



What the Screening Does Not Ask

REFERENCE	AOS-AIS-2026-001
VERSION	1.0
DATE	October 2026
CLASSIFICATION	Public
DIRECTOR	Brunei Al-Bijwaie

Contents

01 Submitter, and what this submission says	3
02 What international approaches, including regulatory and non-regulatory frameworks, should inform the type of safety, transparency or security conditions Australia applies to developers of frontier AI models?	3
03 What information should AI developers be required to share with the Australian Government and how?	4
04 What safeguards should apply?	5
05 Where might this proposed approach interact with existing legislation?	5
06 What this submission does not establish, and one question for the department	8
07 Independence, and payment	9
08 Status of this document	9
Appendix A. Sources, and the counts the body refers to	9

01 Submitter, and what this submission says

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. It answers four of the consultation questions and says plainly which it does not answer and why.

The finding, stated over the instruments it is established on. The paper states that sovereign AI capability “relies on secure, onshore data centre infrastructure”. **Two different things it does should be kept apart.** At page 5 it *describes* the existing Commonwealth regulation bearing on data centres: the *Environment Protection and Biodiversity Conservation Act 1999*, foreign investment and national security screening, the *Security of Critical Infrastructure Act 2018*, and the Hosting Certification Framework. At page 21 it says what it *proposes to do* with existing regulation, which is to minimise burden “by leveraging existing frameworks and policy levers whenever possible, such as the SOCI Act and the FATA”. **That sentence names two, “such as” leaves the list open, and it does not name the Hosting Certification Framework.** This submission addresses three of the instruments page 5 describes, foreign investment screening, the SOCI Act and the Hosting Certification Framework, and says nothing about the EPBC Act. Onshore location is not the test that controls the outcome. What controls it is whether the entity holding the data can be compelled to produce it under a law that is not Australian. The operative Hosting Certification Framework sets out what the Foreign Investment Review Board will consider, and that enumeration does not include compellability. Of the eight Australian assurance instruments this practice has read and pinned, none specifies a method for assessing foreign legal reach, and at least one, the Commonwealth Procurement Rules, does not name it at all. The gap is not that these instruments fail at their own purpose. It is that the purpose the paper asks them to carry is not one any was built to carry, and the paper does not say who will carry it instead.

02 What international approaches, including regulatory and non-regulatory frameworks, should inform the type of safety, transparency or security conditions Australia applies to developers of frontier AI models?

One overseas instrument shows that the distinction can be drawn expressly, in a sentence. The United Kingdom National Cyber Security Centre’s cloud security principle 2.1 tells a reader: “You need to identify which legal jurisdiction(s) your data could be subject to, seeking legal advice as necessary.” This practice read that instrument for one purpose only, to establish that an instrument can state the test rather than gesture at the risk. It is not offered as a survey of overseas practice, and no claim is made here that the

United Kingdom's wider approach should be adopted.

Set against it, this practice put one question to eight Australian assurance instruments: where an instrument names or asserts that a foreign government may reach a provider's data by law, does it specify a method for assessing that reach? Method meant a stated test, a stated source, or a stated standard of evidence by which an assessor would establish who can compel a provider. None of the eight specifies a method for assessing foreign legal reach, and at least one, the Commonwealth Procurement Rules, does not name it at all; of those Rules the assessment records, "One does not name it". That is a finding about those eight and no others.

What should inform Australia's conditions is the difference between naming a risk and stating a test. A condition requiring a developer to consider foreign legal reach is satisfied by consideration. A condition stating who must establish what, from which source, to what standard, can be audited. The paper's expectations for frontier labs will inherit whichever they are drafted as.

03 What information should AI developers be required to share with the Australian Government and how?

The paper offers three forms: a proactive obligation, an obligation on request, and an obligation to publish in a specified form. Before choosing among them, it is worth reading what happens to an existing Commonwealth obligation of the second kind.

The Hosting Certification Framework's Deed of Certification carries a disclosure obligation on a certified provider. Its only law-based carve-out is clause 13.10, under which a provider "is not required to disclose information pursuant to this Deed to the extent that it would cause the Service Provider to breach any Relevant Laws or duty of confidentiality restricting disclosure of the information". The instrument then closes that term by its own definition: "Relevant Laws means any relevant common law, statute, regulation, by-law, ordinance or subordinate legislation (whether made by a State, Territory or the Commonwealth) in force from time to time." **On its face, that definition does not include foreign law.** This is a statement about the published standard form. No executed Deed has been found published, and this practice has read none.

A sharing obligation drafted the same way would inherit the same shape. The carve-out was written so that an Australian obligation cannot force an Australian illegality, and the definition confines it to Australian law. It does not contemplate the case where the constraint is a foreign law. The drafting question that decides whether a new obligation holds is therefore not which of the three forms is chosen. It is what the obligation says when the developer, or a parent company, is subject to a law that prohibits the disclosure

or compels a different one.

04 What safeguards should apply?

One safeguard the published record shows to be missing is observability. In AOS-RCH-2026-001 this practice read eleven instruments against the Hosting Certification Framework's Certified Strategic mechanism: six of the framework's own and five Commonwealth Acts, Rules and policies. Of those eleven, none requires a decision under that mechanism to be published without being asked for. AOS-RCH-2026-001 states the consequence: "A reader of the public record cannot observe that the Certified Strategic mechanism has operated, and cannot observe that it has not." That is a statement about instruments. It is not a statement about anyone's conduct, and nothing in it is capable of being one.

A second is that a safeguard must test the right property. In AOS-CMP-2026-001 this practice established that a provider reachable under the United States CLOUD Act can clear both the Foreign Ownership, Control or Influence Risk Assessment Guidance and the Hosting Certification Framework, and hold the framework's highest tier. **The framework's own name for that tier is Certified Strategic**, and the Act calls it "a certificate of hosting certification (strategic level)". The framework's own definition of the quality it tests is "the ability of the government to specify and maintain stringent ownership and control conditions". Ownership, control and influence are not compellability: an Australian-owned entity can still hold or process data through an affiliate, a subcontractor or a service provider that a foreign authority can lawfully reach. A safeguard built on ownership answers a different question from the one the paper's premise depends on.

So the two safeguards this submission proposes are narrow. Any safety, transparency or security condition on a frontier developer should state the test for establishing who can lawfully compel production of the data or model weights held under it, name who must apply that test and from what sources, and provide that the outcome is recorded where a reader of the public record can see that the test was applied. None of that requires naming any company, and none of it requires the Commonwealth to publish what any particular assessment found.

05 Where might this proposed approach interact with existing legislation?

The proposed reporting and transparency requirements interact with existing Commonwealth regulation, and this submission addresses three of the instruments the paper describes at page 5: foreign investment screening, the SOCI Act and the Hosting Certification Framework. **It says nothing about the EPBC Act, which page 5 also describes**, and nothing about state, territory or local government legislation, which it has not read.

The Security of Critical Infrastructure Act 2018, and the reporting surface that already exists. A federal reporting requirement for large data centres would sit beside an annual report the Act already requires, **and it would reach some of the same entities:** the paper itself states at its page 5 that “Data centres are subject to the Security of Critical Infrastructure Act 2018 (the SOCI Act) if they are critical data storage or processing assets as defined by the SOCI Act.” Section 30AG(2) requires a responsible entity with a risk-management program to give an annual report that “is in the approved form” and, “if the entity has a board, council or other governing body”, is “approved by the board, council or other governing body, as the case requires”. Section 30AB(4) then exempts an asset from that Part where the entity “holds a certificate of hosting certification (strategic level)” and the asset “is used in connection with the provision of any of those services”, and section 30AQ requires those entities to report anyway, in the approved form, board-approved, setting out “the reason why those assets are covered by subsection 30AB(4), (5) or (6)”.

So the surface the Commonwealth would be adding to is already board-approved, already attested, and already asks about suppliers. The approved form, the Cyber and Infrastructure Security Centre (CISC) annual report web form, carries four supplier questions that go beyond the statutory minimum: whether the organisation has “an alternate supply chain identified for its critical operations or services in case of a disruption to primary supplier(s)”; whether it requires “any of its major suppliers to undergo regular security audits”; whether it requires “any of its major suppliers to implement technical and operational controls to protect your organisation’s data to which they have access”; and whether it requires “its suppliers to notify it about any security incidents or data breaches”.

None of the four reaches ownership, jurisdiction, incorporation or foreign legal reach. The form does ask the reporting entity its own “Country of incorporation or creation”; it asks nothing of the same kind about the suppliers those four questions concern.

This practice has already recommended the change to a Senate committee, and repeats it here. Recommendation D2 of AOS-AIDC-2026-001-SUPP-02 asks that the approved annual report form require the responsible entity to state whether the jurisdictional exposure of its major suppliers was considered. It is a change to a form the department already maintains, and it needs no legislation. **The interaction with the paper’s proposal is direct:** a new federal reporting requirement for large data centres that does not ask this question would leave the gap open in a second place, while a single added question closes it in the place the Commonwealth already collects.

Foreign investment screening. The operative Hosting Certification Framework, the March 2021 version 2 document, states at its printed page 7 that the Framework “works in conjunction with a suite of other government policies and frameworks, including

Australia's Foreign Investment Policy". It describes the regime as one "that includes the *Foreign Acquisitions and Takeovers Act 1975* (FATA), the *Foreign Acquisitions and Takeovers Regulation 2015* (the Regulation) and the Foreign Investment Policy". It then says what the Foreign Investment Review Board (FIRB) weighs: "In considering whether investment proposals are contrary to the national interest, FIRB will consider factors such as national security, competition, other Australian Government policies, the impact on the economy and community, and the character of the investor." **Compellability under foreign law is not among the factors that passage lists.** The passage is introduced by "such as" and does not present itself as exhaustive, so this submission claims only what it lists, and asks the question at section 06 rather than assuming the answer.

The same page claims a sufficiency. Working with FIRB and enacting its contractual protections, the Framework says, "the Commonwealth has an effective control regime that mitigates the risk, expense and impact of undesirable changes affecting providers".

The Auditor-General has recorded the premise of the 2020 changes to the critical infrastructure regime: the Government approved them "on the basis that the SoCI Act did not enable it to impose requirements on entities to protect their assets, and an over-reliance on the FATA to manage risks arising from foreign ownership." That is the ANAO's record of the reform's premise, in Auditor-General Report No. 38 2021–22 at its page 17. It is not a finding about the FATA, and this submission draws none from it.

The Hosting Certification Framework. Across the whole of that operative document the vocabulary of legal compulsion does not appear, while the vocabulary of ownership and control recurs. The nil is about the compellability concept and not about legal references: the document cites statutes, including the two foreign investment instruments above. The counts and the method behind that sentence are at Appendix A.

And the paper's own vocabulary. The consultation paper nowhere uses the language of compulsion under foreign law, and every use it makes of the word *jurisdiction* concerns Australian federal, state and territory jurisdictions or overseas regulatory comparators. The counts and the method are at Appendix A.

One interaction the paper may not have in view. The paper records at its page 9 that these facilities "can involve multiple entities, including facility owners, operators, tenants and AI developers", and that the government is still considering how requirements should be allocated among them. *Key terms* defines data centre owner, data centre user, large data centre and frontier AI, and does not define *frontier lab*, *hyperscaler* or *neocloud*, though the paper uses all three. The entity that can be compelled is not necessarily the entity a definition captures, and an allocation settled without that question in view can

place the obligation on one party and the exposure on another.

06 What this submission does not establish, and one question for the department

The questions this submission does not answer. Of the six questions the paper asks on security, safety and transparency and on a simple, consistent national framework, this submission answers four: the first, third, fourth and fifth. It does not answer the second, on designing conditions that keep pace with technological change while giving investors and operators sufficient legal certainty, because this practice has never assessed legal certainty and has no established basis to write from. It does not answer the sixth, on further regulatory reforms or incentives, because this submission is scoped to four questions. The six questions on investing in local capability, skills, research and innovation are outside its subject.

Two limits are stated here rather than left to be found. Since 31 August 2026 the Digital Transformation Agency's principles for coordinated contracting arrangements say the Agency will consider whether a proposed arrangement "presents risk if the seller, including any parent company, may be subject to laws, regulatory directions or other arrangements which could create risks that override or circumvent Australian contractual protections". Those principles were not among the instruments AOS-ASR-2026-001 read, and this submission makes no finding on whether they state a method. They reach no procurement outside those arrangements, which are mandated for non-corporate Commonwealth entities. So for a procurement through one, the Agency's own principles now say it will consider the exposure; this submission's statements are made outside them. Separately, the Commonwealth's guidance on AI procurement asks an agency to "Conduct a foreign ownership, control and influence (FOCI) evaluation", qualified in its own prose as "If applicable". That guidance is recommended rather than required, and such an evaluation tests ownership, control or influence, which is not compellability.

And one limit that bears directly on the paper's own words. The paper names the *Foreign Acquisitions and Takeovers Act 1975* at its pages 5 and 21. **This practice has not read that Act, its Regulation, or the Foreign Investment Policy, and makes no claim about what any of them requires.** Everything said above about foreign investment screening is taken from the Hosting Certification Framework's own description of the regime, which is a Commonwealth instrument describing another, and is cited as that and nothing more.

The question this submission cannot answer, and puts to the department. Does foreign investment screening, at any stage and under any of the instruments that compose it, ask whether the acquirer, the target, or a parent or affiliate of either, can be compelled

by a foreign authority to produce data held in Australia? If it does, the paper's reliance on that screening is sound and this concern is answered by material this practice has not seen. If it does not, the premise that sovereign AI capability relies on onshore infrastructure is carrying a weight none of the three instruments this submission examines has been asked to bear.

07 Independence, and payment

This submission is unsolicited, unfunded and uncommissioned. No party paid for it, asked for it, reviewed it or saw it before lodgement. It is not connected to any engagement and no engagement is sought from it.

This submission was drafted with the assistance of AI tools, including Claude, developed by Anthropic. The paper's conditions for AI training are addressed to developers of frontier AI models, and a reader may count Anthropic among them. **No person at Anthropic or at any other company reviewed or saw this submission before lodgement.**

AustraliaOS Pty Ltd sells assessment of the exposure this submission says is unassessed, and that is disclosed here rather than left to be discovered. The practice's position is that independence lies in the verdict being unbought, not in there being nothing to buy, and the answer it offers is structural rather than a promise. Every factual assertion above about an instrument, a report or the consultation paper traces to a source pinned by SHA-256 that any reader can obtain and hash, and rests on no interview, news report or commentary. Every negative names the population it is established over. What this submission does not establish is printed in it, at section 06, before anyone asks.

08 Status of this document

This document is lodged and is not yet published. AustraliaOS Pty Ltd publishes its assessments with a verification page carrying the document's SHA-256, and will publish this one after lodgement so that the copy the department holds and the copy any reader can fetch are the same bytes. Until then it carries no verification address, and its integrity claim is the hash of the lodged file.

Appendix A. Sources, and the counts the body refers to

Every source below is pinned by SHA-256 in a tracked register of this practice. **An inherited capture states where it came from and when its hash was re-verified**, which is this practice's settled form.

1. *Getting it right: Building AI infrastructure that works for Australia*, Consultation Pa-

- per, September 2026, 28 pp. SHA-256 691891b7d5df2495.
2. Hosting Certification Framework, March 2021 version 2, the operative framework document, 30 pp. SHA-256 7b654f6e435bb905.
 3. *Security of Critical Infrastructure Act 2018*, Compilation No. 9 (C2026C00213), compilation date 4 June 2026, authorised PDF. SHA-256 3a0a2c0a2b49efe9.
 4. Cyber and Infrastructure Security Centre, Responsible Entity CIRMP Part 2A and Part 2AA Annual Report, the approved online form; its complete field schema is embedded in the page source. SHA-256 08d0c24a579e41c8.
 5. Digital Transformation Agency, coordinated contracting arrangement principles, SHA-256 e987fcb79c8d04dc; *CCAs vs other procurement and contracting arrangements*, the source of “mandated for non-corporate Commonwealth entities”, SHA-256 1c9817a1dff1d524; and the release dating the principles 31 August 2026, SHA-256 6e69fc28d667783b.
 6. Guidance on AI procurement in government, SHA-256 0a4756f2a29b22b6; and the AI procurement checklist, SHA-256 2ca910f7b4dad370.
 7. AOS-ASR-2026-001 v1.5, AOS-RCH-2026-001 v1.0, AOS-CMP-2026-001 v1.4, AOS-HCE-2026-001 v1.2, AOS-AIDC-2026-001 v1.1 and its supplement SUPP-02, all published by this practice with verification records carrying their hashes.
 8. Auditor-General Report No. 38 2021–22, *Administration of Critical Infrastructure Protection Policy*, 67 pp, page 17. SHA-256 e33079ba26985ab2.

Items 3, 4 and 8 are inherited captures. The *Security of Critical Infrastructure Act 2018* compilation was retrieved on 4 August 2026 under `general-findings/submarine-cable-scoping-2026-08` and re-verified against its recorded hash on 20 September 2026. The annual report form page was retrieved on 5 August 2026 under `attestation-survey-scoping-2026-08` and re-verified against its recorded hash on 20 September 2026. The Auditor-General’s report was retrieved on 12 August 2026 under `hosting-exemption-followon-2026-08` and re-verified against its recorded hash on 23 September 2026. Retrieval and re-verification are distinct acts and both dates are recorded.

Page citations. The consultation paper’s printed page 1 is its PDF page 3. The Hosting Certification Framework’s printed page 1 is its PDF page 4. In the Act, sections 30AB, 30AG and 30AQ are at printed pages 88, 91 to 92 and 106 to 107 of Compilation No. 9. Every passage this submission quotes was read at image resolution before it was used; the text layer was a locating aid only.

The counts section 05 refers to, each stated with the width it was taken over.

In the Hosting Certification Framework (source 2), over the whole 30-page document,

text extracted with pdftotext -layout, de-hyphenated across line breaks, whitespace normalised, counted case-insensitively as substrings: *jurisdiction*, *compel*, *offshore*, *on-shore*, *located*, *FOCI* and *beneficial* each return nil, as does *law*, including *laws* and *lawful*; *ownership* occurs 40 times, *control* 40 and *foreign* 19. This count is AOS-HCE-2026-001 v1.2's, at its printed page 17, and its method is stated there. **A frequency is not a distribution, so the distribution was measured separately for this submission:** over the same extraction, *ownership* appears on 14 of the 30 pages and *control* on 15. Section 05 says these words recur, which is what the counts show; it does not say they appear throughout, which they do not.

In the consultation paper (source 1), over all 28 pages, on a whitespace-folded extraction of its text layer, counted case-insensitively: *compellab-*, *foreign law*, *extraterritorial* and *CLOUD Act* each return nil. *Jurisdiction* returns ten sentences, and each was read individually.

In the approved annual report form (source 4), over all 308 field labels in its embedded schema: *jurisdiction*, *ownership*, *foreign*, *compel*, *offshore* and *overseas* each return nil. *Incorporation* returns two labels and both ask the **reporting entity** about itself, "Country of incorporation or creation" and a business number "if the Entity was incorporated, formed or created outside Australia"; neither is asked about a supplier.

What a count of this kind is, and is not. Each figure above is a result about the extraction named and the width named, not about the document in the abstract. A contiguous-phrase probe returns a zero about contiguous phrases. Where a sentence in this submission rests on a count, the count is here and the reader can repeat it.

End of document.