Submission to the Australian Energy Market Commission

Improving the NEM Access Standards – Package 2

Reference: ERC0394

Submission type: Response to Draft Determination of 12 March 2026

Date of submission: 7 May 2026

Submitted by

Canus Technologies

Author and signatory: Siddharth Bedre, Founder

Contact email: research@canus.io

Web: www.canus.io

Contact details are provided for AEMC correspondence and industry engagement. This submission is non-confidential and may be published in full.

1. Executive Summary

Canus Technologies welcomes the opportunity to respond to the AEMC's draft determination on Improving the NEM Access Standards – Package 2 (ERC0394). We support the AEMC's direction. The proposed tiering of large load connections, the strengthened access standards for large inverter-based loads, the disturbance ride-through and recovery obligations, and the alignment with international precedents in Texas, Ireland and Finland are all timely and well-grounded.

Our submission focuses on a single additional point. Strong technical performance standards answer the question of what an asset should do. An equally important question, particularly for large computational loads connecting under fast-evolving operating regimes, is how that behaviour is to be verified. The first question is addressed substantively by the draft rule. The second question, which sits at the level of evidence rather than performance, will be resolved primarily in the implementation pathway and in the AEMO interim guidelines that follow.

We submit that the final rule and the supporting AEMO guidance would benefit from three evidentiary principles:

1. Technology neutrality. The framework should not lock in any single vendor, tool, or mechanism for the purposes of visibility, compliance evidence, or ongoing assurance.
2. Recognition of an independent measurement-based evidence pathway. Where operational claims materially affect system security, connection assessment, demand flexibility, or market confidence, the framework should permit independent measurement-based evidence as a recognised pathway, alongside operator-attested telemetry.
3. Boundary-aware design and data minimisation. Visibility and compliance evidence should be designed to verify electrical behaviour at clearly identified electrical boundaries, without requiring disclosure of commercially sensitive workload, customer, model, or operational data.

These principles do not displace the AEMC's proposed technical standards. They sit alongside them, and they help to ensure that the standards remain workable as large computational loads, on-site generation, storage and flexible operation increasingly combine within a single connection point.

We also note a positive framing point. Australia has a substantial opportunity to lead globally on trusted AI energy infrastructure by aligning data-centre growth, renewable energy, battery storage, flexible demand, grid security and privacy-preserving evidence frameworks. This is not a choice between AI growth and grid security. With the right standards and the right evidence frameworks, AI infrastructure in Australia can become more predictable, more financeable, and better aligned with the renewable energy transition than it would be elsewhere.

2. About Canus Technologies

Canus Technologies is an emerging Australian technology venture focused on independent evidence frameworks for computational-load and energy-campus behaviour. We make this submission as a constructive industry voice on the technical and evidentiary aspects of the proposed access standards. Canus Technologies is not seeking endorsement of any proprietary technology, vendor-specific mechanism, or mandated commercial solution through this rule change.

3. Support for the AEMC's Direction

We support the AEMC's draft determination. In particular, we support the following elements.

First, the recognition that data centres and other large inverter-based loads are no longer passive demand. As the AEMC Chair has noted in the accompanying materials, these facilities are active grid participants whose behaviour during disturbances has the potential to affect system security across the National Electricity Market. The reference in the AEMC's materials to the July 2024 Virginia event, where 60 data centres collectively pulled approximately 1,500 MW simultaneously during a grid disturbance, is a clear illustration of why this rule change is timely.

Second, the proposed clearer classification and tiering approach for large loads, including the threshold change for large inverter-based loads at distribution from 5 MW to 30 MW. A clear, codified definition embedded in the National Electricity Rules supports investment certainty, consistent NSP assessment, and proportionate application of new obligations.

Third, the proposed disturbance ride-through and recovery obligations for large inverter-based loads. The principle that facilities of system-security significance should remain connected through defined voltage and frequency disturbances and recover within defined timeframes is sound and is consistent with international practice.

Fourth, alignment with the standards proposed or in use in Texas, Ireland and Finland. International alignment reduces equipment costs, simplifies engineering, supports global supply chains, and accelerates capital deployment. It also positions Australia within a recognisable global framework for emerging large-load operators.

Fifth, improved visibility for AEMO and Network Service Providers. Visibility of large loads, particularly those whose operational behaviour can change rapidly, is a foundational input to power system operation. We support the principle that the framework should improve it.

Together, these elements make Package 2 a substantive update to NEM technical connections standards, and a necessary one for the present operating environment.

4. The Evidentiary Basis for Assessing Large Computational Loads

The AEMC's draft determination correctly identifies that large inverter-based loads, including data centres, differ from traditional industrial loads in how they interact with the grid. We note

that they also differ in another respect that is relevant to the design of the implementation framework: the predictability and observability of their behaviour.

A traditional large industrial load such as a smelter, a chlor-alkali plant or a steel mill operates within relatively narrow behavioural envelopes that are well understood by NSPs and AEMO over decades of operation. Its load profile is determined predominantly by its physical process. Its response to disturbances is determined predominantly by its mechanical and electrical configuration. Its day-to-day behaviour is comparatively stable.

A large computational load is different. Its real-time consumption is a function of software-defined workload scheduling, customer demand, model orchestration, power-management policy, cooling-loop control, and increasingly, co-located generation and storage dispatch. The behavioural envelope is substantially wider, and the rate at which behaviour can change inside that envelope is substantially faster, than for traditional industrial loads. Operating regimes can also be reconfigured by software changes that NSPs and AEMO have no inherent visibility into.

This does not make large computational loads unsafe partners on the grid. It does mean that the evidentiary basis on which their behaviour is assessed, whether at connection, in ongoing compliance, or in support of any flexible or non-firm access arrangements, needs to be designed with this difference in mind. Performance standards alone, without a credible evidence layer, would place AEMO and NSPs in a difficult position. They would have rules that say what large computational loads should do, but limited tools to verify what they actually did.

5. Recognising Independent Measurement-Based Evidence

We submit that the AEMC, AEMO, and the implementation framework would benefit from explicit recognition of independent measurement-based evidence as a pathway alongside operator-attested telemetry, in cases where operational claims materially affect system security, connection assessment, demand flexibility, or market confidence.

This recommendation is not a critique of large-load operators. It is a structural observation about how regulated infrastructure markets function elsewhere. Across electricity settlement (including the FERC, ERCOT and ESO contexts), and across aviation and financial services, third-party measurement and verification is a standard feature of trustworthy operation rather than a sign of distrust. It reduces dispute, lowers audit costs, and provides regulators and counterparties with evidence that does not depend solely on the assurances of the regulated entity. Operators benefit because reliable performance becomes externally verifiable, which materially improves their ability to access flexible connection arrangements, capital, insurance, and bilateral counterparty trust.

Recognition of an independent evidence pathway in the NEM access standards framework would not displace operator telemetry. It would sit alongside it. It would also not be mandatory in all cases. Where operational claims are not material to system security, lighter-touch reliance on operator-attested data remains entirely appropriate.

The pathway we are describing is at the level of principle. We are not advocating any specific technology, vendor, or measurement architecture. We are advocating that the framework leave room for independent measurement-based evidence to be used where it adds value, and that AEMO interim guidelines explicitly contemplate this possibility as the technical detail of the rule is implemented.

6. Boundary-Aware Evidence and Data Minimisation

A practical concern arises whenever visibility and compliance evidence frameworks are extended to data-centre operators and other large computational-load operators. The concern is that operational visibility could, in implementation, require disclosure of commercially sensitive information about workloads, customers, models, scheduling, or internal architecture.

This concern is genuine and it is also avoidable. Electrical behaviour at the connection point, which is the parameter that matters for system security, does not require knowledge of the underlying compute that produced it. Frameworks can be designed so that visibility and compliance evidence verify what is happening electrically, without requiring exposure of what is happening computationally.

We therefore suggest that the AEMC, AEMO and NSPs encourage evidence frameworks that are explicitly boundary-aware. By boundary-aware we mean that any visibility or compliance instrument should clearly identify the electrical boundary at which behaviour is being observed or verified. Examples include the connection point to the network, the boundary between behind-the-meter generation or storage and grid supply, and the boundary at which a flexible operating arrangement is being measured. Different boundaries answer different questions, and confusion between them creates audit and dispute risk.

Boundary-aware design supports two objectives at once. It gives NSPs, AEMO and counterparties the visibility they need into electrical behaviour. It also allows that visibility to be obtained without forcing disclosure of compute-related information that is properly the operator's commercial concern. This approach is consistent with Australian privacy expectations, with international approaches to data minimisation in regulated industries, and with the practical reality that many global data-centre operators will be hesitant to invest in jurisdictions that require disclosure of sensitive workload information as a condition of grid access.

7. Combined Compute, Renewables, Storage and Grid Behaviour

Australia's emerging energy advantage may come from combining renewable generation, battery storage, flexible demand and digital infrastructure on the same site. We are observing the early formation of integrated facilities that combine large computational load with on-site solar, behind-the-meter batteries, backup generation, demand-flexibility arrangements, bilateral PPAs, and in some cases participation in demand response or grid-support services.

Such facilities are not adequately described as either pure loads or pure generators in the traditional sense. The behaviour seen at their connection point is a composite of underlying compute load, on-site generation dispatch, storage state-of-charge management, flexible operating commitments, and the facility's response to internal and external signals. The behavioural envelope is wider still than for a purely grid-supplied data centre, and the relationship between the underlying compute load and the net connection-point behaviour can be entirely reshaped by changes in storage dispatch policy or generation availability.

The implementation framework would benefit from anticipating this. We suggest that the final rule, and the AEMO interim guidelines that follow, distinguish where relevant between site-level net behaviour (what the connection point sees) and underlying load behaviour (what the compute is doing). For most system-security purposes, site-level net behaviour is what matters. For some purposes, distinguishing the two becomes important. An example is the case of evaluating whether a flexible operating commitment is being honoured by underlying compute response, rather than masked by storage discharge.

This is a framework design point rather than a request for specific rule text. The principle is that an evidence framework which cannot distinguish between site-level net and underlying load behaviour will, over time, become brittle as integrated computational facilities grow.

8. Flexible Access and Demand Flexibility

The AEMC's broader work, and AEMO's operating context, increasingly contemplate flexible or non-firm access arrangements for large loads as a tool for managing system security and accelerating connection timelines. We support this direction. Flexible arrangements, properly evidenced, can allow large loads to connect faster, at lower network cost, and with less marginal stress on system security than firm-access arrangements with comparable nameplate capacity.

The viability of flexible access arrangements depends critically on the credibility of the evidence that the agreed operational behaviour is in fact occurring. If a large computational load commits to curtailing during defined system conditions, the value of that commitment to AEMO, the NSP, the counterparty, and the broader system depends on whether the curtailment can be verified, ideally without lengthy ex post audit, dispute, or reliance solely on the operator's self-report.

Independent measurement-based evidence reduces dispute and audit cost. It also makes flexible-access arrangements more financeable. A lender, an insurer, or a PPA counterparty can rely on the same evidence that the NSP and AEMO rely on, rather than negotiating bespoke verification mechanisms with each operator. For these reasons we suggest that the framework permit independent evidence to support flexible access and demand-flexibility arrangements, and that AEMO interim guidelines on assessment leave clear room for it.

9. Recommended Changes or Additions

Our specific recommendations are as follows.

a. That the final rule preserve technology neutrality on visibility and compliance evidence. The rule should not specify a particular vendor, instrument class, telemetry protocol, or attestation mechanism as a condition of compliance. The rule should specify what must be evidenced, not how it must be evidenced.

b. That AEMO interim guidelines, when published, explicitly contemplate independent measurement-based evidence as a recognised pathway for visibility, ongoing compliance, and supporting evidence in connection assessment. This is a recognition at the level of principle, not a mandate.

c. That AEMO interim guidelines and any consequential NSP processes adopt a boundary-aware design. Visibility and compliance instruments should clearly identify the electrical boundary at which behaviour is being observed or verified. This reduces ambiguity, audit cost, and dispute risk.

d. That the implementation framework distinguish where relevant between site-level net behaviour and underlying load behaviour, in recognition of the emergence of integrated facilities combining compute, generation, storage and flexible operation.

e. That the framework permit independent measurement-based evidence to support flexible access and demand-flexibility arrangements, recognising that the value of such arrangements is in part a function of the credibility of the evidence that supports them.

f. That the design of any evidence requirements adhere to the principle of data minimisation. Operators of large computational loads should not be required to disclose commercially sensitive workload, customer, model, or operational data in order to meet visibility or compliance obligations whose actual purpose is to verify electrical behaviour.

g. That the application of new obligations remain proportionate. Light-touch arrangements remain appropriate for loads whose size, connection point, technology mix, or system-security impact does not justify additional rigour. The 30 MW threshold is a sensible starting point for that proportionality, and we support its codification in the National Electricity Rules.

10. Conclusion

The draft determination is timely, well-reasoned, and substantively correct. We support it. Our submission has sought only to add an additional observation. The standards layer is most effective when it is paired with a clear, technology-neutral, boundary-aware evidence layer that respects data minimisation and that recognises independent measurement-based evidence as a permitted pathway.

Australia is well placed for the next phase of this work. The country has world-class renewable resource, leading battery deployment, strong grid governance, an established energy regulator framework, and growing interest from global AI infrastructure operators. With the right rules and the right evidence frameworks, Australia can become a global leader in trusted AI energy infrastructure, with facilities whose behaviour is predictable, financeable, and

verifiable, and which advance rather than obstruct the renewable transition. This is not a trade-off between AI growth and grid security. Both can advance together, supported by frameworks that the AEMC is well placed to shape.

We thank the AEMC for the consultation, and we would welcome the opportunity to engage further as the final determination and AEMO interim guidelines are developed.

Yours sincerely,

Siddharth Bedre
Founder, Canus Technologies
7 May 2026