



2 July 2025

Anna Collyer, Chair  
Australian Energy Market Commission  
GPO Box 2603 SYDNEY, NSW 2001

Dear Ms Collyer,

Amazon Corporate Services Pty Ltd, operating globally as Amazon Web Services (AWS), welcomes the opportunity to respond to the Australian Energy Market Commission's (AEMC) consultation paper on improving the National Electricity Market (NEM) access standards – Package 2 (ERC0394). As the largest cloud provider globally and a significant investor in Australia's digital infrastructure, we appreciate the Commission's efforts to maintain power system security while enabling continued investment in critical infrastructure. This submission sets out our response to AEMC's consultation paper. Appendix A sets out AWS' responses to specific consultation questions.

### **1. Strategic Context**

Data centres form essential digital infrastructure underpinning Australia's economic growth and digital transformation. With our AU\$20 billion investment commitment by 2029, our facilities provide predictable baseload demand supporting grid stability, particularly during high renewable generation periods. Operating at industry-leading efficiency levels, our facilities can reduce carbon emissions by up to 94% compared to on-premises data centres while ensuring high reliability for critical infrastructure. We achieved 100% renewable energy for our global operations in 2024, aiming for net-zero carbon by 2040. Our 11 Australian renewable energy projects, generating over 1.4 million megawatt hours annually, demonstrate our commitment to grid stability and decarbonisation objectives.

### **2. Key Technical Considerations**

The development of access standards must be grounded in actual system security impacts rather than theoretical assumptions about facility capacity. Data centres represent a new class of load which are fundamentally different from traditional industrial consumers. Unlike traditional industrial loads, data centres load ramp-up gradually over time, allowing for careful planning and coordination with network operators. Our data centres provide demand that helps manage minimum system demand issues, while employing sophisticated power management systems that maintain stable operations under normal grid conditions.

### **3. Technology Classification**

We urge the AEMC to reconsider the current categorisation of data centres as inverter-based loads (IBL). Data centres employ complex hybrid power architectures combining different technologies, sophisticated load management systems, and high reliability requirements that distinguish them from traditional IBLs. Given these unique characteristics, including predictable load patterns and baseload characteristics, we recommend establishing a separate technical category for data centre loads in the NEM. This would enable more appropriate technical standards to be developed, recognise data centres' unique contribution to grid stability, and create a framework for future technology evolution while supporting both system security and efficient market outcomes.



#### **4. Proposed Framework**

Our responses to the consultation questions outline specific recommendations regarding technical requirements, implementation approaches, and transition arrangements. We recommend adopting a risk-based, outcomes-focused approach that balances system security needs with practical operational requirements, recognises the unique characteristics and benefits of data centre loads, provides flexibility for technological evolution, and ensures Australia remains competitive for digital infrastructure investment while maintaining speed to market as a critical factor for investment.

#### **5. Path Forward**

We strongly encourage leveraging existing forums and establishing technical working groups to develop a comprehensive understanding of data centre technical capabilities before finalising new requirements. AWS recommends regular consultation on emerging technologies and grid support opportunities, phased implementation aligned with industry capabilities and equipment availability, and information sharing frameworks balancing transparency with security and confidentiality.

We emphasise the importance of appropriate transition arrangements that recognise both the critical nature of data centre operations and the need for thorough technical assessment. Any new requirements should be implemented in a staged manner that allows for proper testing and validation while maintaining service continuity. This is particularly important given the role data centres play in supporting essential digital services and Australia's economic growth.

AWS remains committed to its significant investment in Australia and working constructively with the AEMC, AEMO, and Network Service Providers (NSPs) to develop practical and effective technical standards that maintain system security while enabling continued investment in Australia's digital infrastructure. We would welcome the opportunity to discuss these matters in detail.

Yours sincerely,

Amazon Corporate Services Pty Ltd

### Question 1: Defining large loads in the context of this rule change request

**In the context of this rule change request and AEMO's ongoing consideration of the definition for large loads through its Large Loads Review:**

**1. Are stakeholders supportive of AEMO's ongoing process to address the system security implications and performance standards for large loads, including how large loads ought to be defined in the NER?**

AWS supports AEMO's efforts to better understand how load technologies impact the broader network, as reflected in this rule change request. However, we believe that more detailed technical analysis and industry consultation is necessary before finalizing any formal definition in the NER. We recommend that this technical work be undertaken in close consultation with data centre operators as part of AEMO's current Large Loads Review. This collaborative approach would ensure that the unique characteristics and operational requirements of data centres are fully considered in developing appropriate standards and definitions.

**2. To what extent do stakeholders think that the Commission should consider the definition of 'large loads' in the context of this rule change?**

We do not believe that AEMO's suggestion of classifying any load above 5 MW as a 'large load' is appropriate, as it could capture many facilities that pose no material system security risk. This threshold is not large in the context of modern industrial loads or emerging technologies. While some grid assessments suggest much higher thresholds could be considered, we believe a flexible, multi-criteria approach would be more suitable to address the evolving nature of the industry and varying impacts of different types of loads on system security.

**3. If it is considered, should large loads be defined based on the relevant access standard, or should a large load be more holistically defined in the NER?**

If a definition is deemed necessary, we recommend a multi-criteria approach that considers:

- a) System Strength: Connection point Short Circuit Ratio (SCR) below specified thresholds (e.g.,  $SCR < 10$ )
- b) System Scale Significance: Load size sufficient to impact network frequency
- c) Network Location Benefits: Potential to support network stability around the connection point
- d) Technology Capabilities: Different types of power electronic interfaces and their impacts on system strength and stability

The specific parameters or thresholds for each of these factors would be best developed in consultation with data centre operators and other relevant stakeholders. This collaborative approach would ensure that the definition accurately reflects the technical realities and operational considerations of large loads, particularly in the context of data centres.

**4. Alternatively, should we consider whether to apply guiding principles and timing for AEMO to produce a proposed definition, which is currently being considered in AEMO's Large Loads Review?**

We support establishing guiding principles for AEMO's ongoing work, focusing on:

- a) Evidence-based assessment of system security impacts
- b) Recognition of different load technologies and their characteristics
- c) Consideration of economic implications for critical infrastructure
- d) Alignment with international best practices
- e) Regular review mechanisms as technology evolves

### Question 2: Amending the NER to address the influx of large loads

**1. Do stakeholders have any reflections or data and information they wish to share with the AEMC regarding the prospective growth of large loads connecting to the NEM, including from international experience?**

AWS brings extensive operational experience as a global leader in data centre development and operations. Our operational model differs significantly from traditional industrial loads, incorporating sophisticated design, demand forecasting and staged deployment approaches that enable better coordination with network planning processes.

## Appendix A – Response to Consultation Questions

We would welcome the opportunity to engage in detailed technical discussions with AEMC and AEMO to share insights and experience from our global operations, including our approaches to power management and renewable energy integration. Such collaboration could help develop appropriate frameworks for the Australian context while supporting the nation's digital infrastructure growth.

### **2. Do stakeholders agree with AEMO that the expected growth of large loads may present a risk to power system security?**

While we acknowledge AEMO's responsibility to maintain system security, we believe the focus should be on understanding and leveraging the unique characteristics of modern data centres rather than viewing them primarily as a risk:

- **Growth Pattern:** Data centre capacity increases are staged, allowing for coordinated network development
- **Load Characteristics:** Data centres' predictable load patterns can enhance grid stability near point of connection
- **Location Benefits:** Strategically located data centres can support local network stability and alleviate constraints
- **Technical Capabilities:** Data centre modern power management systems help maintain stable operations under normal grid conditions
- **Economic Benefits:** Data centre investment supports critical digital infrastructure while driving investment in new renewable energy resources

We recommend that AEMO continue its collaborative approach through the Large Loads Review to develop a more comprehensive understanding of data centre capabilities and characteristics before implementing new requirements.

### **Question 3: HVDC links to procure system strength services from third parties**

While the specific questions regarding HVDC links are outside our direct scope, the principle of flexible approaches to meeting system strength requirements is relevant to large loads. Under clause S5.3.11, loads must demonstrate capability to operate at specified SCR levels through appropriate control and protection system settings.

We encourage the AEMC to consider whether additional flexibility in meeting system strength requirements could benefit all connecting parties while maintaining system security objectives.

### **Question 4: Limiting short circuit ratio requirements for customer loads to IBR, and introducing flexibility to the access standard**

**In relation to AEMO's proposal to limit the application of short circuit ratio requirements under clause S5.3.11 to large inverter-based resources that is IBL:**

#### **1. Do stakeholders consider it an issue that the short circuit ratio requirements under clause S5.3.11 apply to all IBR plant without any size threshold?**

##### **a. Should it only apply to large inverter-based resources as defined in AEMO's SSIAG?**

We support limiting the application of clause S5.3.11 to large inverter-based loads. The current application to all IBR plant regardless of size creates unnecessary technical and administrative burden where system security risks may be minimal.

The current system strength framework can result in significant costs for large loads. For example, based on recent connection enquiries, system strength charges for data centres can exceed \$4 million annually. These costs must be considered alongside technical requirements, particularly where alternative approaches through control and protection systems might achieve equivalent system security outcomes more efficiently.

##### **b. Is the definition of a large inverter-based resource in the SSIAG sufficient for the purposes of this proposal?**

## Appendix A – Response to Consultation Questions

In our view, the SSIAG definition's application to data centres needs reconsideration as they employ complex hybrid power architectures that are fundamentally different from traditional IBLs, including:

- Sophisticated power systems with multiple power conversion stages
- Complex load management systems
- High reliability requirements with redundant power systems
- Predictable load patterns and stable characteristics

A separate technical category for data centre loads would enable:

- More appropriate technical standards reflecting data centre architectures
- Recognition of data centres' unique ability to contribute to grid stability
- Standards that account for critical infrastructure requirements
- A framework that supports future technology evolution

### **2. Are there alternative solutions stakeholders consider would be more effective?**

The flexibility provided in clause S5.3.11(b) and (d) offers a good framework, but requires:

- Clear guidelines for assessing "reasonable higher values" of SCR
- Transparent processes for evaluating control and protection system settings
- Recognition of different technology capabilities
- Consideration of actual system security impacts

### **3. Do stakeholders have any concerns or suggestions in relation to this element of AEMO's proposed rule? If so, please describe your concerns and any related suggestions and reasoning.**

We recommend:

- Developing assessment criteria for NSPs and AEMO when considering higher SCR values
- Establishing guidelines for demonstrating compliance through control system settings
- Creating mechanisms for regular review as technology evolves
- Ensuring requirements align with international standards and practices

Any compliance framework must first establish the technical justification and system security benefits of requiring detailed simulation models for data centres, given the significant cost and time implications of developing such models. Alternative compliance approaches should be considered where detailed modelling requirements cannot be technically or economically justified.

**In relation to AEMO's proposal to amend the NER to introduce flexibility in clause S5.3.11 to allow the NSP and AEMO discretion to agree to a minimum short circuit ratio requirement above the minimum requirement of 3.0:**

#### **1. Do stakeholders agree there should be flexibility to agree to higher short circuit ratio requirements? Could there be unintended consequences?**

We support the flexibility provided in clause S5.3.11(b), which allows for higher SCR values based on three phase fault levels existing and projected at the connection point. However, this discretion must be exercised within a clear framework to ensure consistent application and avoid arbitrary requirements.

#### **2. Are there alternative solutions stakeholders consider would be more effective?**

The current proposal allowing demonstration of capability through "any appropriate control system and/or protection system settings" (clause S5.3.11(d)) provides a practical pathway for compliance. This flexibility in demonstrating capability should be maintained and supported by clear technical guidelines.

#### **3. Do stakeholders have any concerns or suggestions in relation to this element of AEMO's proposed rule? If so, please describe your concerns and any related suggestions and reasoning.**

We recommend:

- Establishing clear criteria for assessing appropriate SCR values at different connection points
- Developing guidelines for acceptable methods of capability demonstration

## Appendix A – Response to Consultation Questions

- Ensuring consistency in assessment approaches across different NSPs
- Maintaining flexibility in compliance pathways while ensuring system security

### Question 5: New definitions for protection systems

In relation to Rod Hughes Consulting's *Definitions of protection system requirements* rule change request:

**1. Do stakeholders agree that the requirements for generator protection systems are currently unclear? If so, what are the impacts of this lack of clarity?**

**a. Similarly, do stakeholders consider the requirements for loads' and HVDC links' protection systems are currently unclear?**

Yes, we agree that protection system requirements for loads need greater clarity. Our experience with data centre connections indicates that current requirements lack sufficient detail regarding:

- The distinction between different types of protection systems
- The level of redundancy required
- The interaction between load protection systems and grid stability requirements

**2. Do stakeholders support the proposal to update and add new NER definitions for types of protection systems?**

**a. Do stakeholders have feedback on the proposed new definitions themselves?**

While we support the objective of improving clarity through updated definitions, we recommend:

- Ensuring definitions reflect modern power system protection technologies
- Maintaining flexibility to accommodate different load technologies and configurations
- Focusing on functional requirements rather than prescriptive technical specifications
- Avoiding definitions that could unnecessarily increase complexity or cost for load connections

**3. Do stakeholders have any concerns or suggestions in relation to this element of Rod Hughes Consulting's proposed rule? If so, please describe your concerns and any related suggestions and reasoning.**

We recommend:

- Conducting detailed technical consultation with industry before finalising new definitions
- Ensuring requirements are proportionate to system security risks
- Considering the specific characteristics of different load types
- Providing clear guidance on how definitions apply to load protection systems
- Allowing appropriate transition periods for any new requirements

### Question 6: Conditions for generator protection systems

These questions relate specifically to generator protection systems under clause S5.2.5.9. As a data centre operator connecting load to the network, AWS is not directly impacted by these proposed changes. Therefore, we do not have specific positions on:

1. Whether paragraph (b) of clause S5.2.5.9 is redundant or misleading
2. The proposed changes to minimum access standards for generator protection systems
3. The proposal to give AEMO and NSPs discretion to increase redundancy requirements

However, we note that any changes to protection system requirements should maintain consistency across the NER and avoid unintended consequences for load connections. We encourage the AEMC to ensure that any revisions to generator protection requirements do not create precedents that could inappropriately affect future load connection standards.

### Question 7: Provision of information on ride-through capability

## Appendix A – Response to Consultation Questions

### In relation to AEMO's proposed changes to enable NSPs to request information on loads' ride-through capability:

#### 1. Do stakeholders agree that NSPs and AEMO lack visibility of loads' ride-through capability and that this creates a challenge for system security?

We acknowledge the importance of appropriate information sharing. The proposed framework under S5.3.1(a1)(2A) provides a structured approach where NSPs, after consulting with AEMO, can request specific information about ride-through capability.

While we acknowledge the importance of sharing appropriate information, any framework must recognise fundamental differences between generator and load ride-through capabilities. Data centres' power supply systems have specific operational constraints and protection requirements that differ significantly from generators thus, applying generator ride-through standards to loads may not achieve the intended system security benefits and can also compromise critical infrastructure protection.

#### 2. Do stakeholders support AEMO's proposed rule to require network users to provide information about connecting load's ride-through capability to the NSP on request?

We support the proposed approach where:

- Information requests must follow NSP consultation with AEMO
- Requirements specifically relate to capability to remain connected during frequency or voltage disturbances
- Performance standards may record this capability with AEMO visibility
- Framework maintains clear processes and responsibilities

However, we note that:

- Data centres are particularly sensitive to voltage disturbances
- Load ride-through capabilities may not align with generator standards due to equipment protection requirements
- Detailed ride-through capability information may not be available in early project stages
- Conservative assumptions may need to be used at the connection application stage, with more detailed information provided following detailed design

#### 3. Do stakeholders have any concerns or suggestions in relation to this element of AEMO's proposed rule?

We recommend:

- Clear guidelines for the scope and format of information requests
- Recognition of different technology capabilities and limitations and how these may change over time
- Appropriate protection of commercially sensitive information, particularly regarding:
  - Detailed protection settings and thresholds
  - Proprietary control system configurations
  - Customer-specific operational requirements
- Practical timeframes for information provision
- Clear protocols for information handling and distribution

### Question 8: Protection settings to maximise ride-through performance

#### In relation to AEMO's proposed changes to amend clause S5.3.3(c) of the NER to encourage protection settings that maximise loads' ride-through capability:

#### 1. Do stakeholders agree that the current arrangements allow conservative load protection settings that may unnecessarily reduce loads' ride-through capability?

The current arrangements under clause S5.3.4 already provide an effective framework, requiring NSP approval for protection system settings and allowing NSPs to request setting changes where necessary. The key consideration

## Appendix A – Response to Consultation Questions

should be maintaining equipment protection as the primary objective, while exploring opportunities to support system security where technically feasible and commercially reasonable. Protection settings must first prioritise:

- Safe operation of equipment according to manufacturer specifications
- Maintaining service level commitments to customers
- Ensuring reliable operation of critical infrastructure

Any changes to maximize ride-through capability should only be considered within these operational constraints.

### **2. Do stakeholders support AEMO's proposed rule requiring cooperation between the NSP and the network user in the design of protection systems and settings to maximise ride-through capability?**

We support the intent of the proposed changes to S5.3.3(c)(4) provided that:

- The primacy of maintaining "safe and stable operation of the plant within safety margins consistent with good electricity industry practice" is preserved
- Protection settings required by performance standards take precedence
- The requirement to "maximise" capability is qualified by technical and operational constraints
- Changes to settings remain subject to the approval process in S5.3.4

### **3. Do stakeholders have any concerns or suggestions in relation to this element of AEMO's proposed rule? If so, please describe your concerns and any related suggestions and reasoning.**

We recommend:

- Clear guidelines for assessing maximum achievable ride-through capability
- Recognition of critical infrastructure protection requirements
- Maintaining existing processes for protection setting changes under S5.3.4
- Practical timeframes for implementing any required changes

## **Question 9: New access standard for detection and response to instability**

**In relation to AEMO's proposed new access standard for detection and response to instability that would apply to large inverter-based loads:**

### **1. Do stakeholders agree that there is an emerging need for large inverter-based loads to play a role in managing instability in the NEM?**

While we recognize that inverter-based loads can potentially influence system stability, the case for requiring their active participation in managing instability has not been sufficiently demonstrated, making it difficult to establish:

- Whether loads are contributing to system instability versus merely being affected by it
- The effectiveness of load-based stability management solutions, particularly at the distribution level
- Whether disconnecting loads during instability events can exacerbate system disturbances
- If the benefits of load participation in stability management outweigh the costs and risks to critical infrastructure

Before establishing new requirements, we believe comprehensive technical studies and further industry consultation are needed to validate the actual impact and effectiveness of load participation in stability management.

### **2. Do stakeholders support AEMO's proposed new access standard for instability detection and response by loads as set out in Box 4?**

#### **a. Which parts of the proposal do stakeholders support, or oppose?**

The proposed standard raises several fundamental concerns:

- Schedule 5.3 lacks foundational stability requirements that should be established before introducing new detection obligations. Unlike generator requirements in clause S5.2.5.5, which provides comprehensive stability performance criteria including specific voltage recovery bands and timeframes, Schedule 5.3 does not define baseline stability performance requirements for loads



## Appendix A – Response to Consultation Questions

- Network instability often results from complex interactions between multiple system elements rather than being attributable to a single connecting plant. Without detailed system modelling, it becomes difficult to establish the root cause of instability events, distinguish between instability caused by load control systems versus external network factors; and prevent inappropriate load disconnection that could exacerbate system disturbances.
- Technical specifications for detection systems require development through consultation, particularly considering long procurement lead times for sub-synchronous oscillation detection devices, risk of cascading disconnections from multiple detection systems operating simultaneously and integration complexity with existing critical infrastructure.

### **b. Do stakeholders agree with the materiality thresholds for application of the automatic access standard and minimum access standard (see Table 4.2)?**

The proposed thresholds in Table 4.2 appear overly broad and should be reconsidered based on:

- A higher minimum threshold (e.g., 100MW) to focus on loads with genuine system-wide impact
- Network location and strength considerations
- Technical capability of different load types
- System security benefit versus implementation cost
- Practical effectiveness for loads connected to distribution networks

### **3. Do stakeholders have any concerns or suggestions in relation to this element of AEMO's proposed rule? If so, please describe your concerns and any related suggestions and reasoning.**

While we appreciate AEMO's initial recommendations and ongoing effort to address these important matters, we recommend:

- Building upon AEMO's initial recommendations while continuing industry consultation
- Developing technical specifications through ongoing engagement with data centre operators
- Establishing appropriate transition arrangements
- Creating alternative compliance pathways where technically justified
- Ensuring requirements don't conflict with critical infrastructure obligations

## **Question 10: Under-frequency ramp down of large loads**

**In relation to AEMO's proposed changes to amend the NER to facilitate the ability for loads to ramp down:**

### **1. Do stakeholders agree some loads may be more flexible with the ability to ramp down their load in an emergency rather than disconnecting in blocks?**

While we support the principle of flexible load reduction, data centre protection settings must prioritise equipment protection in accordance with manufacturer specifications and industry standards. Our standard protection settings, which are designed to protect critical infrastructure and maintain service level agreements, create technical constraints on the ability to provide graduated frequency response across all frequency bands currently specified in clause 4.3.5.

### **2. Do stakeholders agree that the NER should be amended to allow for the provision of interruptible load by way of fast ramp down?**

We agree that the NER should be amended to allow for the provision of interruptible load by way of fast ramp down. However, any such amendments should:

- Recognise technical limitations and protection requirements across different data centre configurations and operational models.
- Account for state and local regulations governing back-up generation.
- Acknowledge that cloud customer requirements and workload characteristics may limit participation options.
- Consider Security of Critical Infrastructure obligations.
- Enable flexible participation methods, particularly as data centres may connect at different network levels.

## Appendix A – Response to Consultation Questions

### **3. Do stakeholders have any concerns or suggestions in relation to this element of AEMO's proposed rule? If so, please describe your concerns and any related suggestions and reasoning.**

We recommend:

- Development of technology-specific requirements that recognise protection constraints
- Consideration of alternative frequency response bands for different technologies
- Clear exemption process where equipment protection requirements prevent compliance
- Alternative mechanisms for data centres to support system security within technical limitations

### **Question 11: Clarification of credible contingency definition for disturbance ride-through**

While this question primarily relates to generating systems, the principles of defining credible contingencies have implications for load connections.

We understand the need for clarity in defining contingency events. However, any framework developed should:

- Be based on actual system security risks rather than theoretical scenarios
- Consider the specific characteristics of different network locations
- Provide clear guidance while maintaining appropriate flexibility
- Allow for evolution of the power system

We encourage the AEMC to ensure that any changes to contingency definitions:

- Maintain clear distinction between generator and load requirements
- Avoid creating precedents that could inappropriately affect load connections
- Allow for appropriate consideration of critical infrastructure protection
- Support efficient investment in digital infrastructure

### **Question 12: Testing and commissioning**

#### **1. Do stakeholders support AEMO's proposed amendments to clause 5.7.3 to refer to schedule 5 plant in respect of AEMO's ability to request compliance tests for registered plant?**

We support the proposed amendment to extend AEMO's testing rights to schedule 5 plant, provided the requirements recognize the fundamental differences between load and generation testing. For data centres, compliance testing should leverage existing monitoring systems and operational data where possible, as data centre operators typically manage multiple sites across international jurisdictions with standardized monitoring and operational systems already in place. This approach would allow for efficient compliance verification while maintaining operational consistency across our facilities.

#### **2. Do stakeholders support AEMO's proposed changes to clauses 5.7.2 and 5.7.3 to extend the rights for testing of power system plant to apply to non-registered schedule 5 plant?**

We support this extension with important qualifications:

- Testing procedures must be agreed between participants as per clause 5.7.2(e)
- Tests that may cause outages must be coordinated with AEMO per clause 5.7.2(b)
- Testing must be conducted only by persons with relevant skills and experience per clause 5.7.2(f)
- Cost allocation principles in clause 5.7.2(d) should be defined for non-registered participants

#### **3. Do stakeholders support AEMO's proposed changes to the NER to extend the requirement for coordinating commissioning procedures for non-registered schedule 5 plants with a maximum capacity equal to or greater than 30MW or 30MVA?**

The proposed new clause 5.8.1A appropriately allows AEMO to exempt facilities where, after consulting with the NSP, it determines the plant would not affect power system security. However, we recommend clear guidelines for:

- How AEMO will assess the "expected effect on power system security"
- The consultation process with Network Service Providers

## Appendix A – Response to Consultation Questions

- Timeframes for decision-making on exemptions

### **4. Should the Commission consider extending enforceability and compliance requirements under rules 4.14 and 4.15 to all 'schedule 5 participants', which includes non-registered participants?**

We do not believe that additional enforcement mechanisms are necessary for non-registered participants, and there have been no indications to date to suggest that such measures are needed, given the comprehensive compliance framework already established in clauses 5.7 and 5.8, including civil penalty provisions.

### **5. Do stakeholders have any concerns or suggestions in relation to this element of AEMO's proposed rule? If so, please describe your concerns and any related suggestions and reasoning.**

We recommend:

- Clarifying the interaction between clauses 5.7.2 testing rights and 5.8 commissioning requirements
- Ensuring consistency in terminology between "schedule 5 plant" and "schedule 5 participant"
- Establishing clear protocols for test result sharing and reporting as required by clause 5.7.2(i)
- Protecting commercially sensitive information while meeting reporting obligations
- Setting clear qualification requirements for testing personnel
- Developing coordinated testing procedures with AEMO and NSPs

## **Question 13: Extension of time for complex issues in future access standards reviews**

**In relation to AEMO's proposal to amend clause 5.2.6A of the NER to allow flexibility for extending the time limit for completing each review:**

### **1. Do stakeholders agree that the requirement to complete each review within 12 months of the approach paper being published is too inflexible or may inhibit proper analysis and consultation?**

The current 12-month timeframe in clause 5.2.6A(e) may not allow sufficient time for proper analysis of complex technical requirements, particularly given AEMO must:

- Consider changes in power system conditions
- Account for evolving technology capabilities
- Conduct meaningful stakeholder consultation
- Develop detailed technical recommendations

### **2. Do stakeholders consider that AEMO should be responsible for setting a new date for publication of the final report? Is there an alternative approach that would better address the issue?**

Yes. The proposed clause 5.2.6A(f) appropriately allows AEMO to extend timeframes where necessary due to:

- Issues of complexity or difficulty
- Material changes in circumstances

### **3. Do stakeholders agree that AEMO should publish a notice when an extension is needed, outlining the reasons as they may relate to complexity/difficulty, or a material change in circumstances?**

We agree that AEMO should be required to publish a notice before the expiry of any time limit, clearly specify the new publication date, and provide detailed reasons for the extension, whether these relate to complexity, difficulty, or material changes in circumstances. This approach provides appropriate transparency and accountability while allowing sufficient flexibility to address complex technical matters.

### **4. Do stakeholders have any concerns or suggestions in relation to this element of AEMO's proposed rule? If so, please describe your concerns and any related suggestions and reasoning?**

We recommend:

- Ensuring extensions don't delay critical technical requirement updates
- Maintaining consultation requirements during extended review periods
- Considering interim measures where necessary
- Providing regular progress updates during extended timeframes

## Appendix A – Response to Consultation Questions

### **Question 14: Assessment framework**

**Do you agree with the proposed assessment criteria? Are there additional criteria that the Commission should consider or criteria included here that are not relevant?**

We support the AEMC's proposed assessment criteria of:

1. Safety, security and reliability
2. Innovation and flexibility
3. Implementation considerations

However, we recommend enhancing these criteria to specifically consider:

Cost-benefit balance:

- Recognition of implementation costs for critical infrastructure
- Consideration of system security benefits versus compliance burden
- Assessment of impacts on investment certainty
- Evaluation of market efficiency outcomes

Technology evolution:

- Ability to accommodate emerging technologies
- Flexibility to adapt to changing load characteristics
- Support for innovation in system security solutions
- Recognition of different technology capabilities

Practical implementation:

- Clear transition arrangements
- Reasonable timeframes for compliance
- Protection of critical infrastructure operations
- Consistency across different NSPs

These enhancements would help ensure the assessment framework appropriately balances system security needs with practical implementation considerations for data centre infrastructure.