

AUSTRALIAN TELECOMMUNICATIONS ALLIANCE SUBMISSION

To: The Office of AI

Re: Getting it right: Building AI infrastructure that works for
Australia

9 October 2026



TABLE OF CONTENTS

1. AUSTRALIAN TELECOMMUNICATIONS ALLIANCE	3
2. INTRODUCTION	3
3. APPLYING THE AI STANDARDS: A RISK-BASED INFRASTRUCTURE READINESS APPROACH	4
3.1 Risk-based and staged application	4
3.2 Thresholds and integrated infrastructure assessment	4
4. IMPOSING NO NET COSTS ON CONSUMERS AND COMMUNITIES	5
5. MEANINGFUL ENGAGEMENT WITH COMMUNITIES AND COUNCILS	6
5.1 Communities should understand the full development footprint	6
5.2 Protecting sensitive information	6
6. BUILDING AUSTRALIAN CAPABILITY, SKILLS AND INNOVATION	7
6.1 Workforce capability	7
6.2 Building enduring national capability	7
7. SECURITY, SAFETY AND TRANSPARENCY FOR AI TRAINING AND FRONTIER AI MODELS	8
8. PROVIDING A SIMPLE, CONSISTENT NATIONAL FRAMEWORK	9
8.1 National consistency requires connectivity consistency	9
8.2 Modernising telecommunications deployment arrangements	9
8.3 Potential Commonwealth reform actions	10
9. SUMMARY OF RECOMMENDATIONS	12

1. AUSTRALIAN TELECOMMUNICATIONS ALLIANCE

The Australian Telecommunications Alliance (ATA) is the peak body of the Australian telecommunications industry. We are the trusted voice at the intersection of industry, government, regulators, and consumers. Through collaboration and leadership, we shape initiatives that grow the Australian telecommunications industry, enhance connectivity for all Australians, and foster the highest standards of business behaviour. For more details, visit www.austelco.org.au.

For questions on this submission, please contact Victoria Robertson, Head of Government Relations and Policy, v.robertson@austelco.org.au.

2. INTRODUCTION

The ATA welcomes the opportunity to provide input on the Australian Government's consultation paper, *Getting it Right: Building AI Infrastructure that Works for Australia* (consultation paper).

The ATA supports the Government's objective of establishing nationally consistent standards that attract investment, support sovereign capability, and maintain community confidence while ensuring infrastructure development occurs in Australia's national interest.

The consultation paper correctly identifies energy and water as critical inputs to AI infrastructure. The ATA submits that telecommunications infrastructure must be afforded similar recognition as a foundational enabling input to AI infrastructure, AI training, and data centre development.

Central Proposition

Data centres create AI capability. Telecommunications networks distribute its benefits. Australia's AI infrastructure should therefore be assessed and planned as one integrated connectivity system. Nationally consistent AI standards should be accompanied by nationally consistent telecommunications deployment settings.

Telecommunications infrastructure is not merely a supporting service for AI infrastructure. It is the means through which AI capability is accessed, utilised, and translated into economic and social value. AI infrastructure will place increasing demands across Australia's fixed, mobile, and international connectivity networks. While public discussion often focuses on data centres and mobile technologies, fixed network infrastructure continues to carry the vast majority of Australian data traffic, and will remain central to the delivery of AI-enabled services, cloud connectivity, data replication, and business adoption. Without sustainable, scalable, secure, and resilient connectivity, AI capability risks becoming concentrated infrastructure rather than an economy-wide productivity platform.

AI will increase demand not only for data centre capacity, but also for the telecommunications networks that connect users, devices, businesses, and governments to AI-enabled services. As AI adoption accelerates, growth in data traffic, cloud connectivity, edge computing, machine-to-machine communications, and AI-enabled applications will require ongoing investment in network capacity, resilience, security and coverage. National AI infrastructure policy should therefore support both the development of compute infrastructure, and the long-term sustainability of the telecommunications networks that enable AI capability to be accessed and utilised across the economy.

This is also an economic issue. Australian Government analysis has estimated that telecommunications services contributed approximately 14.7 per cent of economy-wide multifactor productivity growth between 2009-10 and 2019-20.¹ It is safe to assume that this contribution has further increased since then. AI capability creates opportunity, but its economic value depends on adoption. Adoption depends on access, and access depends on secure, resilient, and scalable connectivity.

¹ ATA [submission](#) to the Senate Environment and Communication Committee's *Inquiry into AI and data centres*.

The relationship operates in both directions. As AI adoption grows, policies affecting telecommunications investment increasingly become AI policy decisions. Settings that unintentionally constrain investment in communications infrastructure may ultimately reduce the capacity, resilience, and reach of the networks through which AI services are delivered.

International experience increasingly recognises that data centres depend upon broader infrastructure ecosystems, including fibre connectivity and digital infrastructure.² Australia should adopt a similar whole-of-system approach by focusing on infrastructure readiness. Major developments should demonstrate how telecommunications, energy, water, and other enabling infrastructure will be delivered, coordinated and maintained before significant approvals are granted. This improves investor certainty, identifies community impacts earlier, and reduces the risk that supporting infrastructure becomes a bottleneck to AI investment.

This submission builds on the ATA's recent submissions to Commonwealth and state inquiries into AI and data centres, which have consistently argued that Australia's AI ambitions depend not only on compute infrastructure, but also on the telecommunications infrastructure that enables AI capability to be accessed, adopted, and distributed across the economy.³ The submission applies that same principle to the proposed AI standards, focusing on infrastructure readiness, enabling connectivity, regulatory coordination, and long-term digital infrastructure capability.

3. APPLYING THE AI STANDARDS: A RISK-BASED INFRASTRUCTURE READINESS APPROACH

3.1 RISK-BASED AND STAGED APPLICATION

- 3.1.1 The ATA supports a nationally consistent, risk-based, and outcomes-focused approach to the application of the AI standards. The framework should establish common national objectives and minimum expectations while allowing obligations to be calibrated according to project scale, development stage, location, and reasonably foreseeable impact.
- 3.1.2 Obligations should apply at the stage at which they can most effectively influence project design and manage risk. Site suitability, infrastructure availability, community engagement, and delivery planning should be addressed before final development approval. Operational efficiency, resource consumption, incident reporting, and performance obligations should generally commence when a relevant facility or stage becomes operational.

3.2 THRESHOLDS AND INTEGRATED INFRASTRUCTURE ASSESSMENT

- 3.2.1 Clear capacity thresholds should identify the developments subject to enhanced assessment and assurance. Electricity capacity is a practical primary threshold, but it is not a complete proxy for a project's infrastructure footprint.
- 3.2.2 Once a project exceeds the applicable threshold, the proponent should provide an Integrated Infrastructure and Connectivity Plan with its initial application. The Plan should demonstrate whether the telecommunications, energy, water, and community infrastructure required by the project is available, can be delivered within project timeframes, or remains dependent on further approvals, investment, or third-party commitments.

² Commission for Regulation of Utilities (CRU) (Ireland), [New Electricity Connection Policy for Data Centres](#); Ministry of Digital Development and Information (MDDI) (Singapore), [New Digital Infrastructure Bill to Strengthen the Foundations for Singapore's Digital Economy](#); Virginia Economic Development Partnership (VEDP) (USA) [Cloud and AI Infrastructure](#)

³ ATA [submission](#) to the Senate Environment and Communication Committee's *Inquiry into AI and Data Centres*, the [submission](#) to the Joint Select Committee on AI, and the [submission](#) to the Tasmanian Parliamentary *Inquiry into AI Data Centres in Tasmania*.

- 3.2.3 For telecommunications, the assessment should address capacity, physical route diversity, domestic and international connectivity, restoration capability, land-access and approval requirements, future augmentation, and cumulative reliance on shared infrastructure. The purpose is not to create a separate telecommunications threshold, but to identify enabling-infrastructure constraints before they become project delays.
- 3.2.4 The Plan should operate as a coordination mechanism, not a separate approval or reporting process, and should not impose duplicative obligations on telecommunication providers. Substantially equivalent information already provided under another planning or regulatory process should satisfy the requirement.

ATA position

The AI standards should apply through a risk-based and proportionate infrastructure-readiness framework, using clear primary thresholds to identify projects requiring enhanced assessment. Major developments captured by the standards should provide an Integrated Infrastructure and Connectivity Plan demonstrating how essential telecommunications, energy, water, and community infrastructure will be approved, funded, delivered, and maintained.

4. IMPOSING NO NET COSTS ON CONSUMERS AND COMMUNITIES

- 4.1.1 The ATA supports the principle that data centre development should not transfer project specific infrastructure costs to existing consumers, telecommunications providers, utilities, or the wider community.
- 4.1.2 The framework should distinguish clearly between:
- infrastructure necessary to connect and operate the project;
 - measures necessary to mitigate the project's impacts; and
 - additional benefits delivered to communities.
- 4.1.3 Proponents should ordinarily meet reasonable and directly attributable telecommunications costs, including dedicated fibre extensions, diverse site entries, project-specific civil works, and network augmentation required primarily for the facility. Responsibility should be determined through commercial arrangements with the relevant infrastructure provider.
- 4.1.4 Proponents should not be required to fund unrelated network upgrades or resolve pre-existing constraints from which the project derives no corresponding benefit. Equally, project specific costs should not be transferred to telecommunications providers, existing customers, or the community.
- 4.1.5 Telecommunications investment should be described as a community benefit only where it produces an additional and measurable outcome beyond the facility's operational needs (including the distribution of data), such as improved capacity for other users, regional connectivity, route diversity, restoration capability, or emergency communications resilience.
- 4.1.6 The Integrated Infrastructure and Connectivity Plan should identify these costs and responsibilities before project approval.

ATA position

The framework should distinguish clearly between project infrastructure costs, impact-mitigation measures, and additional community benefits. Proponents should meet reasonable and directly attributable infrastructure costs, while community benefits should be separately identified, measurable, and additional to project and mitigation requirements.

5. MEANINGFUL ENGAGEMENT WITH COMMUNITIES AND COUNCILS

Meaningful engagement should begin before key decisions about site design, infrastructure routes, and construction sequencing become fixed. The Commonwealth should establish nationally consistent principles, definitions, and minimum expectations for community engagement processes under the AI standards. This would provide greater certainty for communities, proponents, and councils, while allowing engagement methods to be tailored to local circumstances and project risks.

5.1 COMMUNITIES SHOULD UNDERSTAND THE FULL DEVELOPMENT FOOTPRINT

5.1.1 Engagement should address both the facility and the associated infrastructure required to construct, connect, and operate it. Communities may experience impacts from fibre routes, road openings, utility works, construction access, and corridor development beyond the facility boundary. These impacts should be explained early enough for communities to participate constructively in project development, contribute local knowledge and perspectives, and understand how feedback has informed project planning and mitigation measures.

5.1.2 At a minimum, engagement should address the following matters:

Table 1: Information communities should receive during engagement

Topic	Matters to be addressed
Project and infrastructure footprint	The facility footprint, supporting telecommunications, energy and water infrastructure requirements, and associated works that may affect the local community.
Community impacts	The nature, timing, and duration of construction and operational impacts, and proposed mitigation and reinstatement arrangements.
Local participation and benefits	Local employment, procurement opportunities and any proposed community benefits.
Engagement and accountability	Feedback mechanisms, escalation pathways, and how community input has influenced project design, routing, mitigation measures, or construction sequencing.

5.2 PROTECTING SENSITIVE INFORMATION

5.2.1 Public engagement must also protect security-sensitive information. Communities should receive sufficient information to understand the nature and impacts of proposed connectivity infrastructure, but detailed fibre routes, facility entry points, network diagrams, vulnerability information, and cyber security configurations must be protected.

5.2.2 Councils should be engaged early, but should not be required to resolve cross-jurisdictional infrastructure issues without Commonwealth and state coordination. A nationally consistent framework should provide councils with common definitions, guidance, and referral arrangements, particularly where infrastructure is regulated partly through Commonwealth telecommunications law.

ATA position

Major developments should undertake early and proportionate community and council engagement covering the facility and its supporting-infrastructure footprint, demonstrate how feedback has influenced project design or mitigation, and protect detailed security-sensitive infrastructure information.

6. BUILDING AUSTRALIAN CAPABILITY, SKILLS AND INNOVATION

Australia's AI ambitions should be measured not only by the scale of infrastructure investment, but by the enduring national capability it creates. This includes workforce capability, research partnerships, supplier development, digital infrastructure capability, and the capacity of businesses, governments, and communities to adopt and use AI.⁴

6.1 WORKFORCE CAPABILITY

6.1.1 Workforce planning should address the full infrastructure lifecycle, including construction, fibre deployment, civil works, network and electrical engineering, systems integration, cyber security, cloud and network operations, incident response, and ongoing maintenance. Skills plans should be developed in partnership with telecommunications providers, contractors, vocational education providers, universities, and local industry.

6.1.2 At a minimum, plans should address the following matters.

Table 2: Workforce capability priorities

Element	Required focus
Workforce needs	Construction, commissioning, and ongoing operational roles
Skills gaps	Telecommunications, engineering, cyber security, cloud, and infrastructure resilience
Training pathways	Apprenticeships, traineeships, and accredited education
Australian participation	Local contractors, suppliers, universities, and training providers
Lasting capability	Portable qualifications and skills, transferable beyond the project
Accountability	Measurable outcomes, timeframes, and reporting

6.1.3 Training should focus on creating portable national capability rather than narrow project specific skills. Capability in fibre deployment, network engineering, systems integration, cyber security, and infrastructure resilience is transferable across AI, critical infrastructure, telecommunications, and other sectors of the digital economy. Investment should therefore support skills that remain valuable beyond the life of any individual project.

6.2 BUILDING ENDURING NATIONAL CAPABILITY

6.2.1 Workforce development is only one element of capability creation. The broader national value of AI infrastructure investment will depend on whether Australian researchers, businesses, public institutions, and regional communities can access and use the capability created.

6.2.2 Telecommunications networks connect these users to compute, cloud, and edge infrastructure, and play a central role in determining how widely AI-enabled services can be adopted. The benefits of AI capability will ultimately depend on whether businesses, households, and institutions can access high-quality connectivity services that support the adoption of AI-enabled tools and applications.

6.2.3 Broader capability objectives should therefore extend beyond workforce development to include research access, supplier development, industry capability, regional participation, and the digital infrastructure

⁴ ATA [submission](#) to the Senate Environment and Communication Committee's *Inquiry into AI and Data Centres*, and the [submission](#) to the Tasmanian Parliamentary *Inquiry into AI Data Centres in Tasmania*.

required to support adoption across the economy. Where developments receive public support, proponents should also consider how associated connectivity investments can improve access to AI-enabled services for regional and underserved communities, helping ensure the benefits of AI infrastructure are distributed more broadly across Australia.

6.2.4 At a minimum, broader capability objectives should address the following priorities:

Table 3: Broader national capability priorities

Priority	Required focus
Research	Access to compute and high capacity connectivity
Partnerships	Australian universities, research institutions, and training providers
Industry capability	Telecommunications, cloud, cyber security, and infrastructure expertise
Suppliers	Australian procurement and supplier development opportunities
Regional participation	Connectivity and access to AI-enabled services
Strategic capability	Secure, resilient, and exportable digital infrastructure expertise

6.2.5 Public support should be directed towards projects that make measurable and enduring contributions to these capabilities, rather than simply increasing installed compute capacity. Any associated obligations should be proportionate to the level of public support provided, outcome focused, and commercially practical.

ATA position

Major AI infrastructure developments receiving public support should demonstrate measurable and enduring contributions to Australian workforce, research, supplier, and digital infrastructure capability, including the telecommunications infrastructure and connectivity needed to support broad adoption of AI across the economy. Investments should create lasting skills, strengthen Australian participation in the digital economy, and improve the ability of businesses, communities, and institutions to access and use AI-enabled services.

7. SECURITY, SAFETY AND TRANSPARENCY FOR AI TRAINING AND FRONTIER AI MODELS

- 7.1.1 The ATA supports proportionate security, safety, and transparency obligations for frontier AI training. The ATA does not seek to prescribe technical model safety requirements. Its principal concern is that infrastructure security and resilience be treated as integral to the security of frontier AI capability.
- 7.1.2 Frontier AI training depends on a delivery chain that extends beyond the data centre boundary. In practice, AI systems can only be as resilient as the infrastructure that connects them. A highly secure facility remains dependent on telecommunications networks, interconnection facilities, international connectivity pathways, and restoration capability. Security and resilience should therefore be assessed as whole-of-system outcomes rather than characteristics of a single facility.
- 7.1.3 Frontier AI capability depends on an infrastructure chain extending beyond the data centre boundary. Security and resilience assessments should therefore consider telecommunications route diversity, domestic and international connectivity, data in transit, material concentrations and common points of failure, energy and supply-chain dependencies, incident response, continuity, and restoration capability.
- 7.1.4 This is also relevant to sovereign capability. Australia's ability to maintain access to AI systems and critical digital services during disruption depends not only on the ownership or location of compute infrastructure,

but on the security, diversity, and resilience of the networks and international connectivity on which those services rely.⁵

- 7.1.5 Obligations should remain risk-based, technology neutral, and aligned with existing telecommunications, cyber security, and critical infrastructure frameworks. Public reporting should focus on governance and assurance outcomes, while detailed route, reserved capacity, vulnerability, and security information should be restricted to authorised decision-makers.

ATA position

Security and resilience should be assessed across the entire AI delivery chain, including telecommunications route diversity, domestic and international connectivity, energy and supply-chain dependencies, incident response, continuity, and restoration capability. Any new obligations should be risk-based, technology-neutral, and aligned with existing telecommunications, cyber-security, and critical-infrastructure frameworks.

8. PROVIDING A SIMPLE, CONSISTENT NATIONAL FRAMEWORK

8.1 NATIONAL CONSISTENCY REQUIRES CONNECTIVITY CONSISTENCY

- 8.1.1 A nationally consistent framework will not deliver consistent investment conditions if it applies only to the data centre facility. The telecommunications infrastructure required to connect major facilities may cross multiple jurisdictions, land tenures, and transport corridors and remain subject to separate planning, environmental, heritage, road-opening, and land-access requirements.
- 8.1.2 ATA member evidence demonstrates the practical consequences. Recent long-haul fibre projects have required more than 3,000 land-access notices and more than 1,100 construction certificates, while a separate project experienced delays of 12 to 18 months.⁶ A data-centre approval does not itself authorise the fibre routes, network facilities, or civil works required to make the facility operational. Telecommunications deployment delays can therefore become AI deployment delays.

8.2 MODERNISING TELECOMMUNICATIONS DEPLOYMENT ARRANGEMENTS

- 8.2.1 Commonwealth leadership is required because telecommunications infrastructure is national in function and frequently cross-jurisdictional in delivery. The Government's current review of deployment arrangements under the *Telecommunications Act 1997* provides an immediate opportunity to modernise settings designed for an earlier generation of network architecture and align deployment reform with Australia's AI infrastructure agenda. The objective should be proportionate, coordinated and timely processes that retain environmental, heritage, safety, planning and community safeguards while reducing unnecessary duplication and delay.
- 8.2.2 Practical reform should focus on removing avoidable barriers to the timely deployment of enabling telecommunications infrastructure. This could include improving access to suitable public land and infrastructure corridors, facilitating additional or upgraded infrastructure within existing telecommunications footprints, providing greater flexibility for the replacement or realignment of existing facilities where impacts are materially unchanged, and streamlining fibre deployment along established transport and utility corridors.

⁵ ATA [submission](#) to the Senate Environment and Communication Committee's *Inquiry into AI and Data Centres*, and the [submission](#) to the Tasmanian Parliamentary *Inquiry into AI Data Centres in Tasmania*.

⁶ ATA [submission](#) to the Senate Environment and Communication Committee's *Inquiry into AI and Data Centres*, and the [submission](#) to the Tasmanian Parliamentary *Inquiry into AI Data Centres in Tasmania*.

- 8.2.3 These are not telecommunications-sector issues in isolation. Telecommunications infrastructure is the enabling infrastructure that connects AI facilities to users, cloud platforms, businesses, governments, and communities. Where deployment barriers delay network construction, they can directly delay the commissioning, expansion, and resilience of nationally significant AI infrastructure.
- 8.2.4 The Commonwealth should therefore accompany the AI standards with reform of national telecommunications deployment settings. Commonwealth policy settings should also support continued investment in telecommunications networks. AI infrastructure policy should recognise that data centres and telecommunications networks are interdependent. Measures that increase barriers, costs, duplication, or uncertainty for telecommunications investment ultimately affect the connectivity needed to support AI adoption, resilience, and productivity outcomes.
- 8.2.5 The proposed AI standards are premised on the idea that nationally consistent settings improve investment certainty and reduce regulatory fragmentation. That same logic applies to the telecommunications infrastructure required to connect major AI facilities. There is little value in establishing a nationally consistent framework for approving AI infrastructure if the fibre routes, interconnection facilities, and supporting networks needed to make that infrastructure operational remain subject to fragmented and inconsistent approval pathways. The objective should not be to remove environmental, heritage, safety, planning, or community safeguards. It should be to ensure those safeguards operate through proportionate, coordinated, and timely processes.

8.3 POTENTIAL COMMONWEALTH REFORM ACTIONS

- 8.3.1 The ATA does not suggest that a single reform will address deployment challenges. Rather, the Commonwealth should consider a package of complementary measures designed to improve coordination, reduce duplication, and accelerate delivery of nationally significant digital infrastructure.

Table 4: Potential Commonwealth actions to accelerate enabling telecommunications infrastructure

Reform area	Potential Commonwealth action
Schedule 3 modernisation	Modernise Schedule 3 of the <i>Telecommunications Act 1997</i> and associated instruments to provide risk-based, technology neutral pathways for contemporary fibre, mobile, upgrade, replacement, restoration, and low-impact infrastructure activities, including within existing telecommunications sites and corridors.
Cross-jurisdictional coordination	Establish common information requirements, coordinated assessment pathways, and recognition of equivalent approvals across Commonwealth, state, territory, and local processes.
Decision timeframes	Introduce clearer referral, assessment, and decision-making timeframes for telecommunications infrastructure supporting nationally significant digital developments.
Strategic corridor planning	Identify and protect strategic telecommunications corridors and sites including fibre routes, inter-capital links, cable-landing connections, and future digital-infrastructure capacity.
Land and infrastructure access	Promote timely access to suitable public land, utility corridors and other infrastructure required for nationally significant telecommunications deployment, including clearer whole-of-government coordination and processes for identifying and securing suitable sites and routes.

Bottleneck resolution	Establish a national mechanism to identify systemic deployment constraints, coordinate agencies, and resolve inter-jurisdictional barriers.
Regulatory duplication	Apply a “report once, use many times” principle and require new reporting obligations to address a demonstrated regulatory gap.

- 8.3.2 These measures would not diminish existing safeguards. Rather, they would help ensure that telecommunications infrastructure can be assessed and delivered through processes that are more predictable, transparent and proportionate.
- 8.3.3 A simple national framework should also apply a “report once, use many times” principle. Information should be collected from the authoritative source and reused across government where lawful and appropriate. New requirements should address a demonstrated gap rather than reproduce an existing return in another format.
- 8.3.4 The cumulative effect of regulatory obligations across digital infrastructure sectors should also be considered. While individual reporting, governance, or compliance requirements may be justifiable in isolation, their combined impact can affect investment capacity and project delivery. Regulatory design should therefore seek to minimise duplication and ensure new obligations address a clearly demonstrated policy need.
- 8.3.5 Reforming telecommunications deployment frameworks should not be viewed solely as telecommunications policy. It is increasingly AI policy, digital infrastructure policy, productivity policy, national security, and resilience policy. The success of the proposed AI standards will ultimately depend not only on how data centres are regulated, but on whether the telecommunications infrastructure required to connect those facilities can be deployed efficiently, consistently, and at scale.⁷
- 8.3.6 The AI standards should form part of a broader National Digital Infrastructure Framework coordinating policy and investment across telecommunications, data centres, cloud services, energy, spectrum, cyber security, and AI. Consistent with the ATA’s previous submissions, a National Digital Infrastructure Framework should also improve visibility of cumulative regulatory impacts across digital infrastructure sectors.⁸ Coordinated policy development can help ensure that new obligations are assessed collectively and implemented in a manner that supports, rather than unintentionally constrains, long-term investment in nationally significant digital infrastructure.
- 8.3.7 Predictable and efficient deployment of enabling telecommunications infrastructure should be treated as part of Australia’s AI investment and competitiveness framework.

ATA position

The AI standards should establish a simple and nationally consistent framework using common definitions, thresholds, reporting methodologies, and assurance arrangements, with substantially equivalent existing obligations recognised through a “report once, use many times” approach.

The Commonwealth should complement that framework by modernising national telecommunications deployment settings and improving coordination across Commonwealth, state, territory, and local approval processes.

These reforms should form part of a broader National Digital Infrastructure Framework coordinating policy and investment across Australia’s interdependent digital infrastructure.

⁷ ATA [submission](#) to the Senate Environment and Communication Committee’s *Inquiry into AI and Data Centres*, and the [submission](#) to the Tasmanian Parliamentary *Inquiry into AI Data Centres in Tasmania*.

⁸ ATA [submission](#) to the Senate Environment and Communication Committee’s *Inquiry into AI and Data Centres*, and the [submission](#) to the Tasmanian Parliamentary *Inquiry into AI Data Centres in Tasmania*.

9. SUMMARY OF RECOMMENDATIONS

9.1.1 The recommendations below apply a single principle: major AI infrastructure should be assessed as an integrated system. Together, they are intended to improve infrastructure readiness, reduce regulatory fragmentation, and ensure that AI capability can be connected, accessed and used across the economy.

Table 5: ATA recommendations for a National AI Infrastructure Framework

No.	Recommendation	Why it matters
1	Recognise telecommunications infrastructure as essential AI infrastructure Telecommunications connectivity, resilience, and future capacity should be recognised alongside energy and water as foundational inputs to AI infrastructure.	Data centres create AI capability; telecommunications networks connect that capability to businesses, governments, and communities. AI benefits cannot be realised without connectivity.
2	Apply the AI standards through a risk-based infrastructure readiness framework. Projects captured by the standards should assess telecommunications capacity, route diversity, resilience, future augmentation requirements, and infrastructure dependencies.	Capacity thresholds alone do not capture the broader enabling infrastructure needs of major AI developments. Early assessment improves investor certainty and identifies delivery risks before approval.
3	Require an Integrated Infrastructure and Connectivity Plan. Major developments should demonstrate how telecommunications, energy, water, and community infrastructure requirements will be delivered, funded, approved, and maintained.	Data centre facilities and supporting infrastructure should be assessed as a single system. Integrated planning improves transparency, coordination, and community confidence.
4	Apply fair and transparent infrastructure cost allocation. Proponents should fund infrastructure reasonably required for their development, while community benefits should be clearly distinguished from project obligations.	Project-specific costs should not be transferred to telecommunications providers, consumers, or communities. Community benefits should be additional, measurable, and enduring.
5	Require meaningful community and council engagement. Require early engagement on the full development and supporting infrastructure footprint, supported by nationally consistent engagement principles, and appropriate protection of sensitive information.	Australia should seek to build capability around AI infrastructure, not simply host it. Telecommunications enabled capability supports long-term productivity, innovation, and regional participation.
6	Build enduring Australian capability. Require major developments receiving public support to demonstrate measurable and enduring contributions to Australian workforce, research, supplier, and digital infrastructure capability, including connectivity and access that support	Australia should seek to build capability around AI infrastructure, not simply host it. Lasting benefits will come from stronger workforce skills, research and supplier capability, digital infrastructure expertise, and broader access to AI-enabled services across the economy.

broad adoption of AI-enabled services across the economy.

7	Assess security and resilience across the entire AI delivery chain. Infrastructure security, telecommunications diversity, international connectivity, energy dependencies, and restoration capability should be considered as part of AI infrastructure resilience.	AI infrastructure is only as resilient as the systems that connect it. Security and resilience should be evaluated as whole-of-system outcomes rather than facility-level characteristics.
8	Establish a simple and nationally consistent framework. Use common definitions, thresholds, reporting methodologies, and assurance arrangements, supported by “report once, use many times” principles.	National consistency improves investment certainty, reduces duplication, avoids unnecessary regulatory burden, and helps manage the cumulative impact of regulatory obligations across Australia’s digital infrastructure ecosystem.
9	Modernise Commonwealth telecommunications deployment settings as part of Australia’s AI infrastructure agenda. Establish nationally consistent deployment pathways and better coordination between Commonwealth, state, territory, and local approval processes.	Telecommunications deployment delays can become AI deployment delays. Nationally consistent AI standards should be matched by nationally consistent connectivity deployment settings.
10	Develop a National Digital Infrastructure Framework. Coordinate policy and investment across telecommunications, data centres, cloud services, energy, spectrum, cyber security, and AI, including a mechanism to identify and resolve cross-jurisdictional infrastructure barriers.	Digital infrastructure is increasingly interdependent. Coordinated planning and policy settings can improve investment certainty, reduce regulatory fragmentation, and support more efficient delivery of AI infrastructure.

Australia cannot build a successful AI economy through compute investment alone. Data centres create AI capability, but telecommunications networks connect that capability to businesses, governments, and communities and enable it to generate wider productivity, resilience, and economic benefits.

The AI standards should therefore be built around infrastructure readiness: proportionate thresholds, integrated assessment, transparent cost allocation, early community engagement, capability development, system-wide resilience, and nationally coordinated regulation. Nationally consistent standards for data centres should be matched by modern, nationally consistent deployment settings for the telecommunications infrastructure required to connect them.

Ends

