remain) distinct from the Power System Emergency Management Plan. The Power System Emergency Management Plan outlines how AEMO, jurisdictional authorities and industry participants would respond to a national electricity emergency to restore secure power supply as quickly as possible, within safe limits.[41] The Australian Energy Sector Cyber Incident Response Plan is cyber security-specific and more pre-emptive. The Australian Energy Sector Cyber Incident Response Plan would complement the Power System Emergency Management Plan by supporting AEMO and industry participants to respond to potential cyber incidents before they impact the supply of electricity to consumers.

AGL Energy noted that "this role has already been somewhat established within AEMO through the AEMO Cyber Duty Manager role (CDM) within AEMO's Australian Energy Sector Cyber Incident Response Plan."[42] For clarity, the Commission notes that the draft rule would not replace nor duplicate the work that AGL refers to, but enable it to continue with more certainty of funding and with protection from liability. The fact that AEMO has already developed the first version of the Australian Energy Sector Cyber Incident Response Plan means they are well placed to fulfil the formal cyber incident response coordinator role, as noted by the Smart Energy Council (SEC).[43]

The Commission considers that the incident coordinator function would benefit consumers by improving cyber incident preparedness and reducing the impacts of any such incidents on electricity supply. Industry stakeholders broadly support clarifying and confirming this function in the NER. Although a few stakeholders raised concerns about duplication, our assessment is that the Australian Energy Sector Cyber Incident Response Plan and AEMO's coordinator role would fill a unique need in responding to cyber incidents specifically affecting the power system.

2.2.2 Function 2: Supporting cyber preparedness and uplift

The industry uplift function would require AEMO to use reasonable endeavours to help market participants improve their cyber security preparedness and maturity. This function could include, but would not be limited to, the following:

39 Submissions to the consultation paper: SMA, p. 5; Ausgrid,p. 3; Anchoram Consulting, p. 1.
40 EQL submission to the consultation paper, p. 4.
41 AEMO, 'Emergency management - National role', https://aemo.com.au/en/energy-systems/electricity/emergency-management/national-role.
42 AGL submission to the consultation paper, p. 4.
43 SEC submission to the consultation paper, p. 3.

- **Stewardship of the Australian Energy Sector Cyber Security Framework** | AEMO previously co-developed the Australian Energy Sector Cyber Security Framework, and they would continue to maintain and update the framework as needed. This function would also include continuing to oversee Australian Energy Sector Cyber Security Framework self-assessments for industry. Note that AEMO already carries out this work, but the rule change would provide ongoing resourcing certainty and liability protection.
- **Organisation of testing and training exercises** | As part of this function, AEMO would support or undertake the development and delivery of scenario exercises to test the cyber resilience of the power system and industry participants. We understand AEMO has undertaken some exercises of this type in the past and the draft rule would support the continuation of this work through ongoing resourcing certainty.
- **Provision of guidance and advice to industry** | As part of this function, AEMO would provide industry cyber security guidance in the form of written materials, digital tools, participation in working groups, or by other means. The draft rule would not enable AEMO to create mandatory guidelines on cyber security.

AEMO is well-placed to support cyber security uplift in the energy industry due to their expertise and position as market operator. Improving industry participants' preparedness for a cyber incident will help mitigate the risk of such incidents and their consequences for consumers.

Stakeholders supported AEMO undertaking an industry uplift and preparedness function

The majority of stakeholders explicitly supported the industry uplift and preparedness function.[44] Some stakeholders expressed concerns or asked for clarifications about the function being performed by AEMO.[45]

The reasons that stakeholders gave for supporting this function included:

- prevention and preparedness work is an efficient approach to cyber risk management,[46]
- strengthening participants' cyber security preparedness would have benefits in many areas including power system security, network planning, and customer privacy,[47]
- stakeholders value the Australian Energy Sector Cyber Security Framework and support AEMO's continued stewardship of the framework,[48]
- establishing the function would ensure that industry uplift work such as the Australian Energy Sector Cyber Security Framework and testing and training exercises are resourced effectively,[49]
- establishing the function could allow AEMO to access additional funding for the Australian Energy Sector Cyber Security Framework in order to expand it and update it more frequently.[50]

AEMO developed the Australian Energy Sector Cyber Security Framework in 2018 and updated it in 2023 in consultation with governments and industry.[51] The Commission also understands that AEMO sometimes undertakes cyber resilience exercises and provides informal advice to industry. Some submissions noted that this type of work means AEMO is already performing some aspects

44 Submissions to the consultation paper: Anchoram Consulting, p. 3; SAPN, pp. 1-2; SMA, pp. 5-6; CEC, p. 2; AEMO, p. 2; Splunk, pp. 8-9; AGL, pp. 4-5; SEC, p. 3; Origin Energy, p. 1; Ausgrid, p. 4.

45 Submissions to the consultation paper: Alinta Energy, p. 2; EQL, p. 4.

46 Splunk submission to the consultation paper, p. 8.

47 SEC submission to the consultation paper, p. 3.

48 Submissions to the consultation paper: CEC, p. 2; TasNetworks, p. 1.

49 Anchoram Consulting submission to the consultation paper, p. 3.

50 SAPN submission to the consultation paper, pp. 1-2.

51 AEMO, 'AESCSF framework and resources', https://aemo.com.au/initiatives/major-programs/cyber-security/aescsf-framework-and-resources.

of the function, without it being specified in the NER.[52] Although supportive in principle, AGL questioned the need to clarify this function in the rules given AEMO's existing work.[53]

The intent of the draft rule is to embed and formalise this function for AEMO and ensure that this work is adequately resourced going forward. Confirming that this is one of AEMO's functions under the NER would also provide liability protection in performing this function, which would allow AEMO to take on appropriate risk to do so effectively. We understand liability protection could be particularly relevant to testing and training exercises which may involve AEMO interacting with participants' systems.

Alinta Energy partially supported the function but believed that some aspects were covered by the role of the Department of Home Affairs. It nevertheless supported the provision of general advice or guidance to industry by AEMO. Alinta Energy referenced the Department of Home Affairs' involvement in the May 2024 Trident exercise, suggesting that a role for AEMO was not necessarily needed.[54] The Commission understands that AEMO led the Trident exercise to test the Australian Energy Sector Cyber Incident Response Plan, with support from the Department of Home Affairs and the Australian Signals Directorate (ASD). The draft rule would support the continuation of such testing and training exercises, including collaborative exercises, which would have benefits for industry and the security of the NEM.

The industry uplift function would provide flexibility to align with existing cyber security governance

Energy Queensland did not support the industry uplift function. It considered that while industry would benefit from the activities described in this function, AEMO would not be the most appropriate party to carry them out. Energy Queensland considered that this function would be duplicative since, in its view, bodies such as the ASD and Cyber and Infrastructure Security Centre (CISC) have more relevant expertise and the ASD is already doing some of this work. It argued that preventative work to mitigate cyber security risks is outside of AEMO's remit, which should be limited to energy (as well as immediate emergency response, noting that a cyber incident is one potential cause of a power system emergency).[55]

However, the Commission considers that it is appropriate to establish a cyber security role for AEMO because:

- the unique insight AEMO provides as the system operator is not provided by other bodies,
- many aspects of NEM operation depend closely on data, data transfer, and digital systems, and
- a cyber security incident could have a significant and geographically widespread impact on power system security in the NEM.

TasNetworks suggested that the Australian Energy Sector Cyber Security Framework's self-assessment timing could be aligned with the timing of the Critical Infrastructure Risk Management Program (CIRMP) annual reporting requirements (Section 30AG of the SOCI Act).[56] AEMO is responsible for Australian Energy Sector Cyber Security Framework self-assessment timing; the draft rule would ensure that AEMO can devote resourcing to modifying the Australian Energy Sector Cyber Security Framework if it considers there is a need. The Commission

52 Submissions to the consultation paper: Anchoram Consulting, p. 1; TasNetworks, p. 1; AGL, p. 1; Origin Energy, p. 1.
53 AGL submission to the consultation paper, p. 4.
54 Alinta Energy submission to the consultation paper, p. 2.
55 EQL submission to the consultation paper, pp. 4-5.
56 TasNetworks submission to the consultation paper, p. 1.

understands that it is AEMO's intent to align Australian Energy Sector Cyber Security Framework financial year 2025 with the SOCI Act reporting timeframes.

A few stakeholders noted that developers and generators sometimes require their suppliers to comply with the Australian Energy Sector Cyber Security Framework, but that some parts of the framework do not logically apply to every part of the supply chain.[57] SMA considers that guidelines should be developed, either by AEMO or a government body explaining how the Australian Energy Sector Cyber Security Framework applies to OEMs and other stages of the supply chain.[58]

The Commission acknowledges that such guidelines would be valuable to OEMs and other businesses in the energy supply chain. However, any changes to the SOCI Act or clarification of how the SOCI Act should be applied are a matter for the Department of Home Affairs. Further, the draft rule would not give AEMO the power to impose mandatory obligations on market participants or OEMs.

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

Under this function, AEMO would develop cyber security advice or carry out cyber security research, specific to the energy sector, for provision to governments and potentially to industry. This research and advice function would enhance cyber security maturity for AEMO, governments, and industry participants. By further enabling AEMO to build up and share its cyber security expertise, this function would help governments and industry to prepare for and respond to cyber incidents to limit the impact on consumers.

This advice would draw on AEMO's unique energy expertise in their position as system operator, and would complement, rather than replace, work undertaken by other cyber security bodies such as the ACSC. Governments could request, for example, AEMO's insight, analysis or risk management planning advice on the risks that cyber events may pose to the electricity industry. Such advice could take the form of written reports which may or may not be made publicly available. The intention is that AEMO can initiate advice when it identifies an issue and would also be obliged to prepare advice as requested by a relevant Minister, subject to consultation on the nature and extent of the research or advice. Additionally, AEMO could collaborate with other bodies to provide advice.

As part of this function, AEMO could also, at its discretion, provide similar advice to NEM registered participants.

The function would be advisory only and would not expand AEMO's regulatory responsibilities, nor affect the roles of other regulatory or government bodies. Advice and risk evaluation provided under this function would be separate to AEMO's responsibilities under the General Power System Risk Review (GPSRR).

Stakeholders supported AEMO developing sector-specific cyber security research and advice

A number of stakeholders supported the function - either as described, or in principle.[59] Energy Queensland did not support the function as discussed below.[60] Some stakeholders suggested modifications to the design or definition of the function.[61]

57 Submissions to the consultation paper: SMA, p. 3; Fronius, p. 2; CEC, p. 2; SEC, p. 2.

58 SMA submission to the consultation paper, pp. 3-5.

59 Submissions to the consultation paper: Anchoram Consulting, p. 3; SAPN, p. 2; Alinta Energy, p. 3; SMA, p. 6; AEMO, p. 2; Vestas, p. 4; Splunk, pp. 9-10; SEC, p. 4; Origin Energy, p. 1; Fronius, p. 3; Ausgrid, p. 4.

60 EQL submission to the consultation paper, p. 5.

61 Submissions to the consultation paper: SAPN, p. 2; Splunk, pp. 9-10.

Several stakeholders considered that AEMO's advice could be highly valued by industry and government due to AEMO's expertise.[62] Stakeholders also noted that the costs for this function would be relatively low compared to the potential benefits.[63] A few stakeholders noted that establishing the function in the NER would support the continuation and refinement of informal industry advice and cyber security uplift work that AEMO already provides.[64]

Stakeholders provided varying comments on whether AEMO was best placed to provide industry-specific advice, to carry out research on cyber security risks, or both.

Energy Queensland considered that the advice function would not be consistent with AEMO's role as market operator. It considered that AEMO does not have the depth of field experience required to fully represent the cyber risks faced by industry. It suggested that governments should seek such insights directly from industry and not solely from AEMO.[65]

By contrast, AGL considered that AEMO would be able to provide unique and relevant industry expertise due to its position as system operator. However, AGL suggested that organisations such as the CSIRO may be better placed to lead cyber security research, with AEMO's subject matter expertise potentially supporting that work.[66]

Ausgrid suggested that AEMO's energy-specific advice could nicely complement the SOCI Act since the Act is "industry agnostic by design". It also noted that the market operator would be "best positioned to provide coordinated, aggregated advice to government on behalf of all energy market participants."[67] The Smart Energy Council considered it would be important for AEMO to take a "collaborative approach" and involve industry participants in the advice it develops for governments.[68]

AEMO could provide proactive or reactive advice that would complement other bodies' expertise

SA Power Networks (SAPN) and Splunk considered that the proposed function did not go far enough in enabling proactive research and advice, since the function was described as AEMO providing advice to energy ministers on request. SAPN's view was that the function "falls short of providing adequate responsibility for AEMO to proactively deal with emerging threats."[69] Splunk suggested that the scope of the proposed function should be expanded to include an annual or six-monthly "horizon scan for emerging threats, risks and capabilities specific to the energy sector."[70]

The Commission notes these comments and reiterates that the draft rule would not make AEMO the sole provider of cyber security advice to government. The proposed research and advice function would not replace other channels by which governments and industry may seek advice - including government agencies, research institutes, or working with industry. Further, AEMO would have the flexibility to seek input from other bodies or from industry when carrying out this function. The Commission also notes that the draft rule (available on the project page) would allow AEMO to provide advice to government or industry proactively without a specific request.[71]

62 Submissions to the consultation paper: Vestas, p. 4; Splunk, p. 9; AGL, p. 5; Ausgrid, p. 4.
63 Submissions to the consultation paper: SMA, p. 6; SEC, p. 4; Fronius, p. 3.
64 Submissions to the consultation paper: Anchoram Consulting, p. 3; Alinta Energy, p. 3.
65 EQL submission to the consultation paper, p. 5.
66 AGL submission to the consultation paper, p. 5.
67 Ausgrid submission to the consultation paper, p. 4.
68 SEC submission to the consultation paper, p. 4.
69 SAPN submission to the consultation paper, p. 2.
70 Splunk submission to the consultation paper, p. 9.
71 AEMC, Cyber security roles and responsibilities rule change, https://www.aemc.gov.au/rule-changes/cyber-security-roles-and-responsibilities.

This could even include regular risk assessment reports as suggested by Splunk.[72] Further, governments could request proactive as well as reactive advice if they consider there is a need.

The Commission therefore considers that AEMO's position and expertise as market operator would enable them to provide valuable research and advice on cyber security risks to the energy sector.

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

The information distribution function would have AEMO use its position as system operator to disseminate critical cyber security information to the energy industry. Since AEMO is a trusted body with communication channels that market participants use regularly, it could add value by providing a single source of cyber security notifications that are relevant to the energy industry. This would support industry participants to maintain cyber security preparedness and respond to cyber incidents in a timely manner.

The type of information that AEMO could distribute would include, but would not be limited to:

- warnings of cyber vulnerabilities or threats
- annual Australian Energy Sector Cyber Security Framework assessment conclusions
- post-cyber incident reports
- preventative patches in commonly used technologies.

The information distribution function could include redistributing other authorities' cyber security advice. AEMO could use their existing Market Notices system to share relevant information with market participants, or another means.

Stakeholders supported the information distribution function for AEMO

The majority of stakeholders supported the proposed information distribution function.[73] AGL and Energy Queensland expressed concerns about the function which are detailed below.[74]

The reasons that stakeholders supported this function included:

- ease of access to cyber security information, enabling industry participants to respond to incidents more quickly and effectively,[75]
- the "favourable cost-benefit ratio" of the proposed function,[76]
- "timely threat awareness, enhanced collaboration, and regulatory compliance",[77]
- the potential to address "blind spots",[78]

AGL considered that the proposed function 4 should be consolidated with function 1 due to an overlap between the two. In AGL's view, disseminating cyber security information would simply be part of AEMO's role as cyber security incident coordinator. The Commission notes that function 4 would be preventative and proactive as it is intended to be carried out during normal day-to-day operations, whereas the cyber security incident response plan and the role of incident coordinator

72 Splunk submission to the consultation paper, p. 9.

73 Submissions to the consultation paper: Anchoram Consulting, p. 3; Alinta Energy, p. 3; SMA, p. 6; Snowy Hydro, p. 1; CEC, p. 1; AEMO, p. 2; Vestas, p. 4; Splunk, p. 10; SEC, p. 4; Origin Energy, p. 1; Ausgrid, p. 4.

74 Submissions to the consultation paper: AGL, p. 5; EQL, p. 5.

75 Submissions to the consultation paper: Splunk, p. 10; Ausgrid, p. 4.

76 SMA submission to the consultation paper, p. 6.

77 Vestas submission to the consultation paper, p. 4.

78 CEC submission to the consultation paper, p. 2.

would only apply in the event of an actual cyber incident, making function 1 a reactive function. While both of these functions may involve AEMO distributing information to market participants, the Commission considers both should be established in the NER to adequately cover all operational scenarios.

Energy Queensland did not support the function, arguing it was not necessary for AEMO to share information that is already available elsewhere.[79]

> [T]his type of information is already published by a range of Australian and international government and commercial organisations, including the ASD. At best, this would become a duplication of these other information sources, creating a challenge for entities. At worst, this may lead organisations to solely rely on the information provided by AEMO, creating a dependency risk.

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

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

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

The Commission considers that the costs of the four functions are outweighed by the benefits of reducing cyber security risks. AEMO can upscale and further resource cyber security activities. This reflects the reality that while AEMO has been performing some of these activities the environment has changed considerably with cyber preparedness and uplift becoming increasingly more important for the NEM, requiring additional resourcing.

AEMO would recover the costs of performing the functions through participant fees. AEMO has provided cost estimates indicating that the functions would cost approximately $5-7 million per year (**Table 2.1**), or only around 2% of participant fees. Stakeholders generally agreed that these costs were justified because they would reduce the costs of responding to a cyber incident in the future, and that further resourcing is required to undertake more cyber security activities under the functions. Some stakeholders raised questions about transparency and consultation on costs, and the extent to which market participants would bear the cost of providing advice under function 3.

The draft rule would enable AEMO to recover cyber security costs through their normal cost recovery process (outlined in **Box 4**). Going forward, this would help ensure the cyber security functions are adequately and sustainably funded.

The draft rule is designed to embed and formalise AEMO's cyber security role and responsibilities in order to mitigate the risk of cyber incidents that could have a serious impact on the reliability and security of the NEM. The Commission considers that the benefit of addressing this risk outweighs the cost of performing the proposed functions.

79 EQL submission to the consultation paper, p. 5.

AEMO has estimated the costs of the functions to be less than $10 million per year (combined), as shown in **Table 2.1**. This is equivalent to only approximately 2% of participant fees.[80] While AEMO has already incurred some establishment costs for the functions, the additional establishment resourcing would allow AEMO to begin scaling up cyber security activities by providing further investment and enhanced resourcing under the functions (see **Table 2.2**). These additional establishment costs, such as deployment of systems and tools like out-of band communications or a Customer Relationship Management tool, could be funded through participant fees following the commencement of the final rule.

Table 2.1: AEMO has estimated the costs of the four functions

Function	Establishment	Year 1	Year 2	Ongoing
1. Cyber incident response coordinator	$4,525,000	$4,250,000	$3,150,000	$3,125,000
2. Cyber security uplift and preparedness	$1,560,000	$2,025,000	$1,525,000	$1,525,000
3. Research and advice	Nil	$775,000	$400,000	$400,000
4. Information distribution	$375,000	$350,000	$350,000	$350,000
Total	**$6,460,000**	**$7,400,000**	**$5,425,000**	**$5,400,000**

Source: AEMO cost estimate provided in the Minister's rule change request.

Several stakeholders expressed the view that the proposed functions would be cost-effective. That is, the expected cost was low compared to the potential benefits in avoiding or mitigating the impact of cyber security incidents.[81] Ausgrid, Fronius and SMA further noted that the cost for the industry to respond to a cyber incident without adequate preparation could be very large.[82]

However, other stakeholders requested:

- Further justification of the costs and transparency around the estimate in **Table 2.1**, and the funding scope considering some functions are not necessarily new,[83]
- Fair allocation of costs between industry and government, especially where the function will provide direct benefit to government,[84]
- Clarification on compliance costs for any industry participants (Ausgrid requested more information on any compliance costs and how they could be recovered; Snowy Hydro's view was that the rule change should not increase the cyber compliance burden),[85]
- A review mechanism after implementation and an independent assessment for AEMO's cyber security resourcing,[86]

Regarding these concerns, the Commission considers that the costs are justified because they formalise AEMO's role and responsibilities in undertaking cyber security work which is already underway and already benefiting participants. This reflects the reality that while AEMO has been performing some of these activities the environment has changed considerably, with cyber

80 Rule change request to the AEMC, Minister Bowen, pp. 9-10.
81 Submissions to the consultation paper: SMA, pp. 5-6; Splunk, pp. 8-10; SEC, p. 4; Fronius, p. 3; Ausgrid, p. 3; Anchoram Consulting, p. 2.
82 Submissions to the consultation paper: Ausgrid, p. 3; Fronius, p. 2; SMA, p. 5.
83 Submissions to the consultation paper: Fronius, p. 3; Alinta Energy, p. 1; ENA, pp. 2-3; SMA, p. 6.
84 AGL submission to the consultation paper, p. 5.
85 Submissions to the consultation paper: Ausgrid, p. 3; Snowy Hydro, p. 2.
86 Submissions to the consultation paper: AGL, p. 6; SAPN, p. 3.

preparedness and uplift becoming increasingly more important for the NEM, requiring additional resourcing. Further, the Commission has engaged in discussions with AEMO to understand how the cyber security work undertaken to date has been funded and how the new funding enabled by this rule change would be used. Where AEMO has completed work that would form part of the proposed functions, we understand this has been achieved either by diverting AEMO's existing resources, or by a one-off provision of funding from jurisdictional or Commonwealth governments. These forms of funding are not sustainable and do not provide any certainty that the cyber security work would continue.

Box 4 outlines how AEMO recovers its costs, including how it consults on its budget and fee structure.

Box 4: How AEMO recovers fees from participants

AEMO recovers its costs from industry participants based on the extent to which participants are involved in AEMO's activities, through 'participant fees'. Participant fees include the recovery of various expenses, including those related to the operation of the national electricity market, power system security and reliability, major reform initiatives, and incremental services. These fees also cover a number of functions (or services) that AEMO performs to support the core operation of the NEM, including:

- national transmission planning
- management of five-minute settlements
- trading in the Settlements Residue Auction
- management of the NEM2025 Reform Program
- facilitation of retail market competition
- provision of a consumer data platform
- integrating CER and DER into the NEM.

To ensure transparency, under the NER, each year AEMO must publish:

- an annual budget of its revenue requirements by the start of each financial year
- a structure setting out how its budgeted revenue is to be recovered through participant fees.

AEMO consults on its budget and fees using the Rules consultation procedures (see note). The Rules consultation procedures involve the publication of a consultation paper, draft document and final document, with opportunities for stakeholders to make submissions. In addition, AEMO has established the Financial Consultation Committee (FCC) to consider and provide feedback on its budget, fees, and corporate plan priorities. The FCC meets at least three times per year and consists of industry, government and consumer representatives.

Under section 119 in the NEL, prescribing functions such as these within the NER provides AEMO immunity from liability for the delivery of these services, consistent with the performance of other functions and activities.

Source: AEMO, 'Draft FY25 budget and fees consultation', https://aemo.com.au/consultations/current-and-closed-consultations/draft-fy25-budget-and-fees-consultation;
AEMO, 'List of industry forums and working groups - Financial Consultation Committee', https://aemo.com.au/en/consultations/industry-forums-and-working-groups/list-of-industry-forums-and-working-groups/financial-consultation-committee;
AEMO, 'Strategic Corporate Plan FY24', https://aemo.com.au/-/media/files/about_aemo/corporate-plan/2023/corporate-plan-2024-final.

Note: NER clause 2.11.1(a) requires AEMO to apply the Rules consultation procedures when developing its participant fee structure. In practice AEMO consults on its budget and fees simultaneously through one process (e.g. see the FY 2024-25 consultation referenced above).

The Energy and Climate Change Ministerial Council or a Minister may request advice from AEMO (on any relevant matter, not limited to cyber security) under section 51 of the NEL. The costs that AEMO recovers through participant fees would be used for, at minimum, governance of this function and assessing and scoping requests for advice (see **Table 2.1**). AEMO and governments could determine on a case-by-case basis whether it is appropriate to fund substantial pieces of work through participant fees or if another source of funding is needed.[87]

Splunk requested clarification on whether the new funding would cover cyber security work relating to both information technology (IT) and operational technology (OT) systems, considering that both domains should be addressed together.[88] The functions as defined in the NER would not distinguish between IT and OT and therefore would be agnostic to the systems impacted.

It is the Commission's understanding that while the tasks and activities associated with the proposed functions have been performed to varying degrees, all of the proposed functions will require investment and enhanced resourcing beyond existing efforts to appropriately deliver these functions. More information is provided in **Table 2.2** below. At present AEMO can only resource a minimum requirement approach to perform these activities, given the authority under the NER has not existed.

Additionally, the Commission considers that by clarifying these costs and funding arrangements, cost implications would be transparent, justified, and not duplicative, because:

- The draft rule does not enable AEMO to create new obligations on participants, and hence we do not expect there to be any mandatory compliance costs for industry participants.
- If the rule is made, the forecast costs of performing cyber security functions would be incorporated into AEMO's annual budget and fee process. AEMO would consult on the costs and how to recover them from participants through both a public consultation process and the FCC, as outlined in **Box 4**.[89] The costs would be recovered as per AEMO's NEM Participant Fee structure which is also subject to consultation under the NER.[90]
- AEMO has also engaged an independent consultant to develop the cost estimate approach.

87 Sections 51 and 51A of the Schedule to the NEL.
88 Splunk submission to the consultation paper, p. 4.
89 AEMO submission to the consultation paper, p. 3.
90 NER clause 2.11.1(a).

Table 2.2: AEMO has diverted existing resources to carry out limited cyber security activities

Function	Activities that could be undertaken if the draft rule is made	Activities that AEMO already undertakes	Funding source for activities AEMO already undertakes
Function 1: Incident coordinator	Scale up activities undertaken so far to capture a wider group of participants. Deploy necessary tools and supporting process and governance structures (e.g. technology platform to collect and assess relevant data). Implement revisions to the Australian Energy Sector Cyber Incident Response Plan more quickly. Align resourcing more appropriately with expected requirements based on risk landscape.	Developed the Australian Energy Sector Cyber Incident Response Plan, and completed an update in 2023. AEMO has otherwise adopted a best endeavours approach where need is urgent, e.g. by prioritising working with the most critical market participants and government agencies.	AEMO has maintained a minimalist approach and allocated limited internal funding.
Function 2: Industry preparedness and uplift	Scale up collection, analysis, and reporting of Australian Energy Sector Cyber Security Framework data. Potential to develop additional Australian Energy Sector Cyber Security Framework tools, resources and guidance, in collaboration with industry and government partners. Champion AEMO across various sector-wide cyber activities and forums.	Development and roll-out of the Australian Energy Sector Cyber Security Framework in 2018. Annual Australian Energy Sector Cyber Security Framework assessments in 2018-2023. Maintenance of Australian Energy Sector Cyber Security Framework versions 1 and 2 and related materials, e.g. on AEMO website.	Activities have been partially funded by the Commonwealth, States and Territories. AEMO has maintained a proportionate approach, allocating internal funding only as needed.

Function	Activities that could be undertaken if the draft rule is made	Activities that AEMO already undertakes	Funding source for activities AEMO already undertakes
	Act as a facilitator between energy organisations and the government across multiple forums, platforms and resources.	Provision of ad hoc guidance on the Australian Energy Sector Cyber Security Framework. Liaising with federal agencies to ensure the Australian Energy Sector Cyber Security Framework is well understood and fit-for-purpose.	
Function 3: Research and advice	Establish and maintain a governance structure for the management of requests. Enhance AEMO's capacity to provide research and advice.	AEMO has provided ad hoc advice to a range of Commonwealth agencies since 2018 without any formal processes being established.	AEMO has maintained a minimalist approach and allocated limited internal funding. Specific cyber security-related advice has been partially funded by the Australian Renewable Energy Agency (ARENA) and the Department of Climate Change, Energy, the Environment and Water.
Function 4: Information distribution	Formalise processes and deploy tools to facilitate 24/7 dissemination of information.	Distribution of critical cyber communications since 2022 on an ad hoc basis (generally at the request of federal agencies).	AEMO has maintained a minimalist approach and allocated limited internal funding.

Source: AEMO.

2.4 The draft rule would commence on 12 December 2024

Box 5: The draft rule would commence on 12 December 2024

The Commission's draft determination is that the draft rule should commence as early as possible. AEMO does not require an implementation period before commencement. The draft rule would come into effect as soon as the final determination is published on 12 December 2024.

This would mean that AEMO could commence consultation on cost recovery immediately. Costs would be recovered from participants starting 6-18 months after the rule commencement.

The Commission's final determination is due on 12 December 2024 and the draft rule would commence immediately. Immediate commencement is possible because AEMO is already performing some parts of the functions without having a cyber security role established in the NER.

An early commencement date would allow AEMO to access cost recovery and protection from liability for the cyber security functions as soon as possible. Benefits for consumers would be realised more quickly in turn. AEMO will only be able to recover costs, and sufficiently commit resources to these four functions, from the commencement of the final rule.

AEMO would need to determine and consult on the participant fee structure and the period for cost recovery. Consultation could begin as soon as the rules take effect. If AEMO sought to determine the cyber security functions as a declared NEM project, as per clause 2.11.1 of the NER,[91] it would need to follow the Rules consultation procedures in making this determination.[92] AEMO would consider the timing of consultation on fees and structure, and the NEM declared project if it elects to do so.

In addition, AEMO would need to carry out work to establish or ramp up some aspects of the cyber security functions. However, the Commission considers that AEMO could do this work while the draft rule is already in effect (resources permitting) because the functions are facilitative and flexible.

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

91 AEMO submission to the consultation paper, p. 3.

92 Clause 2.11.1(bc) of the NER.

2.5 Stakeholders raised cyber security issues being considered in other processes

Several stakeholders raised concerns about cyber security guidance for CER and about the role that networks should play in cyber security. These concerns are being considered in other processes.

- Some submissions noted that the SOCI Act does not apply to generators smaller than 30 MW and does not have a clear classification for CER aggregators which may control much more than 30 MW.[93] The Clean Energy Council added that it can be unclear which SOCI Act requirements should be passed through to OEMs.[94]
- Specifically, a few stakeholders noted that some DNSPs are creating guidelines for how the SOCI Act requirements apply to CER and OEMs in different parts of the supply chain, or indeed imposing their own requirements.[95] SMA considered this could create "potential for misunderstanding and disagreement", while the Smart Energy Council noted a lack of consistency between jurisdictions.[96] (However, Energy Queensland and AGL considered that sufficient guidance, such as the Australian Energy Sector Cyber Security Framework, is already available to participants and that additional guidance would risk duplication and confusion.[97])
- Fronius suggested that a national cyber security strategy was needed to establish a coordinated approach to CER cyber security requirements.[98] The Smart Energy Council requested more clarity from market bodies and governments on these matters.[99]

The Commission acknowledges that cyber security is a pertinent issue for CER and that coordinating cyber security requirements across the supply chain for small-scale generation is challenging. The Department of Climate Change, Energy, the Environment and Water's CER Taskforce is currently looking into this issue. We consider that cyber security for CER and CER aggregators is best addressed through that process.

SMA and Energy Networks Australia (ENA) raised broader questions about the role of transmission networks service providers (TNSPs) and DNSPs in cyber security. ENA suggested that the role of networks could be clarified in the NER in a similar way as the proponent requested for AEMO's responsibilities, so that networks could also access improved funding certainty for cyber security work.[100] The Clean Energy Council noted that cyber security uplift is already included in DNSPs' revenue determinations, commenting that cyber security is important across the energy industry.[101]

The proponent's rule change request was focused on AEMO's cyber security responsibilities and the scope of this rule change is limited to AEMO's role. If networks' role in cyber security needs clarification in the future, this could be addressed through a different process. We note that networks are responsible for the cyber security of their own assets under the SOCI Act.

Further information is provided in **appendix D**.

93 Submissions to the consultation paper: Fronius, p. 1; SEC, p. 2; SMA, p. 5.
94 CEC submission to the consultation paper, p. 2.
95 Submissions to the consultation paper: SMA, p. 3; Fronius, p. 2; CEC, p. 2; SEC, p. 2.
96 Submissions to the consultation paper: SMA, p. 5; SEC, p. 2.
97 Submissions to the consultation paper: EQL, p. 3; AGL, pp. 2-3.
98 Fronius submission to the consultation paper, p. 1.
99 SEC submission to the consultation paper, p. 2.
100 ENA submission to the consultation paper, p. 3.
101 CEC submission to the consultation paper, p. 1.

3 The rule would contribute to the NEO

This chapter sets out how our draft rule promotes the National Electricity Objective (NEO). It explains how our draft rule promotes the safety, security and reliability of the power system. This includes how it is aligned with principles of good regulatory practice and takes implementation considerations into account.

In this chapter:

- **Section 3.1** outlines the NEO test that the Commission must apply to make a draft rule.
- **Section 3.2** explains how our draft rule contributes to the NEO.

3.1 The Commission must act in the long-term interests of electricity 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.[102]

For this rule change, the relevant energy objective is the NEO.

The NEO is:[103]

> to promote efficient investment in, and efficient operation and use of, electricity services for the long term interests of consumers of electricity with respect to—
>
> (a) price, quality, safety, reliability and security of supply of electricity; and
>
> (b) the reliability, safety and security of the national electricity system; and
>
> (c) 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 NEO.[104]

There are also a number of relevant legal requirements for the Commission to consider under the NEL to make a draft rule determination. These are set out in **appendix C**.

3.2 We must also considered how the rule would apply in the Northern Territory

The draft rule would apply in the Northern Territory, as it amends provisions in the NER Chapter 10, which does apply in the Northern Territory. However, these amendments would have no practical effect in the Northern Territory.

See **appendix C** for more detail on the legal requirements for our decision.

102 Section 88(1) of the NEL.
103 Section 7 of the NEL.
104 Section 32A(5) of the NEL.

3.3 Our draft rule to confirm and clarify AEMO's cyber security role would contribute to the achievement of the NEO

The Commission has identified the following **three** criteria to assess whether the proposed rule change would better contribute to achieving the NEO compared to the status quo:

- **Safety, security and reliability:** we have considered whether confirming and clarifying the four functions for AEMO would help enable the secure provision of electricity in the long term, ensuring safety and security outcomes for participants and consumers are promoted.
- **Principles of good regulatory practice:** we have considered if the proposed rule change would enhance predictability, stability, and transparency without being overly prescriptive or duplicative. In doing this we have considered the broader direction of cyber security reforms and frameworks.
- **Implementation considerations:** we have assessed the cost implications, timing considerations, and implementation considerations for industry and relevant jurisdictional conditions.

These assessment criteria reflect the key potential impacts – costs and benefits – of the rule change request, for impacts within the scope of the NEO. Our reasons for choosing these criteria are set out in **section 4.2** of the consultation paper.[105]

Following stakeholder feedback to the consultation paper the Commission is satisfied that the assessment criteria are fit for purpose. Three stakeholders explicitly supported the proposed assessment criteria.[106] Five stakeholders, while supporting the proposed assessment criteria, suggested including additional criteria to consider national security and international obligations, and outcomes for consumers.[107] The Commission does not propose including these additional criteria because:

1. while the cyber security of the power system can be a national security matter the SOCI Act governs national security and international obligations based concerns. AEMO already has obligations under the SOCI Act to maintain the cyber security of its asset.
2. while the Commission agrees that this rule change will provide outcomes for consumers, we consider this occurs through the draft rule promoting safety, security, and reliability outcomes for consumers, where those benefits outweigh any costs.

The Commission has undertaken regulatory impact analysis to evaluate the impacts of the various policy options against the assessment criteria. **Appendix B** outlines the methodology of the regulatory impact analysis.

3.3.1 Confirming four functions for AEMO would contribute to the NEO

The Commission has assessed the qualitative costs and benefits of including the four cyber security functions for AEMO in the NER. We consider that the benefits of confirming and formalising cyber preparedness and responsiveness roles for cyber incidents outweigh the costs. Explicitly referencing cyber security in the rules, as it relates to power system security, contributes to the NEO as it is in the long-term interests of consumers.

105 AEMC, Cyber security roles and responsibilities consultation paper, Consultation paper, 20 June 2024, https://www.aemc.gov.au/sites/default/files/2024-06/ERC0388%20Consultation%20Paper%20-Cyber%20security%20roles%20and%20responsibilities.pdf.

106 Submissions to the consultation paper: Anchoram Consulting, p. 2; Alinta Energy, p. 3; EQL, p. 5.

107 Submissions to the consultation paper: SMA, p. 9; Vestas, p. 4; AGL, p. 6; SEC, p. 4; Ausgrid, p. 4.

We consider the estimates provided by AEMO (see **Table 2.1**) sufficient to illustrate the cost impacts of the four functions. We also consider that the costs are justified because by embedding and formalising AEMO's role and responsibilities under the NER they reduce cyber security risks, and if an incident were to occur the costs would be far greater than providing preparedness measures. Additionally, AEMO already performs some of these activities so participants are already benefiting from some cyber security measures. AEMO can upscale and further resource these activities. This reflects the reality that while AEMO has been performing these activities the environment has changed considerably with cyber preparedness and uplift becoming increasingly more important for the NEM, requiring more resourcing. This not only provides confidence that the benefits will be realised but that AEMO's estimation of costs are likely to be accurate. See **section 2.3** for an analysis of costs.

Our analysis against the relevant assessment criteria is outlined below.

3.3.2 The draft rule would promote safety, security and reliability

The Commission considers that by embedding and formalising AEMO's functions in the NER the draft rule would provide safety, security, and reliability outcomes by securing the provision of electricity, which will also benefit consumers.

Cyber security is important to power system security and reliability because a cyber incident in the electricity sector could have far-reaching implications from widespread outages, to economic disruptions, breach of sensitive data, and threats to national security. Stakeholders agreed that security is a paramount consideration, noting that a "NEM wide cyber event could destabilise large portions of the Nation".[108]

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

At present, the lack of confirmation on AEMO's role and responsibilities for cyber security in the NER means that it is not properly resourced to undertake cyber security functions. This could lead to inconsistency in cyber security preparedness and response measures due to a lack of clarity among participants about what AEMO's role and responsibilities are. This inconsistency and lack of clarity presents an ongoing security risk to the NEM, specifically:

- The lack of confirmation on AEMO's role and responsibilities with regard to cyber security **preparedness** measures could make the power system more vulnerable to cyber incidents due to the lack of coordination among participants.
- In the event of a cyber security incident, without clearly defined functions, this could jeopardise AEMO's and participants' **responsiveness** due to a lack of coordination.

Currently, under AEMO's function to maintain and improve power system security, AEMO can issue system security directions,[109] prepare a system restart plan for managing and coordinating system restoration during a major disruption,[110] and coordinate the protection of power system equipment.[111] As the system operator AEMO is well-placed to support the energy sector with preparedness, learning and uplift activities. The four functions under the draft rule would give

108 Submission to the consultation paper, Anchoram Consulting, p.3.
109 Clause 4.8.9 of the NER.
110 Clause 4.3.1.(p)(2) and (3) of the NER.
111 Rule 4.6 of the NER - Protection of Power System Equipment.

AEMO the ability to be properly resourced to undertake more **proactive** preparedness, learning and uplift activities, as opposed to the more traditional role of maintaining and improving power system security. Specifically, the four functions contribute to **proactive** measures as AEMO could:

- Have a cyber security framework that can help prevent security incidents, such as the AESCSF, which helps industry participants keep their precautionary measures current. See **section 2.2.2.**
- Examine risks and provide proactive cyber security advice to government and industry. See **section 2.2.3.**
- Disseminate critical cyber security information, such as preventative patches in commonly used technologies. See **section 2.2.4.**

In considering stakeholder feedback, the Commission is of the view that confirming and clarifying AEMO's functions in the NER would promote safety, security, and reliability outcomes. Specifically stakeholders said that without clarity and a coordinated strategy to build and maintain cyber security we are at risk of a fragmented security response,[112]and that there needs to be a focus on making the entire system more resilient to ensure energy security.[113]

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

3.3.3 The draft rule is aligned with principles of good regulatory practice

The Commission considers that by embedding and formalising AEMO's functions in the NER the draft rule would be aligned with principles of good regulatory practice because it is seeking to improve predictability, stability and transparency of cyber security where the power system is increasingly digitised. The draft rule also considers broader reforms while avoiding duplication.

Under the draft rule AEMO would have **predictability and stability** because by confirming the functions they would have funding certainty and liability protection which would allow for resourcing certainty to properly establish and undertake cyber security activities on more well-defined and permanent basis. Funding certainty and liability protection would enable AEMO to continue and scale up its cyber security activities. Additionally, market participants would be able to confidently rely on AEMO to perform specific preparedness, uplift and responsiveness activities. Since these activities are outlined as principles and key functions in the draft rule, AEMO is not unduly limited in the activities they can undertake, and there are no overly prescriptive requirements for industry because AEMO would not have the ability to propose mandatory obligations on participants.

It follows that AEMO, government, and market participants would then have **transparency** around activities and around the cost of AEMO's cyber security role and responsibilities. To ensure transparency under the NEM, each year AEMO must publish: an annual budget of its revenue requirements and a structure setting out how its budgeted revenue is to be recovered through participant fees.[114]

Cyber security is a particularly prominent issue in energy security given the NEM's increasing digitisation and connectivity. Bearing this in mind, **broader cyber security reforms** have been taken into consideration (see **section 1.4**, and **appendix A**). Specifically, by including the four functions

112 Submissions to the consultation paper: Vestas, pp. 2-3; SEC, p.2.

113 SEC submission to the consultation paper, p. 3.

114 AEMO, Strategic Corporate Plan FY24, https://aemo.com.au/-/media/files/about_aemo/corporate-plan/2023/corporate-plan-2024-final.pdf?la=en&hash=6B1F5BB7C3173578FB744FB92750F88D.

for AEMO in the NER, the draft rule confirms a recommendation from the Finkel Review that AEMO should have a cyber security role. While AEMO has begun performing some of the activities under the functions, because of their inability to recover costs and lack of liability protection they have been unable to upscale and adapt to circumstances as need arises. Importantly, the proposed functions complement, rather than duplicate, the role of other agencies such as the ACSC and frameworks such as the SOCI Act, because they have a different focus and because of the unique insight AEMO provides as the system operator which is not provided by other bodies.

In considering stakeholder feedback, the Commission is of the view that confirming and clarifying AEMO's functions in the NER would be aligned with principles of good regulatory practice. Specifically stakeholders said that it is problematic that cyber security activities remain unclear as this prevents coordination of activities,[115] that without predictability and stability there is a problem waiting to happen that will be costly to industry,[116] and that market participants benefit from clear definitions which will set clear expectations.[117] See **section 2.2** for more detailed information on the four functions.

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

The Commission considers that by embedding and formalising AEMO's functions in the NER the draft rule would take implementation considerations into account by considering cost implications, governance complexities, timing considerations, and relevant jurisdictional conditions.

The Commission considers that the overall **cost** of formalising cyber preparedness and incident response functions 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. Further, the Commission considers that the costs are justified because the work is already underway and already benefiting participants, meaning AEMO can upscale and further resource these activities. This reflects the reality that while AEMO has been performing these activities the environment has changed considerably with cyber preparedness and uplift becoming increasingly more important for the NEM, requiring more resourcing. This will support participants to improve their levels of cyber preparedness and maturity without any additional mandatory obligations, which will reduce associated costs. This not only provides confidence that the benefits will be realised but that AEMO's estimation of costs are likely to be accurate. See **section 2.3** for more information about the benefits of the four functions outweighing the costs.

The Commission considers that any existing **complexities in cyber security governance** would become more transparent and simplified as the draft rule would formally establish functions for AEMO, which would make cyber security governance more transparent for industry.

The draft rule would clarify any **uncertainty and timing** considerations by providing more certainty around cyber security in the NER. Cyber security is a prevalent issue in the NEM that cannot remain unconfirmed and without adequate resourcing. Additionally, since the functions in the draft rule build on what AEMO is already undertaking, the functions could come into effect immediately, with cost funded through AEMO fees following the commencement of the rule. See **section 2.4**.

The **impact** on AEMO and other participants would be manageable because AEMO is already performing some of the activities under the new proposed functions, meaning that some

115 Submissions to consultation paper: CEC, p. 1; Splunk, p. 5.
116 Fronius -submission to consultation paper, p. 2.
117 Splunk submission to consultation paper, p. 6.

processes are place that can be built on. While the draft rule proposes to establish four functions, AEMO is not limited in its activities under the functions, meaning they are well placed to adapt to cyber security needs. AEMO is supportive on the basis that costs can be recovered and liability protection would be granted.[118] The draft rule does not provide AEMO with the ability to impose additional mandatory obligations on market participants, meaning the compliance costs for participants would be low. AEMO's proposed four functions should assist participants in managing cyber security risks because they would support cyber preparedness and uplift, examine cyber risks and provide advice, and facilitate the distribution of critical information which will help participants manage cyber security risks before they eventuate into an incident. See **section 2.2**.

Additionally, the draft rule takes into consideration **relevant jurisdictional conditions** across the NEM. Cyber security incidents across the NEM could affect individual assets or the system as a whole. In addition to the SOCI Act which places an obligation on AEMO to look after its own asset, addressing the power system from a national security perspective, clarifying and confirming the proposed functions in the draft rule would help ensure that system-wide risks between participants and AEMO are being addressed. Since the NEM is interconnected between regions, a cyber security incident can have a system-wide effect, meaning that necessarily a rule to manage system wide risks should apply to all NEM jurisdictions.

While Western Australian, the Northern Territory, and gas markets also face cyber security risks and potentially lack clear roles and responsibilities, it is the Commission's understanding, as detailed in the rule change request, that these matters will be dealt with through a separate process.[119]

118 AEMO submission to the consultation paper, p. 1.

119 Rule change request to the AEMC, Minister Bowen, p. 4.

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.[120]

A.1 Cyber security governance has expanded over the last 10 years

Cyber security is of critical importance in Australia. While it impacts all sectors, it is a particularly prominent issue in energy security given the NEM's increasing digitisation and connectivity. This includes real-time data of critical power system components, SCADA systems, smart grids, smart meters and smart appliances connected to open networks. Additionally, the NEM's high take up of CER and DER, such as neighbourhood batteries, further amplifies the issue.

Digitisation can bring a range of benefits including new opportunities for innovation and an increase in transparency at both a system-wide level and on an individual customer basis. Australia's high CER uptake also provides benefits including supporting a reduction in overall system costs, improving reliability, and achieving a secure, low-emission energy supply for all consumers.

However, the NEM's integration of information and communications technology and connectivity also increases the power system's cyber vulnerability. A cyber security incident in the electricity sector could have far-reaching implications, from widespread outages, to economic disruptions, breach 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.

The cyber attack in Ukraine in December 2015 is the most well-known cyber security incident on a large energy grid. The attack on three regional electricity distribution companies impacted 225,000 customers.[121] Restoration efforts were delayed as the attack disabled control systems, disrupted communications and prevented automated system recovery.

While there has been no publicly reported large-scale cyber attack on Australia's power system, there has been a growing number of incidents on major corporations. Latitude, an Australian financial service provider, was breached in March 2023 which affected over 14 million individuals from Australia and New Zealand. The previous year, Australia also saw cyber attacks on Medibank and Optus. Each attack impacted just under 10 million customers, nearly 40 per cent of the

120 See our website for more information on the rule change process: https://www.aemc.gov.au/our-work/changing-energy-rules.
121 US Department of Homeland Security, https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01.

Australian population. Both companies saw personal data compromised and Optus also experienced a widespread telecommunication outage. These incidents highlight the growing prevalence of cyber security in the Australian context.

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 electricity sector to enhance their cyber security posture and respond effectively to cyber incidents. The ACSC is one of several government agencies with a role in cyber security governance, listed in **Table A.1**.

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 which 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 which 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.
Cyber and Infrastructure Security Centre (CISC)	Assists critical infrastructure owners and operators to understand risk and meet regulatory requirements. Reports to the Department of Home Affairs.
State and territory cyber security units	The larger jurisdictions have cyber security units that support government (and sometimes public sector) cyber security initiatives. They may also be responsible for leading jurisdictional government responses to cyber incidents. Smaller jurisdictions usually fulfil this function within an existing department.

Source: ASD, www.asd.gov.au/about/who-we-are; ACSC; Department of Home Affairs - 'Cyber security', www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security, 'Critical infrastructure security', www.homeaffairs.gov.au/about-us/our-portfolios/cyber-and-infrastructure-security; CISC, www.cisc.gov.au/; QLD Government - 'About the CyberSecurity Unit', www.forgov.qld.gov.au/information-and-communication-technology/cyber-security/about-the-cyber-security-unit; NSW Government - 'Cyber Security NSW', www.digital.nsw.gov.au/delivery/cyber-security; VIC Government - 'About the Cyber Security Unit', www.vic.gov.au/about-cyber-security-unit; Government of WA - 'CyberSecurity Unit', www.wa.gov.au/organisation/department-of-the-premier-and-cabinet/office-of-digital-government/cyber-security-unit.

Later the Finkel Review, 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, with the report noting "strong cyber security measures for the NEM will be essential for maintaining Australia's growth and prosperity in an increasingly global economy."[122] The review recommended:[123]

> 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. It was developed through collaboration with industry and government stakeholders, including AEMO, the ACSC, the CISC, and representatives from Australian energy organisations. It is both a framework and an annual voluntary assessment program, enabling participants to undertake assessments of their own cyber security capability and maturity. Participants can use the results to inform and prioritise investment to improve cyber security posture.

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

As noted above, the recently amended SOCI Act places cyber security obligations on owners and operators of critical infrastructure, including electricity and gas infrastructure.[124] The Australian Energy Sector Cyber Security Framework can be used by owners and operators to meet SOCI Act requirements.[125] Aside from this, the Commission is not aware of any other Australian policy or regulations on cyber security specifically for the energy sector. The SOCI Act effectively requires NEM participants, including AEMO, to manage their own critical infrastructure in a cyber secure manner, whereas this rule change is primarily concerned with facilitating cohesive cyber security practices across all NEM participants.

One such practice mentioned in the rule change request is a cyber incident response plan for the energy sector.[126] Each NEM state or territory has an emergency management plan developed by a government agency that would apply in a significant cyber or energy supply incident.[127]

---

122 Finkel 2017, 'Independent Review into the Future Security of the National Electricity Market: Blueprint for the Future', p. 67, https://www.dcceew.gov.au/sites/default/files/documents/independent-review-future-nem-blueprint-for-the-future-2017.pdf.

123 Ibid., p. 69.

124 Australian Government, Security of Critical Infrastructure Act 2018, https://www.legislation.gov.au/C2018A00029/latest/text.

125 AEMO, 'AESCSF framework and resources', https://aemo.com.au/en/initiatives/major-programs/cyber-security/aescsf-framework-and-resources.

126 Rule change request to the AEMC, Minister Bowen, p. 4.

127 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-recovery-management/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.

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.[128] Similarly, many jurisdictions have a sub-plan for a serious cyber incident, but these do not consider a cyber incident impacting the energy sector specifically. This means there may be a need for a bespoke NEM cyber incident response plan.

While the scope of this rule change is the NEM - governed by the NER - there may be a similar need to confirm and clarify functions in other Australian energy systems. Like the NER, the National Gas Rules (NGR) cover system security in a general sense but do not include cyber security provisions.[129] The situation is similar for the Wholesale Energy Market (WEM) Rules which apply to the Western Australian electricity system.[130] The rule change proponent states they will look to address cyber security in the WEM and gas markets through separate processes.[131]

A.2 The Minister proposed a rule to confirm and clarify AEMO's role in cyber security functions

The Minister proposed that as energy systems become increasingly interconnected and reliant on digital technologies, the potential impact of a cyber breach amplifies and underscores the urgent need for robust and clearly defined security measures and roles, to support vigilance within the energy space.

The proponent identified two broad issues relating to the current cyber security arrangements in the NER:

1. cyber security is not explicitly referenced in the rules, and is not explicitly defined as it relates to power system security
2. specific functions that AEMO would perform to assist in enhancing cyber security across the energy system are not specified in the rules.

The proponent considered that AEMO's lack of resourcing for these additional functions in the NER poses an ongoing risk to the security of the NEM. To resolve this, the Minister seeks to clarify cyber security as a function within AEMO's existing role to maintain power system security and confirm and clarify four functions for AEMO to perform to assist in maintaining a secure power system.

While AEMO has performed some of the activities under these functions to date, the request considers that this has been done so in a limited capacity using existing resources. These changes would enable AEMO to recover the costs it incurs in carrying out these functions and confirm AEMO's immunity from liability for the delivery of these functions (see chapter 2).

The rule change request can be found on the project page.[132]

128 '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.

129 AEMC, National Gas Rules, https://energy-rules.aemc.gov.au/ngr/558.

130 Government of Western Australia, WEM Rules, https://www.wa.gov.au/government/document-collections/wholesale-electricity-market-rules.

131 Rule change request to the AEMC, Minister Bowen, p. 4.

132 AEMC, Cyber security roles and responsibilities rule change, https://www.aemc.gov.au/rulechanges/cyber-security-roles-and-responsibilities.

A.3 The process to date

On 20 June 2024, the Commission published a notice advising of the initiation of the rule making process and consultation in respect of the rule change request.[133] A consultation paper identifying specific issues for consultation was also published. Submissions closed on 18 July 2024. The Commission received 17 submissions as part of the first round of consultation. The Commission considered all issues raised by stakeholders in submissions. Issues raised in submissions are discussed and responded to throughout this draft rule determination. A summary of other issues raised in submissions and the Commission's response to each issue is contained in **appendix D**.

133 This notice was published under section 95 of the NEL.

B Regulatory impact analysis

The Commission has undertaken regulatory impact analysis to make its draft determination.

B.1 Our regulatory impact analysis methodology

The Commission analysed these options: the rule proposed in the rule change request; and a business-as-usual scenario where we do not make a rule. Following stakeholder feedback, and taking into account the assessment criteria, we did not consider there was a case for developing an option of a more preferable rule. **Chapter 3** presents our assessment of the rule proposed in the rule change request against the business-as-usual scenario.

We identified who would be affected and assessed the benefits and costs of each policy option

The Commission's regulatory impact analysis for this rule change used quantitative and qualitative methodologies. It involved identifying the stakeholders impacted and assessing the benefits and costs of policy options. The depth of analysis was commensurate with the potential impacts. Where commensurate and feasible, the Commission has qualified the impacts. The Commission focused on the types of impacts within the scope of the NEO.

Table B.1 summarises the regulatory impact analysis the Commission undertook for this rule change. Based on this regulatory impact analysis, the Commission evaluated the primary potential costs and benefits of policy options against the assessment criteria. The Commission's determination considered the benefits of the options minus the costs.

Table B.1: Regulatory impact analysis methodology

Assessment criteria	Primary costs (Low, medium or high)	Primary benefits (Low, medium or high)	Stakeholders affected	Methodology (QT = quantitative, QL = qualitative)
Safety, security and reliability outcomes	Nil	Support the safe, secure and reliable provision of energy to consumers (M)	• All grid-connected consumers	• QL: We have considered the benefits of supporting the prevention of, and improved response to, cyber security incidents that could disrupt the supply of energy to consumers.
Implementation considerations • Cost and complexity • Timing and uncertainty • Impact analysis • Success as a market-wide solution	Increase in participant fees of < $10 million annually (approx. 2%) (L)	Relatively simple implementation as it builds on existing roles and activities (M) Fast implementation as it requires no system upgrades (M)	• AEMO • All market participants	• QT: We have considered the cost estimates provided by AEMO. • QL: We have considered the time and resources required for AEMO to implement and continue the functions. • QL: We have considered the impact on other market participants. Participant fees would increase but there would be no new obligations on market participants. • QL: We have considered how the draft rule would benefit the NEM as a whole, considering cyber security risks can be wide-ranging.

Assessment criteria	Primary costs (Low, medium or high)	Primary benefits (Low, medium or high)	Stakeholders affected	Methodology (QT = quantitative, QL = qualitative)
Principles of good regulatory practice • Predictability and stability • Simplicity and transparency • Consider broader direction of reform • Prescription vs. principles-based approach	Nil	Regulatory certainty to improve confidence of market participants (M) Supports the energy transition by providing more confidence in the security of an increasingly digitally interconnected power system (L)	• AEMO • All market participants • All grid-connected consumers	• QL: We have considered how the draft rule would improve stability and transparency by enabling AEMO to perform the functions consistently with appropriate cost recovery. • QL: We have considered how AEMO's role in the draft rule would complement that of other bodies and existing legislation. • QL: We have considered the design of the functions to provide sufficient flexibility for AEMO to adapt its activities to an evolving cyber and energy landscape.

C Legal requirements to make a rule

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

C.1 Draft rule determination and draft rule

In accordance with section 99 of the NEL, the Commission has made this draft rule determination in relation to the rule proposed by the Honourable Chris Bowen MP, Minister for Climate Change and Energy.

The Commission's reasons for making this draft rule determination are set out in **chapters 2 and 3.**

A copy of the draft rule is attached to and published with this draft determination. Its key features are described in **chapter 2**.

C.2 Power to make the rule

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

The draft rule falls within these provisions of section 34 of the NEL:

- Section 34(1)(a)(ii): the operation of the national electricity system for the purposes of the safety, security and reliability of that system;
- Section 34(3)(c)(i): 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.

C.3 Commission's considerations

In assessing the rule change request the Commission considered:

- its powers under the NEL to make the draft rule
- the rule change request
- submissions received during first round consultation
- the Commission's analysis as to the ways in which the draft rule will or is likely to contribute to the achievement of the NEO
- the application of the draft rule to the Northern Territory.

There is no relevant Ministerial Council on Energy (MCE) statement of policy principles for this rule change request.[134]

The Commission may only make a rule that has effect with respect to an adoptive jurisdiction if satisfied that the proposed rule is compatible with the proper performance of AEMO's declared network functions.[135] The draft electricity rule is compatible with AEMO's declared network functions because the draft rule would not affect those functions.

134 Under s. 33 of the NEL 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.

135 Section 91(8) of the NEL.

C.4 Making electricity rules in the Northern Territory

The NER, as amended from time to time, apply in the Northern Territory, subject to modifications set out in regulations made under the Northern Territory legislation adopting the NEL.[136] Under those regulations, only certain parts of the NER have been adopted in the Northern Territory.

As the draft rule relates to Chapter 10 of the NER, which applies in the Northern Territory, the Commission is required to assess Northern Territory application issues, described below.

Test for scope of "national electricity system" in the NEO

Under the NT Act, the Commission must regard the reference in the NEO to the "national electricity system" as a reference to whichever of the following the Commission considers appropriate in the circumstances having regard to the nature, scope or operation of the proposed rule:[137]

1. The national electricity system
2. One or more, or all, of the local electricity systems[138]
3. All of the electricity systems referred to above.

Test for differential rule

Under the NT Act, the Commission may make a differential rule if it is satisfied that, having regard to any relevant MCE statement of policy principles, a differential rule will, or is likely to, better contribute to the achievement of the NEO than a uniform rule.[139] A differential rule is a rule that:

- varies in its term as between:
  - the national electricity systems, and
  - one or more, or all, of the local electricity systems, or
- does not have effect with respect to one or more of those systems

but is not a jurisdictional derogation, participant derogation or rule that has effect with respect to an adoptive jurisdiction for the purpose of s. 91(8) of the NEL.

A uniform rule is a rule that does not vary in its terms between the national electricity system and one or more, or all, of the local electricity systems, and has effect with respect to all of those systems.[140]

In developing the draft rule, the Commission has considered the application to the Northern Territory according to the following questions:

- Should the NEO test include the Northern Territory electricity systems? Yes. The Commission considers that the NEO test should include the Northern Territory electricity systems given that this rule will apply in the Northern Territory (even though it will have no practical effect).
- Should the rule be different in the Northern Territory? No. The Commission's draft rule is a uniform rule because the Commission does not consider it appropriate for the draft rule to be different in the Northern Territory.

136 These regulations under the NT Act are the National Electricity (Northern Territory) (National Uniform Legislation) (Modifications) Regulations 2016.
137 Clause 14A of Schedule 1 to the NT Act, inserting section 88(2a) into the NEL as it applies in the Northern Territory.
138 These are specified Northern Territory systems, listed in schedule 2 of the NT Act.
139 Clause 14B of Schedule 1 to the NT Act, inserting section 88AA into the NEL as it applies in the Northern Territory.
140 Clause 14 of Schedule 1 to the NT Act, inserting the definitions of "differential Rule" and "uniform Rule" into section 87 of the NEL as it applies in the Northern Territory.

C.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' Meeting that new or existing provisions of the NER be classified as civil penalty provisions or conduct provisions.

The draft rule does not amend any clauses that are currently classified as civil penalty provisions or conduct provisions under the National Electricity (South Australia) Regulations.

The Commission does not propose to recommend to Energy Ministers that any of the proposed amendments made by the draft rule be classified as civil penalty provisions or conduct provisions.

D Summary of other issues raised in submissions

Table D.1: Summary of other issues raised in submissions

Stakeholder	Issue	Response
SMA	It is currently not clear who is responsible for governance arrangements for cyber security in the NEM. AEMO should develop a power system security strategy to clarify governance requirements.	Various governance responsibilities are divided between government, AEMO, and participants. This includes: Energy Ministers having responsibility for NEM policy, the Minister for Home Affairs being responsible for cyber security strategy and policy from a national security standpoint under the Department of Home Affairs, and notably comprising the SOCI Act. AEMO has responsibility for developing and maintaining its own cyber security strategy and policy program for its own systems, which includes a General Power System Risk Review report. Market participants are responsible for their own assets.
Splunk		
Fronius	A national strategy for cyber security and Consumer Energy Resources is required.	The CER Taskforce and the Energy and Climate Change Ministerial Council recently released the National Consumer Energy Resources Roadmap which includes a workstream to define the role, including with respect to cyber security of DNSPs/DSOs by 2026. Additionally, Standards Australia and the Energy Security and Resilience Working Group are working on a proposal to adopt some standards and develop technical specifications for CER cyber security, specific to Australian technologies and markets. There may be scope for the CER Taskforce to leverage AEMO's new functions to support the CER roadmap reforms. AEMO will collaborate and support the relevant parties, as appropriate (in its capacity as market operator).
CEC		
Vestas	Clarity on who provides guidelines and mandatory obligations for market participants, including OEMs.	As stated, this rule change request does not give AEMO the power to impose mandatory obligations on participants. OEMs that supply generators will be guided by generators' requirements. This may include SOCI Act obligations such as establishing and maintaining a critical infrastructure risk management program which incorporates compliance with AESCSF or an alternative framework. Application of the SOCI Act to different market participants is a matter for the Australian Government, not AEMO.
CEC		
SMA	Clarity around the role of networks	As mentioned above, the National CER Roadmap provides some clarity on these issues.

Stakeholder	Issue	Response
	and other businesses in developing and enforcing their own cyber security rules.	
SEC		
Fronius		
ENA	In the same way that AEMO is securing funding certainty, Networks should also be provided funding certainty.	Networks can recover the costs of cyber security as part of its revenue reset. The Australian Energy Regulator (AER) has made revenue determinations which included totex for cyber security. For example, the AER approved an opex step change of $18.2 million for ElectraNet to spend on cyber security. (AER, Final decision - ElectraNet transmission determination 1 July 2023 to 30 June 2028, p. 22.) Similarly, the AER approved totex of $101.9 million for cyber security as part of its revenue determination for Ausgrid. (Final Decision Ausgrid Electricity Distribution Determination 2024 to 2029, Attachment 5: Capital Expenditure, p. 12)

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
ARENA	Australian Renewable Energy Agency
ASD	Australian Signals Directorate
CEC	Clean Energy Council
CER	Consumer energy resources
CIRMP	Critical Infrastructure Risk Management Program
CISC	Cyber and Infrastructure Security Centre
CSIRO	Commonwealth Scientific and Industrial Research Organisation
Commission	See AEMC
DER	Distributed energy resources
DNSP	Distribution network service provider
DSO	Distribution system operator
ENA	Energy Networks Australia
EQL	Energy Queensland
FCC	Financial Consultation Committee
GPSRR	General Power System Risk Review
IT	Information technology
MCE	Ministerial Council on Energy
NGR	National Gas Rules
NEL	National Electricity Law
NEM	National Electricity Market
NEO	National Electricity Objective
NER	National Electricity Rules
NT Act	National Electricity (Northern Territory) (National Uniform Legislation) Act 2015
OEM	Original equipment manufacturer
OT	Operational technology
Proponent	The individual / organisation who submitted the rule change request to the Commission
PSEMP	Power System Emergency Management Plan
SAPN	SA Power Networks
SCADA	Supervisory control and data acquisition
SEC	Smart Energy Council
SOCI Act	Security of Critical Infrastructure Act 2018
WEM	Wholesale Energy Market