AustraliaOS

australiaos.com.au

AustraliaOS Pty Ltd
Decision infrastructure
for Australian institutions

The Jurisdiction Gap

How existing regulatory frameworks leave Australian institutional data exposed to foreign legal reach, and what would close the gap. A submission to the Senate inquiry into artificial intelligence and data centres.

REFERENCE	DATE	CLASSIFICATION	VERSION
AOS-AIDC-2026-001-v1.1	May 2026	Public	1.1

Contents

01 Submitter and opening

This submission is made by AustraliaOS Pty Ltd (ABN 69 697 049 291), a Melbourne company that produces jurisdictional exposure assessments of technology providers. It is authored by its director, Brunel Al-Bijwaie, who takes responsibility for its analysis and recommendations.

This submission addresses term (a) of the inquiry: the effectiveness of existing regulatory frameworks in relation to deals between the Government and global AI companies. Its central finding is that a Commonwealth procurement of AI infrastructure can satisfy every existing regulatory requirement, pass every check a diligent official performs, and still place Australian institutional data within the reach of a foreign government, because no framework requires anyone to assess that exposure (ANALYSIS A).

02 Existing frameworks do not require assessment of jurisdictional exposure

Existing regulatory frameworks do not require assessment of jurisdictional exposure. This is not a failure of the frameworks. Each was built for a purpose, and none of those purposes is the assessment of whether a provider's foreign incorporation places Australian data within reach of a foreign government (CLAIM A).

The Security of Critical Infrastructure Act 2018 lists the critical asset classes it covers. Artificial intelligence is not among them. AI infrastructure is reached only where it falls within another listed class, such as data storage or processing (CLAIM D), and even then the Act directs no one to assess its jurisdictional exposure.

The Privacy Act 1988 governs the handling of personal information. It steps aside where an applicable foreign law requires disclosure, and it contains no provision comparable to the compulsion authority that foreign law can exercise over a foreign-incorporated provider.

The Commonwealth Procurement Rules require officials to achieve value for money. Value for money names price and a defined set of other factors. Jurisdictional exposure is not among them.

The Public Governance, Performance and Accountability Act 2013 sets a general duty on accountable authorities to promote the proper use of public resources. A general duty is an aim, not an instruction to determine a provider's jurisdiction and test its reachability under foreign law.

The result is that jurisdictional exposure falls through these frameworks by design, not by failure. An official complying fully with every one of them would still never assess it, because none of them points there. The frameworks are broad where they would need to

be specific. A general duty does not narrow to the particular thing that needs checking, so that thing does not get checked, no matter how well anyone does their job (ANALYSIS A).

03 The government's own documents acknowledge the gap

The gap is not only a feature of the frameworks. It is visible on the face of the government's own published documents.

The Expectations of data centres and AI infrastructure developers names data sovereignty as a national interest consideration. It does not define the term. It provides for general prioritisation of proposals aligned with the expectations, but supplies no method for assessing a proposal against data sovereignty specifically, and identifies no role, body, or official responsible for making that assessment.

The National AI Plan commits the government to deepening its engagement with leading AI providers, including a bilateral Technology Prosperity Deal with the United States. It does not address the foreign jurisdictional exposure that follows when the providers engaged are incorporated under foreign law.

The point is not that the government has failed to consider these matters privately. That is unknowable from outside, and this submission does not assert it. The point is narrower and verifiable. One published instrument states a value. Another published instrument commits to a direction that bears directly on that value. Neither connects the two, and neither supplies a method by which the value could be tested against the direction. The gap is therefore not a matter of interpretation or hidden intent. It is visible in what the documents do and do not contain, and both documents are public and checkable (ANALYSIS B). Even if such an assessment occurs within some unpublished process, the absence of any published method means it cannot be scrutinised by Parliament or the public, cannot be applied consistently across decisions, and cannot be relied upon by the institutions whose data is at stake.

A value asserted without a method of assessment cannot be applied consistently. That is the gap this submission addresses.

04 The exposure is real and assessable

The exposure this gap leaves unassessed is real, and it is assessable.

It is real because it is established in primary law. The CLOUD Act requires a provider subject to United States jurisdiction to disclose data in its possession on United States legal process, regardless of whether that data is held inside or outside the United States. Reach attaches to the provider's subjection to that jurisdiction, not to where the data sits.

The clearest and most verifiable form of that subjection is incorporation in the United States, which an institution can confirm from a provider's corporate registration. The Australia United States CLOUD Act Agreement administers reciprocal access between the two governments; it does not narrow the disclosure obligation a United States provider owes to United States legal process. So an Australian institution can hold its data on Australian soil and still place it within the reach of a foreign government, if the provider holding it is subject to that government's jurisdiction (CLAIM B).

It is assessable because the determining facts are public. A provider's incorporation, the law applicable to it, and the disclosure it can be compelled to make are matters of public record and primary law. Assessing exposure is therefore a matter of method, not of privileged access to classified or commercial information.

That method is not hypothetical. It has been applied to a real provider and the result is public and checkable. A jurisdictional exposure assessment of Telstra, an Australian critical telecommunications carrier, examined its disclosed vendor dependencies, applied the CLOUD Act reach test to each United States incorporated provider, and tested the resulting exposure against Telstra's obligations under the Security of Critical Infrastructure Act. Every claim in that assessment is traceable to a public source, the gaps are flagged rather than papered over, and the record is open to review. The instrumentation that the Expectations document leaves unspecified is therefore demonstrable. It exists, it operates on public sources, and it produces a defensible record (ANALYSIS C).

05 Recommendations

Closing the gap does not require rebuilding the existing frameworks. They function as designed. It requires adding the one thing they lack: a requirement to assess jurisdictional exposure, defined clearly, made mandatory, and tied to a named accountable person. Three elements follow, and the recommendations below set them out. The concern must be defined, so that what is assessed is specified rather than left to interpretation. The assessment must be required, so that it happens systematically rather than only when an official happens to consider it. And the official responsible must be accountable for it, so that the requirement has force (ANALYSIS D).

Recommendation A. Define data sovereignty in the Expectations document by reference to provider incorporation, applicable law, and disclosure requirements (RECOMMENDATION A). The term is named but undefined, and an undefined term cannot be assessed. Exposure is not determined by where data is stored but by whether the provider holding it is subject to foreign compulsion, so a definition framed around data location would turn on the one thing that does not control the outcome. A definition framed around incorporation, applicable law, and compellable disclosure gives an official a concrete and

checkable test.

Recommendation B. Require jurisdictional exposure assessment for Commonwealth procurement of AI infrastructure that involves data or systems exposed to foreign legal reach, regardless of contract value (RECOMMENDATION B). A recommended step happens only when an official thinks to take it, which is the present situation. Only a requirement closes the gap. The trigger should be the sensitivity of what is being procured, not its dollar value, because a small contract can place highly sensitive data with a provider reachable under foreign law while a large one may carry no such exposure.

Recommendation C. Extend the Security of Critical Infrastructure Act 2018 critical asset definitions to include AI infrastructure (RECOMMENDATION C). The procurement assessment is a snapshot, accurate on the day it is made. Exposure is not fixed at purchase: a clean provider can be acquired by a foreign company, or the foreign law governing compelled disclosure can change, and in both cases the exposure arrives after the contract is signed. The Act imposes continuing obligations on critical asset operators, so bringing AI infrastructure within it means exposure is governed continuously, not only at purchase.

Recommendation D. Require the official approving a Commonwealth AI infrastructure procurement assessed under Recommendation B to attest in writing to having considered jurisdictional exposure (RECOMMENDATION D). A requirement to assess can be satisfied on paper without anyone engaging with the result. A written attestation by the approving official means the assessment cannot sit unread in a file, because a signature is something a person must stand behind. The signatory must be the official who approves the procurement, not any party who prepares the assessment, so that accountability rests with the person making the decision.

Recommendation E. Establish a public register of data centre proposal assessments against Expectation 1, accessible to Parliament and to the public (RECOMMENDATION E). Recommendations B and D ensure an assessment is done and that a named official is accountable for it, but that accountability runs only inward. The data and the exposure belong to the public, so accountability for the risk should extend to the public. A public register places each assessment on the record, where Parliament, the press, and the public can see what was assessed and decided and can challenge a decision that does not hold up. The register would be established and maintained by government.

Recommendation F. Establish a methodology standard for jurisdictional exposure assessment, modelled on the existing IRAP and PSPF assurance pathways (RECOMMENDATION F). A requirement to assess, without a standard for what a competent assessment must contain, leaves each assessment to be performed however the assessor sees fit. A methodology standard specifies what an assessment must examine and document, so it

can be tested against a defined measure rather than accepted on trust. This is the same approach already used in Commonwealth security assurance. The Information Security Manual is a published standard, and the Infosec Registered Assessors Program accredits the assessors who apply it; the Protective Security Policy Framework is a published Commonwealth protective security framework. In each case a published standard is set by government and the parties who assess against it operate within a defined accreditation framework. The standard should be established and administered by government. This submission makes no recommendation as to who should conduct assessments under it; that is a matter for the accreditation process government would establish.

The author is available to assist the committee in its consideration of these matters.

End of document.