AUSTRALIAN ENERGY MARKET COMMISSION

RULE

Rule determination

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

Proponent

The Honourable Chris Bowen, Minister for Climate Change and Energy

12 December 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, Rule determination, 12 December 2024

Summary

1 The Australian Energy Market Commission (AEMC or Commission) has made a final 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 the Minister for Climate Change and Energy, the Hon. Chris Bowen MP (the proponent or Minister), the final rule inserts four new cyber security functions into Chapter 4 of the NER.

2 As the system operator, AEMO already had 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 for AEMO, consistent with the performance of other functions and activities.

3 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.

4 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.

5 The Finkel Review, commissioned in response to the 2016 South Australian system black event, 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.

6 Following the Finkel Review's recommendation AEMO worked with 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.

Our final rule allows AEMO to recover costs and confirms immunity from liability to perform prevention and preparedness functions

7 Previously, the NER did not explicitly address cyber security, so there were opportunities to confirm and clarify AEMO's role and responsibilities in this area. Under the 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 final rule builds on this by establishing specific cyber security prevention and preparedness functions for AEMO in the NER.

8 The final rule allows AEMO to recover its costs, and confirms its immunity from liability, consistent

with the performance of AEMO's other activities and functions, to deliver these cyber security functions. This provides certainty to AEMO and participants about recovery of costs and liability arrangements for certain cyber security roles and responsibilities. This clarity helps strengthen the management of cyber risks across the power system from individual participants to whole-of-system considerations.

9 The Commission considers that the overall **cost** of formalising cyber preparedness and incident response functions is low compared to the benefits of doing so, given the magnitude of any potential cyber incident. The final rule enables AEMO to recover cyber security costs through its normal cost recovery process. Going forward, this helps ensure cyber security functions are adequately and sustainably funded. See **section 3.3** for more information.

10 AEMO provided the Commission with updated cost estimates on 27 November 2024.

- Establishment and business-as-usual costs in years one to three are forecast to range between $8 million and $10 million per year.
- Ongoing costs beyond this initial three-year period are forecast to range between $8.5 million and $9.5 million per year.

11 AEMO has informed the Commission that these updated estimates reflect an improved understanding of the implementation and ongoing requirements of the four functions. While the updated costs are higher than previously expected, we continue to consider that the benefits outweigh the costs due to the significant impact and costs that would be incurred if a cyber incident were to occur. See **section 3.3** for more analysis on the updated cost estimates.

Our final rule adds four cyber security functions to AEMO's power system security responsibilities

12 The final rule adds four cyber security functions to AEMO's power system security responsibilities in Chapter 4 of the NER.

13 Specifically, the functions are:

- **Function 1 - Cyber security incident coordinator:** AEMO is able to plan and coordinate the NEM-wide response to a cyber incident affecting the energy sector. AEMO will continue to develop a plan - the Australian Energy Sector Cyber Incident Response Plan - outlining how market, state and federal responses to a cyber incident would be coordinated. In the event of a cyber incident AEMO will lead the implementation of the response in the manner set out by the plan.
- **Function 2 - Supporting cyber preparedness and uplift:** AEMO will continue to 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 will not create additional mandatory requirements for registered participants.
- **Function 3 - Examining cyber risks and providing advice to government and industry:** AEMO will provide cyber security research and advice to governments. This advice will draw on AEMO's unique energy expertise in their position as system operator, and will complement, rather than replace, work undertaken by other cyber security bodies such as the Australian Cyber Security Centre.
- **Function 4 - Facilitating the distribution of critical cyber security information to market participants:** AEMO will act as a distributor of cyber security information to the energy industry, using its position as system operator and existing communication channels. AEMO

can facilitate the distribution of warnings of cyber vulnerabilities of threats, post-cyber incident reports, and preventative information technology patches in commonly used technologies.

14 These four functions are facilitative and flexible and do not enable AEMO to impose mandatory obligations on market participants.

The Commission has considered stakeholder feedback in making its decision

15 A clear majority of stakeholders who provided submissions 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.

16 The key stakeholder observations that shaped the 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 for the four functions, and broad agreement that the benefits would likely justify the costs.

17 However, some stakeholders in submissions to the consultation paper and draft determination:

- asked for clarification around costs, including how cost recovery would be apportioned among participants
- cautioned against duplication of roles with other agencies and within functions
- questioned whether certain functions were consistent with AEMO's role as market operator
- requested further detail in the case of function three and requested advice is proactive rather than reactive
- requested compliance with consultation procedures.

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

- The costs, including the revised cost estimates, 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. Additionally, AEMO will consult on whether the four functions can be determined to be a 'declared NEM project'. Following consultation on this, AEMO will consult on a proposed structure for participant fees to recover AEMO's costs for the project. See **section 3.3**.
- 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 in the rule for governments and industry to seek cyber security advice from other bodies, in addition to AEMO. Further detail on each function is provided in **section 3.2**.

19 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 3.5** for more information.

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

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

21 The final rule contributes to achieving the NEO by:

- **Promoting safety, security and reliability:** by embedding and formalising AEMO's functions in the NER, the rule helps enable the secure provision of electricity in the long term. The rule promotes 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 helps enable the secure provision of electricity to consumers in the long term, ensuring safety and security outcomes are met. See **section 2.3.2** for a more detailed analysis.
- **Aligning with principles of good regulatory practice:** the rule is aligned with principles of good regulatory practice because it helps 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 has clarity over funding and liability protection arrangements (consistent with the performance of AEMO's other activities and functions), which allow for resourcing certainty to properly establish and undertake cyber security activities on more well-defined and permanent basis. This enables 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 now have increased transparency around activities and the cost of AEMO's cyber security role and responsibilities. See **section 2.3.3** for a more detailed analysis.
- **Taking into account implementation considerations:** the rule takes implementation considerations into account by considering cost implications, governance complexities and timing considerations. 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 complexities in cyber security governance are now more transparent and simplified by formally establishing functions for AEMO, which makes cyber security governance more transparent for industry. The rule clarifies any uncertainty and timing considerations by providing more certainty around cyber security in the NER. The impact on AEMO and other participants is manageable because AEMO was already performing some of the activities, meaning that some processes are in place that can be built on. See **section 2.3.4** for a more detailed analysis.

1 Section 7 of the NEL.

There are minor differences between the draft rule and final rule

22 Our final rule reflects minor drafting improvements from the draft rule to reflect standard approaches to drafting in the NER. There are no substantive policy changes. In line with these minor drafting improvements we also made the small clarifying changes AEMO recommended in its submission to the draft determination.

The final rule commences on 12 December 2024

23 The Commission's final determination is that the rule commences as early as possible. AEMO does not require an implementation period before commencement. The rule comes into effect on publication of this determination on 12 December 2024.

24 AEMO has informed the Commission that it intends to commence consultation about whether the functions may be determined to be a 'declared NEM project' in early 2025. Following consultation this, AEMO will consult on a proposed structure for participant fees to recover AEMO's costs for the project. AEMO has informed the Commission that this fee structure will be in place until the next general determination of NEM participant fees is made for the period commencing 1 July 2026.

Contents

Tables

Figures

1 The Commission has made a final determination

The Australian Energy Market Commission (the Commission or AEMC) has make a final 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 proponent or the Minister).

This chapter provides an overview of the Commission's final rule and our rationale for making it.

- **Section 1.1** outlines the final determination and final rule, which makes the rule proposed by the proponent.
- **Section 1.2** outlines AEMO's powers under the current NER for managing cyber security.
- **Section 1.3** outlines the expected costs for AEMO to perform the cyber security functions under the final rule.
- **Section 1.4** outlines the input from stakeholders that shaped our final determination and rule.
- **Section 1.5** explains how our final rule supports a strategic and coordinated approach to cyber security.

1.1 Our final rule confirms and clarifies AEMO's role and responsibilities for cyber security

The final rule is consistent with the proponent's 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. The final rule does this by building on AEMO's existing powers to maintain power system security in response to certain events by specifying in the NER the roles and responsibilities that AEMO will perform to assist in enhancing cyber security across the energy system. Importantly, the final rule allows AEMO to recover costs and confirms its immunity from liability, consistent with the performance of AEMO's other activities and functions, to deliver these cyber security functions. See **section 1.2 and 3.4** for more information on liability protection and **section 3.3** for more information on cost recovery.

Specifically, the final rule formalises and embeds four new functions for AEMO in the NER:

- **Function 1 - Cyber security incident coordinator:** AEMO will be able to plan and coordinate the response, across the whole National Electricity Market (NEM), to a cyber incident affecting the energy sector. AEMO will continue to develop a plan, the Australian Energy Sector Cyber Incident Response Plan, outlining how market, state, and federal responses to a cyber incident will be coordinated. If there is a cyber incident, AEMO will lead the implementation of the response in the manner set out by the plan.
- **Function 2 - Supporting cyber preparedness and uplift:** AEMO will continue to 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 will not create additional mandatory guidelines on cyber security.
- **Function 3 - Examining cyber risks and providing advice to government and industry:** AEMO will be able to provide cyber security research and advice to governments. This advice will draw on AEMO's unique energy expertise in its position as system operator, and will complement, rather than replace or duplicate, work undertaken by other cyber security bodies such as the Australian Cyber Security Centre.

- **Function 4 - Facilitating the distribution of critical cyber security information to market participants:** AEMO will distribute cyber security information to the energy industry, using its position as system operator and existing communication channels. AEMO will be able to facilitate the distribution of warnings of cyber vulnerabilities or threats, post-cyber incident reports, and preventative patches in commonly used technologies.

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

1.2 Previously the NER did not explicitly address AEMO's cyber security role

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

It is worth noting that while it is not specifically referenced, AEMO's 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 provided further detail on 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, the absence of an explicit reference to cyber security in the NER had created uncertainty about funding and liability protection for the cyber security preparedness functions AEMO performs. This uncertainty about funding and liability protection for the delivery of cyber security functions meant AEMO was performing these functions without sufficient resources and certainty. This uncertainty had 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 could respond to an actual cyber incident as it would to any power system security incident (such as by issuing directions), it lacked clear authority to undertake preventative work. The final rule embeds and formalises an existing practice that is AEMO's cyber security incident and preparedness work, as well as formalising four new functions.

Following the Finkel Review[2] recommendation that AEMO should have an explicit cyber security role, AEMO has adopted some cyber security roles and responsibilities. However, because cyber security was not, until this final rule, explicitly referenced in the NER, it did not have the ability to recover costs and it did not have liability protection.

Importantly, by embedding and formalising these functions in the NER:

- AEMO will be able to recover costs from participants ensuring adequate resourcing, allowing it to upscale and further expand these activities. While AEMO had been performing some of these activities, the environment and operating realities of the power system have changed considerably, with cyber security and uplift becoming increasingly more important for the

2 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".

NEM. The final rule ensures that AEMO can undertake activities that benefit market participants and consumers by ensuring the security and reliability of the power system.

- AEMO will have liability protection for the performance of these functions, consistent with the performance of its other functions, under Section 119 of the NEL. 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 will 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.[3]
- Participants will be supported to improve their level of cyber security preparedness and maturity as they will be able to access the latest information about risks, learnings, and preparedness which will help minimise the risk of a cyber incident. In turn, this 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 AEMO has provided updated cost estimates

AEMO provided the Commission with updated cost estimates on 27 November 2024:

- Establishment and business-as-usual costs in years one to three are forecast to range between $8 million and $10 million per year.
- Ongoing costs beyond this initial three-year period are forecast to range between $8.5 million and $9.5 million per year.

AEMO has informed the Commission that these updated estimates reflect an improved understanding of the implementation and ongoing requirements of the four functions. The Commission continues to consider that the benefits outweigh the costs due to the significant impact and costs that would be incurred if a cyber incident were to occur. See **section 3.3** for more analysis on the updated cost estimates.

1.4 Stakeholder input and support for AEMO's cyber security role shaped our final rule

A clear majority of stakeholders in their submissions to the consultation paper and draft determination agreed that the NER lacked clarity on cyber security and that it was 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 final rule included:

- support for the need to confirm and clarify, in the NER, AEMO's role and responsibilities in relation to cyber security. Stakeholders considered this is important for ensuring that 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:

3 Liability protection is especially relevant to AEMO's exercising of the Australian Energy Sector Cyber Incident Response Plan which involves interactions with market participants' systems to test the robustness of the plan.

- Asked for clarification and further detail around the costs proposed[4]
- Cautioned against duplication of roles with other agencies and within functions[5]
- Did not agree that certain functions were consistent with AEMO's role as market operator[6]
- Requested further detail in the case of function 3, which relates to providing advice to governments,[7] and requested advice is proactive rather than reactive[8]
- Requested compliance with consultation procedures[9]
- Requested clarity on how AEMO will coordinate with the proposed National Cyber Incident Response Board.[10]

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

- The costs, including the revised cost estimates, 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 its cyber security roles and responsibilities for the power system. This reflects the reality that while AEMO has been performing some of these activities the environment has changed considerably, even within the last few years, with cyber preparedness and uplift becoming increasingly more important for the NEM, requiring further expansion and additional resourcing. For example the Australian Energy Sector Cyber Security Framework's application has expanded in recent years, and now supports regulatory obligations under the *Security of Critical Infrastructure Act 2018* (SOCI Act) and provides guidance to new market entrant types (such as batteries and aggregators). See **section 3.3**.
- Roles are not duplicative because AEMO's responsibilities under these 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 final rule for governments to seek cyber security advice from other bodies, in addition to AEMO. See **section 3.2.3**.
- The Commonwealth's *Cyber Security Act 2024* (Cyber Security Act) and the proposed National Cyber Incident Response Board will complement and work with AEMO, rather than duplicate any of its functions. See **section 3.2.4**.

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

Stakeholders raised a range of issues being addressed in other processes

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[11]

4 Submissions to the consultation paper: Energy Queensland, p. 1; AGL, pp. 4-5; Splunk, p. 4; SA Power Networks (SAPN), p. 2. Submissions to the draft determination: Transgrid, p.2; Epic Energy, p.2; AGL, p.2.

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

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

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

8 SAPN submission to the consultation paper, p. 2

9 TasNetworks submission to the consultation paper, p.3.

10 Submission to the draft determination, AGL, p.2.

11 Submissions to the consultation paper: SMA, p. 4; Splunk, pp. 6-7.

- A national strategy for cyber security and consumer energy resources (CER)[12]
- Clarity on who provides guidelines, standards, or mandatory obligations for market participants, including original equipment manufacturers (OEMs)[13]
- Clarity around the role of networks.[14]

We consider the above issues are being considered through other reform processes, including the work being undertaken by:

- The AEMC in the rule changes on Accelerating smart meter deployment.[15]
- The CER Taskforce of the Energy and Climate Change Ministerial Council, which recently released the National Consumer Energy Resources Roadmap which includes a workstream to define, by 2026, the roles and responsibilities of distribution network service providers (DNSPs)/distribution system operators (DSOs) in a high CER world, including cyber security. 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 multiple options for the allocation of cyber security roles. The Roadmap also indicates that voluntary CER cyber standards and technical specifications will be available in 2027.[16]
- 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.[17]
- The Department of Home Affairs' consultation on potential legislative reforms to support the Australian Government's cyber security strategy for 2023-2030, which also includes proposed new cyber security legislation and changes to the SOCI Act.[18]

See **appendix D** for more information.

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

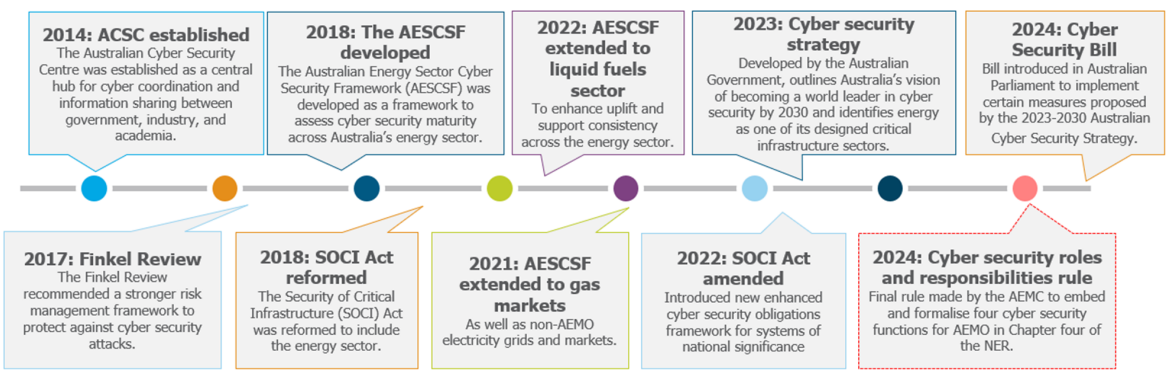
Cyber security is of critical importance in Australia. While it impacts all sectors, it is a particularly prominent issue in energy security given the NEM's increasing digitisation and connectivity and the importance of energy for other sectors of the economy. The system now includes real-time data on 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, the NEM also requires enhanced capabilities to mitigate threats from any malicious cyber activity.

12 Submissions to the consultation paper: Smart Energy Council (SEC), pp. 1-2; Fronius, p. 2.
13 Submissions to the consultation paper: Vestas, pp. 1-2; Clean Energy Council (CEC), p. 2. Submission to the draft determination, SMA, p.2.
14 Submissions to the consultation paper: SMA, p. 3; SEC, pp. 1-2; Fronius, pp. 1-2; ENA, p. 3; CEC, pp. 1-2.
15 AEMC, Accelerating smart meter deployment, https://www.aemc.gov.au/rule-changes/accelerating-smart-meter-deployment
16 National Consumer Energy Resources Roadmap, https://www.energy.gov.au/sites/default/files/2024-07/national-consumer-energy-resourcesroadmap.pdf, p43.
17 Roadmap for CER cybersecurity, https://www.standards.org.au/news/securing-the-future—-a-cybersecurity-roadmap-for-consumer-energy-resources.
18 Australian Government Department of Home Affairs, Cyber security legislative reforms, https://www.homeaffairs.gov.au/reports-andpublications/submissions-and-discussion-papers/cyber-legislative-reforms.

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

Figure 1.1: Timeline of cyber security reforms and frameworks



Source: AEMC.

The Finkel Review 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 the final rule embeds and formalises 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 The rule will contribute to the NEO

This chapter sets out how our final rule promotes the National Electricity Objective (NEO). It explains how our 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 2.1** outlines the NEO test that the Commission must apply to make a rule.
- **Section 2.2** explains how our final rule contributes to the NEO.

2.1 The Commission must act in the long-term interests of energy 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.[19]

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

The NEO is:[20]

> 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.[21]

There are also other relevant legal requirements for the Commission to consider under the NEL to make a rule determination. The Commission has considered these, as set out in **appendix C**.

2.2 The final rule to confirm and clarify AEMO's cyber security role will contribute to the achievement of the NEO

The Commission used the following **three** criteria to assess whether the rule change will better contribute to achieving the NEO compared to the status quo or other rules-based options:

- **Safety, security and reliability:** we have considered whether formalising and embedding the four functions for AEMO will help enable the secure provision of electricity in the long term, ensuring safety and security outcomes for participants and consumers are promoted.

19 Section 88(1) of the NEL.
20 Section 7 of the NEL.
21 Section 32A(5) of the NEL.

- **Principles of good regulatory practice:** we have considered if the proposed rule change will enhance predictability, stability, and transparency, without being overly prescriptive or duplicative. We have done this by considering the broader direction of cyber security reforms and frameworks.
- **Implementation considerations:** we have assessed the cost implications and timing considerations.

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 rationale for each of the assessment criteria is as follows:

- **Safety, security, and reliability:** The end goal of the rule change is the safety and security of consumers. Cyber security incidents present an energy sector risk that could have significant consumer impacts. The final rule ensures AEMO is well resourced to undertake cyber security activities. The final rule creates a formal cyber security role for AEMO, which helps enable the secure provision of electricity to end customers over the long term. The formalisation of AEMO's four cyber security functions will support its ability to manage and operate a secure system.
- **Principles of good regulatory practice:** the final rule ensures the NER are fit for purpose by specifically identifying AEMO's role and responsibilities in relation to cyber security. By considering principles of good regulatory practice the Commission has selected the best solution for this rule change request, which will promote predictability and stability in cyber security (for the electricity industry) by placing more well-defined responsibilities on AEMO. The final rule improves transparency around AEMO's cyber security role for all stakeholders including governments and industry. The final rule also outlines principles and key functions without being overly prescriptive. The formalisation of four cyber security functions will enable AEMO to play a clear role in cyber security, without unduly limiting its cyber security work or placing new mandatory obligations on industry. The final rule also considers the broader reforms in cyber security to avoid duplication and capitalise on synergies where possible.
- **Implementation considerations:** the cost of the proposed solution is both directly and indirectly justified because the benefits of AEMO having formalised uplift and preparedness functions outweigh the cost of these functions. Now is the right time for this rule change because cyber security is becoming an ever more prevalent issue, especially as the power system becomes increasingly digitised and interconnected. The final rule will be a market-wide solution for all NEM jurisdictions because cyber security risks are not necessarily tied to one physical location.

Following stakeholder feedback to the consultation paper and draft determination, the Commission is satisfied that the assessment criteria are fit for purpose.[22]

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.

22 In response to the consultation paper three stakeholders explicitly supported the assessment criteria. Five stakeholders, while supporting the assessment criteria, suggested including additional criteria to consider national security and international obligations, and outcomes for consumers. The Commission did not include 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 assets. 2. While the Commission agrees that this rule will improve outcomes for consumers, we consider this occurs through the final rule promoting safety, security, and reliability outcomes for consumers, where those benefits outweigh any costs.

2.2.1 Confirming four functions for AEMO will 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 for the reasons outlined below.

We consider the cost estimates provided by AEMO - which are discussed more in **section 3.3** - sufficient to illustrate the cost impacts of the four functions. We also consider that the costs are justified because embedding and formalising AEMO's role and responsibilities under the NER will reduce cyber security risks. If a cyber security 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. The final rule supports AEMO to upscale and further resource these activities. This reflects the reality that, while AEMO has been performing cyber security activities, the environment has changed considerably. Cyber preparedness and uplift is becoming increasingly important for the NEM, requiring more resourcing. This context - that cyber security is growing in importance - provides confidence that the benefits of the rule change will outweigh the costs. See **section 3.3** for an analysis of costs.

Our analysis against the relevant assessment criteria is outlined below.

2.2.2 The rule will promote safety, security and reliability

The Commission considers that the final rule will enhance safety, security, and reliability outcomes. By embedding and formalising AEMO's cyber functions in the NER, the rule will contribute to securing the provision of electricity for consumers.

Cyber security is important to power system security and reliability because a cyber incident in the electricity sector could have far-reaching implications including widespread outages, economic disruptions, breaches of sensitive data, and threats to national security. Stakeholders agreed that security is a paramount consideration,[23] and noted that "interruptions to the power system would have major impacts on lives and livelihoods."[24]

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

Prior to this rule, the lack of clarity on AEMO's role and responsibilities for cyber security in the NER meant that it was not properly resourced to undertake cyber security functions. This could have led to inconsistency in cyber security preparedness and response measures. 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, ill-defined functions could result in a lack of coordination, jeopardising AEMO and participants' **responsiveness**.

23 Submissions to the draft determination: Epic Energy, p.1; AGL, p.1.

24 Submission to the draft determination, Ausgrid, p.1.

AEMO can issue system security directions,[25] prepare a system restart plan for managing and coordinating system restoration during a major disruption,[26] and coordinate the protection of power system equipment[27] as part of its function to maintain and improve power system security. As the system operator, AEMO is well-placed to support the energy sector with preparedness, learning and uplift activities. The final rule unlocks enhanced resourcing for AEMO to undertake more **proactive** preparedness, learning and uplift activities, as opposed to the more established role of maintaining and improving power system security. Specifically, as part of the four functions, AEMO will be able to undertake or strengthen a number of **proactive** measures, such as:

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

In considering stakeholder feedback, the Commission is of the view that formalising and embedding AEMO's cyber functions in the NER will promote safety, security, and reliability outcomes. Specifically, stakeholders said that this is essential for facilitating preparedness and resilience,[28] and that, without clarity and a coordinated strategy to build and maintain cyber security, we are at risk of a fragmented security response.[29] Stakeholders have emphasised that there needs to be a focus on making the entire system more resilient to ensure energy security.[30]

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

2.2.3 The rule is aligned with principles of good regulatory practice

The Commission considers that the final rule, to embed and formalise AEMO's cyber functions in the NER, aligns with principles of good regulatory practice. It does this by improving the predictability, stability, and transparency of cyber security in an increasingly digitised power system. The final rule also considers broader reforms while avoiding duplication.

Under the final rule, funding and liability protection will provide AEMO with **predictability and stability**. This will provide AEMO with resourcing certainty to expand and undertake cyber security activities on a more well-defined and permanent basis. Funding certainty and liability protection will enable AEMO to continue and scale up its cyber security activities. Additionally, market participants will be able to confidently rely on AEMO to perform specific preparedness, uplift, and responsiveness activities while having the ability to adapt as needs evolve. AEMO is not unduly limited in the activities it can undertake since these activities are outlined as principles and key functions in the rule. Additionally, requirements will not be overly prescriptive for industry because AEMO does not have the ability to impose mandatory obligations on participants.

25 Clause 4.8.9 of the NER.
26 Clause 4.3.1(p)(2) and (3) of the NER.
27 Rule 4.6 of the NER - Protection of Power System Equipment.
28 Submissions to the draft determination: Epic Energy, p.1; AGL, p.1.
29 Submissions to the consultation paper: Vestas, pp.2-3; SEC, p.2.
30 Submission to the consultation paper, SEC, p.3.

It follows that AEMO, government, and market participants will then have **transparency** around AEMO's functions and around the cost of its 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.[31]

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 for AEMO in the NER, the final rule implements a recommendation from the Finkel Review that AEMO should have a cyber security role. While AEMO has begun performing some activities under the functions, because of its inability to recover costs and lack of liability protection it has 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 Australian Cyber Security Centre and frameworks such as the SOCI Act, because they have a broader focus, and because AEMO provides a unique insight as the system operator.

In considering stakeholder feedback, the Commission is of the view that confirming and clarifying AEMO's cyber functions in the NER is aligned with principles of good regulatory practice. Specifically, stakeholders emphasised that a stable and consistent approach to cyber security governance in the NEM is important[32] because, without predictability and stability, an incident is bound to occur that will be costly to industry and ultimately to consumers.[33] Additionally, stakeholders have said that market participants benefit from clear definitions which will set clear expectations.[34] See **section 3.2** for more detailed information on the four functions.

2.2.4 We have taken implementation considerations into account for the final rule

The Commission considers that by embedding and formalising AEMO's cyber functions in the NER the final rule takes into account implementation considerations including cost implications, governance complexities, and timing considerations.

As discussed in **section 2.2.1** and **section 3.5**, the Commission considers that the overall **cost** of formalising cyber preparedness and incident response functions is low compared to the benefits of doing so, given the magnitude of any potential cyber incident.

The Commission considers that any existing **complexities in cyber security governance** will become more transparent and simplified for industry as the rule formally establishes functions for AEMO.

The rule will provide more **certainty** around cyber security in the NER. Cyber security is a prevalent issue in the NEM that cannot remain unaddressed and without adequate resourcing. Additionally, since the functions are built on actions AEMO is already undertaking, the rule can come into effect immediately, with costs recovered through AEMO fees following the commencement of the rule. See **section 3.5**.

The **impact** on AEMO, the Australian Energy Regulator (AER), and other participants will be manageable. AEMO is already performing some activities under the four functions, meaning that some processes can be expanded and formalised. While the rule establishes four functions,

31 NER rule 2.11. 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.

32 Submission to the draft determination, Ausgrid, p.1.

33 Submission to the consultation paper, Fronius, p. 2.

34 Submission to the consultation paper, Splunk, p. 6.

AEMO is not limited in its activities under the functions, meaning it is well placed to adapt to cyber security needs. AEMO is supportive on the basis that costs can be recovered and liability protection will be granted.[35] The rule does not provide AEMO with the ability to impose additional mandatory obligations on market participants, meaning mandatory compliance costs for participants will be low. AEMO's four functions should assist participants in managing cyber security risks because they support cyber preparedness and uplift, examine cyber risks and provide advice, and facilitate the distribution of critical information which will help participants manage cyber security risks before they eventuate into an incident.

While the AER has stated that the final rule may result in an incremental impact on its role of reviewing and assessing network revenue determination proposals, it does not anticipate any significant resourcing impacts, and therefore considers the impact of the final rule manageable.[36]

Stakeholders have said that a holistic and concerted effort to ensure resilience and protection across the entire Australian energy sector should be considered.[37] We appreciate that Western Australia, the Northern Territory, and gas markets also face cyber security risks and potentially lack clear roles and responsibilities. The Commission understands, as detailed in the rule change request, that these matters will be considered through separate processes.[38]

35 Submission to the draft determination, AEMO, p. 1.
36 Submission to the draft determination, p.2.
37 Submission to the draft determination, AGL, p.1.
38 Rule change request to the AEMC, Minister Bowen, p. 4.

3 Our rule will confirm and clarify AEMO's cyber security functions in the NER

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

- **Section 3.1** explains why the final rule sets out cyber security responsibilities in Chapter 4 of the NER.
- **Section 3.2** outlines the four functions following stakeholder feedback on these functions.
- **Section 3.3** outlines the expected costs of the functions and why they are justified.
- **Section 3.4** explains the timing for the commencement of the final rule.
- **Section 3.5** notes that some key issues raised by stakeholders are being addressed through other processes.

3.1 Cyber security is a power system security concern

Box 1: Cyber security is established as a power system security responsibility

The final rule includes a set of specific cyber security functions in AEMO's power system security responsibilities in Chapter 4 of the NER. These functions reflect some activities that AEMO undertook without a rules-based obligation. Having these in the rules allows AEMO and market participants to have clarity over funding and liability arrangements.

In the consultation paper the Commission asked stakeholders whether cyber security should be considered a power system security issue, and stakeholders broadly agreed. In the draft determination the Commission consulted on a proposed draft rule in Chapter 4 of the NER and received no substantive suggested amendments.

The final rule adds four cyber security functions to AEMO's power system security responsibilities in Chapter 4 of the NER.

Previously, the NER did not specifically address cyber security, so AEMO did not have a clear role or confirmed responsibilities in this area. While under the previous rules AEMO could respond to a cyber security incident if the security of the power system is compromised, for example by issuing directions to market participants, the final rule establishes 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 3.2.2**).

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 these actions. The functions we have now included in the NER also reflect this. For example:

- Function 1 (incident coordinator) clarifies roles and protocols in responding to a cyber incident
- Function 2 (industry uplift) will involve more extensive and frequent testing and training exercises
- Function 4 (distribution of information) supports sharing of threat intelligence amongst local industry, government, and international bodies.

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

The final rule makes these cyber security activities part of AEMO's power system security responsibilities in clause 4.3.1 of the NER. The specific functions are set out in clause 4.3.2A as outlined in the remainder of this section. Clause 4.3.2A(g) also states, for the avoidance of doubt, that these functions do not limit AEMO's other, pre-existing functions and do not impose mandatory obligations on other participants. See the final rule available on the project page.

The Commission considers it appropriate to include cyber security in Chapter 4 of the NER because cyber security incidents can pose a threat to power system security. While cyber security is not specifically referenced in the NEL, AEMO's existing statutory function under the 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, despite this, there is a need to **clarify** AEMO's cyber security uplift and preparedness role and responsibilities in the NER.

By including the four functions in Chapter 4, AEMO's cyber security uplift, preparedness, and incident response powers, which necessarily complement each other, are now codified in one place.

Stakeholders agree that cyber security is a power system security concern

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 has explicitly supported the rule as proposed, including that it is best placed in Chapter 4 of the NER.**[39] See **section 2.1.1** of the consultation paper for more information.[40] Additionally, stakeholders did not raise any concerns or issues about the draft rule amending Chapter 4 in submissions to the draft determination.

39 Submission to the consultation paper, p.3.

40 AEMC, Cyber security roles and responsibilities, consultation paper.

3.2 The final rule establishes four functions

Box 2: AEMO's cyber security functions in the NER

The final rule establishes four cyber security functions to be performed by AEMO. The four 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 as proposed in the draft rule. Some stakeholders asked for further information on how costs will be apportioned among participants, and for clarification on how the proposed National Cyber Incident Response Board in the Commonwealth's Cyber Security Act will coordinate with AEMO.

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

3.2.1 Function 1: Cyber security incident coordinator

The cyber security incident coordinator function involves AEMO developing and maintaining a NEM cyber incident response plan and coordinating the industry's response in the event of a cyber incident.[41]

The Commission understands AEMO has already developed a version of this plan, the Australian Energy Sector Cyber Incident Response Plan. This 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.

Having an incident response plan enables AEMO and market participants to be more agile and effective when responding to a cyber incident - this will help prevent or mitigate impacts on the energy system. The plan would aim to achieve this by allocating clear roles and responsibilities in a cyber incident, including outlining AEMO's coordinating role. This would help protect consumers from any potential consequences of a cyber incident including impacts on reliability or system security.

In order to facilitate a timely and effective response, function 1 could also involve activities such as maintaining sector and jurisdictional contact lists, monitoring the cyber risk landscape, and triaging cyber events.

The final rule is designed to ensure AEMO has adequate resourcing and protection from liability to perform the incident coordinator role and maintain the Australian Energy Sector Cyber Incident Response Plan. Funding certainty and liability protection will enable AEMO to continue and scale up its incident response preparation, for example by updating the Australian Energy Sector Cyber

41 Final rule, clause 4.3.2A(a).

Incident Response Plan more frequently or establishing tools and technologies to support it (see **Table 2.2**).

Stakeholders support AEMO's cyber incident coordinator role

There was strong stakeholder support for the cyber incident coordinator function.[42] Specifically, submissions to the draft determination considered that:

- It is appropriate for AEMO to take on this function, particularly considering the growing prevalence and concerns around cyber security[43]
- AEMO has an important role to play in coordinating with market participants and government to ensure effective and timely responses to any cyber incidents affecting the NEM[44]
- The development of the Australian Energy Sector Cyber Incident Response Plan is important.[45]

Epic Energy requested that AEMO's role is aligned with obligations under the *SOCI Act to* ensure comprehensive national energy security.[46] Importantly, the proposed functions complement, rather than duplicate, the role of other frameworks such as the SOCI Act, because they have a different focus and because of the unique insight AEMO provides as the energy system operator. Additionally, the Commission understands that it is AEMO's intent to align the Australian Energy Sector Cyber Security Framework for financial year 2025 with the SOCI Act reporting time frames.

Transgrid also asked the AEMC to clarify the level and type of involvement from AEMO in a NEM-wide cyber response.[47] The Commission notes that the coordination arrangements, through the Energy Sector Cyber Incident Response Plan, have been in place for some time and have been developed in consultation with market participants, including NSPs. The final rule provides AEMO with resourcing certainty to enhance this function which will include ongoing engagement and coordination with industry. Importantly, the final rule does not give AEMO powers to manage market participants' or other bodies' responses to a cyber incident; this responsibility remains with individual market participants.

3.2.2 Function 2: Supporting cyber preparedness and uplift

The industry uplift function requires AEMO to use reasonable endeavours to help market participants improve their cyber security preparedness and maturity.[48] This function may include, but would not be limited to, the following:

- **Stewardship of the Australian Energy Sector Cyber Security Framework** | AEMO previously co-developed the Australian Energy Sector Cyber Security Framework, and it would continue to maintain and update the framework as needed. This function will also include continuing to oversee Australian Energy Sector Cyber Security Framework self-assessments for industry. Note: AEMO already carries out this work, but the final rule would provide ongoing resourcing certainty and liability protection.
- **Organisation of testing and training exercises** | AEMO will 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

42 Submissions to the draft determination: ENA, p.1; AGL, p.1
43 Submission to the draft determination, Ausgrid, p.1.
44 Submission to the draft determination, AGL, p.1.
45 Submission to the draft determination, Epic Energy, p.1.
46 Submission to the draft determination, Epic Energy, p.1
47 Submission to the draft determination, Transgrid, p.2.
48 Final rule, clause 4.3.2A(b).

this type in the past, with the final rule supporting the continuation of this work through ongoing resourcing certainty.

- **Provision of guidance and advice to industry** | AEMO will provide industry cyber security guidance in the form of written materials, digital tools, participation in working groups, or by other means. The final rule will 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 its expertise and position as the market operator. Improving industry participants' preparedness for a cyber incident will help mitigate the risk of such incidents and consequences for consumers.

Stakeholders support AEMO undertaking an industry uplift and preparedness function

There was strong stakeholder support for the supporting cyber preparedness and uplift function.[49] Specifically, submissions to the draft determination considered that:

- AEMO's Energy Markets Cyber Exercise (Trident) helped identify several opportunities to enhance capabilities, and stakeholders welcome the continued delivery of practical cyber exercises[50]
- AEMO's stewardship of the Australian Energy Sector Cyber Security Framework is valuable[51]
- Participants should be supported by AEMO to improve their cyber security readiness and maturity through access to information on risks, learnings, and preparedness, while not imposing any mandatory obligations or costs.[52]

Epic Energy has requested that the Australian Energy Sector Cyber Security Framework align with the SOCI Act reporting requirements, particularly the Critical Infrastructure Risk Management Program to help streamline compliance and avoid duplication.[53] AEMO is responsible for the Australian Energy Sector Cyber Security Framework self-assessment timing, and the final rule ensures that AEMO can devote resourcing to modifying the Framework if it considers there is a need. As mentioned, the Commission understands that it is AEMO's intent to align the Framework for financial year 2025 with the SOCI Act reporting timeframes.

SMA recommended moving from encouraging self-assessment towards mandating third-party assessment, and that the Australian Energy Sector Cyber Security Framework should apply to inverters.[54] The final rule does not allow AEMO to create additional mandatory requirements for registered participants; this is consistent with the rule change request[55] and stakeholder feedback.[56] The Australian Energy Sector Cyber Security Framework was not designed to apply to device level standards for products like inverters, and the final rule does not confer powers on AEMO to determine eligibility or mandate participation. However, the Commission understands that Registered Participants and industry more broadly can apply the framework in managing their risk to electricity assets, including inverters.

49 Submissions to the draft determination: AGL, p.1; Epic Energy, p.2.

50 Submission to the draft determination, AGL, p.1.

51 Submissions to the draft determination: Epic Energy, p.2; SMA, p.1: "SMA has worked with cyber security consultants CAPA Intelligence to develop guidelines for compliance with the Australian Energy Sector Cyber Security Framework applicable to suppliers of inverters to utility-scale generators. The guidelines were completed in June 2024 and by August 2024 SMA had completed a self-assessment to demonstrate SP1 compliance with the framework guidelines. We have subsequently used the guidelines and our assessment against them to satisfy electricity generators who have included cyber security compliance as a contractual requirement for inverter original equipment manufacturers (OEMs)."

52 Submission to the draft determination, ENA, p.1.

53 Submission to the draft determination, p.2.

54 Submission to the draft determination, p.2.

55 Rule change request, The Honourable Chris Bowen, p.12.

56 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.

Vestas has recommended that AEMO should adopt a risk management approach and set a power plant criticality threshold.[57] As mentioned, the final rule does not confer powers on AEMO to determine eligibility or mandate participation. Market participants will remain responsible for managing risks to their plants; AEMO cannot direct participants to conduct risk assessments based on power plant thresholds. However, the Commission understands that AEMO is able to and has previously sought to facilitate an uplift in awareness and capability through a risk-based approach. The final rule supports this approach.

Importantly, as noted by Ausgrid,[58] AEMO will be resourced under this function to drive a more consistent and comprehensive approach to best practice cyber security approaches in the NEM.

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

Under this function, AEMO will develop cyber security advice or carry out cyber security research, specific to the energy sector, for provision to governments and potentially to industry.[59] This research and advice function will help 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 will help governments and industry to prepare for and respond to cyber incidents to limit the impact on consumers.

This advice will draw on AEMO's unique energy expertise in its position as system operator, and would complement, rather than replace, work undertaken by other cyber security bodies such as the Australian Cyber Security Centre. 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 is also 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 will be advisory only and will not expand AEMO's regulatory responsibilities, or 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.

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

There was broad stakeholder support for this function.

While AGL recognised AEMO's valuable expertise as the system operator, AGL believes that "cyber security advisory services may be better provided by organisations with broader cyber security knowledge and experience" such as the Australian Cyber Security Centre or CSIRO. AGL also suggests that AEMO's research and advice is complemented by insights from specialist organisations.[60]

57 Submission to the draft determination, Vestas, p.2.
58 Submission to the draft determination, p.1.
59 See final rule clauses 4.3.2A(c)-(e).
60 Submission to the draft determination, pp. 1-2.

The Commission notes that the final rule does not make AEMO the sole provider of cyber security advice to governments or industry. The research and advice function does not replace other channels by which governments and industry may seek advice, including government agencies, research institutes, or working with industry. Further, AEMO has the flexibility to seek input from other bodies or from industry when carrying out this function.

The Commission also notes that the final rule (available on the project page) allows AEMO to provide advice to government or industry proactively without a specific request.[61] 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 enables it to provide valuable research and advice on cyber security risks to the energy sector.

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

The information distribution function has AEMO use its position as system operator to disseminate critical cyber security information to the energy industry.[62] Since AEMO is a trusted body with communication channels that market participants regularly use, it can add value by providing a single source of cyber security notifications that are relevant to the energy industry. This will 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 includes, but is not 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 its existing Market Notices system to share relevant information with market participants, or it could use another method.

Stakeholders support the information distribution function for AEMO

There was broad stakeholder support for this function. Specifically, submissions to the draft determination considered that AEMO's role in disseminating relevant cyber security information through established channels is valuable.[63]

AGL queried the "incremental value this function brings" and believes information provided by the Australian Signals Directorate through the Cyber Threat Intelligence Sharing platform already undertakes this.[64] In contrast, Epic Energy noted that this function "complements the existing work by the Australian Signals Directorate and is essential for enhancing sector resilience".[65]

The Commission understands that participants, such as AGL, may already receive cyber security information from sources such as the Australian Signals Directorate. However, we note that the dissemination of information by AEMO is likely to be particularly useful to smaller participants which may not have the resources to keep track of cyber security information from multiple

61 Final rule, clause 4.3.2A(c).
62 Final rule, clause 4.3.2A(f).
63 Submission to the draft determination, Epic Energy, p.2.
64 Submission to draft determination, AGL, p.2.
65 Submission to the draft determination, Epic Energy, p.2.

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.

Stakeholders also asked for clarification around how the National Cyber Incident Response Board proposed in the Commonwealth's Cyber Security Act will coordinate with AEMO.[66] In discussions with the Commonwealth Department of Climate Change, Energy, the Environment and Water and AEMO, the Commission understands that the Cyber Security Act complements, rather than duplicates the final rule. The Act will establish a Commonwealth mechanism responsible for undertaking a review of vulnerabilities of any significant cyber security incidents, or the effectiveness of the government or industry response to the incident. Under the final rule AEMO will have a mechanism to assist the sector to prepare for and manage cyber security incidents in real time. In this respect the Cyber Incident Review Board may undertake a review of energy sector cyber incidents, and AEMO and other market participants may be asked or required to provide information to the review.

66 Submission to the draft determination, AGL, p.2.

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

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

The Commission considers that the overall **cost** of formalising cyber preparedness and incident response functions is low compared to the benefits of doing so, given the magnitude of any potential cyber incident. This reflects the reality that while AEMO has been performing some of these activities, the operational environment has changed considerably with cyber preparedness and uplift becoming increasingly more important for the NEM, requiring additional and permanent resourcing.

AEMO will recover the costs of performing the functions through participant fees. AEMO has provided updated cost estimates as of November 2024 indicating that the functions would cost approximately between $8 and $10 million per year in years one to three, and between $8.5 million and $9.5 million per year beyond this initial three year period.

In response to the consultation paper,draft determination and previous estimates, stakeholders generally agreed that 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. While the updated costs are higher than previously estimated by AEMO, we continue to consider that the benefits outweigh the costs due to the significant impact and costs that would be incurred if a cyber incident were to occur.

Some stakeholders asked for further clarification around how costs will be apportioned among participants. AEMO has informed the Commission that it intends to commence this consultation in early 2025 with a final determination to be made by 31 March 2026.

The final rule enables AEMO to recover cyber security costs through its normal cost recovery process (outlined in Box 4). Going forward, this helps ensure that cyber security functions are permanently and sustainably funded.

The final rule embeds and formalises 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.

AEMO has provided the Commission with updated cost estimates as of 27 November 2024:

- Establishment and business-as-usual costs in years one to three are forecast to range between $8 million and $10 million per year.
- Ongoing costs beyond this initial three-year period are forecast to range between $8.5 million and $9.5 million per year.

Table 3.1 below highlights the average cost split across the four functions in years one to three.

AEMO has informed the Commission that these updated estimates reflect an improved understanding of the implementation and ongoing requirements of the four functions, including:

- establishing secure and resilient communications to support cyber incident coordination activities
- expanding the Australian Energy Sector Cyber Security Framework to provide appropriate and relevant guidance to new market entrants (such as batteries or aggregators)
- factoring in inflation and labour costs.

Table 3.1: AEMO has estimated the average cost split in years 1-3

Function	Average Cost Split
1. Cyber incident response coordinator	53%
2. Cyber security uplift and preparedness	34%
3. Research and advice	7%
4. Information distribution	5%
Total percentage	**100%**

Source: AEMO cost estimate provided to the Commission on 27 November 2024.

AEMO still estimates, as of 27 November 2024, that the updated costs of the functions will be less than $10 million per year ongoing. While previously the Commission stated in the consultation paper and the draft determination that this is equivalent to only approximately two per cent of participant fees,[67] AEMO has informed the Commission that the overall participant fee impact will not be known until AEMO has completed its annual budget and fees consultation process (commencing in early 2025).

In response to the consultation paper and draft determination and the previous estimates, stakeholders expressed the view that the proposed functions would be cost-effective. That is, the expected cost was low compared to the potential impact of cyber security incidents.[68] Stakeholders also supported formalising these functions to provide funding and resourcing certainty.[69]

While the updated costs are higher than previously expected, we continue to consider that the benefits outweigh the costs due to the significant impact and costs that would be incurred if a cyber incident were to occur. Notably, as seen above in **Table 3.1** over 85 per cent of the costs will be going towards the Cyber Incident Response Coordinator and the Cyber Security Uplift and Preparedness roles which includes the Australian Energy Sector Cyber Incident Response Plan and the Australian Energy Sector Cyber Security Framework. Importantly the framework's application has expanded in recent years, and as noted above now supports regulatory obligations under the SOCI Act, as well as providing guidance to new market entrant types.

The Commission considers the revised estimates of costs are still justified because they formalise AEMO's role and responsibilities in undertaking cyber security work which is already underway and already benefiting participants, specifically the Australian Energy Sector Cyber Security Framework. This reflects the reality that while AEMO has been performing some of these activities the environment has changed considerably, even within the last few years, with cyber preparedness and uplift becoming increasingly more important for the NEM, requiring further expansion and additional resourcing.

The Commission has also 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

67 Rule change request to the AEMC, Minister Bowen, pp. 9-10.

68 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. Submission to the draft determination, Ausgrid, p.1.

69 Submissions to the draft determination: ENA, p.1; Epic Energy, p.2.

of funding are not sustainable and do not provide any certainty that the cyber security work would continue.

Transgrid has requested more accurate costings and asked for AEMO to provide seven-year rolling budgets so TNSPs can anticipate and incorporate these costs into their five-year regulatory period.[70] The Commission is aware that AEMO currently discusses five year forward estimates with the Financial Consultation Committee (see Box 4, below). AEMO indicated to the Commission that it will continue to work with members of the Committee and wider stakeholders to provide transparency and forecasts on its budget and fees. 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' under NER rule 2.11. 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 to consider and provide feedback on its budget, fees, and corporate plan priorities. The Financial Consultation Committee meets at least three times per year and consists of industry, government and consumer representatives.

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/financialconsultation-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).

AEMO will be consulting on fee structure to determine how these functions will be apportioned across participants

Epic Energy and AGL requested additional clarity on how costs will be apportioned among participants.[71]

70 Submission to the draft determination, Transgrid, p.2.

71 Submissions to the draft determination: Epic Energy, p.2; AGL, p. 2.

AEMO will consult on the allocation of costs in accordance with rule 2.11 of the NER (see Box 4). AEMO has informed the Commission that it intends to first consult on whether the four functions can be determined to be a 'declared NEM project', then consult further on the fee structure for the 'declared NEM project'.

See **section 3.5** for more detail.

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 will be used for, at minimum, governance of this function and assessing and scoping requests for advice (see **Table 3.2**). 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.[72]

It is the Commission's understanding that while the tasks and activities associated with the four functions have been performed to varying degrees, all of the proposed functions will require investment and enhanced resourcing beyond existing efforts to appropriately deliver them. While AEMO has already incurred some establishment costs for the cyber security activities, the additional establishment resourcing would allow AEMO to scale up cyber security activities under the formalised functions. These additional establishment costs, such as deployment of systems and tools like out-of-band communications or a Customer Relationship Management tool, will be funded through participant fees following the commencement of the final rule. More information is provided in **Table 3.2** below. Prior to this rule change, AEMO could only resource a minimum requirement approach to perform these activities, given the authority under the NER did not exist.

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

- The final 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.
- The forecast costs of performing cyber security functions will be incorporated into AEMO's annual budget and fee process. AEMO will consult on the costs and how to recover them from participants through both a public consultation process and the Financial Consultation Committee, as outlined in Box 4.[73] The costs will be recovered as per AEMO's NEM Participant Fee structure which is subject to consultation under the NER.[74]

72 Sections 51 and 51A of the NEL.
73 AEMO submission to the consultation paper, p. 3.
74 NER clause 2.11.1(a).

Table 3.2: Previously, AEMO diverted existing resources to carry out limited cyber security activities

Function	Activities that can be undertaken under the final rule	Activities that AEMO undertook previously	Funding source for activities AEMO undertook previously
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 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. Involve AEMO across various sector wide cyber activities and forums. Act as a facilitator between energy organisations and the government across multiple forums, platforms and resources.	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. 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.	Activities were partially funded by the Commonwealth, States and Territories. AEMO maintained a proportionate approach, allocating internal funding only as needed.

Function	Activities that can be undertaken under the final rule	Activities that AEMO undertook previously	Funding source for activities AEMO undertook previously
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 provided ad hoc advice to a range of Commonwealth agencies since 2018 without any formal processes being established.	AEMO maintained a minimalist approach and allocated limited internal funding. Specific cyber security-related advice was 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 maintained a minimalist approach and allocated limited internal funding.

Source: AEMO.

3.4 AEMO now has liability protection to perform cyber security functions

The Commission's final rule ensures AEMO has liability protection (under an existing provision of the NEL) to perform activities under the four cyber security functions.

- Section 119 of the NEL provides AEMO, its officers and employees with immunity from civil monetary liability for an act or omission in the performance or exercise, or purported performance or exercise, of a function or power of AEMO - now including these cyber security functions - unless the act or omission is done or made in bad faith or through negligence.

Where AEMO is negligent, its civil liability is limited to $2 million per claim (under regulation 14 in the National Electricity (South Australia) Regulations).

The extension of liability protections to AEMO for these cyber security functions is necessary and is consistent with the performance of AEMO's existing functions. For example, in exercising the Australian Energy Sector Cyber Incident Response Plan, AEMO may initiate interactions with participants' systems to test the robustness of the plan. There are inherent risks in this activity which will be carefully managed.

Additionally, as a not-for-profit, liability protection is a key consideration in determining AEMO's access to appropriate insurance arrangements and limiting corporate costs.

3.5 The rule commences on 12 December 2024

Box 5: The rule commences on 12 December 2024

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

AEMO has informed the Commission that it will commence consultation on whether the functions may be determined a 'declared NEM project' and proposed fee structure in early 2025.

The final rule commences on publication of this determination on 12 December 2024. Immediate commencement is possible because AEMO is already performing some activities under the functions without having a cyber security role established in the NER.

An immediate commencement date allows AEMO to access cost recovery and protection from liability for the cyber security functions as soon as possible. This way benefits for consumers will be realised more quickly because AEMO will only be able to recover costs, and sufficiently commit resources to these four functions, from the commencement of the final rule. AEMO has indicated support for immediate commencement of the rule.[75]

AEMO has informed the Commission that it intends to commence consultation on whether the functions may be determined to be a 'declared NEM project' under NER clause 2.11.1(ba) shortly after publication of the final determination. This consultation will be done in accordance with the Rules consultation procedures in rule 8.9 of the NER and will allow stakeholders the opportunity to express their views and input on whether the cyber roles and responsibilities should be a 'declared NEM project'. Following consultation on determining if it is a 'declared NEM project', AEMO will

75 Submission to the draft determination, AEMO, p.1.

consult on a proposed structure for participant fees to recover AEMO's costs for the project, as required by NER clauses 2.11.1(bb) and (bc). Additionally, AEMO has informed the Commission that this fee structure will be in place until the next general determination of NEM participant fees is made for the period commencing 1 July 2026. AEMO intends to commence this consultation in early 2025 with a final determination to be made by 31 March 2026.

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

3.6 Stakeholders raised cyber security issues being considered in other processes

Throughout the consultation process 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.[76] The Clean Energy Council added that it can be unclear which SOCI Act requirements should be passed through to OEMs.[77]
- 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 imposing their own requirements.[78] SMA considered this could create "potential for misunderstanding and disagreement", while the Smart Energy Council noted a lack of consistency between jurisdictions.[79] (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.[80]
- Fronius suggested that a national cyber security strategy was needed to establish a coordinated approach to CER cyber security requirements.[81] The Smart Energy Council requested more clarity from market bodies and governments on these matters.[82] SMA requested mandating standards for CER systems.[83]
- Vestas requested that the rules also include OEMs and service providers.[84]

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 Commonwealth 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

76 Submissions to the consultation paper: Fronius, p. 1; SEC, p. 2; SMA, p. 5.
77 CEC submission to the consultation paper, p. 2.
78 Submissions to the consultation paper: SMA, p. 3; Fronius, p. 2; CEC, p. 2; SEC, p. 2.
79 Submissions to the consultation paper: SMA, p. 5; SEC, p. 2.
80 Submissions to the consultation paper: EQL, p. 3; AGL, pp. 2-3.
81 Fronius submission to the consultation paper, p. 1.
82 SEC submission to the consultation paper, p. 2.
83 Submission to the draft determination, p.2.
84 Submission to the draft determination, p.2.

cyber security work.[85] 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.[86]

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.**

85 ENA submission to the consultation paper, p. 3.

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

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.[87]

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.[88] 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 have 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

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

88 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 Australian Cyber Security Centre in 2014. The Australian Cyber Security Centre 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 Australian Cyber Security Centre 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	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	An agency of the Australian Signals Directorate 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: Australian Signals Directorate, www.asd.gov.au/about/who-we-are; Australian Cyber Security Centre; Department of Home Affairs - 'Cyber security', www.homeaffairs.gov.au/aboutus/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 Cyber Security Unit', www.forgov.qld.gov.au/information-and-communication-technology/cyber-security/about-the-cybersecurity-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 - 'Cyber Security 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 system black, 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."[89] The review recommended:[90]

> 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 Australian Cyber Security Centre, 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.[91] The Australian Energy Sector Cyber Security Framework can be used by owners and operators to meet SOCI Act requirements.[92] 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.[93] 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.[94]

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.[95] Similarly, many jurisdictions have a sub-plan for a serious cyber incident, but these

89 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.

90 Ibid., p. 69.

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

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

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

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

95 '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.

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.[96] The situation is similar for the Wholesale Energy Market (WEM) Rules which apply to the Western Australian electricity system.[97] The rule change proponent states they will look to address cyber security in the WEM and gas markets through separate processes.[98]

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 sought 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, the request considered that this has been done in a limited capacity using existing resources. The proponent considered that the proposed 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 3).

The rule change request can be found on the project page.[99]

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.[100] The Commission also published a consultation paper identifying specific issues for consultation. 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 the draft determination.

96 AEMC, National Gas Rules, https://energy-rules.aemc.gov.au/ngr/558.
97 Government of Western Australia, WEM Rules, https://www.wa.gov.au/government/document-collections/wholesale-electricity-market-rules.
98 Rule change request to the AEMC, Minister Bowen, p. 4.
99 AEMC, Cyber security roles and responsibilities rule change, https://www.aemc.gov.au/rulechanges/cyber-security-roles-and-responsibilities.
100 This notice was published under section 95 of the NEL.

On 26 September 2024, the Commission published a draft rule determination including a draft rule. The Commission received nine submissions on the draft rule determination. Issues raised in submissions are discussed and responded to throughout this final rule determination. A summary of other issues raised in submissions and the Commission's response to each issue is contained in **Appendix D**.

B Regulatory impact analysis

The Commission has undertaken regulatory impact analysis to make its 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 2 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 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. 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 (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 final rule determination.

C.1 Final rule determination and final rule

In accordance with section 102 of the NEL, the Commission has made this final rule determination in relation to the rule proposed by the Honourable Chris Bowen MP, Minister for Climate Change and Energy.

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

A copy of the final rule is attached to and published with this final determination. Its key features are described in **chapter 3**.

C.2 Power to make the rule

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

The final rule falls within 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 final rule
- the rule change request
- submissions received during the first and second rounds of consultation
- the Commission's analysis as to the ways in which the final rule will or is likely to contribute to the achievement of the NEO
- whether the final rule would apply in the Northern Territory (see below).

There is no relevant Ministerial Council on Energy (MCE) statement of policy principles for this rule change request.[101]

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.[102] The electricity rule is compatible with AEMO's declared network functions because the rule would not affect those functions.

101 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.

102 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.[103] Under those regulations, only certain parts of the NER have been adopted in the Northern Territory.

The final rule does not relate to parts of the NER that apply in the Northern Territory. As such, the Commission has not considered Northern Territory application issues.

The draft rule would have amended provisions in Chapter 10 of the NER, which applies in the Northern Territory, but those provisions would not have had any practical effect in the Northern Territory. The Commission assessed Northern Territory application issues for the draft rule in **Appendix C.4** of the draft determination. However, due to minor drafting changes for the final rule, the final does not amend any provisions in Chapter 10 and does not apply 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 final 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 amendments made by the final rule be classified as civil penalty provisions or conduct provisions.

103 These regulations under the NT Act are the National Electricity (Northern Territory) (National Uniform Legislation) (Modifications) Regulations 2016.

D Summary of other issues raised in submissions

Table D.1: Summary of other issues raised in submissions to the consultation paper and draft determination

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 and service providers.	As stated, the final rule 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 Australian Energy Cyber Security Framework or an alternative framework. Application of the SOCI Act to different market participants is a matter for the Australian Government, not AEMO. Additionally, OEMs and service providers are being considered in reforms such as the Cyber Security Act and the National CER Roadmap.
CEC		
SMA		

Stakeholder	Issue	Response
SMA	Clarity around the role of networks and other businesses in developing and enforcing their own cyber security rules.	As mentioned above, the National CER Roadmap provides some clarity on these issues.
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 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
CISC	Cyber and Infrastructure Security Centre
Commission	See AEMC
CSIRO	Commonwealth Scientific and Industrial Research Organisation
Cyber Security Act	*Cyber Security Act 2024*
DER	Distributed energy resources
DNSP	Distribution network service provider
DSO	Distribution system operator
ENA	Energy Networks Australia
MCE	Ministerial Council on Energy
NEL	National Electricity Law
NEM	National Electricity Market
NEO	National Electricity Objective
NER	National Electricity Rules
NGR	National Gas Rules
NT Act	*National Electricity (Northern Territory) (National Uniform Legislation) Act 2015*
OEM	Original equipment manufacturer
Proponent	The individual / organisation who submitted the rule change request to the Commission
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