

AEMO's NEW CYBER SECURITY ROLES AND RESPONSIBILITIES

February 2025

Consultation Paper

Part A – Declared NEM Project

Part B – NEM Participant Fee Structure





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 3 February 2025.

Disclaimer

This document or the information in it may be subsequently updated or amended. This document does not constitute legal or business advice, and should not be relied on as a substitute for obtaining detailed advice about the National Electricity Law or National Electricity Rules or any other applicable laws, procedures or policies. AEMO has made every effort 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.

Version control

Version	Release date	Changes
#1	4 February 2025	

Executive summary

AEMO consults on, and subsequently recovers its budgeted revenue requirements, in accordance with its National Electricity Market (**NEM**) Participant fee structures under clause 2.11 of the National Electricity Rules (**NER**, the **Rules**). The current NEM Participant fee structures apply from 1 July 2021 to 30 June 2026. In accordance with the Rules, AEMO may determine that specific projects are declared NEM projects for which an additional fee can be used to recover the costs of those projects until the next general determination of the NEM Participant fee structure.

The publication of this Consultation Paper commences the first stage of the Rules consultation process for two separate but inter-related consultation processes:

- 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.

AEMO have already commenced work on implementing the changes required as a result of the Rule which came into effect on 12 December 2024. AEMO is undertaking the first stage of both consultation processes in parallel, in order to confirm a cost recovery approach with stakeholders in time for FY26. However, AEMO does not regard the outcome of the Part A consultation as pre-determined and seeks stakeholder feedback on the questions in Part A. The Part B consultation is undertaken to satisfy the relevant Rules requirements in clauses 2.11 and 8.9 in the event that AEMO determines that the new cyber security roles and responsibilities are a declared NEM project.

AEMO may charge for and recover fees for the performance of its statutory functions in accordance with section 52 of the National Electricity Law 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.

If AEMO determines, through consultation, that the new cyber security roles and responsibilities do not meet the criteria to be a declared NEM project, AEMO will seek to recover its costs of performing these roles and responsibilities in accordance with the current NEM Participant fee structure (for example through the NEM Core fee), until such time as a new Participant fee structure is determined by AEMO in consultation with stakeholders – the consultation is scheduled to begin in calendar Q1 2025.

Stakeholders should note that, as the Rule does not apply to the roles and responsibilities for the national gas system under the National Gas Rules (NGR) or Western Australian markets at this stage¹, this consultation only considers the impact of the Rule on NEM participants.

¹ Rule change processes will shortly be underway to apply similar roles and responsibilities in the national gas and Western Australian markets.

Background

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 Australian's 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"*.²

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.³ 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.

In March 2024, the AEMC received a rule change request from the Honourable Chris Bowen MP, Minister for Climate Change and Energy, seeking to formally establish AEMO's cyber security functions, obligations and powers in the Rules. The AEMC subsequently published its final determination and final rule on 12 December 2024,⁴ which commenced on that date. The final rule amended the Rules to explicitly include the coordination and support of cyber security preparedness, response and recovery as one of AEMO's power system security responsibilities in Chapter 4 of the NER, as well as four cyber security functions that AEMO is to perform. These four functions are described in clause 4.3.2A of the Rules:

- **Function 1 – Cyber security incident coordinator:** AEMO is required to coordinate the NEM-wide response of Registered Participants to a cyber incident affecting the energy sector. It may do so by continued development of the Australian Energy Sector Cyber Incident Response Plan (AESCI RP) and leading the implementation of the AESCI RP.
- **Function 2 – Supporting cyber preparedness and uplift:** AEMO is to continue to have stewardship of the Australian Energy Sector Cyber Security Framework (AESCSF), which may include organising testing and scenario training exercises, and developing and providing guidance and advice to industry in the form of written materials, digital tools and working groups.
- **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.

² 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>

³ 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>

⁴ AEMC. National Electricity Amendment (Cyber Security Roles and Responsibilities) Rule 2024. 12 December 2024. Available here: <https://www.aemc.gov.au/rule-changes/cyber-security-roles-and-responsibilities>

- **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.

These four functions are to complement AEMO's existing powers to respond to an actual cyber security incident and are focussed on preventing cyber incidents and preparing the industry to respond if an incident does occur. The cyber security functions are facilitative and flexible and are not designed to enable AEMO to impose new obligations on market participants.

AEMO has commenced upscaling the cyber security functions currently being performed and investing in system changes and additional resourcing to enable delivery of the new cyber security roles and responsibilities. AEMO considers it is well placed to implement changes required promptly following the final rule and that no transition period is required. Based on assumptions as of November 2024, AEMO estimate establishment and ongoing costs in Years 1 to 3 of delivering the four cyber security functions 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. These cost estimates were provided to and subsequently published in the AEMC's final determination.

Part A – Declared NEM project

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.

AEMO are seeking stakeholder feedback on whether the new cyber security roles and responsibilities meet all or any of these requirements, having consideration of the cost of delivering the new functions, the extent to which those functions have required changes to the Rules and will require development of procedures, processes and systems, and the impacts of the changes on AEMO and Participants more broadly.

Part B – Participant fee structure

When AEMO determines a project to be a declared NEM project, it must also determine the start date for recovery and the period or periods over which recovery will occur for the declared NEM project. AEMO must also determine the structure of any 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.⁵

The AEMC's final rule and determination on AEMO's cyber security roles and responsibilities came into effect on 12 December 2024. AEMO may, in principle, begin recovering its costs related in performing its new cyber

⁵ National Electricity Rules. Clause 2.11.1(bb).

security roles and responsibilities on and from this date. Since this date, AEMO has commenced work to upscale the cyber security functions it was performing before the Rule and will invest in system changes and additional resourcing to enable delivery of the four new roles and responsibilities.

To align with AEMO's annual budget and fees process, it is proposed that cost recovery commence on and from 1 July 2025 for a period of seven years, to best align with AEMO's depreciation model for other assets. AEMO intends that costs incurred on and from 12 December 2024, that is, the date the Rule became effective, would be recovered in FY26 and subsequent budgets.

AEMO are also seeking stakeholder feedback on potential options for an appropriate fee structure to recover the costs of the new cyber security roles and responsibilities, including expanding the scope of one of AEMO's existing NEM Participant fee structures (e.g. NEM Core fee), or alternatively establishing an additional separate fee structure (i.e. an additional separate cyber security roles and responsibilities related Participant fee). AEMO has undertaken an indicative assessment of these two options against the National Electricity Objective (NEO) and the principles specified in NER clause 2.11.1(b) (Fee Structure Principles).

Details of this assessment are outlined in Section 4.

AEMO is seeking input on the fee structure options proposed, the proposed start date and period for recovery of the costs, together with any other options AEMO should consider as part of this consultation.

Submissions – Closing date and information

Stakeholders are invited to submit written responses on the issues and questions identified in either or both of Part A and Part B of this Consultation Paper by 5.00 pm (Australian Eastern Daylight Time [AEDT]) on Tuesday 4 March 2025 to reformdevelopmentandinsights@aemo.com.au. Please refer to the Notice of First Stage of Consultation published with this paper or section 1.1 for further details.

Contents

Executive summary	3
1 Consultation overview	9
1.1 Key information	9
1.2 Rules requirements and guiding principles	10
1.3 Budget and Fee Structure	12
1.4 Relationship to upcoming general NEM Participant fee consultation	13
2 Cyber-readiness of the National Electricity Market	14
2.1 AEMO's cyber security roles and responsibilities	15
2.2 Estimated costs of the new cyber security roles and responsibilities	16
3 Part A – Declared NEM project	18
3.1 Criterion 1 – Major reform or development of the market	18
3.2 Criterion 2 – Major change to function, responsibility, obligation or power of AEMO	20
3.3 Criterion 3 – Major change to computer software or system	21
4 Part B – Participant fee structure	23
4.1 Recovering fees from Registered Participants	23
4.2 Existing NEM Participant fee structure options	25
4.3 Alternative Participant fee structure options	28
4.4 Start date and period/s of fee recovery	29
4.5 Preliminary assessment of all Participant fee structure options (if determined a declared NEM project)	30
A1. Questions for stakeholders	33
A2. Glossary	34
A3. Fee structure principles	35

Figures

Figure 1. Aligning Participant fee structure consultation outcomes	13
Figure 2. Timeline of cyber security reforms and frameworks	19
Figure 3. Historical AESCSF market participation (NEM only)	24
Figure 4. Existing general NEM Participant fee structures	26
Figure 5. Allocation of the NEM Core fee from 1 July 2023 to 30 June 2026	27
Figure 6. Example additional, separate fee for the new cyber security roles and responsibilities	29



Tables

Table 1. Preliminary assessment of all fee structure options against NEO and Fee Structure Principles

31

1 Consultation overview

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

1.1 Key information

Purpose	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).												
Date applicable	To be determined in this consultation.												
Electricity roles and responsibilities covered in this consultation	<ul style="list-style-type: none">• Cyber security preparedness, response and recovery• Cyber security incident coordinator• Supporting cyber preparedness and uplift• Examining cyber risks and providing advice to government and industry, and• Facilitating the distribution of critical cyber security information to market participants.												
Timetable	<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 15 April 2025 (at the earliest)⁶</td></tr><tr><td>Submissions due on Draft Report</td><td>Friday 16 May 2025</td></tr><tr><td>Final Report published</td><td>By Monday 30 June 2025</td></tr></table> <p>Subject 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 15 April 2025 (at the earliest) ⁶	Submissions due on Draft Report	Friday 16 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 15 April 2025 (at the earliest) ⁶												
Submissions due on Draft Report	Friday 16 May 2025												
Final Report published	By Monday 30 June 2025												
Meetings	Stakeholders may request a meeting in their submission. Matters discussed at the meeting may be made available to other stakeholders.												
Submissions – Closing date and information	<p>AEMO requests that submissions are provided in electronic format (either pdf and Word) by 5.00pm AEDT Tuesday 4 March 2025 to reformdevelopmentandinsights@aemo.com.au.</p> <p>Please note that submissions will be published, other than confidential material, as per AEMO's Consultation submission guidelines. 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>												

⁶ This assumes that AEMO concludes that it is not desirable or necessary to hold any meetings under clause 8.9(f) of the Rules (If meetings are held, meetings must be held within a further 25 business days after submissions close, and this will then impact the consultation dates following the meeting).

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).⁷

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 compares the appropriateness of expanding existing fee structures and alternative (separate) fee structures to recover costs.

⁷ 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 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.
- Fees and charges are to be determined on a non-profit basis that provides for full cost recovery.
- The structure of the Participant fees should provide for the recovery of AEMO's budgeted revenue requirements on a specified basis.

The Rules do not indicate that any one Fee Structure Principle should have greater weight than the others. Where it is not practicable for AEMO to satisfy all of the principles or satisfy them all to an equal degree, AEMO may adopt a structure which is not equally consistent with all the principles. Therefore, meeting the requirements established under the Rules typically requires a trade-off between principles. That is, an option to improve the fee structure against one principle may lessen the applicability of 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.(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 AEMC's Final Rule Determination National Electricity Amendment (Cyber security roles and responsibilities) Rule 2024 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 the first stage of 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. However, AEMO does not regard the outcome of the Part A consultation as pre-determined and seeks stakeholder feedback on the questions in Part A.

AEMO may charge for and recover fees for the performance of its statutory functions in accordance with section 52 of the National Electricity Law 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 4.

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 upcoming 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.

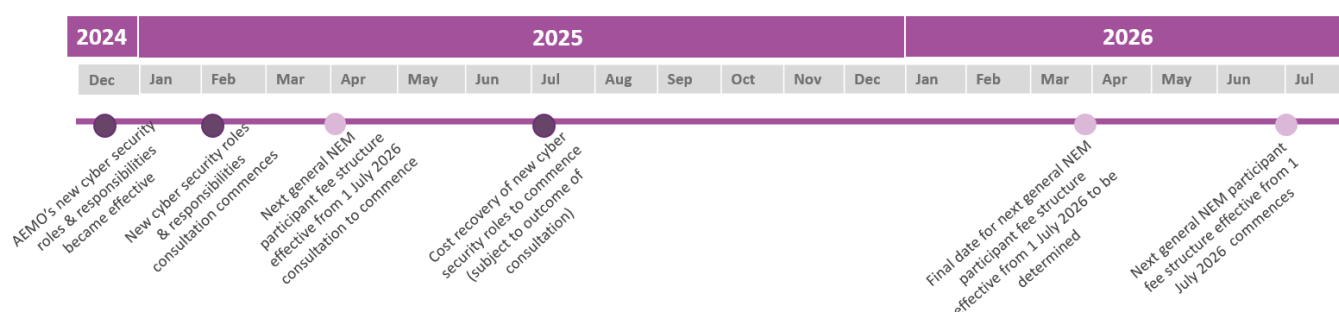
AEMO's next general NEM Participant fee structure is to be consulted on and determined by 30 March 2026 for the next fee recovery period to commence on 1 July 2026. The outcomes of the consultation processes initiated in Part A and Part B (if required) of this paper will be reflected in and further consulted upon as part of this broader consultation.

Therefore, should AEMO determine, following consultation which it aims to complete by the end of June 2025, that the new cyber security roles and responsibilities meet the criteria of a declared NEM project and establish an additional Participant fee structure for the declared NEM project, then:

- that additional Participant fee structure would only apply until 30 June 2026 (inclusive), and
- cost recovery for the new cyber security roles and responsibilities would be included as part of the next general NEM Participant fee structure consultation beginning in calendar Q1 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 Cyber-readiness of the National Electricity Market

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 Australian's 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*".⁸ 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.⁹

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.

Australian Energy Sector Cyber Security Framework

Established in 2018, the AESCSF is both a framework and an annual voluntary assessment program. The program covers Australia's electricity, gas markets (since 2021) and liquid fuels sector (since 2022).

Participation in the AESCSF program enables participants to undertake assessments of their own cyber security capability and maturity. Participants can use the results to inform and prioritise investment to improve cyber security posture. Participation is voluntary.


Each participating organisation's assessments are anonymised, and the aggregated results analysed to produce the annual *Report into the cyber security preparedness of the Australian electricity, gas and liquids sector*. The confidential report is provided to Energy Ministers to support the energy sector's developing cyber maturity. The program provides valuable national energy cyber security capability and maturity insights to complement *Security of Critical Infrastructure Act 2018* reforms.

Further details on the AESCSF are available via AEMO's website: <https://aemo.com.au/initiatives/major-programs/cyber-security>

The Commonwealth Energy Minister submitted a rule change request to the AEMC in March 2024, seeking to formalise the following AEMO cyber security roles and responsibilities:

⁸ 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>

⁹ 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>

- 
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.

2.1 AEMO's cyber security roles and responsibilities

In addition to the AESCSF, the *Security of Critical Infrastructure (SOCI) Act 2018* (Cth) (SOCI Act) as well as jurisdictional emergency management arrangements have come into effect. Under the SOCI Act, AEMO and many market participants (who are responsible entities for critical infrastructure assets) have existing security obligations to their critical infrastructure assets. These include:

- providing information about their critical infrastructure assets to the Register of Critical Infrastructure Assets,
- reporting cyber security incidents that have a significant or relevant impact on critical infrastructure assets to the Australian Cyber Security Centre, and
- establishing, maintaining, and complying with a written critical infrastructure risk management program for critical infrastructure assets that identify and mitigate material risks that could have a relevant impact on critical infrastructure assets.

AEMO understands that the new cyber roles and responsibilities appropriately considered, and are consistent, with these obligations. Specifically, as part of each function described in the AEMC's final determination and final Rule¹⁰:

- **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.

¹⁰ AEMC. National Electricity Amendment (Cyber Security Roles and Responsibilities) Rule 2024. 12 December 2024. Available here: <https://www.aemc.gov.au/rule-changes/cyber-security-roles-and-responsibilities>

- **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.

Importantly Registered Participants in the NEM continue to be responsible for ensuring their own cyber security preparedness and posture, including to comply with any obligations under the *Security of Critical Infrastructure (SOCI) Act 2018 (Cth)* (SOCI Act).

2.2 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.

AEMO note that activities for Function 2 have been partially funded by the Commonwealth, States and Territories for FY25. Similarly, specific cyber security-related advice to be provided by AEMO contemplated under Function 3 has been partially funded to date by the Australian Renewable Energy Agency (ARENA) and the Commonwealth Department of Climate Change, Energy, the Environment and Water (DCCEEW).

Costs associated with the new cyber security roles and responsibilities will be included in AEMO's annual Budget and Fees report from FY26. The approach by which those costs will be recovered 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 do not meet the criteria of a declared NEM



project, then its costs will be recovered through one of the existing Participant Fee structures (e.g., NEM Core fee) and reflected in this manner in the FY26 Budget and Fees report.

3 Part A – Declared NEM project

Pursuant to clause 2.11.1(ba) of the Rules, AEMO may determine a project to be a declared NEM project if the project meets any of the following requirements:

- 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.

The NER does not define ‘major reform or development’ or a ‘major change’ for the purpose of clause 2.11.1(ba).

Part A of this paper considers whether the new cyber security roles and responsibilities would meet any of these requirements, including consideration of the cost to facilitate the new cyber security roles and responsibilities, the extent of the cyber security roles and responsibilities changes to the Rules, procedures, processes and systems and the 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 general 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.

3.1 Criterion 1 – Major reform or development of the market

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

The Australian Government defines cyber security as measures used to protect the confidentiality, integrity and availability of systems and information. A cyber incident is an unwanted or unexpected cyber security event, or a series of such events, that have a significant probability of compromising business operations.¹¹

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.¹² 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.¹³ For example, through increased integration of distributed energy 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.

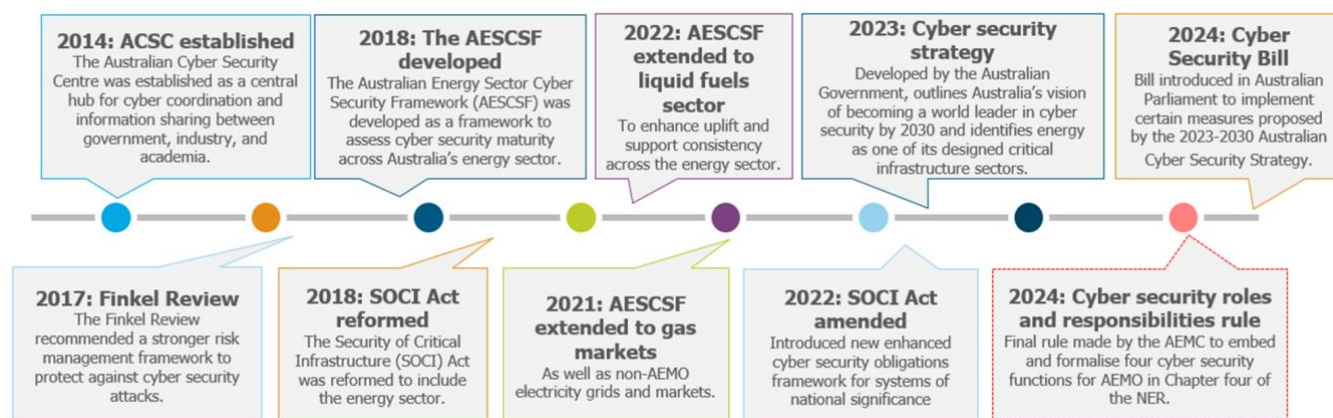
¹¹ Australian Signals Directorate. Glossary. Last accessed 6 January 2025. Available here: <https://www.cyber.gov.au/learn-basics/view-resources/glossary>

¹² 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>

¹³ Ibid.

A cyber security incident in the electricity sector could have far-reaching implications, from widespread outages to economic disruptions, breach of sensitive data and threats to national security. While the benefits of increased digitisation and connectivity are worth pursuing, it also requires enhanced capabilities to mitigate threats from any malicious cyber activity.¹⁴ As such, cyber security governance in Australia, particularly within the energy sector, has evolved over the past decade as shown in Figure 2.

Figure 2. Timeline of cyber security reforms and frameworks



Source: AEMC


One of the key milestones in the history of cyber security governance in Australia was the establishment of the ACSC in 2014. It plays a crucial role in helping organisations within the electricity sector to enhance their cyber security posture and respond effectively to cyber incidents.

Later the Finkel Review, commissioned in response to the 2016 South Australian blackout, emphasised the importance of cyber security within the energy sector. Its recommendations underscored the necessity for resilient and secure energy infrastructure, with the report recommending that “an annual report into the cyber security preparedness of the National Electricity Market should be developed by the Energy Security Board, in consultation with the Australian Cyber Security Centre and the Secretary of the Commonwealth Department of the Environment and Energy.”¹⁵

Building upon this recommendation, the AESCSF was developed as a framework to assess cyber security maturity across Australia's energy sector. It was developed through collaboration with industry and government stakeholders, including AEMO, ACSC, Cyber and Infrastructure Security Centre (CISC), and representatives from Australian energy organisations. In addition, the amended Security of Critical Infrastructure Act 2018 (the SOCI Act) expanded its scope to encompass the energy sector, acknowledging its vital role in national security. This legislative update mandated rigorous cyber security standards and incident reporting requirements for energy providers, elevating the industry's cyber security posture to align with contemporary threats.

¹⁴ 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>

¹⁵ Finkle, Dr Allan. Chair of the Expert Panel. Independent Review into the future Security of the National Electricity Market. Blueprint for the future. June 2017. Available here: <https://www.dcccew.gov.au/sites/default/files/documents/independent-review-future-nem-blueprint-for-the-future-2017.pdf>



The AEMC's final determination to make a new rule to introduce a new power system security responsibility and new cyber security functions for AEMO represents further 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. This includes the breadth of approximately 600+ market participants impacted, as well as the various activities that will be required to implement and support the new roles and responsibilities such as process changes, consultations with industry, implementation of technical platforms as well as alignment of activities across all participants.

The new cyber security roles and responsibilities have been designed to complement AEMO's existing powers to respond to an actual cyber incident and to mitigate the ongoing risk to the power system security of the NEM. The Rules now expressly authorise (and, where relevant, require) AEMO to perform these new roles and responsibilities. AEMO will recover the associated costs in accordance with the NEL and NER.

Question 1

Do you consider the cyber security roles and responsibilities is a major reform or development of the NEM?

3.2 Criterion 2 – Major change to 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


AEMO operates under and in accordance with national and Western Australian electricity and gas laws. In respect of the NEM, the National Electricity Law (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.¹⁶ 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.

Therefore, the rule change request proposed establishing cyber security as part of AEMO's responsibility to maintain power system security, supported by the four new functions. The changes proposed would also enable

¹⁶ 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>



AEMO to recover costs it incurs in carrying out these functions and confirm AEMO's immunity from liability for the delivery of these functions.¹⁷

Following consultation, the AEMC's Final Rule 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 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.

Further, the changes to the Rules provide 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. This will provide market participants and governments confidence that AEMO will perform the functions to support its power system security responsibilities.

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. AEMO considers it is well placed to implement changes required promptly following the final rule and that no transition period was subsequently required. As noted in Section 3.1, the environment has changed considerably and as a result, cyber preparedness and uplift are becoming increasingly important for the NEM and will require greater resourcing moving forward.

Question 2

Do you consider the cyber security roles and responsibilities is a major change to an AEMO function, responsibility, obligation or power under the Rules?

3.3 Criterion 3 – Major change to computer software or system

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

Changes and additional capabilities will be required to support delivery of the new cyber security roles and responsibilities. These will be provided via a range of technology functions and software but will not require alterations to core systems or market applications. It is anticipated that new software platforms will be required to be implemented and operated by AEMO in order to support the following:

- Assessment and benchmark reporting on AESCSF cyber maturity.
- Cyber exercise delivery, evaluation and reporting.
- Incident coordination and response activities.

¹⁷ AEMC Consultation Paper - Cyber security roles and responsibilities. Last accessed 24 December 2024. Available at: <https://www.aemc.gov.au/sites/default/files/2024-06/ERCO388%20Consultation%20Paper%20-Cyber%20security%20roles%20and%20responsibilities> .

- Identification, prioritisation and review of research requests.
- Communicating sensitive cyber threat information to market participants.

More detailed elements 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.

Elevation of the cyber coordination function (Function 1) will require material uplift in systems, software and processes. Specifically, secure and resilient platforms for communication with market participants during incidents, systems and processes for securely tracking incidents to resolution and producing post incident review reports, and engagement and consultation with market participants, State Government and Commonwealth authorities on refining response coordination arrangements where these interface with those organisation and agency arrangements.

Furthermore, exercising of these arrangements is a complicated undertaking. Previous exercises such as TRIDENT I involved engagement with 23 market participants and 13 government agencies. Given the clarified role for exercising arrangements these exercises will need to be expanded to include a greater number of market participants from across all Participant categories.

Assuming the responsibility and stewardship of the security maturity uplift work (Function 2) will require process design around the governance of the AESCSF and implementation and promulgation of updates, a task which requires careful consideration given the inclusion of this framework in regulatory instruments such as the SoCI Act. Additionally, AEMO will need to establish assessment and benchmarking platform capabilities and associated processes to support the annual engagement of market participants in an assessment program.

Process design, platforms and software applications will also need to be established to support Functions 3 and 4.

The above changes are likely to be delivered within the cost estimates outlined in section 2.2.

Question 3

Do you consider the cyber security roles and responsibilities is 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?

4 Part B – Participant fee structure

sections below seek 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 that the new cyber security roles and responsibilities meet any of the criteria (outlined in Section 3) to be 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 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 fee¹⁸ to be used in the recovery of costs,
- the start date for recovery, and
- the period or periods over which recovery will occur.

If AEMO determines, through consultation, that the new cyber security roles and responsibilities are a declared NEM project, this Part B consultation is undertaken to satisfy the relevant Rules consultation requirements in clauses 2.11 and 8.9.

However, if the new cyber security roles and responsibilities are determined *not* to meet the criteria of a declared NEM project, the costs of the new cyber security roles and responsibilities will be recovered through AEMO's existing NEM Participant fee structures (e.g., NEM Core fee) determined in AEMO's Final Report of the Structure of Participant Fees in AEMO's Electricity Markets published on AEMO's website in March 2021¹⁹. These costs will be recovered in the manner explained in section 4.2.1 below, with costs incurred from 12 December 2024 to be included in AEMO's annual Budget and Fees report from FY26.

AEMO's next general NEM Participant fee structure is to be consulted on and determined by 30 March 2026 for the next fee recovery period to commence on 1 July 2026. The outcomes of the consultation processes initiated in Part A and Part B (if required) of this paper will be reflected in and further consulted upon as part of this broader consultation.

4.1 Recovering fees from Registered Participants

Pursuant to clause 2.11.1(a) of the NER, AEMO recovers costs from Registered Participants in accordance with the structure of Participant fees determined by AEMO.

The attribution of the allocated costs to each Registered Participant is based on AEMO's activities and outputs and the cost drivers associated with them and the extent of the involvement of the participants for each of the outputs

¹⁸ 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 of 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.

¹⁹ 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>

and revenue requirements. When developing the structure of Participant fees, AEMO take into account several factors including, for example:

- the class of Registered Participant interacts with AEMO in relation to the output;
- the class of Registered Participant uses the output;
- the class of Registered Participant receives the output;
- the class of Registered Participant benefits from the output; and
- those revenue requirements are given rise to, or caused by, that class of Registered Participant's presence in the NEM.

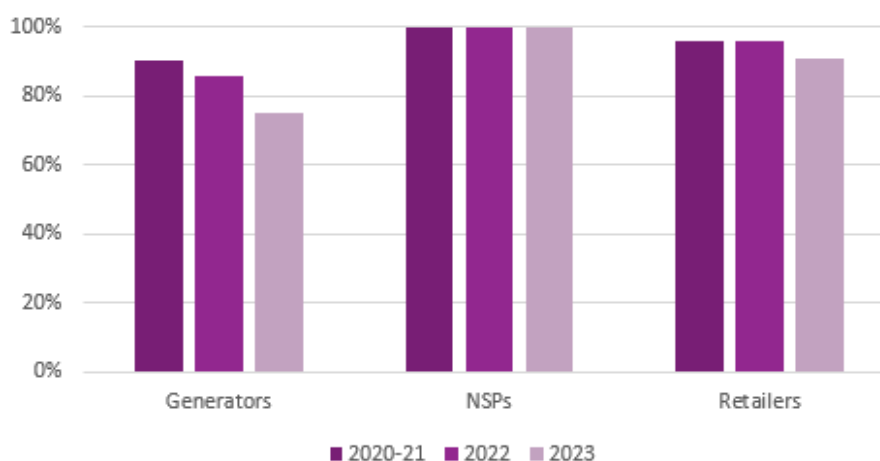
Government bodies, intending or new participants that are not yet Registered Participant categories under the Rules cannot be considered for recovery through AEMO's fee structure. New Registered Participant categories can only be considered for fee recovery once they are legislated in the NEL/NER, and the extent of their involvement with AEMO's revenue requirements can be determined.


4.1.1 New cyber security roles and responsibilities – Participant involvement

It is anticipated that the new cyber security roles and responsibilities will impact all NEM Registered Participants. Specifically, Function 1 (the incident coordination function), Function 2 (supporting cyber preparedness and uplift) and Function 4 (facilitating information distribution) will *involve* all Registered Participants, particularly Generators, Market Customers (retailers), Transmission Network Service Providers (TNSPs) and Distribution Network Service Providers (DNSPs). The level of involvement and therefore impact upon each Registered Participant category will be subject to Registered Participants' leverage and adoption of the AESCSF and associated assessment programs, involvement or role under the AESCIRP, as well as the nature of any future cyber security incident, exercise or testing.

Historical market participation (which includes participants accessing the portal, submitting assessment results and viewing their organisation's result and benchmarking data) with the AESCSF is shown in Figure 3 below as an indicative baseline for future use of the upscaled framework to support the increasing importance of cyber security.

Figure 3. Historical AESCSF market participation (NEM only)





As the market operator, AEMO is well placed to plan and provide information to warn Registered Participants and industry of cyber security vulnerabilities or threats, as well as conduct various assessments, cyber security tests or exercises. Collectively these functions seek not only to benefit AEMO and its ability to maintain power system security, but it will also assist Registered Participants protect their own systems and take steps necessary to respond to cyber security threats more broadly mitigating the risk of such incidents and consequences for consumers in the long term.

Clauses 4.3.2A(c) and (d) describe Function 3 of AEMO's new cyber security roles and responsibilities which seeks to leverage AEMO's unique understanding of the NEM and its associated systems with an aim to support effective and strategic decision-making by government and industry. Clause 4.3.2A(c) of the Rules provides discretion for AEMO to undertake research and provide advice to a Minister and to Registered Participants in relation to identified cyber security risks that may impact the power system and the management or mitigation of those risks. Similarly, clause 4.3.2A(d) of the Rules requires AEMO, at the request of a Minister, to undertake research and provide advice in relation to cyber security risks to the power system and the management or mitigation of those risks.

The level of involvement and therefore impact on Participants is likely to be affected by the scope and nature of the research or advice to be provided and the party requesting the advice.

4.2 Existing NEM Participant fee structure options

Any Participant fee structure must be developed and determined in accordance with clause 2.11.1 of the NER.

The existing general NEM Participant fee structures, including the fee metrics for each Participant category, commenced on 1 July 2021 for a term of five years, ending 30 June 2026. The scope for each of these fee structures were defined in AEMO's Final Report of the Structure of Participant Fees in AEMO's Electricity Markets published in March 2021.²⁰

Additionally, following consultation with stakeholders and determination of the NEM2025 Reform Program as a declared NEM project in September 2022, an additional NEM2025 Reform Program Participant fee was determined in October 2023.²¹

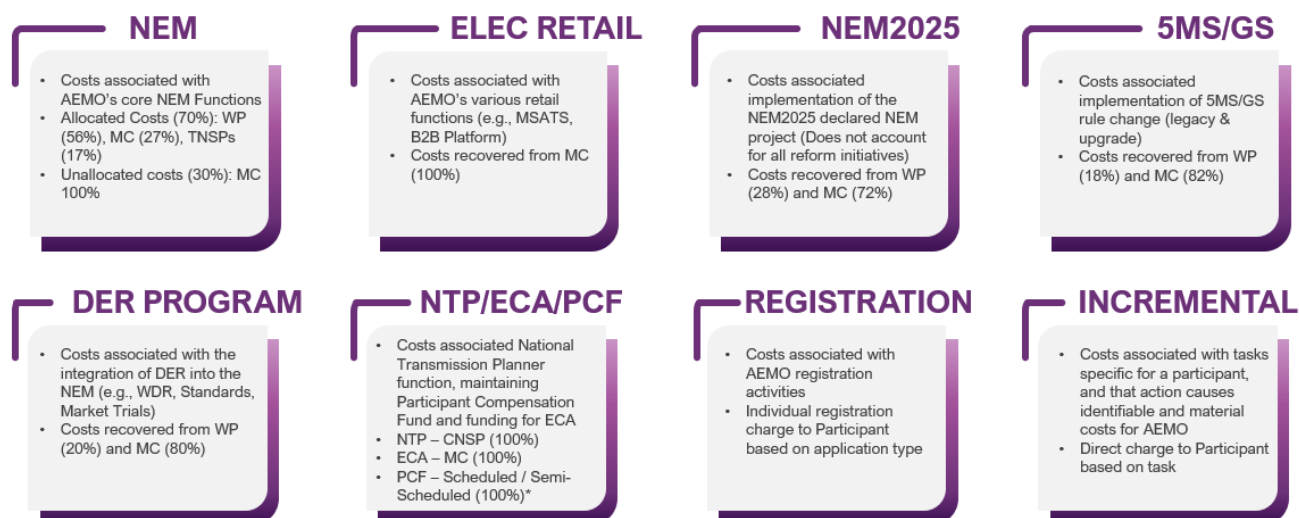
Figure 4 highlights AEMO's current NEM Participant fee structure.

As the term of the existing general NEM Participant fee structure concludes on 30 June 2026, consultation on the next general NEM Participant fee structure and any other additional fee structure determined for a declared NEM project before 30 June 2026 will commence in Q1 2025 for the new fee structure period commencing 1 July 2026. The term of the next fee structure period is to be determined as part of that consultation.

²⁰ 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>

²¹ AEMO. Participant Fee Structure for the NEM2025 Reform program Declared NEM Project Final Report and Determination. 6 October 2023. Available here: <https://www.aemo.com.au/consultations/current-and-closed-consultations/participant-fee-structure-for-the-nem2025-reform-program-declared-nem-project>

Figure 4. Existing general NEM Participant fee structures



^A Allocations rounded for the purpose of presentation. Various charging metrics applied including \$/MWh, \$/MW, and \$/NMI
^{*} Costs charged to Scheduled and Semi-Scheduled Generators and Scheduled Network Service Providers.

The following sections compare the relevant existing Participant fee structures that could be expanded to enable recovery of costs associated with the new cyber security roles and responsibilities with alternative options outlined in section 4.3.

4.2.1 NEM Core Fee

The NEM Core fee applying from 1 July 2023 to 30 June 2026 is presented below in Figure 5.

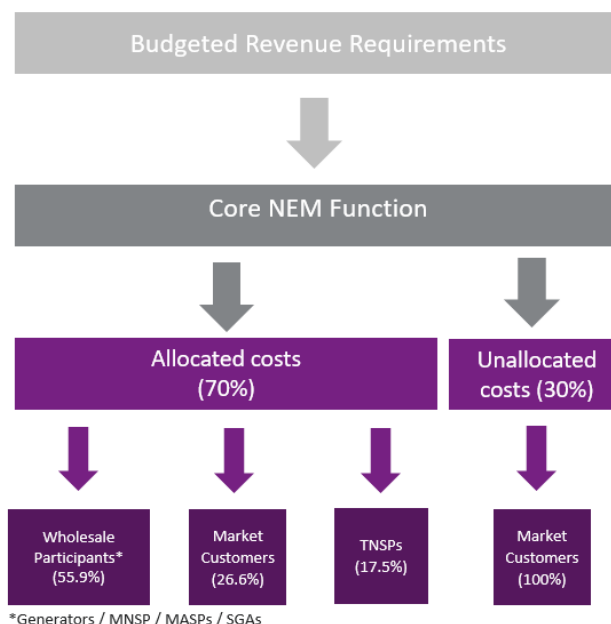
The NEM Core fee is used to recover costs associated with the functions defined in the fee structure determination as AEMO's core NEM functions. The core NEM functions relevant to the performance of the new cyber security roles and responsibilities include:

- Power system security and reliability.
- Market operations and systems.

The NEM Core fee recovers two types of costs, allocated (direct) costs and unallocated (indirect costs). The current apportionment of the budgeted revenue requirements is 70% to allocated costs and 30% to unallocated costs. Allocated costs are costs which can be readily allocated to either a particular function (e.g. system security and reliability functions), or to a participant category or class. Unallocated (indirect) costs are costs which cannot be readily allocated to a particular participant category or function (e.g. corporate overheads) and based on principles of economic efficiency having regard to the NEO, are fully recovered from Market Customers.

The attribution of the allocated costs is based on AEMO's assessment of AEMO's activities and outputs in relation to each function, the cost drivers associated with them, and the extent of the involvement of the participants for each of the outputs and revenue requirements.

Figure 5. Allocation of the NEM Core fee from 1 July 2023 to 30 June 2026



The NEM Core fee recovers costs from:

- Wholesale Participants (WP) on an equal allocation to 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 (MC) on an equal allocation to 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 on the basis of energy consumed for the latest completed financial year (consistent with the basis for charging the NTP fee).

Clause 4.3.1(c1) of the Rules sets out AEMO's power system security responsibility to coordinate and support cyber security preparedness, response, and recovery. This responsibility now forms part of AEMO's core responsibilities more broadly for managing the power system security as outlined in clause 4.3.1 of the Rules, which supports the core functions of power system security and reliability and market operations and systems. The four cyber security functions also support these core NEM functions.

Accordingly, AEMO may seek to use the existing NEM Core fee to recover the costs associated with the new cyber security roles and responsibilities, noting the fee generally covers Registered Participants more broadly relative to other existing fee structures. AEMO notes the existing allocation in this fee structure might not necessarily accurately reflect which categories of Registered Participants benefit from or are involved in each cyber security function at this time.

4.2.2 Incremental charges

Where it is practical for AEMO to identify doing something specific for a Registered Participant, and that action causes identifiable and material costs for AEMO, AEMO can seek to levy incremental charges directly from that Registered Participant. Depending on the nature of the research undertaken or advice sought, including who initiated that research or requested that advice, AEMO notes that costs incurred under Function 3 to provide cyber security research or advice requested by Registered Participants might best be recovered directly using an incremental charge approach (i.e. via an agreement with the relevant Registered Participant) from the Registered Participant who has requested the research or advice.

4.3 Alternative Participant fee structure options

An additional separate fee could be established that recovers costs of the new cyber security roles and responsibilities from the Registered Participant/s that are involved in, benefit from, or impacted by one of the functions arising from the new cyber security roles and responsibilities. This fee structure would include developing the appropriate attribution of costs to be allocated to each category of Registered Participant involved and applying fee metrics to those categories of Registered Participants accordingly.

As highlighted in Figure 3 historical market participation utilising or participating in an assessment program under the AESCSF has been significant across all Participant categories in the NEM. Using this participation as a basis for the developing Participant attribution levels, one approach may be for an equal attribution of costs of the cyber security roles and responsibilities across Wholesale Participants, TNSPs and Market Customers (see below Figure 6) with each of those participant category charged on the same basis as the existing NEM Core fee outlined in section 4.2.1.

It is to be noted that DNSPs are not currently allocated any of AEMO's Participant fees, and as a cost recovery mechanism for this category is required prior to allocating fees to this Registered Participant, AEMO does not propose to recover costs from these Participants for the new cyber security roles and responsibilities at this stage. This option can be reconsidered as part of the upcoming general NEM Participant fee structure consultation for the fee period commencing 1 July 2026, regardless of whether the new cyber security roles and responsibilities are determined a declared NEM project or not.

Additionally, AEMO only has the power under clause 2.11 of the Rules to recover fees from Registered Participants. While Functions 1, 2 and 4 of the new cyber security roles and responsibilities involve a wider cohort of Registered Participants, Function 3 provides discretion for AEMO to undertake research and provide advice to a Minister (i.e. a non-Registered Participant) and to individual Registered Participants as outlined in section 4.1.1. AEMO notes the nature and therefore costs of Function 3 could be included within the fee structure shown in Figure 6 where research is completed, shared with, and benefits a wider cohort of Registered Participants (i.e., as per Functions 1, 2 and 4).

Where AEMO is undertaking research or providing advice specifically requested by a Minister (i.e. a non-Registered Participant) AEMO must first consult with the relevant Minister in accordance with clause 4.3.2A(e) on:

- the nature of the research and advice being sought,

- AEMO’s capacity and capability to undertake the research and provide the advice having regard to its role as the power system and market operator; and
- the likely costs that AEMO will incur in undertaking the research and advice.

If the Minister requests AEMO to proceed with the research or advice task, AEMO would seek to recover costs directly from the Minister requesting the advice via an agreement. AEMO notes this form of agreement is separate to an incremental charge which is applicable to Registered Participants only.

Figure 6. Example additional, separate fee for the new cyber security roles and responsibilities



4.4 Start date and period/s of fee recovery

If the new cyber security roles and responsibilities are determined a declared NEM project, the Rules require AEMO to also determine the start date and period/s of cost recovery, in consultation with stakeholders.

The AEMC’s final rule and determination on AEMO’s cyber security roles and responsibilities came into effect on 12 December 2024. AEMO notes it may begin recovering its costs related in performing the new cyber security roles and responsibilities from this date. 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.

To align with AEMO’s annual budget and fees process, it is proposed that, under a Participant fee structure for the declared NEM project, cost recovery commence from 1 July 2025 for a period of seven years to best align with

AEMO’s depreciation model for other assets. AEMO intends that costs incurred on and from 12 December 2024, that is, the date the Rule became effective, would be recovered from FY26.

As previously noted, AEMO will begin consultation towards the end of calendar Q1 2025 on the general NEM Participant fee structures for the period commencing 1 July 2026. Any additional fee structure determined before then for the new cyber security roles and responsibilities would be included as part of that consultation scope.

Question 1

Do stakeholders agree AEMO should recover AEMO’s costs for the cyber security roles and responsibilities from 1 July 2025 for a period of seven years (pending any different determinations that may be made in the next general NEM Participant fee structure consultation)?

4.5 Preliminary assessment of all Participant fee structure options (if determined a declared NEM project)

While AEMO is required under the Rules to determine the structure of an additional Participant fee if the criteria for a declared NEM project is met, any 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 possible, be consistent with the Fee Structure Principles.

Table 1 below presents a preliminary assessment of the various options for the recovery of costs associated with AEMO’s new cyber security roles and responsibilities, should it be determined a declared NEM project, against the fee structure principles and the NEO. AEMO are seeking stakeholder feedback on the options proposed and its preliminary assessment against the NEO and Fee Structure Principles, as well as any other options that AEMO should consider.

AEMO notes that other existing fee structures, such as the Electricity Retail Markets fee, were considered as potential options to recover costs of the new cyber security roles and responsibilities but have not been included in the assessment table below. This is because those fee structures are less consistent with the Fee Structure Principles than the options detailed in Table 1, particularly the *reflective of involvement* and *not unreasonably discriminate* principles.

The assessment key is as follows:

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

Table 1. Preliminary assessment of all fee structure options against NEO and Fee Structure Principles

Example options	General Comments	Indicative assessment against NEO or Fee Structure Principle
1. Expand existing Participant fee structure – NEM Core Fee <i>(As outlined in section 4.2.1)</i>	Pros <ul style="list-style-type: none"> Existing structure and metrics are understood by participants. Aligns with AEMO's broader core responsibilities for power system security under the Rules. AEMO's power system security responsibility to coordinate and support cyber security preparedness, response, and recovery forms part of AEMO's core responsibilities for managing power system security more broadly. Attribution of allocated costs to Registered Participants would be as per the existing NEM Core Participant fee (WP, MC and TNSP) providing for broad coverage relative to other existing fees. Cons <ul style="list-style-type: none"> Expanding the existing Participant fee structure may only apply until the end of the current Participant fee period subject to the outcomes of the next general NEM Participant fee consultation to commence in late calendar Q1 2025. Existing attribution of allocated costs may over- or under-state the involvement of one or more Registered Participant categories with the costs of the new cyber security roles and responsibilities. Reduced transparency of costs associated with new cyber security roles and responsibilities with their aggregation into NEM Core fee (relative to additional, separate fee). Does not align with AEMO's budgeted pathway nor likely expansion of future cyber security roles and responsibilities. 	Simplicity
		Reflective of involvement
		Not unreasonably discriminate
		Recovery of AEMO's budgeted requirements on a specified basis
		NEO
2. Establish an additional (separate) cyber security function fee <i>(As outlined in section 4.3)</i>	Pros <ul style="list-style-type: none"> A new Participant fee structure ensures cost transparency for those actions undertaken as part of the roles and responsibilities. Allows for determination of the relevant Registered Participant/s to recover costs from as well as the allocation of costs and metrics for each Registered Participant category, providing for a better reflection of those impacted or involved across all new cyber security roles and responsibilities. 	Simplicity
		Reflective of involvement

Example options	General Comments	Indicative assessment against NEO or Fee Structure Principle
	<ul style="list-style-type: none"> Provides an approach to recover costs specifically related to Function 3 requests made by Ministers. Subject to the outcomes from this consultation, can be implemented ahead of proposed 1 July 2025 start. <p>Cons</p> <ul style="list-style-type: none"> The new Participant fee structure may only apply until the end of the current Participant fee period subject to the outcomes of the next general NEM Participant fee consultation to commence in late calendar Q1 2025. AEMO notes this separate consultation might determine to continue with a separate fee for the new period. Further disaggregation of AEMO fees potentially creating additional complexity and costs in their administration. 	Not unreasonably discriminate
		Recovery of AEMO's budgeted requirements on a specified basis
		NEO

Question 2

- Which, if any, of the above fee structure options are appropriate for the recovery of costs associated with AEMO's cyber security roles and responsibilities and why or why not?
- Is there another fee structure (not presented above) that would be more appropriate for recovering the costs associated with AEMO's cyber security roles and responsibilities and why?
- Which Registered Participant/s should the costs of AEMO's cyber security roles and responsibilities be recovered from and why?

Question 3

In relation to example options 1 and 2, are the fee metrics used for the relevant Participant fee structures appropriate to apply to the recovery of costs associated with cyber security roles and responsibilities? If not, what metric(s) is/are more appropriate?

A1. Questions for stakeholders

AEMO appreciates stakeholder feedback on the following questions, as well as any additional comments stakeholders may have in relation to Part A and Part B of this Consultation Paper.

PART A – Declared NEM Project

Question 1

Do you consider the cyber security roles and responsibilities is a major reform or development of the NEM?

Question 2

Do you consider the cyber security roles and responsibilities is a major change to an AEMO function, responsibility, obligation or power under the Rules?

Question 3

Do you consider the cyber security roles and responsibilities is 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?

PART B – Participant Fee Structure

Question 1

Do stakeholders agree AEMO should recover AEMO's costs for the cyber security roles and responsibilities from 1 July 2025 for a period of seven years (pending any different determinations that may be made in the next general NEM Participant fee structure consultation)?

Question 2

- a. Which, if any, of the above fee structure options are appropriate for the recovery of costs associated with AEMO's cyber security roles and responsibilities and why or why not?
- b. Is there another fee structure (not presented above) that would be more appropriate for recovering the costs associated with AEMO's cyber security roles and responsibilities and why?
- c. Which Registered Participant/s should the costs of AEMO's cyber security roles and responsibilities be recovered from and why?

Question 3

In relation to example options 1 and 2, are the fee metrics used for the relevant Participant fee structures appropriate to apply to the recovery of costs associated with cyber security roles and responsibilities? If not, what metric(s) is/are more appropriate?

A2. Glossary

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

A3. Fee structure principles²²

Fee Structure Principle	Requirement	Application and examples
National Electricity Objective (NEO)	<p>In determining Participant fees, AEMO must have regard to the national electricity objective.</p> <p>The objective of the NEL is to promote efficient investment in, and efficient operation and use of, electricity services for the long term interests of consumers of electricity with respect to—</p> <ul style="list-style-type: none"> a) price, quality, safety, reliability and security of supply of electricity; and b) the reliability, safety and security of the national electricity system 	<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, which have followed a similar interpretation. See, for example, Application by ElectraNet Pty Ltd (No 3) [2008] ACompT [15]:</p> <p>“The national electricity objective provides the overarching economic objective for regulation under the Law: the promotion of efficient investment in the long term interests of consumers. Consumers will benefit in the long run if resources are used efficiently, i.e. resources are allocated to the delivery of goods and services in accordance with consumer preferences at least cost.”</p> <p>The NEO is clearly a relevant consideration where AEMO has to exercise judgment or discretion in reaching its determination, for example, if there is a number of Participant fee structures each of which can satisfy the Fee Structure principles, or where the relevant provisions of the Rules are ambiguous.</p>
Simplicity	<p>The structure of Participant fees should be simple</p>	<p>As “simple” is not defined in the Rules, it must be given its ordinary meaning as understood in the context of clause 2.11 of the Rules.</p> <p>The New Shorter Oxford English Dictionary’s definition of “simple” (in this context) is: “not complicated or elaborate” and “plain, unadorned”. Whether a fee structure fits these definitions is largely a matter of judgement.</p> <p>There is a wide range of possible fee structures. There is no single identifiable point where “simple” becomes “complicated”.</p> <p>It is clear from this provision that a certain degree of complexity was envisaged in that the structure of Participant fees may involve several components and budgeted revenue consists of several elements. The structure of Participant fees need not demonstrate absolute simplicity.</p> <p>The simplest fee structures are unlikely to be consistent with the other criteria. However, it is possible to find fee structures that, while consistent with the other criteria, are relatively simple, in comparison to alternative structures.</p>

²² This appendix replicates Appendix A (Fee structure principles) of the Electricity Fee Structures: Final Report and Determination, March 2021, available here: https://www.aemo.com.au/-/media/files/stakeholder_consultation/consultations/nem-consultations/2020/electricity-market-participant-fee-structure-review/final-report/aemo-electricity-fee-structure-final-report-and-determination.pdf?la=en

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

Fee Structure Principle	Requirement	Application and examples
		<p>principles in clause 2.11.1(b) of the Rules, or the NEL, the discrimination will not be “unreasonable”.</p> <p>In considering a past fee determination, the Dispute Resolution Panel accepted that this principle is to be applied to the extent practicable and it is only unreasonable discrimination that offends.</p>
Comparability	<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>Note that this is not strictly a principle but is included for completeness in describing the matters for which AEMO must have regard.</p>	<p>Other relevant fee structures could include:</p> <ul style="list-style-type: none"> • Other electricity market fee structures such as Western Australia or globally • Gas markets operated by AEMO