



Draft 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) AEMO is consulting:

- In Part A of this document, on 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, on 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.

AEMO notes that consultation in Part B on the determination of the fee structure is undertaken to satisfy the relevant Rules requirements in clauses 2.11 and 8.9 in the event that the AEMO cyber security roles and responsibilities are determined to be a declared NEM project under the Rules.

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 21 April 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 Draft Report and Determination (Draft Report) commences the second stage of 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 (**the 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 draft determination is as follows:

- **Part A** – to determine the new cyber security roles and responsibilities as a declared NEM project having met two criteria to be a declared NEM project pursuant to clause 2.11.1(ba) 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 FY26 to include costs incurred on and from the AEMC's final rule and determination effective date of 12 December 2024.<sup>1</sup>

## AEMO's Consultation Paper on the new cyber security roles and responsibilities

AEMO received three submissions in response to its Notice of First Stage Consultation and Consultation Paper for Part A and Part B on the new cyber security roles and responsibilities from SMA-Australia, Energy Networks Australia (ENA) and Transgrid.

AEMO appreciates the stakeholder feedback received in the first stage of our consultation process. Further detail on each of the submissions is outlined in Section 3 of this Draft Report, with AEMO's assessment and response to the submissions set out in Appendix A1.

## AEMO's Draft Determination

AEMO considers the new cyber security roles and responsibilities to be 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).

The reasons for each criterion being satisfied or not have been outlined in Sections 4.1 to 4.3 of this Draft Report.

---

<sup>1</sup> As no capital expenditure is forecast, a cost recovery period is not applicable.

AEMO considers an additional, separate 'Cyber Security' fee structure option to be more consistent with the Fee Structure Principles and the NEO (in particular, the reflective of involvement and non-discriminatory principles), relative to alternative options considered including AEMO's existing NEM Core fee.

Under a 'Cyber Security' fee, the costs associated with the new cyber security roles and responsibilities would be apportioned equally across Wholesale Participants (33.3%), Market Customers (33.3%) and Transmission Network Service Providers (33.3%), applying the same fee metrics as the existing NEM Core fee for those Registered Participant groups.

For clarity, where AEMO is undertaking research or providing advice in relation to identified cyber security risks which is specifically requested by a Minister (i.e. a non-Registered Participant) under Function 3, AEMO will seek to recover those costs directly from the relevant jurisdiction requesting the research/advice.<sup>2</sup>

An exception to the above is 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 'Cyber Security' fee to be established.

The reasons supporting the above draft determination have been outlined in Sections 5.2 and 5.3 of this Draft Report. The actual amount charged to each Registered Participant group will be consulted on through AEMO's annual budget and fees process.

Consultation on AEMO's general NEM Participant fee structure has commenced and therefore any Final Determination on a Participant fee structure for the new cyber security roles and responsibilities will be included as part of that consultation scope of the general review.

## Submissions – Closing date and information

Stakeholders are invited to submit written responses on AEMO's draft determination in either or both of Part A and Part B of this Draft Report by 5.00 pm (Australian Eastern Standard Time [AEST]) on Wednesday 21 May 2025 to [reformdevelopmentandinsights@aemo.com.au](mailto:reformdevelopmentandinsights@aemo.com.au).

Please refer to the Notice of Second Stage of Consultation published with this paper or Section 1.1 for further details.

---

<sup>2</sup> As outlined in section 5.1, this is outside of NEM Participant fee structures under the NER which can apply only to Registered Participants.



# Contents

Executive summary	3
1 Consultation Overview	7
1.1 Key information	7
1.2 Rules requirements and guiding principles	8
1.3 Budget and Fee Structure	10
1.4 Relationship to current general NEM Participant fee consultation	10
2 AEMO's new cyber security roles and responsibilities	12
2.1 Estimated costs of the new cyber security roles and responsibilities	13
3 Stakeholder submissions	15
4 Part A – Declared NEM project	16
4.1 Criterion 1 – Major reform or development of the market	16
4.2 Criterion 2 – Major change to a function, responsibility, obligation or power of AEMO	19
4.3 Criterion 3 – Major change to computer software or systems	20
4.4 Part A – Draft Determination	22
5 Part B – Participant fee structure	23
5.1 Participant fee structure options	23
5.2 Assessment of Participant fee structure options	25
5.3 Start date and period/s of fee recovery	28
5.4 Part B – Draft Determination	28
A1. Summary of submissions and AEMO responses	30
A2. Detailed requirements for AEMO's new roles and responsibilities	35
A3. NEO & Fee Structure Principles	37
A4. Glossary	40

## Figures

Figure 1. Aligning Participant fee structure consultation outcomes	11
Figure 2. Timeline of cyber security reforms and frameworks	17
Figure 3. Additional (separate) fee for the new cyber security roles and responsibilities	24

## Tables



Table 1. Anticipated changes required to deliver the new cyber security roles and responsibilities	18
Table 2. AEMO's new cyber security roles and responsibilities	20
Table 3. Draft determination assessment of all fee structure options against NEO and Fee Structure Principles	26

# 1 Consultation Overview

The Australian Energy Market Operator (AEMO) invites stakeholder submissions on either or both of Part A and Part B of this Draft Report and Determination (Draft Report) – New cyber security roles and responsibilities.

## 1.1 Key information

<b>Purpose</b>	To provide stakeholders with the opportunity to have input into AEMO's determination of the 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).												
<b>Date applicable (draft determination)</b>	1 July 2025 <sup>3</sup>												
<b>Electricity roles and responsibilities covered in this consultation</b>	<ul style="list-style-type: none"><li>• Cyber security preparedness, response and recovery</li><li>• Cyber security incident coordinator</li><li>• Supporting cyber preparedness and uplift</li><li>• Examining cyber risks and providing advice to government and industry, and</li><li>• Facilitating the distribution of critical cyber security information to market participants.</li></ul>												
<b>Timetable</b>	<table><tr><th>Deliverable</th><th>Indicative date</th></tr><tr><td>Consultation Paper published</td><td>Tuesday 4 February 2025</td></tr><tr><td>Submissions due on Consultation Paper</td><td>Tuesday 4 March 2025</td></tr><tr><td>Draft Report published</td><td>Tuesday 22 April 2025</td></tr><tr><td>Submissions due on Draft Report</td><td>Wednesday 21 May 2025</td></tr><tr><td>Final Report published</td><td>By Monday 30 June 2025</td></tr></table> <p>Having regard to stakeholder feedback additional stages may be included as part of the consultation process.</p>	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	By Monday 30 June 2025
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	By Monday 30 June 2025												
<b>Meetings</b>	Stakeholders may request a meeting in their submission. Matters discussed at the meeting may be made available to other stakeholders.												
<b>Submissions – Closing date and information</b>	<p>AEMO requests that submissions are provided in electronic format (either pdf or Word) by 5.00pm AEST Wednesday 21 May 2025 to <a href="mailto:reformdevelopmentandinsights@aemo.com.au">reformdevelopmentandinsights@aemo.com.au</a>.</p> <p>Please note that submissions will be published, other than confidential material, as per <a href="#">AEMO's Consultation submission guidelines</a>. Please identify any part of your submission that is confidential, and you do not wish to be published.</p> <p>Respondents should also note that if material identified as confidential cannot be shared and validated with other stakeholders then it may be accorded less weight in AEMO's decision making process than published material.</p>												

<sup>3</sup> AEMO note that, should the new cyber security roles and responsibilities be determined a declared NEM project, and an additional Participant fee structure be established, that 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.

## 1.2 Rules requirements and guiding principles

### 1.2.1 Declared NEM projects

Subject to consultation, the Rules allow for AEMO to determine an additional fee to recover the costs of specific projects (declared NEM project) during the term of a Participant fee structure determination. Pursuant to clause 2.11.1(ba) 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(ba), it must determine under clause 2.11.1(bb):

- 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).<sup>4</sup>

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.

<sup>4</sup> 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>



### 1.2.2 Development of Participant fee structure

AEMO develops its proposed Participant fee structures in accordance with clause 2.11.1 of the Rules. Under the Rules, AEMO only has the power to recover market fees 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.

### 1.2.3 Consultations

AEMO is required to comply with the Rules consultation procedures in clause 8.9 of the Rules in determining a Participant fee structure under clause 2.11.1 and making determinations under clauses 2.11.1(ba) and (bb) of the Rules.

AEMO has therefore divided this consultation into two parts:

- **Part A** – The determination of the new cyber security roles and responsibilities described in the National Electricity Amendment (Cyber security roles and responsibilities) Rule 2024 (**the 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 is undertaking both consultation processes in parallel, in order to confirm a cost recovery approach with stakeholders in time for FY26 in the event that AEMO determines that the new cyber security roles and responsibilities are a declared NEM project and consultation on the matters in Part B is required under the Rules.

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 NER. The new cyber security roles and responsibilities were added to AEMO's statutory functions by the Rule on 12 December 2024. This consultation seeks to determine, through consultation, the way in which AEMO recovers its costs for the new cyber security roles and responsibilities, that is, the Registered Participants that costs will be recovered from, the start date for recovery and the period or periods over which recovery will occur.

If AEMO determines, through consultation with stakeholders, that the new cyber security roles and responsibilities do not meet the criteria of a declared NEM project, AEMO will seek to recover its costs of performing these roles and responsibilities in accordance with existing NEM Participant fee structures until a new general NEM Participant fee structure is determined by AEMO in consultation with stakeholders. Further details on this approach are provided in Section 5.

### 1.3 Budget and Fee Structure

The operation of clause 2.11.1 (Development of Participant fee structure) of the Rules also needs to be understood in the context of its surrounding provisions which deal with AEMO's budgets and the payment of Participant fees.

Under clause 2.11.3 (Budgeted revenue requirements), AEMO is required to prepare and publish its budgeted revenue requirements for each financial year. That budget must consider and identify revenue requirements for the matters set out in clause 2.11.3(b). Some, but not all of these matters are referred to in the non-exhaustive list of components of Participant fees in clause 2.11.1(c). AEMO may include components in a fee structure which are different to those set out in clause 2.11.1(c).

Clause 2.11.1(b)(2) of the Rules is the principle that Participant fees should recover the budgeted revenue requirements for AEMO determined under clause 2.11.3.

Under clause 2.11.2 of the Rules, AEMO may charge Registered Participants the relevant component/s of Participants fees in accordance with the structure of Participant fees.

Consequently, the scheme of clauses 2.11.1 to 2.11.3 of the NER is:

- To require AEMO to determine the structure of Participant fees according to certain Rules;
- To require AEMO to determine AEMO's budgeted revenue requirements according to certain Rules; and
- To empower AEMO to recover the budgeted revenue requirements through charging Registered Participants in accordance with the structure of Participant fees.

### 1.4 Relationship to current general NEM Participant fee consultation

An additional Participant fee structure for a declared NEM project may only be used to recover costs associated with the declared NEM project until the determination of the next general NEM Participant fee structure.

Consultation is underway for the next general NEM Participant fee structure to be determined by 31 March 2026 for the next fee recovery period commencing 1 July 2026. The outcomes of the consultation processes initiated in Part A and Part B of this paper will be reflected in and further consulted upon as part of this broader consultation.

Therefore, should AEMO’s draft determination that the new cyber security roles and responsibilities meet the criteria of a declared NEM project and that an additional Participant fee structure for the declared NEM project is to be established, become AEMO’s final determination following consultation, then:

- the additional Participant fee structure would only apply until 30 June 2026 (inclusive), and
- cost recovery for the new cyber security roles and responsibilities will be included in the next general NEM Participant fee structure consultation which commenced on 10 April 2025.

Figure 1 highlights AEMO’s proposed approach for incorporating the outcomes of this consultation into the general NEM Participant fee structure consultation.

Figure 1. Aligning Participant fee structure consultation outcomes



## 2 AEMO's new cyber security roles and responsibilities

Cyber security is an energy security risk which is inextricably linked with the management of electricity and gas systems. A cyber-attack on Australia's energy systems could undermine critical services that Australians rely on, such as telecommunications, health, policing and defence. In December 2022, Energy Ministers expressed commitment to cyber-readiness of the sector and “*endorsed the development of rule change to confirm and clarify AEMO's cyber security roles and responsibilities*”.<sup>5</sup> AEMO had been performing a subset of the contemplated cyber security roles and responsibilities, having been initially contracted and funded by the Commonwealth Department of Climate Change, Energy, Environment and Water (DCCEEW) to co-develop the Australian Energy Sector Cyber Security Framework (AESCSF), in line with the recommendations of the 2017 Finkel Review.<sup>6</sup>

AEMO's position as the energy market operator affords it unique access to energy market stakeholder intelligence, which it can leverage to provide expert advice and analysis to government and Registered Participants on current and emerging cyber security issues for the energy sector.

The the Honourable Chris Bowen MP, Minister for Climate Change and Energy submitted a rule change request<sup>7</sup> 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:

<sup>5</sup> Energy and Climate Change Ministerial Council. Meeting communique. December 2022. Available here: <https://www.energy.gov.au/energy-and-climate-change-ministerial-council/meetings-and-communications>

<sup>6</sup> Commonwealth Department of Climate Change, Energy, the Environment and Water. Independent Review into the Future Security of the National Electricity Market. Final Report 9 June 2017. Available here: <https://www.dcceew.gov.au/energy/markets/independent-review-future-security-nem>

<sup>7</sup> 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 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 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.
- **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.

These four functions do not impose additional mandatory obligations on Registered Participants. Neither do they confer additional directive powers beyond AEMO's existing authority to take actions in response to an immediate or proximate cyber-attack (or a specific threat of cyber-attack) affecting or potentially affecting power system security in the NEM. The four cyber security functions are instead designed to assist in the coordination and adoption of cyber security measures by Registered Participants in the NEM.

## 2.1 Estimated costs of the new cyber security roles and responsibilities

As part of the AEMC's rule change process, AEMO estimated costs in relation to the new cyber security roles and responsibilities. Based on assumptions as of November 2024, reflecting an improved understanding of the implementation and ongoing requirements of the new roles and responsibilities that were anticipated to be described in the final Rule, establishment and BAU 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. In line with these earlier estimates, AEMO's Draft Budget and Fees for FY26<sup>8</sup> 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. AEMO do not anticipate any material capital expenditure to be incurred in relation to performing its new roles and responsibilities.

<sup>8</sup> AEMO. Draft FY26 Budget and Fees Consultation. Available here: <https://aemo.com.au/consultations/current-and-closed-consultations/draft-fy26-budget-and-fees-consultation>



The approach for recovering these costs is subject to the outcomes of this consultation, which is expected to conclude by 30 June 2025. For example, should AEMO determine, following the consultation, that the new cyber security roles and responsibilities did not meet the criteria of a declared NEM project, then these costs would be recovered through one of the existing Participant Fee structures (e.g., NEM Core fee) and this would be reflected in the final FY26 Budget and Fees report.



## 3 Stakeholder submissions

AEMO received three submissions during the first stage of consultation from SMA-Australia, Energy Networks Australia (ENA) and Transgrid. The following provides a summary of the three submissions received:

- SMA-Australia:
  - Support a determination of the new cyber security roles and responsibilities as a declared NEM project.
  - Agree that it was reasonable to expand the existing Participant fee structure for costs incurred on and from 12 December 2024.
  - Suggest that if an additional (separate) cyber security function fee is established, it would be preferable for that to be considered as part of the current NEM Participant fee consultation.
  - Note that the allocation could commence with equal attribution of costs of the cyber security roles and responsibilities across Wholesale Participants, Transmission Network Service Providers (TNSPs) and Market Customers, with allocation to Distribution Network Service Providers (DNSPs) to be considered as part of the current general NEM Participant fee structure consultation
  - Suggest further review on the fee structure could be undertaken as part of the general NEM Participant fee structure.
- ENA and Transgrid:
  - Do not support the new cyber security roles and responsibilities as a declared NEM project.
  - Support costs being recovered from the existing NEM Core fee structure.
  - Encourage transparency of costs of the new cyber security roles and responsibilities.

The main reasons put forward by the ENA and Transgrid for not supporting a determination include:

- The criteria under clause 2.11.1(ba) of the NER for a project to be determined a declared NEM project have not been met.
- The Rule builds upon and enhances AEMO's activities rather than introducing a new and significant function.

No submissions proposed an alternative Participant fee structure to those outlined in the Consultation Paper for the recovery of costs associated with the new cyber security roles and responsibilities. Further detail on each submission, along with AEMO's response to feedback received can be found in Appendix A1.

## 4 Part A – Declared NEM project

Part A of this paper considers whether the new cyber security roles and responsibilities meet any of the criteria to be determined a declared NEM project pursuant to clause 2.11.1(ba) of the Rules. As part of this assessment, AEMO considers the costs to facilitate the new cyber security roles and responsibilities, the extent of the cyber security roles and responsibilities result in changes to the Rules, procedures, processes and systems and the wider impact on AEMO and participants.

If the new cyber security roles and responsibilities are determined not to meet the criteria to be a declared NEM project after consultation with stakeholders, the costs of the cyber security roles and responsibilities will be recovered by AEMO in accordance with its current NEM Participant fee structure determination for the period until 30 June 2026, and until such time as a new Participant fee structure is determined by AEMO in consultation with stakeholders. Part B of this paper details the cost recovery approach in these circumstances.

### 4.1 Criterion 1 – Major reform or development of the market

*A major reform or development (including an anticipated reform or development) of the market*

#### Criterion 1 – Draft determination

AEMO considers that the new cyber security roles and responsibilities **are** a major reform or development of the NEM for the following reasons:

- The AEMC's final rule and determination 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.
- The new cyber security roles and responsibilities represent a significant reform for AEMO as foreshadowed by the number of additional activities outlined in Table 1 related to cyber security incident preparedness, response and information dissemination to be implemented.
- In addition to the impacts to AEMO, the Rule change represents a significant reform for the NEM noting the breadth and volume of market participants impacted by the Rule change as a result of the various activities that will be required to implement and support the new cyber security roles and responsibilities.

AEMO considers 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.<sup>9</sup> The requirements for robust cyber security risk management will continue to change quickly to adapt to new vulnerabilities, correlating closely with developments in telecommunications and digitalisation.<sup>10</sup> For example, through increased integration of distributed energy

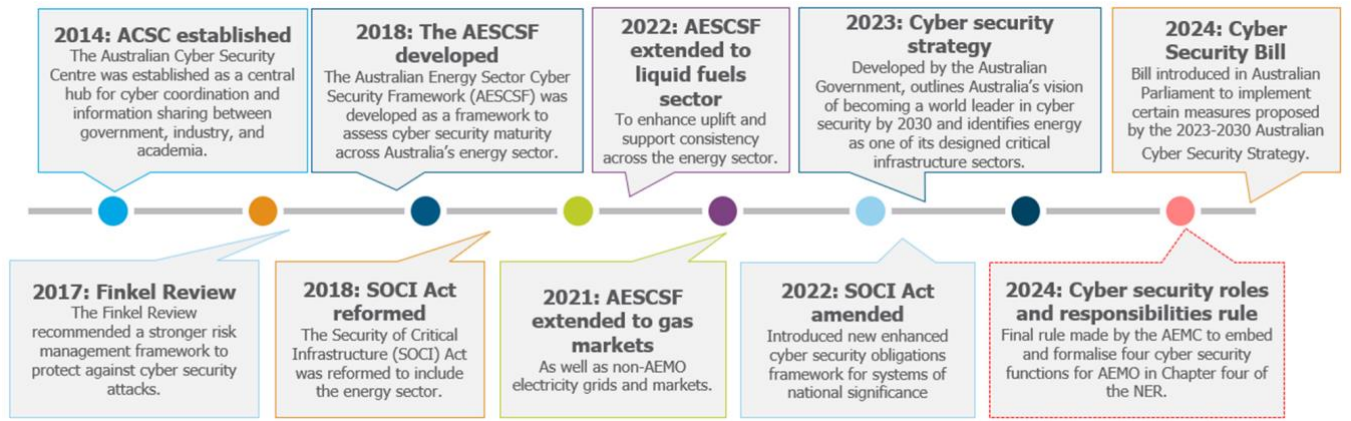
<sup>9</sup> Department of Climate Change, Energy, the Environment and Water. Rule Change Request – AEMO Cyber Security Role. March 2024. Available here: <https://www.aemc.gov.au/sites/default/files/2024-03/The%20Honourable%20Chris%20Bowen%20MP%20-%20Rule%20change%20request%20%281%29.pdf>

<sup>10</sup> Ibid.



resources (DER), consumer energy resources (CER) and smart grids this diverse mix of resources subsequently increases information and communications technology which increases the NEM’s cyber vulnerability.

Figure 2. Timeline of cyber security reforms and frameworks



Source: AEMC

While the benefits of increased digitisation and connectivity are worth pursuing, it also requires enhanced capabilities to mitigate threats from any malicious cyber activity.<sup>11</sup> Figure 2 above outlines the way in which the landscape of cyber security governance in Australia, particularly within the energy sector has evolved, commencing from 2014 with the establishment of the ACSC – a key milestone in the history of cyber security governance in Australia.

To accommodate and adapt to the above changes occurring in the NEM environment relating to the preparedness, response and information dissemination of cyber incidents, the regulatory frameworks must support the needs of the increasing risk of cyber threats.

The new cyber security roles and responsibilities will provide AEMO, NEM participants and government confidence that an actual cyber incident to the power system will be managed efficiently and effectively, and any ongoing risk to the power system security of the NEM will be mitigated.

AEMO notes while there has been several cyber security reforms and frameworks established in recent years, the new cyber security roles and responsibilities represent a significant reform for AEMO, expanding its core power system security obligations and placing it at the centre of coordinating and supporting cyber security preparedness, response and recovery across the NEM.

In performing its new cyber security roles and responsibilities, AEMO is mindful that approximately 600+ market participants are impacted by the Rule change. These impacts are a result of the various activities that will be required to implement and support the new cyber security roles and responsibilities such as process changes, consultations with industry, implementation of technical platforms as well as alignment of activities across all participants. Specifically, to give effect to the Rule, AEMO will be required to implement the following changes outlined in Table 1 to deliver each of the new cyber security roles and responsibilities.

<sup>11</sup> AEMC. Cyber security roles and responsibilities, Consultation Paper. 10 June 2024. Available here: <https://www.aemc.gov.au/sites/default/files/2024-06/ERCO388%20Consultation%20Paper%20-Cyber%20security%20roles%20and%20responsibilities.pdf>

**Table 1. Anticipated changes required to deliver the new cyber security roles and responsibilities**

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

Function	Anticipated changes to be implemented
4. Facilitating the distribution of critical cyber security information to market participants	<ul style="list-style-type: none"> <li>• Maintain and test communications channels ensuring cybersecurity and jurisdictional contacts can be reached as required.</li> <li>• Engage resource in a cyber comms role, responsible for maintaining communications channels and templates.</li> <li>• Identify and establish platforms and capabilities for sharing tactical and strategic cyber threat and vulnerability information.</li> </ul>

## 4.2 Criterion 2 – Major change to a function, responsibility, obligation or power of AEMO

*A major change (including an anticipated change) to a function, responsibility, obligation or power of AEMO under the Rules*

### Criterion 2 – Draft determination

AEMO considers that the new cyber security roles and responsibilities **are** a major (or anticipated) change to an AEMO's function, responsibility, obligation or power under the NER for the following reasons:

- The AEMC's final rule and determination has added to AEMO's responsibilities to maintain power system security an additional obligation to coordinate and support cyber security preparedness, response and recovery.
- The AEMC's final rule and determination has also added four new cyber security functions, each requiring AEMO to undertake the additional requirements highlighted in Table 2 and Appendix A2.
- The Rule change 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 operates under and in accordance with national and Western Australian electricity and gas laws. In respect of the NEM, the NEL (and the national electricity rules and regulations) prescribe AEMO's functions and requires AEMO to have regard to the NEO in section 7 of the NEL in carrying out its functions.

The rule change request submitted to the AEMC by the Honourable Minister Bowen in March 2024 noted that AEMO did not have clear authority to deliver functions for cyber security within the broader context of power system security.<sup>12</sup> In particular, it was identified that there were two broad issues relating to cyber security arrangements:

1. Cyber security is not explicitly referenced in the Rules, as it relates to power system security.
2. Specific cyber security roles and responsibilities that AEMO would perform to assist in enhancing cyber security across the energy system are not specified in the Rules.

<sup>12</sup> 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>

Following consultation, the 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 in clause 4.3.2A of the Rules (and outlined in Section 2) explicitly require or allow AEMO to coordinate and support cyber security preparedness, response and recovery to maintain power system security. The AEMC stated throughout its consultation process that, without explicitly establishing these functions in the Rules, there is potential for harm the power system, as cyber risks may adversely impact any part of the power system, from individual participants to the system as a whole.

As noted in Section 4.1 above, the new cyber security roles and responsibilities place AEMO at the centre of coordinating and supporting cyber security preparedness, response and recovery across the NEM. The four new functions established under the Rule – 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 – expand AEMO’s responsibilities and obligations beyond its existing remit. Specifically, the responsibilities associated with each additional function are outlined in the table below with more detailed information related to the requirements in fulfilling those responsibilities provided in Appendix A2.

To implement the Rule changes which took effect 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.

**Table 2. AEMO’s new cyber security roles and responsibilities**

Function	Responsibilities
1. Cyber security incident coordinator	<ul style="list-style-type: none"><li>Coordinate the response to cyber security incidents that threaten the security of power systems and markets</li><li>Prepare and maintain sector cyber contact lists</li><li>Prepare and maintain jurisdiction cyber contact list</li><li>AESCIRP maintenance and exercises</li><li>Continuously correlate and triage the active cyber threat landscape</li></ul>
2. Supporting cyber preparedness and uplift	<ul style="list-style-type: none"><li>Champion AEMO across various sector-wide cyber activities and forums</li><li>Create and maintain guidance information to be provided to market participants and relevant bodies as required</li></ul>
3. Examining cyber risks and providing advice to government and industry	<ul style="list-style-type: none"><li>Establish and maintain a governance structure for the management of requests</li><li>Create and sustain processes for responding to requests for research/advice</li></ul>
4. Facilitating the distribution of critical cyber security information to market participants	<ul style="list-style-type: none"><li>Establish and maintain communications channels and templates for cyber security information dissemination</li></ul>

### 4.3 Criterion 3 – Major change to computer software or systems

*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*

### Criterion 3 – Draft determination

AEMO considers that 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 for the following reasons:

- While functionality in systems, software and processes will require uplift and redesign to deliver the new roles and responsibilities, these are not expected to be material.
- Costs related to the software or technology uplift are also not expected to be material for the new cyber security roles and responsibilities.

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. Specifically, investment in AEMO's software systems or platforms will be required to:

- Capture and assess the security maturity of market participants, undertake analysis and produce reporting for Energy Ministers.
- Capture triage, allocate and coordinate research requests.
- Facilitate secure, near real-time collaboration on sector specific incidents, tracking activities until incident resolution.
- Share near real-time tactical cyber threat intelligence.
- Coordinate the development of sector specific cyber threats and vulnerability assessments, including securely sharing that information with market participants.

More detailed elements of the computer software, systems and capabilities relate to:

- The design and implementation of resilient incident coordination capabilities able to operate during times of extensive cyber disruption / system black and integration of these with market participant and government agency processes.
- High levels of coordination and engagement in exercise design and delivery.
- Establishing AESCSF assessment portal and governance processes which includes supporting input and participation from a very broad range of market participants.
- New technology platforms required for the management of research requests and sharing of information to market participants in a trusted and verifiable manner.

These changes will be provided via a range of technology functions and software to be assessed as AEMO upscales the cyber security functions currently being performed and invests in system changes and additional resourcing to enable delivery of the new cyber security roles and responsibilities. AEMO notes these changes will not require alternations to AEMO's core systems or market applications.

Despite having identified various changes to its computer software and systems, as well as additional capabilities required to support delivery of the new cyber security roles and responsibilities, AEMO does not consider these changes or costs related to these changes to be material for the new cyber security roles and responsibilities.



## 4.4 Part A – Draft Determination

Having considered the matters raised in submissions and upon further assessment, AEMO's draft determination is to determine the new cyber security roles and responsibilities meet **two of the three** criteria to be a declared NEM project pursuant to clause 2.11.1(ba) of the Rules. The reasons for each criterion being satisfied (or not) have been outlined in Sections 4.1 to 4.3 of this Draft Report.

Additionally, AEMO is of the view that a determination for a declared NEM project is appropriate as:

- It provides for greater transparency of costs associated with the new cyber security roles and responsibilities by allowing for the establishment of an additional fee structure. The requirement for transparency of costs was raised by ENA and Transgrid in their submissions (outlined further in Appendix A1).

If a declared NEM project status is not determined, the costs of the new cyber security roles and responsibilities would be incorporated into the existing NEM Core fee and would not be as easily distinguishable from other costs related to AEMO's core NEM functions.

- Determining the new cyber security roles and responsibilities as a declared NEM project will require an additional fee structure to be determined, which in turn allows for an assessment the most appropriate attribution of costs to Registered Participants, or groups of Registered Participants and the corresponding charging metrics for recovery of costs under that fee structure.

As AEMO's draft determination is that the new cyber security roles and responsibilities should be determined to be a declared NEM project, Part B of this paper sets out the structure for an additional Participant fee for recovery of the costs.

## 5 Part B – Participant fee structure

The sections below seek to determine, through consultation, the fee structure through which AEMO should recover its costs for the new cyber security roles and responsibilities as a declared NEM project.

As AEMO's draft determination, outlined in Part A (Section 4), determined that the new cyber security roles and responsibilities met two of the three criteria for a declared NEM project, clause 2.11.1(bb) 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. This additional Participant fee is to be in place until such time as the next general determination of all Participant fees is made under clause 2.11 of the Rules.

Specifically, when a project is determined to be a declared NEM project under clause 2.11.1(ba), AEMO must also determine:

- the structure of an additional Participant fee<sup>13</sup> to be used in the recovery of costs,
- the start date for recovery, and
- the period or periods over which recovery will occur.

As such, should the draft determination for Part A become the Final Determination through consultation, this Part B consultation is undertaken to satisfy the relevant Rules consultation requirements in clauses 2.11.1 and 8.9.

AEMO has commenced our next general NEM Participant fee structure to be determined by 31 March 2026 for the next fee recovery period commencing on 1 July 2026.<sup>14</sup> The outcomes of the consultation processes in this paper will be reflected in and further consulted upon as part of this broader consultation.

### 5.1 Participant fee structure options

Part B of AEMO's Consultation Paper<sup>15</sup> outlined Participant fee structure options for the recovery of costs if the new cyber security roles and responsibilities are determined a declared NEM project. These options included two existing NEM Participant fee structures:

- NEM Core fee, where costs are recovered from:
  - Wholesale Participants (WP) (55.9% 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;

<sup>13</sup> 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.

<sup>14</sup> AEMO. National Electricity Market (NEM) Participant Fee Structure Review. Available here: <https://www.aemo.com.au/consultations/current-and-closed-consultations/national-electricity-market-participant-fee-structure-review>

<sup>15</sup> AEMO. New Cyber Security Roles and Responsibilities – Declared NEM Project. Consultation Paper. Available here: <https://aemo.com.au/consultations/current-and-closed-consultations/new-cyber-security-roles-and-responsibilities-for-aemo-declared-nem-project>



- Market Customers (MC) (26.6% 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 during that financial year, and 50% on a \$/NMI basis per week; and
- TNSPs (17.5% apportionment) on the basis of energy consumed for the latest completed financial year (consistent with the basis for charging the NTP fee).
- Incremental Charges fee, which recovers costs directly from the Registered Participants where doing something specific for a participant causes identifiable and material costs for AEMO.

A third option that would establish an additional, separate 'Cyber Security' fee for the recovery of costs of the new cyber security roles and responsibilities was also presented by AEMO as shown in Figure 3.


**Figure 3. Additional (separate) fee for the new cyber security roles and responsibilities<sup>16</sup>**



In developing this option, AEMO anticipates the new cyber security roles and responsibilities will impact all NEM Registered Participants. The attribution of costs to Registered Participant groups for an additional, separate 'Cyber Security' fee have therefore applied the historical market participation (which includes participants accessing the portal, submitting assessment results and viewing their organisation's result and benchmarking data with the AESCSF) as an indicative baseline for future use of the upscaled framework to support the increasing importance of cyber security.

<sup>16</sup> Wholesale Participants, Market Customers and TNSPs would be charged on the same basis to that outlined for the NEM core fee.





As the evidence on market participation resulting from the delivery of AEMO's new cyber security roles and responsibilities matures with time, the attribution of costs to Registered Participants determined in this process could be updated, if required, in subsequent Participant fee structure reviews.

At this time, Distribution Network Service Providers (DNSPs) are 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. AEMO does not propose to recover costs from DNSPs for the new cyber security roles and responsibilities at this stage. 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.

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-Registered Participant) under Function 3 (for example, as shown within the red circle in Figure 3), AEMO will recover those costs directly from the relevant jurisdiction requesting the research/advice. If cost recovery cannot be agreed during the consultation with the jurisdiction before the request is accepted under NER 4.3.2A(e), AEMO can decide not to accept the request.

For clarity, this approach sits outside of NEM Participant fee structures, which can apply only to Registered Participants. This cost recovery approach for services provided under Function 3 will be the same regardless of which Participant fee structure option determined for recovering of the new cyber security roles and responsibilities (i.e. NEM Core or separate 'Cyber Security' fee).

An exception to the above is 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 fee to be established.

Finally, as highlighted in Section 3 of this Draft Report, submissions did not provide alternative fee structures to the ones presented in the Consultation Paper.

## 5.2 Assessment of Participant fee structure options

### Fee structure – Draft determination

AEMO considers that the Participant fee structure most appropriate to recover costs of a new cyber security declared NEM project (if determined) would be Option 2 – the additional (separate) Cyber Security fee.

AEMO considers this fee structure option to be the most consistent with the Fee Structure Principles and the NEO, in particular the *reflective of involvement* and *non-discriminatory* principles.

AEMO is required under the Rules to determine the structure of an additional Participant fee if it determines a project to be a declared NEM project. This fee structure must be determined in accordance with clauses 2.11.1(ab) and 2.11.1(b) of the Rules: that is, the structure must have regard to the NEO and must, to the extent practicable, be consistent with the Fee Structure Principles.

AEMO’s Consultation Paper presented a preliminary assessment of the options outlined in section 5.1 of this Draft Report, should a declared NEM project be determined.

Now under our draft determination as a declared NEM project, AEMO has assessed the Participant fee structure options most suitable to the new cyber security roles and responsibilities. This is shown in Table 3 Table 3below.

AEMO notes the Rules do not indicate that one Fee Structure Principle should have greater weight over 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.<sup>17</sup>

Similarly, in considering the NEO, AEMO note the new cyber security roles and responsibilities are in part to promote the safe and secure operation of electricity services and the system in the long-term interests of consumers. As a result, how AEMO 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.

The assessment key is as follows:

	Meets the principle
	Some aspects meet the principle
	Does not meet the principle

**Table 3. Draft determination assessment of all fee structure options against NEO and Fee Structure Principles**

Fee structure options	Draft assessment against NEO or Fee Structure Principle	Rationale
1. Existing Participant fee structure – NEM Core Fee	Simplicity	<ul style="list-style-type: none"> <li>Existing structure and metrics are already in use and understood by Participants.</li> <li>Aligns with AEMO’s broader core responsibilities for power system security under the Rules.</li> </ul>
	Reflective of involvement	<ul style="list-style-type: none"> <li>Does not accurately reflect the historical market participation or <i>involvement</i> of Registered Participants associated the new cyber security roles and responsibilities.</li> </ul>
	Not unreasonably discriminate	<ul style="list-style-type: none"> <li>Existing apportionment of costs to one or more Registered Participant categories may over- or under-state their share associated with performing the new cyber security roles and responsibilities.</li> </ul>

<sup>17</sup> For example, there is commonly tension between the principles of 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 decrease simplicity of the fee structure, and the systems needed to manage the fees would become more complex.

Fee structure options	Draft assessment against NEO or Fee Structure Principle	Rationale
	Recovery of AEMO's budgeted requirements on the basis specified in clause 2.11.1(b)(2)	<ul style="list-style-type: none"> <li>Budgeted revenue requirements for the new cyber security roles and responsibilities in respect of Registered Participants can be fully recovered through the existing NEM Core fee structure.</li> </ul>
	NEO	<ul style="list-style-type: none"> <li>The NEM Core fee would recover costs from Registered Participants who would utilise and benefit from the services delivered across the new functions, but is restricted in how costs are recovered based on the existing apportionment to Registered Participant groups for this fee, which may not reflect the most efficient recovery approach.</li> </ul>
2. Additional (separate) 'Cyber Security' function fee	Simplicity	<ul style="list-style-type: none"> <li>Less simple relative to leveraging the existing NEM Core fee structure as the creation of an additional, separate 'Cyber Security' fee would require minor changes to AEMO finance and settlement systems, processes and reporting.</li> <li>Further disaggregation of AEMO's NEM Participant fees could add to overall complexity in understanding of AEMO's budget and fees. However, this needs to be considered in light of the potential transparency afforded by establishing an additional fee.</li> </ul>
	Reflective of involvement	<ul style="list-style-type: none"> <li>Allows for more accurate reflection of the <i>involvement</i> level of Registered Participants or groups of Registered Participants based on historical information.</li> </ul>
	Not unreasonably discriminate	<ul style="list-style-type: none"> <li>Ensures that there is no over- or under-stating of the apportionment of costs to any Registered Participant category or group of Registered Participants avoiding potential cross-subsidies associated with the new functions</li> </ul>
	Recovery of AEMO's budgeted requirements on the basis specified in clause 2.11.1(b)(2)	<ul style="list-style-type: none"> <li>Budgeted revenue requirements for the new cyber security roles and responsibilities in respect of Registered Participants can be fully recovered through an additional, separate 'Cyber Security' fee to be established in time for commencement 1 July 2025</li> </ul>
	NEO	<ul style="list-style-type: none"> <li>An additional, separate 'Cyber Security' fee would recover costs from Registered Participants who would utilise and benefit from the services delivered across the new functions, but with the flexibility to determine the apportionment to different Registered Participants or groups of Registered Participants that reflects their level of involvement and provide incentives to use or participate in the services moving forward.</li> </ul>

## 5.3 Start date and period/s of fee recovery

### Start date & Period of recovery – Draft determination

AEMO considers that a Participant fee structure for the declared NEM project (if determined) should have a start date for recovery of costs of 1 July 2025. In accordance with AEMO's approach to recovering operating expenditure, all operating costs are to be recovered in the financial year in which they are incurred. A recovery period is therefore not applicable as there is no capital expenditure forecast at this stage.

As outlined in section 1.2.1, if a declared NEM project is determined, AEMO must determine the start date and period/s of fee recovery in accordance with clause 2.11.1(bb) of the Rules.

AEMO's Consultation Paper proposed that, under a Participant fee structure for the declared NEM project, cost recovery should commence from 1 July 2025 (to align with AEMO's annual budget and fees process) for a period of seven years, which is consistent with AEMO's depreciation model for other assets. It is also intended that costs incurred on and from 12 December 2024 (the date the relevant Rule changes became effective) would be recovered from FY26.

Since the publication of the Consultation Paper, AEMO has further assessed the costs to be incurred in establishment and BAU activities associated with the new cyber security roles and responsibilities. As outlined in section 2.1 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, and therefore a determination of a cost recovery period for capital expenditure is not required.

AEMO will seek to recover its operating expenditure associated with performing its new roles and responsibilities in the financial year incurred. AEMO still proposes in this Draft Report that costs incurred on and from 12 December 2024 (the date the relevant Rule changes became effective) are to be recovered from FY26.

As previously noted, AEMO has commenced consultation on the general NEM Participant fee structures for the period commencing 1 July 2026. Any determination regarding an additional fee structure for the new cyber security roles and responsibilities is to be included in that consultation scope of the general review.

## 5.4 Part B – Draft Determination

Having considered the matters raised in submissions and upon further assessment, AEMO's draft determination in relation to a Participant fee structure to recover the costs of a declared NEM project for the new cyber security roles and responsibilities (if determined), is 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; 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 FY26 including costs incurred on and from the Rule's effective date of 12 December 2024.<sup>18</sup>

The reasons supporting the above draft determination have been outlined in Sections 5.2 and 5.3 of this Draft Report.

For clarity, 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.

Where AEMO is undertaking research or providing advice in relation to cyber security risks which is specifically requested by a Minister (i.e. a non-Registered Participant) under Function 3, AEMO will seek to recover those costs directly from the relevant jurisdiction requesting the research/advice.<sup>19</sup>

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 AEMC's final rule and determination. AEMO has been engaged with the Commonwealth and State and Territory governments and market bodies in relation to broader, anticipated cyber related reforms that, were they to eventuate, may have wider implications for the NEM. An additional, separate Cyber Security fee could 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.

Consultation on the general NEM Participant fee structure has commenced and therefore any Final Determination on a Participant fee structure for the new cyber security roles and responsibilities will be included as part of that consultation scope of the general review.

<sup>18</sup> As no capital expenditure is forecast, a cost recovery period is not applicable.

<sup>19</sup> As outlined in section 5.1, this is outside of NEM Participant fee structures under the NER which can apply only to Registered Participants.

# A1. Summary of submissions and AEMO responses

Stakeholder	Key points	AEMO response
1. Transgrid	a) Supports AEMO's expanded cyber security role but it is not a 'major' development or change in functions and/or systems. <ul style="list-style-type: none"> <li>AEMC's final rule is building on and enhancing activities rather than introducing a new and significant function</li> <li>Anticipated costs are not particularly large relative to AEMO's overall costs</li> <li>New function can be reasonably easily incorporated into AEMO's existing organisational structure</li> </ul>	<p>AEMO notes Transgrid's comments that the new cyber security roles and responsibilities do not meet the criteria of a declared NEM project.</p> <p>Section 4 of this Draft Report outlines AEMO's reasons for its draft determination that the new cyber security roles and responsibilities meet two of the three criteria for a declared NEM project.</p> <p>That is, the roles and responsibilities as outlined in the AEMC's Final Determination and Rule are new roles and responsibilities and are also a major reform or development. For example, the activities to coordinate a response of a cyber threat or incident impacting the power system which requires significant additional effort from AEMO to support this function.</p>
	b) Encourages close collaboration with industry to deliver work program efficiently, avoiding duplication at the lowest cost to energy consumers <ul style="list-style-type: none"> <li>Streamlining cyber security incidents coordination – may be beneficial to consolidate Cyber security Incident Coordinator across AEMO, ASD and Home Affairs</li> </ul>	<p>AEMO agrees with Transgrid's comment that close collaboration between AEMO and all industry participants is required and AEMO is committed to working closely with industry and stakeholders throughout the implementation process.</p> <p>AEMO also notes that streamlining cyber security incidents coordination is one of AEMO's primary aims.</p> <p>For example, the AESCIRP for the NEM will be reviewed every two years at a minimum by AEMO in consultation with the membership of the National Electricity Market Emergency Management Forum (NEMEMF), NEM participants and related federal agencies to reflect changes to regulation, updated advice from the ACSC and other cyber bodies. Additionally, exercise TRIDENT has been a collaborative exercise with Australian Cyber Security Centre (ACSC), Department of Home Affairs (DHA) and State and Territory Governments.</p>
	c) Encourage costs transparency through: <ul style="list-style-type: none"> <li>Consult with stakeholders (including TNSPs) on proposed work plans, including providing forward visibility of costs, proposed activities and benefits</li> </ul>	<p>AEMO is committed to improving financial transparency through its annual budget and fees report and engagement with stakeholders including via the Financial Consultative Committee. This is a key</p>

Stakeholder	Key points	AEMO response
	<ul style="list-style-type: none"> <li>Provide fixed forward budgets for at least five years (likely seven years) to enable TNSPs to accurately account for associated costs when preparing revenue proposals for future revenue periods and support full cost-recovery. This should include detailed cost breakdowns, including escalation assumptions and supporting information that can be used to explain new fees to consumers (who ultimately bear their cost)</li> </ul>	<p>factor behind AEMO's draft determination as outlined in Sections 4.4 and 5.4 of this Draft Report.</p> <p>AEMO's response to 1(b) also provides an example on AEMO's approach for stakeholder consultation on work plans.</p>
	d) Essential that project-related fees over the outlook period are provided on a firm basis (i.e. capped) as TNSPs would have no mechanisms available to recover unanticipated cost increases once revenue determinations are completed	<p>AEMO provides and consults on a forecast of its expected budget and revenue requirements annually through the Budget and Fees process which commences in April of each year.</p> <p>AEMO's FY25 Budget and Fee document outlines areas of AEMO's costs that the new cyber security roles and responsibilities are contributing towards. AEMO's Draft FY26 Budget and Fee document was published in early April 2025 for stakeholder feedback.<sup>20</sup></p>
	e) Function 3 costs should be recovered from government via an agreement rather than from consumers trident	<p>AEMO notes Transgrid's comment regarding the cost recovery approach for Function 3.</p> <p>AEMO highlighted in Section 4.3 of its Consultation Paper there is a process to be followed prior to undertaking research or advice requested by a Minister under Function 3, which is set out in clause 4.3.2A(e) of the Rules. AEMO's draft determination as outlined in Section 5.4 of this Draft Report proposes that if a Minister requests such information AEMO would seek to recover its costs directly from the jurisdiction requesting the research/advice. If cost recovery cannot be agreed during the consultation with the jurisdiction before the request is accepted under NER 4.3.2A(e), AEMO can decide not to accept the request.</p> <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>

<sup>20</sup> AEMO. Energy market fees and charges. Available here: <https://www.aemo.com.au/about/corporate-governance/energy-market-fees-and-charges>

Stakeholder	Key points	AEMO response
2. ENA	a) Recognises expanded roles and responsibilities of AEMO to perform cyber security related function but do not support functions being considered NEM declared project	AEMO notes ENA's comment that the new cyber security roles and responsibilities do not meet the criteria of a declared NEM project.  See AEMO response to 1a).
	b) Encourages recovery of costs for the new functions through NEM Core fees according to the existing TNSP allocations <ul style="list-style-type: none"> <li>More appropriate and administratively simpler</li> </ul>	AEMO acknowledges ENA's comment that recovery of fees through the NEM Core fees would be more appropriate and administratively simpler.  AEMO notes that when developing and determining Participant fee structures, AEMO must have regard to the Fee Structure Principles and NEO as outlined in clause 2.11.1. While inclusion of the costs associated with the new cyber security roles and responsibilities into NEM Core may be simpler, AEMO is mindful this needs to be considered against the principles of reflective of involvement and non-discrimination. AEMO considers the existing attribution of costs to Registered Participants under NEM Core do not accurately reflect the involvement of individual Registered Participant types at this time.
	c) Encourages increased transparency on the costs of each of the new functions going forward, including: <ul style="list-style-type: none"> <li>Budget forecasts for inclusion in revenue proposals</li> <li>Recommends AEMO reflect TNSP allocations and forecast by 15 Feb 2026</li> <li>Would like understanding on how \$10 million per annum meets criteria under 2.11.1(ba)(1) when compared with AEMO's total budget</li> </ul>	AEMO provides and consults on a forecast of its expected budget and revenue requirements annually through the Budget and Fees process which commences in April of each year.  As per clause 11.153.2 of the NER, AEMO advises TNSPs of the amount of Participant fees (excluding the NTP function fees) to be recovered from that TNSP for the relevant financial year.  AEMO notes that the cost of a project is not the only way in which a project can meet the clause 2.11.1(ba)(1) criterion to be determined a declared NEM project. AEMO has outlined in section 4.1 of this Draft Report our reasons why the new cyber security roles and responsibilities meet clause 2.11.1(ba)(1) of the NER.
	d) Considers there is benefit in better aligning allocation of costs consistent with regulatory timeframe to improve cost recovery and help smooth customer bills <ul style="list-style-type: none"> <li>E.g. providing 7-year expenditure forecast (networks are subject to 5-year regulatory period and initial revenue</li> </ul>	AEMO acknowledges ENA's comment on alignment of regulatory timeframes. AEMO notes that each NSP has a different regulatory period and therefore aligning its assessment of its Participant fee structures with all NSP regulatory periods is not practical.



Stakeholder	Key points	AEMO response
	proposals are due to the AER 18 months prior to start of that regulatory period)	
	e) Welcome the opportunity to discuss new costs as part of the upcoming determination of NEM participant fees	AEMO appreciates the ENA's continued engagement through past Participant fee structure reviews and looks forward to ongoing engagement in our upcoming general NEM Participant fee structure review.
<b>3. SMA-Australia</b>	a) Believe new cyber roles and functions meet 2.11.1(ba)(1) and (2), not enough sufficient information to provide informed comment on 2.11.1(ba)(3) <ul style="list-style-type: none"> <li>Can see from own experience though that cyber security uplift can involve significant changes to software and systems</li> </ul>	AEMO notes SMA-Australia's comments on whether the new cyber security roles and responsibilities meet the declared NEM project criteria.  See AEMO response to 1a).
	b) 7 year recovery period is reasonable	AEMO note SMA-Australia's comment on the cost recovery period.  As outlined in Section 5.3 of this Draft Report, AEMO's draft determination is to recover operating expenditure costs the year as incurred.
	c) If an additional separate fee is to be established, it is more preferable for this to be considered as part of the general NEM fee structure review in context of other changes to AEMO's roles and responsibilities including costs incurred fulfilling them	AEMO notes this comment. However, as outlined in Section 5.2 of this Draft Report, AEMO considers that the alternative fee structure option (the additional (separate) cyber security fee) is more consistent with the Fee Structure Principles and NEO than the existing NEM Core structure.  AEMO will still consider the final Participant fee structure in our general NEM fee structure review, which has commenced, along with other changes which may impact assessment of the fee structure against the Fee Structure Principles and NEO.
	d) Argument could be made to recover costs from DNSPs with the increasing importance of managing cyber security or CER, DER and other distribution network assets and their impact on the bulk power system <ul style="list-style-type: none"> <li>But support AEMO's view to consider this as part of upcoming general NEM fee structure consultation</li> </ul>	AEMO acknowledges SMA-Australia's comment on recovery from DNSPs.  As noted in Section 5.1 of this Draft Report, at this time, DNSPs are 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. AEMO does not propose to recover costs from DNSPs for the new cyber security roles and responsibilities at this stage. Given the timing of the general NEM Participant fee structure review and to

Stakeholder	Key points	AEMO response
		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.
	e) Allocation could commence with equal attribution to Wholesale Participants, Market Customers and TNSPs (initially) and then DNSPs to be considered in general NEM fee consultation	AEMO notes this comment. See AEMO response to 3d).
	f) Cost recovery metrics should be based on beneficiary-pays principle and proportional to the demand for cyber security services placed by relevant participants. <ul style="list-style-type: none"> <li>AEMO will be better placed to judge where demand for its services is greatest and how to allocate fees fairly and in proportion to the demands placed on it once AEMO has several years of experience with implementing new cyber roles and responsibilities</li> </ul>	<p>AEMO notes SMA-Australia's comment on an appropriate basis for the cost recovery metrics and the allocation of costs to Participants.</p> <p>The development of any Participant fee structure (which includes the cost recovery metrics and allocation percentages) must have regard to the Fee Structure Principles and NEO as outlined in clause 2.11.1(b) of the NER.</p> <p>AEMO has also outlined in Section 5.1 of this Draft Report that the proposed Participant allocations for the fee structure commencing 1 July 2025 have been based on historical market participation, and that any allocations determined now can be updated, if required, in subsequent general NEM fee structure reviews to reflect the <i>involvement</i> level of participants at that time.</p>

## A2. Detailed requirements for AEMO's new roles and responsibilities


Function	Responsibilities	Requirements
<b>1. Cyber security incident coordinator</b>	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"> <li>• 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.</li> <li>• have an industry-facing contact ready to be made aware that a cyber incident which could affect</li> <li>• 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)</li> <li>• have resources to respond to cyber incidents, including burst capacity via 3rd parties to deal with events requiring a significant response as they arise.</li> <li>• have suitable tools to manage and track incidents from their identification through to resolution and post-incident review.</li> <li>• 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)</li> <li>• be able to coordinate incidents over a 24x7 period should the need arise</li> </ul>
	Prepare and maintain sector cyber contact lists	<p>To fulfill this responsibility AEMO must:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• keep the contact list up to date and the quality of the data must be maintained through regular review / reconciliation.</li> <li>• update existing processes where contact details are registered and maintained to ensure that the information is not overridden or deleted.</li> <li>• test and maintain communications tools to ensure that market participants are able to be contacted as required.</li> </ul>
	Prepare and maintain jurisdiction cyber contact list	<p>To fulfill this responsibility AEMO must:</p> <ul style="list-style-type: none"> <li>• be able to document and maintain a set of contacts across relevant governments and jurisdictions (e.g. State Gov, law enforcement, industry bodies).</li> <li>• keep the contact list up to date and the quality of the data must be maintained.</li> <li>• test and maintain communications tools to ensure that jurisdictional contacts are able to be contacted as required.</li> </ul>

Function	Responsibilities	Requirements
	AESCIRP maintenance and exercises	<ul style="list-style-type: none"> <li>maintain a plan for incident response through an annual update, reflecting changes in the technology and threat landscape.</li> <li>conduct exercises to test its incident response plan, ensuring readiness for a real incident, and document outcomes in a formal report.</li> </ul>
	Continuously correlate and triage the active cyber threat landscape	<p>To fulfill this responsibility AEMO must:</p> <ul style="list-style-type: none"> <li>have access to relevant threat information from various sources, including government organisations and subscription services offering relevant threat information.</li> <li>have processes and systems in place to ingest relevant data/log sources from market participants and correlate this with relevant cyber threat intelligence.</li> <li>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.</li> </ul>
<b>2. Supporting cyber preparedness and uplift</b>	Champion AEMO across various sector-wide cyber activities and forums	<p>To fulfill this responsibility AEMO must:</p> <ul style="list-style-type: none"> <li>be able to attend industry and cyber security events, championing cyber security and providing thought leadership.</li> <li>be able to hold cyber security related events where appropriate.</li> <li>maintain an active online / social media presence to elevate its cyber profile across the sector</li> </ul>
	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"> <li>be able to formulate and provide responses to security-related questions when enquiries are made by market participants.</li> <li>be able to maintain documentation and previous responses, preventing rework.</li> <li>have access to third party specialists, where required, in order to provide expert / up-to-date guidance to market participants</li> <li>continue to maintain the AESCSF.</li> </ul>
<b>3. Examining cyber risks and providing advice to government and industry</b>	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"> <li>have sufficient resources to respond to and fulfill research requests where AEMO is best placed to respond.</li> <li>have a mechanism to recover the cost of providing responses to research requests as part of this defined process.</li> </ul>
	Create and sustain processes for responding to requests for research/advice	<p>To fulfill this responsibility AEMO must:</p> <ul style="list-style-type: none"> <li>establish a process for receiving, tracking and estimating effort to respond to research requests.</li> </ul>
<b>4. Facilitating the distribution of critical cyber security information to market participants</b>	Establish and maintain communications channels and templates for cyber security information dissemination	<p>To fulfill this responsibility AEMO must:</p> <ul style="list-style-type: none"> <li>maintain and establish communications channels, templates and processes for the dissemination of cyber security information.</li> </ul>

## A3. NEO & Fee Structure Principles

Objective / Principle	Requirement	Application and examples
<b>National Electricity Objective (NEO)</b>	<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"> <li>(a) price, quality, safety, reliability and security of supply of electricity; and</li> <li>(b) the reliability, safety and security of the national electricity system; and</li> <li>(c) the achievement of targets set by a participating jurisdiction – <ul style="list-style-type: none"> <li>i. for reducing Australia’s greenhouse gas emissions; or</li> <li>ii. that are likely to contribute to reducing Australia’s greenhouse gas emissions.</li> </ul> </li> </ul>	<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>
<b>Simplicity</b>	<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 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>

Objective / Principle	Requirement	Application and examples
		<ul style="list-style-type: none"> <li>• straight-forward</li> <li>• easily understood by participants</li> <li>• readily applied by Registered participants and AEMO</li> <li>• foreseeable and forecastable in terms of impacts and costs.</li> </ul>
<b>Reflective of Involvement</b>	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"> <li>a) interacts with AEMO in relation to the output;</li> <li>b) uses the output;</li> <li>c) receives the output; and</li> <li>d) benefits from the output.</li> </ol> <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>
<b>Non-discriminatory</b>	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 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>



Objective / Principle	Requirement	Application and examples
		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.
<b>Comparison with existing fee structures</b>	<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"> <li>• Other electricity market fee structures such as Western Australia or globally</li> <li>• Gas markets operated by AEMO</li> </ul>

## A4. Glossary

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