



PERSONAL SUBMISSION

Submission to the Senate Inquiry into Artificial Intelligence and Data Centres

SUBMITTED BY	Zen Dodd
SUBMITTED	22 Jun 2026
RECIPIENT	Senate Environment and Communications References Committee
DOCUMENT	Senate AI and data centres inquiry

1. Introduction

I make this submission in my personal capacity.

I am a Queensland-based infrastructure and security practitioner, open-source maintainer and technical writer. My interest in this inquiry concerns the implementation layer with how public claims about innovation, sustainability, security and economic benefit are translated into infrastructure, contracts, operating requirements and evidence.

The Senate referred this inquiry on 13 May 2026. Its terms cover the effectiveness of existing regulatory frameworks, current and future government arrangements with global AI companies and the effects of Artificial Intelligence and Data Centres on communities, industries, the environment, water and energy.

Australia should pursue useful artificial intelligence, research computing, cloud capability and secure digital infrastructure. Public policy should remain capable of distinguishing those benefits from the proposition that every proposed facility, subsidy or government agreement necessarily serves the national interest.

The appropriate standard is evidence.

A project seeking electricity capacity, water access, expedited approval, government procurement or public financial support should explain:

- what will be built;
- what resources it will require;
- what infrastructure it will depend upon;
- which costs it will fund;
- which risks it will create;
- which benefits will remain in Australia;
- how performance will be measured; and
- what happens if the project fails to deliver.

2. Data centres are consequential infrastructure

Data centres are essential to modern digital life. They provide processing, storage and network capacity for communications, banking, government services, business systems, health, research, entertainment and security. Their physical form may make them appear similar to warehouses or ordinary industrial buildings. Their operational characteristics are materially different.

A large data centre may combine:

- continuous and high-density electricity demand;
- complex cooling and water systems;
- large uninterruptible power supplies;
- backup generation and fuel storage;
- high-capacity fibre connections;
- restricted physical access;
- concentrated digital services;
- valuable data and computing equipment;
- foreign ownership or control;

- interdependence with critical services; and
- rapid changes in load as customer demand grows.

The International Energy Agency estimates that an AI-focused hyperscale data centre can consume electricity comparable to 100,000 households, while the largest facilities currently under construction could consume as much electricity as 2 million households. In its Base Case, it expects global data centre electricity consumption to increase from approximately 415 terawatt-hours in 2024 to approximately 945 terawatt-hours in 2030. These comparisons should not be mechanically transferred to every Australian project but they illustrate the industrial scale involved.

Australian projections also show rapid growth. AEMO-commissioned research estimates that data centre electricity use increased by approximately 15 per cent annually between the 2018 and 2025 financial years, reaching 3.9 terawatt-hours and 2.2 per cent of NEM-supplied electricity in 2025. The modelled 2030 range is wide because future projects, AI adoption, efficiency improvements and load ramp-up are uncertain.

This uncertainty does not justify either unrestricted approval or blanket prohibition. It justifies staged decisions, measurable milestones, reliable forecasts and obligations that grow with actual impact.

2.1 Regulation should be impact-based

The physical infrastructure effects of a facility do not depend entirely on whether its operator calls the workload artificial intelligence, cloud computing, high-performance computing, digital services or enterprise hosting.

A national framework should therefore regulate major facilities according to:

- maximum and expected electricity demand;
- annual energy consumption;
- water demand;
- land and network impacts;
- public assistance;
- critical-service concentration;
- ownership and control;
- environmental risk; and
- cumulative regional effects.

AI-specific conditions remain appropriate where a government agreement makes claims about AI capability, research, innovation or national benefit. The baseline infrastructure requirements should remain technologically neutral so that projects cannot avoid obligations through workload classification.

2.2 Scale and concentration matter

A data centre load may be relatively small at national level while being highly consequential within a particular network, water system or region.

The IEA notes that local effects can be substantially greater than global averages because data centre capacity is geographically concentrated. AEMO similarly states that predictable operation of large loads such as data centres will affect power-system needs and that reforms improving the predictability of these loads will be important.

Project assessment should therefore examine:

- the local network and substation;
- the relevant generation and transmission outlook;
- competing industrial and residential demand;

- the water catchment and utility;
- concentration of data centres within one precinct;
- geographic concentration of nationally important digital services; and
- the consequences of simultaneous connection, disconnection or failure.

3. Existing regulatory frameworks are important but fragmented

Australia does not begin from a regulatory vacuum. Several existing frameworks address legitimate parts of the issue.

3.1 Planning and environmental law

State and territory planning systems assess matters such as land use, development design, traffic, construction, noise and local environmental effects.

The Commonwealth's Environment Protection and Biodiversity Conservation Act 1999 is Australia's principal national environmental law. Its assessment system focuses on actions affecting nationally protected matters, Commonwealth land and certain Commonwealth actions. This remains essential but it is not a general national framework for every energy, water, infrastructure or community effect of large data centres.

A development can therefore avoid triggering a major Commonwealth environmental assessment while still imposing material cumulative demands on a metropolitan electricity or water system.

3.2 Energy and emissions reporting

The National Greenhouse and Energy Reporting Scheme provides a national framework for reporting company greenhouse emissions, energy production and energy consumption. Companies exceeding prescribed thresholds must register and report annually. This is valuable national data.

NGER does not by itself answer all questions relevant to a particular data centre including:

- local network augmentation;
- temporal matching of renewable electricity;
- water demand;
- operational energy efficiency;
- staged load forecasts;
- public financial support;
- community impacts;
- digital-service concentration; and
- whether project-specific obligations have been met.

3.3 Operational efficiency

NABERS provides operational energy ratings for Australian data centres based on actual performance rather than design estimates. It uses Power Usage Effectiveness and supports separate ratings for IT equipment, infrastructure and whole facilities. This structure is useful because responsibility may be divided between facility operators and tenants.

NABERS should form part of the national framework. A rating scheme alone does not allocate grid costs, assess water scarcity, govern public subsidies or establish cyber resilience.

3.4 Critical infrastructure security

The Security of Critical Infrastructure Act 2018 expressly includes critical data storage or processing assets. Depending on the asset and applicable rules, the Act can require registration, risk-management programmes, annual reporting, cyber-incident reporting and additional enhanced obligations. The Critical Infrastructure Security Centre administers the Act and has powers relating to asset reporting, risk programmes, information gathering and ministerial directions.

This framework should remain authoritative for national-security and protected critical-infrastructure information.

The SOCI register is not public, appropriately reflecting the sensitivity of some information. A separate public register can disclose resource use, approvals, public support and performance without exposing protected critical-infrastructure details.

3.5 Electricity planning and connection

AEMO and network service providers already forecast and manage large loads. AEMO's 2025 Electricity Statement of Opportunities states that predictable operation of emerging large loads will influence power-system requirements. It also identifies a need for mechanisms and reforms that improve technical visibility and unlock useful demand flexibility.

The AEMO-commissioned data centre report also notes that project pipelines and connection requests can include duplicate bids, projects that do not reach investment decisions and landholders seeking capacity without a purchaser or anchor tenant. This reinforces the need for milestone-based reservations and release of unused capacity.

3.6 The resulting gap

Each existing framework has a different purpose. None should be displaced casually. The policy gap lies between them. Australia needs a common, public and evidence-based account of major data centre developments that connects:

- approval;
- electricity;
- water;
- environment;
- emissions;
- cyber resilience;
- ownership;
- public assistance;
- local benefit;
- performance; and
- decommissioning.

4. A National Data Centre Infrastructure Framework ---

The Commonwealth should establish a national framework in cooperation with states and territories. The objective should be nationally consistent minimum evidence and performance standards while preserving state and territory roles in planning, utilities and local development.

4.1 Materiality thresholds

Thresholds should be defined following technical consultation. They should consider:

- requested and contracted maximum demand;
- expected annual consumption;
- water demand;
- area and development scale;
- use of public infrastructure;
- public financial support;
- critical-service dependency;
- control over sensitive Australian data; and
- cumulative development in the same region.

A single electricity threshold may not capture every relevant risk. A facility with moderate power demand could still be significant because it hosts critical services, consumes scarce water or receives substantial public assistance.

Obligations should scale with materiality. For example:

- small facilities could remain subject to ordinary planning and utility requirements;
- medium facilities could have standardised reporting obligations;
- major facilities could require independent resource and resilience assessment; and
- nationally significant or publicly supported facilities could face enhanced public-benefit, cyber security and parliamentary transparency requirements.

4.2 Staged approvals

Major projects are often developed over several buildings and many years. Their contracted capacity can substantially exceed early operational load. Approvals and infrastructure reservations should be staged against evidence such as:

- secured land;
- planning approval;
- final investment decision;
- customer commitments;
- equipment procurement;
- construction progress;
- commissioning; and
- demonstrated load ramp-up.

This would reduce speculative reservation of scarce capacity while allowing credible projects to plan confidently.

4.3 One evidence package, multiple regulators

The framework should create a common data model so that an operator can submit core evidence once. Different authorities would retain their functions:

- planning agencies assess land and development;
- environmental authorities assess protected matters and conditions;
- utilities assess water and local infrastructure;
- AEMO and networks assess electricity;
- the Clean Energy Regulator assesses NGER obligations;
- Home Affairs administers SOCI obligations;

- procurement bodies assess government contracts; and
- competition authorities assess market effects.

Regulators should be authorised to reuse verified information rather than require inconsistent versions of the same evidence.

5. Electricity, additionality and system responsibility ---

Electricity is likely to be the most immediate constraint on data centre growth. Australia's electricity system is already managing:

- retirement of large synchronous generators;
- rapid renewable deployment;
- storage and transmission requirements;
- electrification of transport and industry;
- increasing distributed energy resources; and
- system-strength and operability challenges.

AEMO's 2025 outlook states that new generation, storage, transmission and coordinated demand resources will be required to meet growing demand and maintain reliability.

5.1 Data centres should pay attributable infrastructure costs

Where a data centre requires:

- a new substation;
- transmission or distribution augmentation;
- protection-system changes;
- system-strength services;
- telecommunications works;
- emergency-service infrastructure; or
- dedicated generation or storage,

the operator should fund the proportion fairly attributable to the project.

Costs should not be transferred to residential consumers or smaller businesses merely because the project is characterised as strategically important.

Public funding may be justified where Parliament or government identifies a genuine public benefit. That support should be explicit, valued and conditional rather than hidden within general network charges.

5.2 Renewable-energy claims need more precision

An operator may purchase renewable-energy certificates or enter power-purchase agreements equal to annual electricity use. This may support renewable investment.

Annual matching does not establish that:

- the facility is supplied by renewable generation at each hour;
- the renewable generation is located where it relieves the relevant constraint;
- local transmission and distribution capacity is sufficient;
- storage or firming is available;
- the claimed generation is additional; or
- network costs are avoided.

Public reporting should therefore distinguish:

1. annual contractual or certificate matching;
2. new generation enabled by the project;
3. geographic relationship between generation and load;
4. temporal matching;
5. storage and firming;
6. grid-supplied residual electricity; and
7. direct fossil-fuel use including backup generation.

The aim should be truthful accounting rather than a single perfect metric.

5.3 Additionality

A major new load should contribute to new supply and system capability. Acceptable contributions may include:

- financing new renewable generation;
- storage;
- dispatchable low-emissions capacity;
- transmission or distribution augmentation;
- demand flexibility;
- system services; and
- investment in the relevant local network.

The framework should prevent double counting where multiple entities claim the same generation or certificate.

5.4 Demand flexibility

Some workloads can be shifted, slowed or scheduled without affecting essential services. Others require continuous operation. Operators should assess workloads by criticality and identify what proportion can:

- reduce demand;
- shift geographically;
- defer non-urgent computing;
- use stored energy;
- participate in demand response; or
- support controlled recovery after a grid disturbance.

Requirements should remain technically realistic. A hospital service, emergency system or financial platform should not be curtailed indiscriminately. Batch AI training, some research computing and non-urgent processing may provide greater flexibility.

The framework should reward credible flexibility while prohibiting operators from claiming capabilities that have not been tested.

5.5 Operational visibility

AEMO and relevant network operators should receive appropriate real-time or scheduled information about:

- demand;
- ramp rates;
- planned maintenance;

- backup operation;
- connection status;
- demand-response availability; and
- material changes in expected load.

This information may require confidentiality. Electricity-system operators still need sufficient visibility to manage large and concentrated loads safely.

6. Water, cooling and environmental effects

Data centre water demand varies materially by cooling design, climate, operating density and electricity source. IEA analysis also links direct and indirect water demand to cooling technology, electricity supply, chip manufacturing and the distinction between withdrawals and consumption.

Water policy should avoid two errors:

1. assuming every data centre has the same water demand; and
2. treating water use as immaterial because the facility is part of a digital industry.

6.1 Withdrawal and consumption

Public reporting should distinguish:

- water withdrawn from a source;
- water consumed and not returned;
- water discharged;
- water lost through evaporation;
- water incorporated into treatment or cooling processes; and
- indirect water use associated with electricity generation.

Annual totals alone may conceal seasonal pressure. A facility's peak demand during a heatwave or drought may be more important to the local system than its yearly average.

6.2 Source hierarchy

Operators should assess whether cooling and ancillary uses can rely on:

- recycled water;
- treated wastewater;
- captured stormwater;
- rainwater;
- non-potable sources; or
- closed-loop systems.

Potable water should remain available where alternatives are technically unsuitable, unsafe or disproportionately damaging. The operator should explain why potable supply is required and how demand will be managed during scarcity.

6.3 Energy-water trade-offs

Power Usage Effectiveness and Water Usage Effectiveness should be reported together.

An air-cooled system may reduce direct water consumption while increasing electricity demand. Evaporative cooling may improve energy efficiency while increasing water consumption. The best design depends on local temperature, humidity, water scarcity, electricity emissions and network capacity.

Regulation should require evidence and performance outcomes rather than mandate one technology nationally.

6.4 Cumulative assessment

A project-by-project assessment may find that each individual facility is manageable while failing to assess the cumulative effect of an entire data centre precinct.

Planning and water authorities should model:

- approved projects;
- proposed projects;
- credible expansion stages;
- residential growth;
- other industrial users;
- drought scenarios;
- climate projections; and
- emergency requirements.

Infrastructure capacity should be reserved transparently and reviewed when projects do not proceed.

6.5 Backup generation and local pollution

Large facilities may operate substantial diesel or gas backup generation during testing and outages. Assessment should include:

- number and capacity of generators;
- fuel storage;
- testing frequency;
- expected emissions;
- noise;
- local air-quality effects;
- emergency fuel access;
- spill risk; and
- transition to lower-emissions backup options where feasible.

Backup generators should not be treated as irrelevant merely because they operate infrequently.

6.6 Equipment lifecycle

Accelerators, servers, batteries, cooling equipment and power systems have finite lives. Major operators should maintain plans for:

- safe equipment reuse;
- recycling;
- secure media destruction;
- battery handling;
- hazardous materials;
- electronic waste;
- decommissioning; and
- restoration of the site.

Where long-term remediation risk is material, financial assurance should be considered.

7. Transparency and operational evidence

Public confidence will not be sustained by general promises that facilities will be “green”, “sovereign”, “world-class” or “job creating”. Commitments should be specific and verifiable.

7.1 Public register

A national register should link each major facility to:

- approval decisions;
- environmental conditions;
- electricity and water commitments;
- public assistance;
- annual performance reports;
- compliance actions; and
- community-benefit obligations.

The register should provide machine-readable data as well as accessible summaries.

7.2 Design claims and operational results

Planning applications necessarily rely on forecasts. Annual reporting should later compare forecasts with actual performance. Material differences should be explained for:

- electricity demand;
- water use;
- emissions;
- energy efficiency;
- construction timetable;
- permanent jobs;
- local procurement;
- renewable-energy commitments; and
- community contributions.

A project should not be penalised merely because a reasonable forecast changed. Persistent, unexplained or strategically misleading discrepancies should trigger review.

7.3 Independent assurance

Major reports should be subject to independent assurance proportionate to risk. The assurance provider should verify:

- data sources;
- metering boundaries;
- calculation methods;
- renewable-energy claims;
- water reporting;
- performance against conditions; and
- material limitations.

Audit should test evidence rather than reproduce operator statements.

7.4 Security-sensitive information

Transparency must not create a security directory.

Public reporting should exclude or aggregate:

- exact network diagrams;
- security-system layouts;
- privileged-access arrangements;
- tenant identities where confidential;
- exploitable vulnerabilities;
- precise capacity allocations for sensitive services;
- incident indicators under active investigation; and
- protected SOCI information.

Regulators and authorised security bodies should receive more detailed confidential information.

8. Cyber security, resilience and critical services

Data centres form part of the physical and digital supply chains supporting Australian institutions. Resilience requires more than guards, fences and backup generators.

8.1 Shared responsibility

In a colocation facility:

- the facility operator may control power, cooling and physical security;
- a cloud provider may control servers, virtualisation and control planes;
- customers may control identities, applications and data;
- subcontractors may maintain hardware or building systems; and
- overseas teams may administer software remotely.

Risk-management obligations should identify responsibilities clearly. Gaps between operator, tenant, cloud provider and customer controls are themselves a source of risk.

8.2 Concentration risk

Policy should assess concentration across:

- provider;
- physical campus;
- metropolitan region;
- electricity network;
- water system;
- fibre route;
- identity provider;
- cloud control plane;
- equipment supplier; and
- foreign jurisdiction.

A collection of individually resilient facilities may still create systemic risk where many services depend upon the same hidden control plane, network route or supplier.

8.3 Tested recovery

Operators and major tenants should demonstrate:

- recovery-time and recovery-point objectives;
- restoration of control systems;
- backup integrity;
- alternate communications;
- manual operating procedures;
- fuel and spare-part access;
- regional failover;
- recovery from identity compromise;
- response to malicious software updates;
- response to insider activity; and
- secure recovery where primary management systems cannot be trusted.

Exercises should include plausible multi-system failures rather than test only the loss of one component.

8.4 Supply-chain security

Data centre assurance should address:

- firmware and management controllers;
- network equipment;
- cooling and building-management systems;
- uninterruptible power systems;
- backup generators;
- remote vendor access;
- hardware provenance;
- software updates;
- monitoring agents;
- contractors;
- maintenance laptops; and
- end-of-life equipment.

Security requirements should remain outcome-focused and compatible with existing SOCI obligations.

8.5 Incident reporting

Where the SOCI Act already requires reporting, the national framework should reuse those mechanisms.

Additional non-sensitive public reporting may be appropriate for incidents causing:

- major service interruption;
- material environmental harm;
- significant backup-generator use;
- prolonged water or electricity disruption; or
- failure to meet approval conditions.

Public summaries should be delayed or limited where immediate disclosure would increase security risk.

9. Government agreements with global AI and cloud companies

Government agreements deserve scrutiny because they may allocate scarce public resources and determine long-term technology dependence.

9.1 What constitutes public support

Public support can include:

- grants;
- tax concessions;
- concessional finance;
- government land;
- infrastructure construction;
- guaranteed procurement;
- minimum-spend commitments;
- priority electricity or water access;
- expedited approvals;
- access to public datasets;
- favourable planning treatment; and
- assumption of project risks by government entities.

All material forms should be valued and disclosed.

9.2 Public-interest assessment

Before a material agreement is signed, government should explain:

- the problem being solved;
- why the selected company or model is appropriate;
- alternatives considered;
- expected Australian benefits;
- costs and opportunity costs;
- resource requirements;
- ownership and jurisdiction;
- competition effects;
- data and security controls;
- implementation milestones;
- termination rights; and
- how the public will know whether the arrangement succeeded.

The assessment should distinguish national capability from private capacity merely located in Australia.

9.3 Local economic benefit

Claims about jobs and investment should separate:

- temporary construction employment;

- ongoing operational employment;
- direct employment;
- contractors;
- local procurement;
- imported equipment;
- Australian intellectual property;
- Australian research capability;
- tax paid in Australia; and
- value ultimately transferred overseas.

Large capital expenditure does not automatically imply proportionate permanent employment or public benefit.

9.4 Performance and clawback

Public support should be conditional. Agreements should contain:

- measurable milestones;
- reporting;
- independent audit;
- repayment or clawback where commitments are not met;
- consequences for material misrepresentation;
- change-of-control provisions;
- termination rights; and
- transition arrangements.

Governments should avoid arrangements in which public infrastructure is built for a project while the company retains complete discretion to delay, reduce or abandon its commitments.

9.5 Transparency and commercial confidentiality

Some commercial and security information requires protection but any redactions should be:

- narrowly scoped;
- accompanied by a stated reason;
- reviewed after a defined period; and
- incapable of concealing the total public cost, core obligations or measures of success.

The principal agreement, public-interest assessment and performance reports should be tabled or published wherever lawful.

10. Sovereignty, competition and exit

A data centre situated in Australia may still depend on foreign:

- ownership;
- legal jurisdiction;
- software;
- encryption-key systems;
- remote administrators;
- identity services;

- hardware;
- firmware;
- supply chains; and
- corporate decision-making.

Sovereignty should be assessed as a set of operational controls rather than a geographic label.

10.1 Government data and sensitive services

Government contracts should specify:

- where data is stored and processed;
- which jurisdictions may compel access;
- who controls encryption keys;
- which personnel can administer systems;
- how remote access is monitored;
- which subcontractors participate;
- incident-notification obligations;
- audit rights;
- data-export formats;
- transition assistance;
- deletion verification; and
- continuity following corporate failure or geopolitical disruption.

10.2 Avoiding lock-in

Government should retain a credible ability to change providers. Contracts should require:

- documented data exports;
- open or standard interfaces where feasible;
- current architecture and dependency records;
- reasonable transition periods;
- migration assistance;
- testing of exit procedures;
- transparent egress charges; and
- preservation of public records.

Multi-provider architecture should not be required where it adds disproportionate complexity. The government should still understand and accept the risks of provider concentration.

10.3 Publicly supported compute

Where a project receives substantial public assistance, government should consider whether part of the resulting capability should support:

- Australian universities;
- public research;
- startups;
- small and medium businesses;
- safety and assurance research;
- public-interest technology;
- skills development; or

- nationally important scientific work.

These commitments should be specific, time-limited and measurable.

11. Communities, industry and fair burden-sharing

Data centre policy should protect communities without assuming that every local concern requires national prohibition.

11.1 Early disclosure

Public consultation should occur before:

- electricity capacity is effectively reserved;
- government support is committed;
- major water infrastructure is designed;
- land is compulsorily acquired;
- approvals are expedited; or
- a precinct becomes dependent upon a project.

Consultation after the decisive commitments have been made is procedurally weak.

11.2 Community impacts

Assessment should cover:

- construction traffic;
- noise;
- generator testing;
- visual and land-use effects;
- water competition;
- electricity infrastructure;
- emergency risks;
- local housing pressure;
- employment;
- public access to information; and
- cumulative industrial development.

11.3 Traditional Owners

Where a project affects Country, water, cultural heritage or land of significance to Aboriginal and Torres Strait Islander peoples, engagement should occur early and in good faith. Indigenous knowledge should not be used symbolically or extracted without permission. Relevant communities should have access to technical information, appropriate resourcing and a meaningful role in decisions affecting Country.

11.4 Community benefit

A community-benefit agreement may be appropriate where a project:

- receives public support;
- imposes substantial local infrastructure costs;
- consumes scarce resources;
- creates persistent noise or traffic;

- requires public land; or
- materially changes the local industrial environment.

Benefits should respond to identified local needs. They should not operate as payment for accepting otherwise unacceptable environmental or safety risks.

11.5 Fair burden allocation

The costs of data centre growth should be assigned according to:

- responsibility;
- benefit received;
- capacity to pay;
- contribution to infrastructure demand; and
- ability to manage risk.

Households should not bear avoidable increases in network or water costs created principally by private facilities. Public support should occur through explicit policy and appropriation, not opaque cross-subsidy.

12. Innovation, investment and regulatory certainty

A strong framework can support investment. Serious investors benefit from knowing:

- what information is required;
- how connection capacity is allocated;
- what infrastructure they must fund;
- which environmental standards apply;
- how water use will be assessed;
- which cyber obligations apply;
- what public reporting is required; and
- how government support will be evaluated.

Poor regulation can take two forms:

1. rules so weak that communities, networks and political institutions resist every project; and
2. rules so uncertain or duplicative that credible projects cannot reasonably plan.

The recommended framework would establish a transparent middle path.

12.1 No blanket moratorium

This submission does not recommend a national blanket moratorium. A moratorium may be considered locally where infrastructure capacity, water scarcity or cumulative impacts make further approvals unsafe pending assessment. National policy should instead establish evidence thresholds and enforceable conditions.

12.2 Proportionality

Small edge facilities, telecommunications sites and ordinary enterprise data rooms should not face the same obligations as hyperscale campuses. The regulatory burden should increase with:

- resource consumption;
- public assistance;
- criticality;

- concentration;
- environmental effect; and
- systemic dependence.

12.3 Transition

Existing facilities should receive a reasonable transition period for new reporting and assurance requirements. Material expansions should trigger contemporary standards even where the original facility predates the framework.

12.4 Efficient approval

Projects that provide complete, independently assured evidence and meet published standards should receive more predictable assessment. Fast assessment should result from better evidence and coordination. It should not mean waiving substantive environmental, infrastructure or security review.

13. Implementation pathway

The following staged approach would allow Australia to act without creating an immediate, untested regulatory system.

Stage 1: National data and interim guidance

Within 12 months:

- establish a cross-government coordinating office;
- define preliminary materiality thresholds;
- publish standard terminology;
- create an interim project statement template;
- consolidate existing project, electricity and planning data;
- identify regulatory overlap and gaps;
- consult communities, Traditional Owners, industry, utilities and security agencies; and
- publish guidance for government agreements.

Stage 2: National reporting and approval standards

Within 24 months:

- establish the public register;
- require resource and resilience statements for new major projects;
- introduce standard annual reporting;
- establish independent assurance requirements;
- adopt milestone-based capacity-reservation principles;
- integrate NABERS, NGER and planning information; and
- implement public-interest tests for material government support.

Stage 3: Performance obligations and review

Within 36 months:

- evaluate actual project performance;
- introduce or refine minimum energy, water and resilience requirements;
- review cost allocation;

- assess competition and concentration;
- publish national and regional forecasts;
- table the first annual report; and
- begin the statutory independent review.

Lead coordination

A lead Commonwealth office should coordinate work across:

- Industry, Science and Resources;
- Climate Change, Energy, the Environment and Water;
- Home Affairs;
- Treasury;
- Finance;
- Infrastructure;
- AEMO;
- the Clean Energy Regulator;
- the Australian Energy Regulator;
- competition and consumer authorities;
- state and territory governments; and
- relevant water and planning authorities.

A new standalone regulator may not be necessary initially. Clear leadership and enforceable responsibilities are necessary.

14. Recommendations

Recommendation 1: Establish a National Data Centre Infrastructure Framework

The Australian Government should work with states and territories, AEMO, electricity and water regulators, network service providers, planning authorities, cyber security agencies, industry and community representatives to establish a nationally consistent Data Centre Infrastructure Framework.

The framework should:

1. use impact-based thresholds rather than relying on marketing categories such as “AI data centre”;
2. distinguish hyperscale and other major facilities from small enterprise, edge and telecommunications facilities;
3. coordinate planning, electricity, water, emissions, cyber security and public-benefit requirements;
4. provide proportionate transition arrangements for existing facilities;
5. apply new requirements to material expansions of existing facilities; and
6. allow information collected once to be reused by authorised regulators, reducing duplicative reporting.

The Commonwealth need not assume control of every planning decision. National minimum standards can operate through Commonwealth legislation, intergovernmental agreements, electricity-market rules, public procurement conditions and nationally consistent state and territory planning requirements.

Recommendation 2: Require a Data Centre Resource, Resilience and Public Benefit Statement

Before final approval, network capacity reservation or material public support is granted, every major data centre proposal should prepare an independently reviewed statement covering:

- ownership, control and responsible entities;
- intended facility type and broad workload categories;
- proposed development stages and credible demand ramp-up;
- maximum and expected electricity demand;
- connection point and required network augmentation;
- proposed new generation, firming and storage;
- operational flexibility and restart arrangements;
- annual and peak water withdrawals and consumption;
- water source, quality, discharge and recycling;
- cooling technology and expected energy-water trade-offs;
- greenhouse emissions including backup generation;
- land, biodiversity, noise, heat, air-quality and traffic effects;
- bushfire, flood, heatwave and other climate risks;
- fibre and telecommunications dependencies;
- physical and cyber security arrangements;
- critical-service and provider-concentration risks;
- construction and permanent employment;
- local procurement and skills commitments;
- public financial or infrastructure support;
- community-benefit commitments; and
- decommissioning, equipment disposal and site-remediation plans.

A public version should disclose material impacts and commitments. A protected annex should contain genuinely security-sensitive or commercially sensitive technical information.

Recommendation 3: Apply additionality, cost attribution and grid-coordination requirements

Large data centres should be required to fund network augmentation and other electricity infrastructure costs directly attributable to their development. Approval and connection conditions should require:

- credible load forecasts and staged capacity reservations;
- milestones for construction, commissioning and load ramp-up;
- release of unused reserved capacity where milestones are not met;
- transparent commitments to additional generation and storage;
- disclosure of the location and timing of renewable-energy matching;
- prevention of double counting;
- technical visibility for AEMO and relevant network operators;
- controlled ramping, reconnection and disconnection procedures;
- demand flexibility where technically feasible and consistent with critical-service obligations; and
- compliance with relevant system-strength, fault-ride-through and power-quality requirements.

Annual renewable-energy certificates may remain part of electricity procurement. They should not be represented as evidence that a facility is continuously supplied by new renewable generation or that it imposes no local network cost.

Recommendation 4: Introduce national water and lifecycle environmental standards

Major facilities should report water withdrawals and water consumption separately. Reporting should include:

- potable, recycled, stormwater and other sources;
- annual, monthly and peak-day demand;
- normal and extreme-weather use;
- expected demand during drought restrictions;
- water discharged or returned;
- water quality and treatment;
- efficiency measures;
- contingency and curtailment arrangements; and
- cumulative impacts on the relevant catchment and water network.

Regulators should consider energy and water together. A cooling design may reduce electricity use while increasing water consumption or reduce water use while increasing electricity demand. Approval conditions should reflect local scarcity, climate, network capacity and community needs rather than impose a single national cooling technology.

Environmental assessment should also address backup diesel generation, local air pollution, noise, waste heat, embodied emissions, equipment replacement, electronic waste, land clearing, biodiversity and decommissioning.

Recommendation 5: Establish a national public data centre register and annual operational reporting

A public register should record non-sensitive information about major facilities including:

- owner and operator;
- broad location;
- project and operational status;
- approved electricity-demand band;
- approved water-demand band;
- relevant planning decisions;
- public support received;
- annual electricity use;
- annual water withdrawals and consumption;
- operational energy-efficiency indicators;
- greenhouse emissions;
- renewable-energy and storage commitments;
- material environmental or service incidents;
- compliance outcomes; and
- progress against public-benefit commitments.

Exact physical-security details, network topology, tenant identities, vulnerabilities, sensitive capacity allocations and information protected under the critical-infrastructure regime should remain confidential.

NABERS, NGER, planning reports, electricity-market information and other existing systems should be integrated where practical. Operators should not have to submit materially identical data through multiple disconnected processes.

Recommendation 6: Strengthen cyber security, resilience and concentration-risk assurance

The Commonwealth should align the new framework with the Security of Critical Infrastructure Act 2018 and existing critical-infrastructure rules. Major facilities and strategically significant providers should be required to demonstrate:

- risk-management programmes proportionate to their role;
- tested incident-response and recovery plans;
- regular exercises involving relevant government and infrastructure bodies;
- resilience of power, cooling, telecommunications and control systems;
- supply-chain and firmware risk management;
- secure identity and privileged-access controls;
- multi-tenant isolation;
- personnel and contractor controls;
- vulnerability-management processes;
- backup and restoration arrangements;
- dependency mapping;
- secure decommissioning and media destruction; and
- plans for simultaneous, regional or provider-wide disruption.

Assessment should consider concentration across operators, geographic regions, electricity networks, fibre routes, cloud control planes and key technology suppliers.

Recommendation 7: Apply a public-interest and transparency test to government agreements

Before entering a material agreement with a global AI, cloud or data centre company, the Australian Government should publish a public-interest assessment covering:

- the purpose of the agreement;
- financial support, tax concessions or foregone revenue;
- government land or infrastructure provided;
- priority access to electricity, water or approvals;
- government procurement or minimum-purchase commitments;
- data access or data-sharing arrangements;
- expected construction and permanent employment;
- local procurement and skills transfer;
- research, startup or public-interest compute access;
- Australian taxation and economic-value assumptions;
- data jurisdiction and security arrangements;
- environmental and resource commitments;
- milestones and performance measures;
- audit and reporting rights;
- clawback and termination provisions; and

- exit and transition arrangements.

Commercial-in-confidence claims should be specific, justified and periodically reviewed. They should not prevent disclosure of the public cost, principal obligations, performance measures or consequences of non-performance.

Recommendation 8: Protect sovereignty, competition, portability and exit

Onshore infrastructure alone does not guarantee Australian control. Government procurement and supported projects should address:

- legal jurisdiction over data and systems;
- foreign government access risks;
- encryption-key control;
- remote administrative access;
- subcontractors and offshore support;
- software and hardware supply chains;
- data portability;
- open and documented interfaces;
- migration support;
- continuity if a provider exits Australia;
- insolvency or acquisition scenarios;
- fair and predictable data-export costs; and
- avoidance of unnecessary single-provider dependence.

Material public support should be conditional on measurable Australian benefits. Depending on the project, these may include research compute, startup and small-business access, skills programmes, local procurement, Australian-controlled security capability or support for public-interest research.

Recommendation 9: Require early community participation and fair allocation of costs and benefits

Communities should receive clear information before governments and utilities make decisions that are practically irreversible. Major proposals should provide:

- early public notice;
- accessible resource and impact information;
- local consultation;
- engagement with Traditional Owners where Country, land, water or heritage may be affected;
- a clear complaints and review process;
- evidence of cumulative precinct impacts;
- separation of construction employment from permanent employment claims;
- local infrastructure contributions where justified; and
- enforceable community-benefit commitments where public resources or substantial local burdens are involved.

Households and smaller businesses should not subsidise network, water or emergency-service infrastructure built principally to support a private hyperscale development.

Recommendation 10: Provide independent oversight and scheduled review

The Commonwealth should designate a lead coordinating office and require an annual report to Parliament on:

- approved and proposed major facilities;
- forecast and actual electricity demand;
- forecast and actual water use;
- public assistance;
- infrastructure investment;
- compliance;
- significant incidents;
- community impacts;
- local economic benefits; and
- progress against national objectives.

The framework should receive an independent statutory review after three years. The review should assess effectiveness, duplication, market effects, public costs, environmental outcomes, national-security implications and whether thresholds remain appropriate.

15. Conclusion

Australia has an opportunity to build digital infrastructure that supports research, public services, security, industry and responsible artificial intelligence.

That opportunity will be weakened if data centre growth:

- transfers electricity and water costs to the public;
- reserves infrastructure for speculative projects;
- relies on environmental claims that cannot be verified;
- concentrates critical services without adequate recovery;
- creates dependence on a small number of foreign providers;
- conceals government concessions;
- promises jobs and innovation without measurable delivery; or
- excludes affected communities from meaningful decisions.

The correct response is neither uncritical acceleration nor automatic prohibition. Australia should require major projects to reasonably show their work.

Approvals, infrastructure access and public support should be tied to evidence about resource demand, additional supply, resilience, public benefit, community effects and long-term obligations. Government agreements should be transparent, auditable and reversible. Security-sensitive details should remain protected while public costs and commitments remain visible.

Data centres will increasingly underpin both ordinary digital life and nationally important systems. The standards established during the present expansion will determine whether that infrastructure remains affordable, secure, accountable and publicly legitimate.

The Committee should recommend a nationally consistent, impact-based Data Centre Infrastructure Framework built around:

- resource and resilience evidence;
- fair cost allocation;
- additional energy and infrastructure;

- sustainable water use;
- operational transparency;
- critical-infrastructure security;
- public-interest government agreements;
- sovereignty and exit;
- community participation; and
- independent review.

References

- Australian Energy Market Operator (2025a) 2025 Electricity Statement of Opportunities: A 10-year outlook of investment requirements to maintain reliability in the National Electricity Market. Available at: https://www.aemo.com.au/-/media/files/electricity/nem/planning_and_forecasting/nem_esoo/2025/2025-electricity-statement-of-opportunities.pdf
- Clean Energy Regulator (2026) National Greenhouse and Energy Reporting Scheme. Available at: <https://cer.gov.au/schemes/national-greenhouse-and-energy-reporting-scheme>
- Commonwealth of Australia (2018, current compilation 4 June 2026) Security of Critical Infrastructure Act 2018. Federal Register of Legislation. Available at: <https://www.legislation.gov.au/Series/C2018A00029>
- Critical Infrastructure Security Centre (2026) Legislation, regulation and compliance. Department of Home Affairs. Available at: <https://www.cisc.gov.au/legislation-regulation-and-compliance>
- Department of Climate Change, Energy, the Environment and Water (2026) Environment Protection and Biodiversity Conservation Act 1999. Available at: <https://www.dcceew.gov.au/environment/epbc>
- International Energy Agency (2025) Energy and AI. Available at: <https://www.iea.org/reports/energy-and-ai>
- NABERS (2026) Data centres. Available at: <https://www.nabers.gov.au/ratings/spaces-we-rate/data-centres>
- Oxford Economics Australia (2025) Data centre energy consumption report: Final report prepared for the Australian Energy Market Operator. Available at: https://www.aemo.com.au/-/media/files/stakeholder_consultation/consultations/nem-consultations/2024/2025-iasr-scenarios/final-docs/oxford-economics-australia-data-centre-energy-consumption-report.pdf