

AEMO'S NEW CYBER SECURITY ROLES AND RESPONSIBILITIES

23 June 2025

Final Report and Determination

Part A – Declared NEM Project

Part B – Participant Fee Structure





We acknowledge the Traditional Custodians of the land, seas and waters across Australia. We honour the wisdom of Aboriginal and Torres Strait Islander Elders past and present and embrace future generations.

We acknowledge that, wherever we work, we do so on Aboriginal and Torres Strait Islander lands. We pay respect to the world's oldest continuing culture and First Nations peoples' deep and continuing connection to Country; and hope that our work can benefit both people and Country.

'Journey of unity: AEMO's Reconciliation Path' by Lani Balzan

AEMO Group is proud to have launched its first [Reconciliation Action Plan](#) in May 2024. 'Journey of unity: AEMO's Reconciliation Path' was created by Wiradjuri artist Lani Balzan to visually narrate our ongoing journey towards reconciliation - a collaborative endeavour that honours First Nations cultures, fosters mutual understanding, and paves the way for a brighter, more inclusive future.

Important notice

Purpose

In accordance with clause 2.11 and clause 8.9 of the National Electricity Rules (Rules), this document concludes AEMO's consultation on:

- In Part A of this document, the determination of the AEMO cyber security roles and responsibilities described in the National Electricity Amendment (Cyber security roles and responsibilities) Rule 2024 as a declared National Electricity Market (NEM) project.
- In Part B of this document, if those AEMO cyber security roles and responsibilities are determined a declared NEM project, the determination of the structure of an additional Participant fee to be used to recover the costs associated with those cyber security roles and responsibilities until the next general determination of NEM Participant fees.

This document has effect only for the purposes set out in the Rules, and the Rules and the National Electricity (Law) prevail over this document to the extent of any inconsistency. This publication has been prepared by AEMO using information available as at 22 June 2025.

Disclaimer

This document or the information in it may be subsequently updated or amended. This document does not constitute legal, business, engineering or technical advice, and should not be relied on as a substitute for obtaining detailed advice about the National Electricity Law, the National Electricity Rules or any other applicable laws, procedures or policies. AEMO has made reasonable efforts to ensure the quality of the information in this document but cannot guarantee its accuracy or completeness.

Accordingly, to the maximum extent permitted by law, AEMO and its officers, employees and consultants involved in the preparation of this document:

- make no representation or warranty, express or implied, as to the currency, accuracy, reliability or completeness of the information in this document; and
- are not liable (whether by reason of negligence or otherwise) for any statements or representations in this document, or any omissions from it, or for any use or reliance on the information in it.

Copyright

© 2025 Australian Energy Market Operator Limited. The material in this publication may be used in accordance with the [copyright permissions on AEMO's website](#).

Executive summary

The publication of this Final Report and Determination (Final Report) concludes the National Electricity Rules (NER, Rules) consultation process conducted by AEMO to consider two separate but inter-related consultation processes for AEMO's cyber security roles and responsibilities:

- **Part A** – consultation on the determination of the AEMO cyber security roles and responsibilities (the **new cyber security roles and responsibilities**) described in the National Electricity Amendment (Cyber security roles and responsibilities) Rule 2024 (**Amending Rule**) as a declared NEM project.
- **Part B** – if those AEMO cyber security roles and responsibilities are determined a declared NEM project, consultation on the determination of an additional Participant fee structure to be used to recover AEMO's costs associated with those cyber security roles and responsibilities, including the Registered Participants that will be charged the fee, the start date for recovery and the period or periods over which recovery will occur.

Having considered the submissions and upon further assessment, AEMO's final determination is as follows:

- **Part A** – to determine the new cyber security roles and responsibilities to be a declared NEM project meeting two of the criteria to be a declared NEM project pursuant to clause 2.11.1(b1) of the Rules.
- **Part B** – for an additional, separate 'Cyber Security' fee structure to be established to recover the costs of the new cyber security roles and responsibilities declared NEM project as determined under Part A.

The recovery of costs associated with new cyber security roles and responsibilities would commence from 1 July 2025, with recovery during financial year (FY) 2026 to include costs incurred on and from the AEMC's final rule and determination effective date of 12 December 2024.¹

Submissions to AEMO's Draft Report & Determination

AEMO received two submissions in response to its Notice of Second Stage Consultation and Draft Report and Determination (Draft Report) for Part A and Part B on the new cyber security roles and responsibilities from AGL and Energy Networks Australia (ENA).

AEMO appreciates the stakeholder feedback received in the second stage of our consultation process. Further information on each of the submissions is outlined in Section 1.2 of this Final Report, with AEMO's assessment and response to the submissions set out in Appendix A2.

AEMO's Final Report & Determination - New cyber security roles and responsibilities

In developing this Final Report, AEMO has carefully considered the issues raised in response to its Consultation Paper and Draft Report, stakeholder views raised through submissions, the NER requirements (the National Electricity Objective (NEO) and in particular the Fee Structure Principles). Based on this consideration and analysis, AEMO's final determination, consistent with its proposal as per the Draft Report, is:

¹ As no capital expenditure is forecast, a cost recovery period is not applicable.

- The new cyber security roles and responsibilities is a declared NEM project as they are a major reform or development of the market (Criterion 1), as well as a major change to its existing functions, responsibilities, obligations or power under the Rules (Criterion 2).
- An additional, separate 'Cyber Security' fee structure will be established that allocates costs of the new cyber security roles and responsibilities in the following manner:
 - Wholesale Participants (33.3% apportionment) charged equally on the basis of capacity and energy. That is, 50% is a daily rate based on the aggregate of the higher of the greatest registered capacity and the greatest notified maximum capacity in the previous calendar year of units from the WP, and 50% is a daily rate based on MWh energy in the previous calendar year;
 - Market Customers (33.3% apportionment) charged equally on the basis of a variable and fixed charging metric. That is, 50% on a \$/MWh basis for a financial year based on AEMO's estimate of total MWh to be settled in spot market transactions, and 50% on a \$/NMI basis per week; and
 - TNSPs (33.3% apportionment) charged on the basis of energy consumed for the latest completed financial year.
- Recovery of costs associated with new cyber security roles and responsibilities is to commence from 1 July 2025, with recovery during financial year 2026 including costs incurred on and from the Amending Rule's effective date of 12 December 2024.²

AEMO notes that a determination of the new cyber security roles and responsibilities as a declared NEM project and corresponding Participant fee structure is limited to the scope of the Amending Rule. The reasons supporting the final determination under Part A and Part B are outlined in Sections 3.3 and 4.3 of this Final Report respectively.

The actual amount charged to each Registered Participant group will be consulted on through AEMO's annual budget and fees process.

² As no capital expenditure is forecast, a cost recovery period is not applicable.



Contents

Executive summary	3
1 Stakeholder Consultation Process	6
1.1 Key information	6
1.2 Stakeholder submissions	7
1.3 Relationship to open general NEM Participant fee consultation	8
2 Background & Context	9
2.1 Rule requirements and guiding principles	9
2.2 Context for this consultation	11
3 Part A – Declared NEM Project	13
3.1 Summary of Part A consultation	13
3.2 Stakeholder feedback	14
3.3 Part A final determination and rationale	14
4 Part B – Participant Fee Structure	16
4.1 Summary of key issues for consultation	16
4.2 Stakeholder feedback	17
4.3 Part B final determination and rationale	18
A1. NEO & Fee Structure Principles	20
A2. Summary of submissions and AEMO responses	23
A3. Changes to deliver AEMO’s new roles and responsibilities	27
A4. Detailed requirements for AEMO’s new roles and responsibilities	29
Glossary	32

Tables

Table 1. Declared NEM project criteria and the new cyber security roles & responsibilities	13
Table 2. Part B consultation matters	16

1 Stakeholder Consultation Process

AEMO may charge for and recover fees for the performance of its statutory functions in accordance with section 52 of the National Electricity Law (NEL) and the National Electricity Rules (NER, Rules). The new cyber security roles and responsibilities were added to AEMO's statutory functions in accordance with National Electricity Amendment (Cyber security roles and responsibilities) Rule 2024 (Amending Rule) on 12 December 2024.

Subject to consultation, the Rules allow for AEMO to determine an additional fee to recover the costs of specific projects which AEMO has determined to be a declared National Electricity Market (NEM) project during the term of a Participant fee structure determination. AEMO is required to comply with the consultation procedures under clause 8.9 of the Rules in determining: if a project meets a criterion to be a declared NEM project specified in clause 2.11.1(b1) of the Rules, and any corresponding Participant fee structure determined under clause 2.11.

AEMO has therefore divided this consultation into two parts:

- **Part A** – The determination of the new cyber security roles and responsibilities described in the Amending Rule as a declared NEM project.
- **Part B** – If a determination of a declared NEM project is made, the structure of an additional Participant fee to be used to recover costs associated with those new cyber security roles and responsibilities until the next general determination of all Participant fees is made under clause 2.11 of the Rules, including the Registered Participants that will be charged the fee, the start date for recovery and the period or periods over which recovery will occur.

AEMO has undertaken both consultation processes in parallel to confirm a cost recovery approach with stakeholders in time for financial year (FY) 2026 in the event that a determination was made that the new cyber security roles and responsibilities are a declared NEM project and consultation on the matters in Part B was subsequently required under the Rules.

1.1 Key information

Purpose	To provide stakeholders with the opportunity to have input into AEMO's determination of the new cyber security roles and responsibilities as a declared NEM project (Part A) and, should a declared NEM project be determined, the development of the structure of Participant fees for the cyber security roles and responsibilities (Part B).
Date applicable (final determination)	1 July 2025 ³
Electricity roles and responsibilities covered in this consultation	<ul style="list-style-type: none">• Cyber security preparedness, response and recovery• Cyber security incident coordinator• Supporting cyber preparedness and uplift• Examining cyber risks and providing advice to government and industry, and• Facilitating the distribution of critical cyber security information to market participants.
Timetable	

³ The final Participant fee structure will be included in AEMO's general NEM Participant fee structure review that is currently being consulted on for the period commencing 1 July 2026.

Deliverable	Indicative date
Consultation Paper published	Tuesday 4 February 2025
Submissions due on Consultation Paper	Tuesday 4 March 2025
Draft Report published	Tuesday 22 April 2025
Submissions due on Draft Report	Wednesday 21 May 2025
Final Report published	Monday 23 June 2025

1.2 Stakeholder submissions

AEMO received two submissions to our second stage of consultation from AGL and Energy Networks Australia (ENA). The following provides a summary of these submissions received:

- AGL:
 - Support a determination of the new cyber security roles and responsibilities as a declared NEM project.
 - Support a separate fee to recover costs of the new cyber security roles and responsibilities.
 - Propose that costs should also be allocated to Distribution Network Service Providers (DNSPs).
 - Propose that any advisory services to the government that exceed \$500,000 and serve for wider market benefit should be subject to review or a disclosure mechanism to provide transparency to participants.
- ENA:
 - Do not support determining the cyber roles as a *major reform* under the declared NEM project criteria.
 - Do not support a separate fee as there are alternative approaches to providing transparency and opportunities for scrutiny of financial and project management performance of new responsibilities.
 - Support the allocation of fees to each state [jurisdiction] on the basis of pure energy consumption figures as being the fairest approach for customers and do not consider the special AEMO Victorian arrangement [established under the NEM Core fee] should apply for the new functions.
 - Agree it is desirable for both AEMO and participants that operating expenditures are recovered in the financial year in which they are incurred.
 - Support the final determination of the [cyber security roles and responsibilities] fee structure consultation this year, noting that while timings may not have allowed for earlier clarity, AEMO needs to be mindful of the timing of its determination and impact on network service provider (NSPs') abilities for their own timely cost recovery.

No submissions proposed an alternative Participant fee structure to those outlined in AEMO's Draft Report and Determination (Draft Report). Further detail on each submission, along with AEMO's response to feedback received can be found in Appendix A2.



1.3 Relationship to open general NEM Participant fee consultation

Any additional Participant fee structure for a declared NEM project may only be used to recover costs associated with that declared NEM project until cost recovery for the relevant functions can be considered as part of the determination of the next general NEM Participant fee structure.

Consultation is underway for the next general NEM Participant fee structure following publication of AEMO's consultation paper on 10 April 2025.⁴

This consultation, to be concluded by 31 March 2026 at the latest, will determine AEMO's NEM Participant fees for the fee recovery period commencing 1 July 2026. As such, the outcomes of the consultation processes initiated in Part A and Part B will be reflected in and further consulted upon as part of this broader consultation.

⁴ AEMO. NEM Participant Fee Structure – Consultation Paper. 10 April 2025. Available here: <https://www.aemo.com.au/consultations/current-and-closed-consultations/national-electricity-market-participant-fee-structure-review>.



2 Background & Context

2.1 Rule requirements and guiding principles

2.1.1 Declared NEM projects

Pursuant to clause 2.11.1(b1) of the NER, AEMO may determine any of the following projects to be a declared NEM project:

- a major reform or development (including an anticipated reform or development) of the market; or
- a major change (including an anticipated change) to a function, responsibility, obligation or power of AEMO under the Rules; or
- a major change (including an anticipated change) to any of the computer software or systems that AEMO uses in the performance of any of its functions, responsibilities, obligations or powers under the Rules.

When AEMO determines a project to be a declared NEM project under clause 2.11.1(b1), it must determine under clause 2.11.1(b2):

- the start date for recovery and the period or periods over which recovery will occur for the declared NEM project, and
- the structure of an additional Participant fee to be used in the recovery of costs associated with a declared NEM project until the next general determination of all Participant fees is made under clause 2.11.1(a) of the NER.

An additional Participant fee may be either:

- An addition to the scope of an existing fee structure determined by AEMO (in this case, the general NEM Participant fee structure determined in AEMO's Final Report of the Structure of Participant Fees in AEMO's Electricity Markets published in March 2021).⁵

Under this approach AEMO may expand the scope of a relevant existing Participant fee structure to recover the costs associated with the declared NEM project comprised of its new cyber security roles and responsibilities from Registered Participants.

- An additional, separate fee structure specific to the recovery of costs associated with a declared NEM project.

Under this approach, AEMO would establish a new fee structure to recover the costs of the declared NEM project comprised of its new cyber security roles and responsibilities from Registered Participants. This approach would include developing the appropriate attribution of costs to be allocated to each Registered Participant and applying fee metrics to those Registered Participants accordingly.

Part B therefore assesses the appropriateness of applying existing fee structures or alternative (separate) fee structures to recover costs.

⁵ AEMO. Electricity Fee Structure Final Report and Determination. 26 March 2021. Available here: <https://aemo.com.au/consultations/current-and-closed-consultations/electricity-market-participant-fee-structure-review>



2.1.2 Development of Participant fee structure

Under the Rules, AEMO only has the power to recover fees, when relying on a fee structure determined under clause 2.11 of the Rules, from Registered Participants. In determining the structure of Participant fees, AEMO must have regard to the National Electricity Objective (NEO). In addition, the structure of Participant fees must, to the extent practicable, be consistent with the principles specified in clause 2.11.1(b) of the Rules (referred to in this document as the Fee Structure Principles and set out in detail in Appendix A2). These principles include that:

- The structure of Participant fees should be simple.
- The structure of the Participant fees should provide for the recovery of AEMO's budgeted revenue requirements on the basis specified in clause 2.11.1(b)(2) of the Rules.
- The components of Participant fees charged to each Registered Participant should be reflective of the extent to which AEMO's budgeted revenue requirements involve that Registered Participant.
- Participant fees should not unreasonably discriminate against a category or categories of Registered Participants.

The Rules do not indicate that any one Fee Structure Principle should have greater weight than the others. There will often be a degree of tension between some of these principles, in which case AEMO will need to consider the appropriate weight to be given to each one. Therefore, meeting the requirements established under the Rules typically requires a trade-off or degree of compromise between principles. That is, an option to improve the fee structure against one principle may affect consistency with another principle.

For example, commonly competing principles are cost-reflectivity and simplicity. While cost-reflectivity in a fee structure could be improved through measures such as disaggregation of fees, markets or services, this would reduce the simplicity of the fee structure, resulting in greater complexity in the systems needed to manage the fees.

Similarly, in considering the NEO, AEMO notes the new cyber security roles and responsibilities furthers electricity consumers' long term interests in AEMO's effective performance of its functions to maintain the safe and secure operation of the national electricity system. AEMO considers that how it seeks to recover its costs associated with those roles and responsibilities should best align with the efficient delivery and operation of those functions. A preferred fee structure will seek to:

- recover costs from Registered Participants who benefit from AEMO's new cyber security roles and responsibilities, and
- provide an incentive to the Registered Participants who are allocated the costs to use and to participate in the services delivered across those new cyber security roles and responsibilities, thereby improving the overall quality and robustness of those services to the benefit of the electricity system.

2.2 Context for this consultation

2.2.1 AEMO's new cyber security roles and responsibilities

The Honourable Chris Bowen MP, Minister for Climate Change and Energy submitted a rule change request⁶ to the AEMC in March 2024, seeking to formalise the following AEMO cyber security roles and responsibilities:

1. Coordinate the system and market response to cyber incidents which impact, or potentially impact, system security and/or reliability.
2. Support cyber security maturity uplift and cyber preparedness efforts led by industry.
3. Provide advice to government and industry on sector-specific cyber security vulnerabilities and threats which impact, or have the potential to impact system security, where this relates to AEMO's expertise and capabilities as the system and market operator.
4. Provide, directly and by redistributing expert advice, such as from the Australian Cyber Security Centre (ACSC), critical cyber security information and advice to market participants, where the advice relates to potential risks to power system security or energy supply.

The AEMC published a consultation paper on 20 June 2024 outlining the context of the rule change, the problem raised, the proposed solution and decision-making matters. The final determination and final rule published on 12 December 2024 explicitly establishes cyber security as one of AEMO's power system security responsibilities in Chapter 4 of the NER and the above four functions are described in clause 4.3.2A of the Rules:

- **Function 1 – Cyber security incident coordinator:** AEMO is required to coordinate the NEM-wide response of Registered Participants to a cyber incident affecting the energy sector. It may do so by continued development of the Australian Energy Sector Cyber Incident Response Plan (AESCIRP) and leading the implementation of the AESCIRP.
Refer to clause 4.3.2A(a) of the Rules.
- **Function 2 – Supporting cyber preparedness and uplift:** AEMO is to continue to have stewardship of the Australian Energy Sector Cyber Security Framework (AESCSF), which may include organising testing and scenario training exercises, and developing and providing guidance and advice to industry in the form of written materials, digital tools and working groups.
Refer to clause 4.3.2A(b) of the Rules.
- **Function 3 – Examining cyber risks and providing advice to government and industry:** AEMO is required to provide cyber security research and advice to governments at the request of Ministers, and may additionally undertake its own research and provide advice to a Minister and to Registered Participants in relation to identified cyber security risks and the management or mitigation of those risks.
Refer to clause 4.3.2A(c) to (e) of the Rules.

⁶ AEMC Rule change request. The Honourable Chris Bowen MP – AEMO Cyber Security Role March 2024. Last accessed 24 December 2024. Available at: <https://www.aemc.gov.au/sites/default/files/2024-03/The%20Honourable%20Chris%20Bowen%20MP%20-%20Rule%20change%20request%20%281%29.pdf>

- **Function 4 – Facilitating the distribution of critical cyber security information to market participants:**
AEMO is required to facilitate distribution of critical cyber security information to jurisdictions and Registered Participants.

Refer to clause 4.3.2A(f) of the Rules.

2.2.2 Costs of the new cyber security roles and responsibilities

Estimated establishment and ongoing costs in Years 1 to 3 are forecast to range between \$8 million and \$10 million per annum, with ongoing costs beyond this initial three-year period forecast to range between \$8.5 million and \$9.5 million per annum.⁷

In line with these estimates, AEMO's Final Budget and Fees for FY26⁸ has proposed a \$14.7 million revenue requirement which accounts for costs to perform the new cyber security roles and responsibilities in the budget year as well as addressing the costs incurred in FY25 but not recovered.⁹

AEMO has assessed that no material capital expenditure will be incurred in establishment and ongoing activities associated with the new cyber security roles and responsibilities. All costs are therefore to be treated as operating expenditure only and are to be recovered in the financial year in which they are incurred.

⁷ AEMC. National Electricity Amendment (Cyber security roles and responsibilities) Rule 2024 Rule determination. 12 December 2024. Available at: <https://www.aemc.gov.au/rule-changes/cyber-security-roles-and-responsibilities>

⁸ AEMO. Final FY26 Budget and Fees Consultation. Available here: https://aemo.com.au/-/media/files/about_aemo/energy_market_budget_and_fees/2025/aemo-final-budget-and-fees-fy26.pdf?la=en

⁹ These costs have been incurred by AEMO since the Rule came into effect on 12 December 2024.

3 Part A – Declared NEM Project

Part A of this paper outlines AEMO’s Final Determination on whether the new cyber security roles and responsibilities meet any of the criteria for a declared NEM project pursuant to clause 2.11.1(b1) of the Rules.

As part of this assessment, AEMO has considered the costs of facilitating the new cyber security roles and responsibilities, the extent that the cyber security roles and responsibilities have resulted in changes to the Rules, procedures, processes and systems and the wider impact on AEMO and participants.

3.1 Summary of Part A consultation

The table below outlines the criteria to be met to be determined a declared NEM project under the Rules (of which at least one must be met) and a summary of the assessment of the impact of the new cyber security roles and responsibilities against each of the criteria from AEMO’s Draft Report. The table also includes AEMO’s draft decision for each of the criteria.

Table 1. Declared NEM project criteria and the new cyber security roles & responsibilities

Criterion	Impact of the new cyber security roles & responsibilities in relation to the criterion
1. Major reform or development of the market	<ul style="list-style-type: none">Cyber security has evolved rapidly as an energy security risk and is now inextricably linked with the management of the electricity and gas systems and markets.The landscape of cyber security governance in the Australian energy sector has evolved commencing from 2014 with the establishment of the ACSC.The new cyber security roles and responsibilities expand AEMO’s core power system security obligations, placing it at the centre of coordinating and supporting cyber security preparedness, response and recovery across the NEM.Approximately 600+ market participants are impacted by the Amending Rule that includes the various activities that will be required to implement and support the new cyber security roles and responsibilities including process changes, consultations with industry, implementation of technical platforms as well as alignment of activities across all participants (see Appendix A3 for full list).Draft decision: The new cyber security roles and responsibilities are a major reform or development of the market.
2. Major change to a function, responsibility, obligation or power of AEMO	<ul style="list-style-type: none">The rule change request submitted to the AEMC by the Honourable Minister Bowen March 2024 noted that AEMO did not have clear authority to deliver functions for cyber security within the broader context of power system security.¹⁰The AEMC’s final rule and determination made on 12 December 2024 includes new clauses that describe AEMO’s responsibilities for cyber security under Chapter 4.3 of the Rules (Power System Security Responsibilities and Obligations).The four new cyber security functions for AEMO explicitly require or allow AEMO to coordinate and support cyber security preparedness, response and recovery to maintain power system security. These four new functions expand AEMO’s responsibilities and obligations beyond its existing remit (see Appendix A4 for detailed requirements for each of the additional responsibilities).

¹⁰ AEMC Rule change request. The Honourable Chris Bowen MP – AEMO Cyber Security Role March 2024. Last accessed 24 December 2024. Available at: <https://www.aemc.gov.au/sites/default/files/2024-03/The%20Honourable%20Chris%20Bowen%20MP%20-%20Rule%20change%20request%20%281%29.pdf>

Criterion	Impact of the new cyber security roles & responsibilities in relation to the criterion
	<ul style="list-style-type: none"> The AEMC stated throughout its consultation process that, without explicitly establishing these functions in the Rules, there is potential for harm whereby cyber risks may adversely impact any part of the power system, from individual participants to the system as a whole. Draft decision: The new cyber security roles and responsibilities are a major (or anticipated) change to an AEMO function, responsibility, obligation or power under the NER.
3. Major change to computer software or systems	<ul style="list-style-type: none"> Changes to AEMO's computer software and systems, as well as additional capabilities will be required to support delivery of the new cyber security roles and responsibilities. Changes will be provided via a range of technology functions and software as AEMO upscales its cyber security teams resulting in additional investment in systems and resources. Changes will not require alterations to AEMO's core systems or market applications, and capital expenditure costs related to these changes are not expected to be material. Draft decision: The new cyber security roles and responsibilities are not a major change to the computer software or systems that AEMO uses in the performance of AEMO's functions, responsibilities, obligations and powers under the NER.

3.2 Stakeholder feedback

AEMO received the following stakeholder feedback on Part A as set out in AEMO's Draft Report:

- AGL is broadly supportive of AEMO categorising the cyber security functions as a [declared] 'NEM project' under the Rules.
- ENA acknowledged the crucial nature of cyber security and the new functions, recognising it is an important change to AEMO's functions, responsibilities and obligations / powers under the NER essentially adding four new functions. However, the ENA did not support determining the roles and responsibilities as a major reform noting it may establish a precedent of setting a lower threshold and proliferation of participant fees moving forward.

Further detail on these comments and AEMO's responses can be found in Appendix A2.

3.3 Part A final determination and rationale

AEMO's final determination for Part A consultation remains consistent with our draft determination – that the new cyber security roles and responsibilities meet **two of the three** criteria for a project to be determined a declared NEM project pursuant to clause 2.11.1(b1) of the Rules:

- a major reform or development (including an anticipated reform or development) of the market; and
- a major change (including an anticipated change) to a function, responsibility, obligation or power of AEMO under the Rules.

AEMO believes the above two criteria are met as the Amending Rule:

- Introduced a new power system security responsibility and new cyber security functions for AEMO. They represent an evolution and adaptation of the governance arrangements supporting the operation of the power system and corresponding markets in light of the changing NEM environment and expanding size and complexity of cyber security issues more broadly.
- Represents a significant reform for AEMO as foreshadowed by the number of additional activities outlined in Appendix A3 related to cyber security incident preparedness, response and information dissemination to be implemented.
- In addition to the impacts to AEMO, represents a significant reform for the NEM noting the breadth and volume of market participants impacted by the Rule change and the various activities that will be required to implement and support the new cyber security roles and responsibilities.
- Has added to one of AEMO's core responsibilities to maintain power system security an additional obligation to coordinate and support cyber security preparedness, response and recovery.
- Has also added four new cyber security functions, each requiring AEMO to undertake the additional requirements highlighted in Appendix A4.
- Provides AEMO with clear obligations or authority to undertake preventative work for cyber incidents, as well as formalising and reinforcing functions to enable appropriate and robust management of cyber security risks.

AEMO acknowledges the ENA's concerns that a determination of the new cyber security roles and responsibilities as a declared NEM project may establish a low threshold for a *major reform* which will lead to a proliferation of Participant fees.¹¹ AEMO assesses how, and from whom, it is to recover its costs in respect of each rule change on a case-by-case basis. AEMO does not intend the determination of the new cyber security roles and responsibilities as a declared NEM project to be a signal for growth in the number of declared NEM projects (and subsequent Participant fee structure) consultations and determinations going forward.

A declared NEM project consultation allows AEMO to test with stakeholders not only whether any criteria of a declared NEM project are likely to be met, but also whether its existing Participant fee structures are appropriate for recovering the costs associated with a new rule (and at least until the next general NEM Participant fee structure consultation) and are aligned with the NEO and Fee Structure Principles.¹² Given the significant change in governance and regulatory cyber security arrangements in Australia impacting the energy sector since 2014¹³ and the scope of the new cyber security roles and responsibilities, AEMO considered it prudent at this time to test those assumptions with stakeholders.

AEMO notes the current general NEM participant fee structure review provides an opportunity for further stakeholders input to ensure that the Participant fee structure is fit-for-purpose for the next fee structure period.

¹¹ ENA Submission to AEMO's Draft Determination (Page 1). Available at: <https://www.aemo.com.au/consultations/current-and-closed-consultations/new-cyber-security-roles-and-responsibilities-for-aemo---declared-nem-project>

¹² AEMO notes the outcomes where a determination is made that a project meets the declared NEM project criteria does not automatically result in an additional (separate) Participant fee structure being determined. For example, AEMO's Participant fee structure consultation for the Consumer Data Rights (CDR) declared NEM project in 2023 determined that costs are to be recovered through the existing Electricity Retail Markets fee. Available at: <https://www.aemo.com.au/consultations/current-and-closed-consultations/participant-fee-structure-for-the-consumer-data-right-cdr-declared-nem-project>.

¹³ AEMO. Draft Report and Determination. New Cyber Security Roles and Responsibilities. Available at: https://www.aemo.com.au/-/media/files/stakeholder_consultation/consultations/nem-consultations/2025/new-cyber-security-roles/draft-report-and-determination---cyber-security-declared-nem-project_final.pdf?la=en

4 Part B – Participant Fee Structure

As AEMO's final determination outlined in Part A (Section 3) determined the new cyber security roles and responsibilities to be a declared NEM project, clause 2.11.1(b2) of the Rules requires AEMO to determine the structure for an additional Participant fee to be used to recover those costs associated with the declared NEM project until such time as the next general determination of all Participant fees is made under clause 2.11 of the Rules. Specifically, AEMO must also determine:

- the structure of an additional Participant fee¹⁴ to be used in the recovery of costs,
- the start date for recovery, and
- the period or periods over which recovery will occur.

4.1 Summary of key issues for consultation

The table below provides an overview of the matters to address under Part B consultation with AEMO's draft decision as per our Draft Report.

Table 2. Part B consultation matters

Consultation Matter	Summary of key issues
Participant fee structure (including fee metrics and Registered Participants to be charged)	<ul style="list-style-type: none">• AEMO proposed and assessed two options in its Draft Report for stakeholder feedback:<ol style="list-style-type: none">1. To use the existing NEM Core fee structure.2. To establish a separate 'Cyber Security' fee that allocates costs to Wholesale Participants (33.3%), Market Customers (33.3%) and Transmission Network Service Providers (TNSPs) (33.3%) using existing the NEM Core fee structure<ul style="list-style-type: none">– Registered Participant allocations were based on historical market participation (which includes participants accessing the portal, submitting assessment results and viewing their organisation's result and benchmarking data with the AESCSF) that showed all NEM Participants are impacted.– DNSPs were not allocated any of the costs at this stage consistent with existing NEM Participant fee structures.• Draft decision: Following assessment against the Fee Structure Principles and NEO, Option 2, a separate 'Cyber Security' fee was preferred by AEMO to be applied to recover costs associated with the new cyber security roles and responsibilities.<p>Where research or advice related to Function 3 is requested, shared with, and / or benefits a wider cohort of Registered Participants (i.e., as per Functions 1, 2 and 4) irrespective of whether the research or advice was requested by a Minister or a Registered Participant, AEMO will seek to recover its costs of performing this function via the additional (separate) 'Cyber Security' fee to be established.</p><p>Where AEMO is required to undertake research or provide advice in relation to cyber security risks which is specifically requested by a Minister (i.e. a non-</p>

¹⁴ An additional Participant fee is taken to mean either an addition to the scope of an existing fee structure already defined by AEMO as part its Final Report of the Structure of Participant Fees in AEMO's Electricity Markets published in March 2021 or the creation of an additional, separate fee structure specific to the recovery of costs associated with a declared NEM project.

Consultation Matter	Summary of key issues
	Registered Participant) under Function 3, AEMO will recover those costs directly from the relevant jurisdiction requesting the research/advice. ¹⁵
Cost recovery commencement date and recovery period	<ul style="list-style-type: none"> The new cyber security roles and responsibilities were added to AEMO's statutory functions by the Rule on 12 December 2024. AEMO has commenced upscaling the cyber security functions currently being performed and investing in system changes and additional resourcing to enable delivery of the new cyber security roles and responsibilities. AEMO does not anticipate any material capital expenditure to be incurred in relation to performing its new roles and responsibilities. All costs incurred are to be treated as operating expenditure only. Draft decision: Cost recovery to commence from 1 July 2025 and all operating costs to be recovered in the financial year in which they are incurred. A recovery period is not applicable as there is no capital expenditure to be incurred.

4.2 Stakeholder feedback

The following stakeholder feedback was received relating to Part B consultation matters:

- Participant fee structure:
 - AGL supported a separate cost recovery framework that is distinct from the existing participant fees.
 - AGL noted concerns regarding the provision which allows advisory services sought from Ministers or government (i.e. Function 3) to be allocated to the broader participant base when deemed beneficial to the wider market and proposed that any advisory project exceeding \$500,000 to be subject to a review or disclosure mechanism.
 - AGL was of the view that DNSPs should be allocated costs of the new cyber roles and responsibilities, noting that it strongly supports this issue being considered as part of AEMO's general NEM Participant fee structure review.
 - ENA outlined that the new functions are not a major reform warranting a separate fee and that setting a low threshold for a major reform will introduce a proliferation of NEM declared projects and ultimately fee types, particularly when the simplification and aggregation of fee types is being considered in the general Participant fee structure consultation.
 - ENA suggested there are alternative approaches that would not involve new fee types to provide transparency of costs and opportunities for scrutiny of financial and project management performance of new responsibilities.
 - ENA supported allocation of fees to each state [jurisdiction] on the basis of energy consumption as being the fairest approach for customers and do not consider the special AEMO Victorian arrangement [established under the NEM Core fee] should apply for the new functions.
- Cost recovery commencement date and recovery period:
 - ENA supported operating expenditure being recovered in the financial year incurred.

¹⁵ This approach sits outside the NEM Participant fee structures, which can apply only to Registered Participants.

- ENA noted a determination by 30 June 2025 that would result in charging NSPs on 1 July 2025 is exceedingly late and does not afford the NSP adequate time to make arrangements for timely cost recovery. The ENA acknowledged timings may not have allowed earlier clarity, however welcomed the finalisation of the fee structure consultation to be this year and early notification of fees to the respective NSPs.

Further detail on these comments and AEMO's responses can be found in Appendix A2.

4.3 Part B final determination and rationale

AEMO's final determination for the Part B consultation remains consistent with our draft determination – that costs of a declared NEM project for the new cyber security roles and responsibilities will be recovered as follows:

- An additional (separate) 'Cyber Security' fee to be established, recovering costs in the following manner:
 - Wholesale Participants (33.3% apportionment) charged equally on the basis of capacity and energy. That is, 50% is a daily rate based on the aggregate of the higher of the greatest registered capacity and greatest notified maximum capacity in the previous calendar year of units from the WP, and 50% is a daily rate based on MWh energy in the previous calendar year.
 - Market Customers (33.3% apportionment) charged equally on the basis of a variable and fixed charging metric. That is, 50% on a \$/MWh basis for a financial year based on AEMO's estimate of total MWh to be settled in spot market transactions, and 50% on a \$/NMI basis per week.
 - TNSPs (33.3% apportionment) charged on the basis of energy consumed for the latest completed financial year.


Where research or advice related to Function 3 is requested, shared with, and / or benefits a wider cohort of Registered Participants (i.e., as per Functions 1, 2 and 4) irrespective of whether the research or advice was requested by a Minister or a Registered Participant, AEMO will seek to recover its costs of performing this function via the additional (separate) 'Cyber Security' fee to be established.

AEMO is mindful that there will be circumstances where there are disclosure risks with work AEMO undertakes in relation to cyber security which is specifically requested by a Minister under Function 3. AEMO will engage appropriately with Registered Participants depending on the nature of the work, and may seek to recover costs from jurisdictions where appropriate.

- Recovery of costs associated with new cyber security roles and responsibilities is to commence from 1 July 2025, with recovery during FY26 including costs incurred on and from the Amending Rule's effective date of 12 December 2024. A cost recovery period is not applicable as no capital expenditure is forecast with all costs subsequently to be recovered in the financial year in which they are incurred.

AEMO acknowledge AGL's concerns with the unpredictability of the cost base for advisory services provided to Ministers under Function 3 that may be allocated to the broader participant base when deemed beneficial to the wider market.¹⁶ To provide transparency over activities that may result in additional costs allocated to Registered

¹⁶ AGL submission to AEMO's Draft Determination (Page 1). Available at: <https://www.aemo.com.au/consultations/current-and-closed-consultations/new-cyber-security-roles-and-responsibilities-for-aemo---declared-nem-project>



Participants, AEMO intends to establish a governance framework as part of the implementation activities for research or advice requested by Ministers that may be shared with and/or benefit a wider cohort of Registered Participants.

This final Participant fee structure is determined for the following reasons:

- Greater alignment with the NEO and consistency with the Fee Structure Principles compared to applying the existing NEM Core fee structure as:
 - More accurately reflects the involvement level of groups of Registered Participants based on historical information.
 - Assurance that there is no over- or under-stating of the apportionment of costs to any group of Registered Participants, thereby avoiding potential cross-subsidies associated with the new functions, i.e. does not unreasonably discriminate against a group of Registered Participants.
 - Cost recovery is from Registered Participants who would utilise and benefit from the services delivered across the new functions, with apportionment to different groups of Registered Participants that reflects their level of involvement and provides incentives to use or participate in the services moving forward.
- Attributing costs to groups of Registered Participants mirrors the approach taken in existing NEM Participant fee structures.
- Provides appropriate transparency on costs related to the new cyber security roles and responsibilities.
- Having an additional, separate Cyber Security fee may also allow for the potential recovery of all cyber reform related costs under a single fee structure moving forward, subject to the policy or rule determinations on those future reforms, and AEMO's next general NEM Participant fee structure consultation.
- Recovery commencing on 1 July 2025 ensures alignment with AEMO's annual budget and fees process and allows costs already incurred since 12 December 2024 (when the Amending Rule became effective) for implementing the new cyber security roles and responsibilities to be recovered as soon as possible.

AEMO notes that consultation on the general NEM Participant fee structure has commenced and therefore the additional Participant fee structure for the new cyber security roles and responsibilities will be included in the scope of that consultation.

A1. NEO & Fee Structure Principles

Objective / Principle	Requirement	Application and examples
National Electricity Objective	<p>In determining Participant fees, AEMO must have regard to the national electricity objective.</p> <p>The NEO as stated in the NEL is 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—</p> <ul style="list-style-type: none"> (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 – <ul style="list-style-type: none"> i. for reducing Australia's greenhouse gas emissions; or ii. that are likely to contribute to reducing Australia's greenhouse gas emissions. 	<p>The Second Reading Speech to the National Electricity (South Australia) (New National Electricity Law) Amendment Bill 2005 makes it clear that the NEO is an economic concept and should be interpreted as such.</p> <p>The Speech gives an example that investment in and use of electricity services will be efficient when services are supplied in the long run at least cost, resources, including infrastructure, are used to deliver the greatest possible benefit and there is innovation and investment in response to changes in consumer needs and productive opportunities.</p> <p>The Speech goes on to state that the long-term interests of consumers of electricity requires the economic welfare of consumers, over the long term, to be maximised.</p> <p>If the NEM is efficient in an economic sense, the long-term economic interests of consumers in respect of price, quality, reliability, safety and security of electricity services will be maximised. Applying an objective of economic efficiency recognises that, in a general sense, the NEM should be competitive, that any person wishing to enter the market should not be treated more, or less, favourably than persons already participating, and that particular energy sources or technologies should not be treated more, or less, favourably than others.</p> <p>Since 2006, the NEO has been considered in a number of Australian Competition Tribunal determinations and Federal Court matters, which have followed a similar interpretation. See, for example, Application by ElectraNet Pty Ltd (No 3) [2008] ACompT (paragraph 15):</p> <p>“The national electricity objective provides the overarching economic objective for regulation under the Law: the promotion of efficient investment in the long term interests of consumers. Consumers will benefit in the long run if resources are used efficiently, i.e. resources are allocated to the delivery of goods and services in accordance with consumer preferences at least cost.”</p> <p>The NEO is clearly a relevant consideration where AEMO has to exercise judgment or discretion in reaching its determination, for example, if there is a number of Participant fee structures each of which can satisfy the Fee Structure principles, or where the relevant provisions of the Rules are ambiguous.</p>
Simplicity	<p>The structure of Participant fees should be simple</p>	<p>As “simple” is not defined in the Rules, it must be given its ordinary meaning as understood in the context of clause 2.11 of the Rules.</p> <p>The New Shorter Oxford English Dictionary's definition of “simple” (in this context) is: “not complicated or elaborate” and “plain, unadorned”. Whether a fee structure fits these definitions is largely a matter of judgement.</p> <p>There is a wide range of possible fee structures. There is no single identifiable point where “simple” becomes “complicated”.</p> <p>It is clear from this provision that a certain degree of complexity was envisaged in that the structure of Participant fees may involve several components and budgeted revenue consists of several elements. The structure of Participant fees need not demonstrate absolute simplicity.</p> <p>The simplest fee structures are unlikely to be consistent with the other criteria. However, it is possible to find fee structures that, while</p>

Objective / Principle	Requirement	Application and examples
		<p>consistent with the other criteria, are relatively simple, in comparison to alternative structures.</p> <p>Further, AEMO considers that the use of the word “simple” in this context also involves a degree of transparency.</p> <p>AEMO considers that the simplicity principle means that the basis of the fee structure and its application to various Registered participants should be:</p> <ul style="list-style-type: none"> • straight-forward • easily understood by participants • readily applied by Registered participants and AEMO <p>foreseeable and forecastable in terms of impacts and costs.</p>
Reflective of Involvement	The components of Participant fees charged to each Registered Participant should be reflective of the extent to which the budgeted revenue requirements for AEMO involve that Registered Participant	<p>In determining whether the extent to which the budgeted revenue requirement relating to a particular output involves a class of Registered Participant, AEMO relies on the experience and expertise of its general managers and staff, and considers factors such as the degree to which the class of Registered Participant:</p> <ol style="list-style-type: none"> a) interacts with AEMO in relation to the output; b) uses the output; c) receives the output; and d) benefits from the output. <p>AEMO also considers how the revenue requirements are given rise to, or caused by, that class of Registered Participant's presence in the NEM.</p> <p>AEMO must determine the structure of Participant fees “afresh”.</p> <p>That is, it must freshly consider the application of the criteria in clause 2.11.1 of the Rules and the NEL to the facts, circumstances and analysis available to it at this time.</p> <p>In doing so, however, AEMO will have regard to its previous determinations under clause 2.11.1 of the Rules, where appropriate.</p> <p>The principle of “reflective of extent of involvement” does not have a specialised meaning in economics. It is consistent with the economic notion of ‘user pays’ but as a matter of ordinary language, it indicates a degree of correspondence (between AEMO and its costs and participants) without connoting identity.</p> <p>However, this principle does not involve a precise degree of correspondence.</p> <p>Where fixed and common costs are involved, multiple registered participants may be involved with AEMO costs in relevantly similar ways. AEMO's analysis and experience shows that there are categories or classes of Registered Participants that share certain characteristics that mean that the way in which they interact with AEMO is likely to have the same or similar cost implications for AEMO.</p> <p>Where it is practical for AEMO to identify costs that are fixed or common in nature that can reasonably be allocated to a class or classes of Participants that share characteristics such that their involvement with AEMO's outputs is likely to have the same or similar cost implications, AEMO will seek to do so.</p>
Non-discriminatory	Participant fees should not unreasonably discriminate against a category or categories of Registered Participants	<p>In past Participant Fee determinations, AEMO (and its predecessor, NEMMCO) adopted the following definition of discriminate:</p> <p>“Discriminate means to treat people or categories of people differently or unequally. Discriminate also means to treat people, who are different in a material manner, in the same or identical fashion. Further, “discriminate against” has a legal meaning which is to</p>

Objective / Principle	Requirement	Application and examples
		<p>accord “different treatment ... to persons or things by reference to considerations which are irrelevant to the object to be attained”.</p> <p>This principle allows AEMO to discriminate against a category or categories of Registered participants where to do so would be reasonable.</p> <p>Where a degree of discrimination between categories of Registered Participants is necessary or appropriate to achieve consistency with the other principles in clause 2.11.1(b) of the Rules, or the NEL, the discrimination will not be “unreasonable”.</p> <p>In considering a past fee determination, the Dispute Resolution Panel accepted that this principle is to be applied to the extent practicable and it is only unreasonable discrimination that offends.</p>
Comparison with existing fee structures	<p>In developing, reviewing and publishing, the structure of Participant fees, AEMO must consider other fee structures in existence which it thinks appropriate for comparison purposes.</p> <p><i>Note that this is not strictly a principle but is included for completeness in describing the matters to which AEMO must have regard.</i></p>	<p>Other relevant fee structures could include:</p> <ul style="list-style-type: none"> • Other electricity market fee structures such as Western Australia or globally • Gas markets operated by AEMO

A2. Summary of submissions and AEMO responses

Stakeholder	Key points	AEMO response
1. AGL	a) Broadly supportive of AEMO categorising the cyber security functions as a 'NEM project' under the NER.	<p>AEMO notes AGL's comment.</p> <p>Section 3.3 of this Final Report outlines AEMO's determination that the new cyber security roles and responsibilities meet two of the three criteria for a declared NEM project under clause 2.11.1(b1) of the NER.</p> <p>That is, the roles and responsibilities as outlined in the Amending Rule are new roles and responsibilities and are also a major reform or development.</p>
	b) In principle agree that a separate cost recovery framework, distinct from the existing integrated participant fees, is appropriate given the specialised and evolving nature of these roles <ul style="list-style-type: none"> Strongly encourage AEMO to prioritise transparency in the way the fees are determined and allocated. Given evolving nature of the project and potential for cost escalation over time, important that market participants are provided with clear visibility into the basis of cost estimations, assumptions underpinning them and the mechanisms for updating the estimates. Transparency will be essential in maintaining stakeholder confidence and ensuring that costs remain proportionate and justifiable. 	<p>AEMO agrees with AGL's comments.</p> <p>As outlined in Section 4.3 of this Final Report, AEMO considers that the additional (separate) Cyber Security fee is more consistent with the Fee Structure Principles and NEO than the existing NEM Core structure.</p> <p>AEMO is committed to improving financial transparency through consultation on its annual budget and fees report and engagement with stakeholders including via the Financial Consultative Committee (FCC).</p>
	c) Concerns regarding the provision which allows advisory services sought from Ministers or government more broadly to be costed to the broader participant base when deemed beneficial to the wider market <ul style="list-style-type: none"> Pieces of advice that serve a wider benefit can introduce a degree of unpredictability into the cost base. Propose that any advisory project exceeding \$500,000 in cost should be subject to a review or disclosure mechanism – ensuring that participants can understand, scrutinise, and if 	<p>AEMO acknowledges AGL's concerns.</p> <p>As outlined in section 4.3 of this Final Report, for Function 3 where research or advice is requested by Ministers that may be shared with and / or benefit a wider cohort of Registered Participants, AEMO is looking to establish a governance framework to provide transparency to stakeholders / participants on the work required and costs that may result from any Ministerial request.</p>


Stakeholder	Key points	AEMO response
	<p>necessary, provide input on whether the scope and objectives are delivering value to the broader market</p> <ul style="list-style-type: none"> • Believe there should be some opportunity to review costs for other functions that significantly exceed original cost estimates 	<p>Additionally, as noted in response 1b), AEMO is committed to improving financial transparency through its annual budget and fees report (consultation commencing in April of each year) and engagement with stakeholders including via the FCC.</p>
	<p>d) Believe DNSPs should be required to contribute to funding of the new cyber functions</p> <ul style="list-style-type: none"> • DNSPs are key stakeholders in the resilience of the energy sector and also direct beneficiaries of coordinated cyber defence and information sharing. • DNSPs operate critical systems such as SCADA, remote switching infrastructure, and digital interfaces with both market participants and the public, and are expected to participate more fully with the ongoing management of CER • Strongly support the question of whether DNSPs should become registered fee-paying participants being examined through AEMO's NEM Participant Fee Structure Review, particularly considering DNSPs' increasing operational involvement with AEMO through reforms such as the National CER Roadmap and the NEM Reform Program. 	<p>AEMO acknowledges AGL's comment on allocating some of the costs of the new cyber security roles and responsibilities to DNSPs.</p> <p>DNSPs are currently not apportioned any of AEMO's costs via the existing NEM Participant fees as a cost recovery mechanism has not been established under the Rules for this Registered Participant type.</p> <p>As outlined in section 4.3 AEMO does not propose to recover costs from DNSPs for the new cyber security roles and responsibilities at this stage.</p> <p>Given the timing of the general NEM Participant fee structure review and to ensure cost recovery of the new cyber security roles and responsibilities can commence as soon as practically possible, AEMO will consider the allocation of Participant fees to DNSPs within that general review.</p>
	<p>e) As outlined in previous submissions to the AEMC on their consultation of AEMO's Cyber Security Roles and Responsibilities, AGL urge AEMO alongside the AEMC and co-regulators to take a broader and more integrated view of cyber risk across Australia's energy systems.</p> <ul style="list-style-type: none"> • The current framing of cyber risk through the lens of the NEM and the NER does not fully capture the interconnected nature of the modern energy ecosystem. • Cyber threats will likely not distinguish between gas, electricity, WEM, CER or jurisdictional boundaries. • Recommend that future reform efforts seek to establish consistent, whole-of-system cyber governance frameworks that align protections across energy markets, for the most resilient outcome. 	<p>AEMO notes AGL's sentiments that reflect the need for the market bodies to have a holistic approach to cyber security protection in Australia's energy sector.</p> <p>As highlighted in section 4.3 of this Final Report, an additional, separate Cyber Security fee can allow for the potential recovery of all cyber reform related costs under a single fee structure moving forward, subject to the policy or rule determinations on those future reforms.</p>
2. ENA	<p>a) ENA acknowledges the crucial nature of cyber security and the new functions – recognise that this is an important change to</p>	<p>AEMO notes ENA's comment.</p>

Stakeholder	Key points	AEMO response
	AEMO's functions, responsibilities and obligations/powers under the NER, essentially adding four new functions.	Section 3.3 of this Final Report, highlights the reasons AEMO consider the new cyber security roles and responsibilities are a major change to AEMO's functions, responsibilities, obligations or powers under clause 2.11.1(b1) of the NER.
	b) New functions are not a major reform warranting a separate fee. <ul style="list-style-type: none"> Concerned this will establish a precedent of setting a low threshold for a major reform that will see a proliferation of NEM declared projects and ultimately fee types, particularly when the simplification and aggregation of fee types is being considered in the general participant fee structure consultation. Suggests there are alternative approaches, that would not involve new fee types, to providing transparency and opportunities for scrutiny of financial and project management performance of new responsibilities. 	<p>AEMO acknowledges ENA's views that the new cyber security roles and responsibilities are not a major reform warranting a separate fee and potential implications of this determination.</p> <p>Sections 3.3 and 4.3 of this Final Report highlight the reasons AEMO has determined the new cyber security roles and responsibilities are a major reform to the market under clause 2.11.1(b1) of the NER and to establish an additional, separate Cyber Security fee.</p> <p>Further, AEMO has considered alternative options not involving new fee types, on providing the required transparency and scrutiny of financial and project management performance, for example more granular reporting in the budget and fee report, however this option does not satisfy the Fee Structure Principles to a higher level than the Final Participant fee structure outlined in this report.</p>
	c) Critical to ensure fair allocations across states and supports the allocation of fees to each state on the basis of pure energy consumption figures as being the fairest approach for customers. <ul style="list-style-type: none"> ENA requests clarification regarding the basis on which the fee is intended to be allocated. In section 5.4 of the draft report the allocation to TNSPs is noted to be on the basis of energy consumed for the latest completed financial year, which is the same % allocation for the NTP fee. Table 3 however infers a fee structure allocation like the existing NEM core fee, which recognises special arrangements and a lower allocation for Victoria. 	<p>AEMO notes ENA's comments on the basis of charging fees to TNSPs.</p> <p>AEMO has clarified in section 4.3 of this Final Report that TNSPs are to be charged on the basis of energy consumed for the latest completed financial year.</p>
	d) ENA agree that operating expenditures recovered in the financial year in which they are incurred is desirable for both AEMO and for participants in the NEM. <ul style="list-style-type: none"> AEMO to be mindful CNSPs' charges have already been published on 15 March 2025. An AEMO determination by 30 June 2025 on the cyber fees to start charging NSPs on 1 July 	<p>AEMO acknowledges ENA's comments on the notification and start date of Participant fees for the new cyber security roles and responsibilities.</p> <p>As outlined in section 4.3 of this Final Report, AEMO intends to recover operating expenditure related to the new cyber security roles and responsibilities in the financial year incurred.</p>

Stakeholder	Key points	AEMO response
	2025 is exceedingly late and affords the NSP no similar arrangement for timely cost recovery.	AEMO must conduct its consultation on the development of a Participant fee structure in accordance with the timeframes outlined in clause 8.9 of the NER.
	<p>e) Welcome fee structure consultation to be finalised this year and early notification of fees to the respective networks.</p> <ul style="list-style-type: none"> Noted that AEMO proposes a cyber fee of \$14.7m which includes costs in FY25/26 from 11 December 2024 and also FY26/27 and that AEMO will charge the respective allocation/participants in FY25/26 for 18 months of costs and there may be similar allocation in FY26/27. ENA are therefore mindful that transmission charges will include several years of cyber fees next year and there may be similar catch up from market customers, which has impacts on consumers bills. Allocating charges for market functions is best done with the party who is closest to end consumer billing and has more flexibility to pass costs on and affords AEMO slightly longer to determine budgets and allocations each year. 	<p>AEMO notes ENA's comments on AEMO's Participant fee structure consultation timing and its impact on transmission charges.</p> <p>AEMO's Final Determination on a Participant fee structure for the new cyber security roles and responsibilities will be finalised by 30 June 2025 for cost recovery to commence from 1 July 2025.</p> <p>AEMO is obligated by clause 2.11.1(bc) of the NER to conduct its consultations on declared NEM projects and related Participant fee structures within the Rules consultation procedures timeframes set out in clause 8.9 of the NER (as per AEMO's response 2d).</p> <p>Additionally, clause 11.153.2 of the NER requires AEMO to notify specified TNSPs (as defined in the NER) by 15 February of each year of the amount of their respective Participant fees (excluding the NTP function) for the coming financial year.</p>

A3. Changes to deliver AEMO's new roles and responsibilities

Function	Changes to be implemented
1. Cyber security incident coordinator	<ul style="list-style-type: none"> • Deliver a program of training and uplift to 'cyber-enable' the control room, allowing them to identify and facilitate the triaging of cyber incidents. • Engage resources to provide an 'incident coordination retainer' arrangement partnership with AEMO to prepare for significant incidents requiring burst capacity. • Annual fees in relation to the procured incident response retainer arrangement. • Response to major security incidents each year over and above the retainer arrangement and internal resourcing. • Formal documentation and process models of incident response playbooks. • Update and maintain incident response playbooks. • Establish technology to ensure reliable communications are possible between participants in a sector-wide incident response. • Maintain the above-mentioned tools. • Hire and train resources responsible for creating, updating and maintaining the sector contact list. • Integrate the contacts list with AEMO's CRM as a central source of truth for cyber security contacts over two years. • Maintain data quality and test communications methods. • Hire and train resources responsible for creating, updating and maintaining the jurisdiction contact list. • Maintain communications channels with cyber security contacts and test at intervals. • Finalise creation and embedding of the AESCIRP over a year. • After finalising the AESCIRP, develop and deliver an annual test plan, and engage resources to support in the execution and documentation of exercises. • Engage resources to own, socialise and perform an annual refresh of the AESCIRP. • Subscribe to energy sector specific cyber threat intelligence services. • Increase the number of resources over three years to correlate and analyse threat information collected across these various sources
2. Supporting cyber preparedness and uplift	<ul style="list-style-type: none"> • Engage resource to prepare for, attend and champion at industry and cyber security events. • Attend cybersecurity related events and conferences specific to the sector, and if gaps are present deliver knowledge and champion cyber within the industry. Costs may include branding, marketing and comms. • Engage resource to perform cyber knowledge and insight management across the sector, providing information to market participants as required. • Implement or use an existing technology solution to consistently store and manage knowledge and documentation. • Engage with and coordinate third party providers to support in provision of responses to information requests if required. • Annual maintenance of the AESCSF and associated programme (assessment, communications, training).
3. Examining cyber risks and providing advice to government and industry	<ul style="list-style-type: none"> • Establish the required systems and governance structures to manage and respond to requests for cyber security research.



Function	Changes to be implemented
	<ul style="list-style-type: none"> • Maintain the required systems and governance structures to manage and respond to requests for cyber security research. • Engage resource to monitor requests and chair this governance structure as required. • Implement or use an existing technology solution to consistently store and manage knowledge and documentation. • Ongoing maintenances of systems and data quality. • Engage resource to manage and coordinate the response to requests.
4. Facilitating the distribution of critical cyber security information to market participants	<ul style="list-style-type: none"> • Maintain and test communications channels ensuring cybersecurity and jurisdictional contacts can be reached as required. • Engage resource in a cyber comms role, responsible for maintaining communications channels and templates. • Identify and establish platforms and capabilities for sharing tactical and strategic cyber threat and vulnerability information.

A4. Detailed requirements for AEMO's new roles and responsibilities

Function	Responsibilities	Requirements
1. Cyber security incident coordinator	Coordinate the response to cyber security incidents that threaten the security of power systems and markets	<p>To fulfill this responsibility AEMO must:</p> <ul style="list-style-type: none"> • be able to identify indicators of suspicious activity or a cyber incident where possible based on the information available at any given time. Note this information may come from internal systems, incident reporting or information provided by market participants. • have an industry-facing contact ready to be made aware that a cyber incident which could affect • have a tested plan and process for coordinating significant cyber incidents which are likely to affect power systems and markets, and playbooks to deal with specific circumstances as they arise (e.g. ransomware, OT incident) • have resources to respond to cyber incidents, including burst capacity via 3rd parties to deal with events requiring a significant response as they arise. • have suitable tools to manage and track incidents from their identification through to resolution and post-incident review. • have suitable tools and technology to enable bridge calls and other communications to occur with relevant parties throughout the response, including out-of-band channels of communication (i.e. off-email) • be able to coordinate incidents over a 24x7 period should the need arise
	Prepare and maintain sector cyber contact lists	<p>To fulfill this responsibility AEMO must:</p> <ul style="list-style-type: none"> • be able to document and maintain a set of contacts across all market participants to ensure communications are possible in the event of a cyber incident. • keep the contact list up to date and the quality of the data must be maintained through regular review / reconciliation. • update existing processes where contact details are registered and maintained to ensure that the information is not overridden or deleted. • test and maintain communications tools to ensure that market participants are able to be contacted as required.
	Prepare and maintain jurisdiction cyber contact list	<p>To fulfill this responsibility AEMO must:</p>

Function	Responsibilities	Requirements
		<ul style="list-style-type: none"> be able to document and maintain a set of contacts across relevant governments and jurisdictions (e.g. State Gov, law enforcement, industry bodies). keep the contact list up to date and the quality of the data must be maintained. test and maintain communications tools to ensure that jurisdictional contacts are able to be contacted as required.
	AESCIRP maintenance and exercises	<p>To fulfill this responsibility AEMO must:</p> <ul style="list-style-type: none"> maintain a plan for incident response through an annual update, reflecting changes in the technology and threat landscape. conduct exercises to test its incident response plan, ensuring readiness for a real incident, and document outcomes in a formal report.
	Continuously correlate and triage the active cyber threat landscape	<p>To fulfill this responsibility AEMO must:</p> <ul style="list-style-type: none"> have access to relevant threat information from various sources, including government organisations and subscription services offering relevant threat information. have processes and systems in place to ingest relevant data/log sources from market participants and correlate this with relevant cyber threat intelligence. be able to identify active cyber threats within the sector in its own environment and the environments of market participants and trigger incident response processes as required.
2. Supporting cyber preparedness and uplift	Champion AEMO across various sector-wide cyber activities and forums	<p>To fulfill this responsibility AEMO must:</p> <ul style="list-style-type: none"> be able to attend industry and cyber security events, championing cyber security and providing thought leadership. be able to hold cyber security related events where appropriate. maintain an active online / social media presence to elevate its cyber profile across the sector
	Create and maintain guidance information to be provided to market participants and relevant bodies as required	<p>To fulfill this responsibility AEMO must:</p> <ul style="list-style-type: none"> be able to formulate and provide responses to security-related questions when enquiries are made by market participants. be able to maintain documentation and previous responses, preventing rework. have access to third party specialists, where required, in order to provide expert / up-to-date guidance to market participants continue to maintain the AESCSF.
3. Examining cyber risks and providing advice to	Establish and maintain a governance structure for the management of requests	<p>To fulfill this responsibility AEMO must:</p> <ul style="list-style-type: none"> have sufficient resources to respond to and fulfill research requests where AEMO is best placed to respond.

Function	Responsibilities	Requirements
		<ul style="list-style-type: none"> have a mechanism to recover the cost of providing responses to research requests as part of this defined process.
	Create and sustain processes for responding to requests for research/advice	To fulfill this responsibility AEMO must: <ul style="list-style-type: none"> establish a process for receiving, tracking and estimating effort to respond to research requests.
4. Facilitating the distribution of critical cyber security information to market participants	Establish and maintain communications channels and templates for cyber security information dissemination	To fulfill this responsibility AEMO must: <ul style="list-style-type: none"> maintain and establish communications channels, templates and processes for the dissemination of cyber security information.

Glossary

Term or acronym	Meaning
ACSC	Australian Cyber Security Centre
AEMO	Australian Energy Market Operator
AEMC	Australian Energy Market Commission
AESCSF	Australian Energy Sector Cyber Security Framework
DCCEEW	Commonwealth Department of Climate Change, Energy, Environment and Water
DHA	Commonwealth Department of Home Affairs
DNSP	Distribution Network Service Provider
NEM	National Electricity Market
NEO	National Electricity Objective
NER	National Electricity Rules
SOCI	Security of Critical Infrastructure
TNSP	Transmission Network Service Provider
WP	Wholesale Participant