AustraliaOS Pty Ltd

The Jurisdiction Gap

The mechanism already exists: how a rule made in June 2026 asks the jurisdictional question of nine asset classes and not of the classes that hold government data. A second supplement to submission AOS-AIDC-2026-001 to the Senate inquiry into artificial intelligence and data centres.

REFERENCE	DATE	CLASSIFICATION	SUPPLEMENTS
AOS-AIDC-2026-001-SUPP-02	August 2026	Public	AOS-AIDC-2026-001-v1.1

Contents

01 Purpose of this supplement, and a narrowed recommendation

This supplement is made by AustraliaOS Pty Ltd (ABN 69 697 049 291) and is authored by its director, Brunel Al-Bijwaie. It supplements submission AOS-AIDC-2026-001 and the first supplement, and should be read with both.

Recommendation D of the original submission asked the committee to "require the official approving a Commonwealth AI infrastructure procurement assessed under Recommendation B to attest in writing to having considered jurisdictional exposure."[1] That recommendation, as drafted, asked for a mechanism to be created.

Further primary-source work since lodgement has established that the mechanism does not need to be created. The Commonwealth already operates a board-approved annual security report with an attestation on its face, and a rule made on 10 June 2026 has already written the jurisdictional question into a vendor-assessment obligation — for nine asset classes that do not include the ones that hold government data. This supplement therefore narrows Recommendation D. The narrowed ask is smaller, not larger: it no longer asks the committee to recommend a new regime, only that an existing rule's application be extended and an existing form ask one further question. A smaller ask matters to the committee because it can be implemented without legislation, within instruments the responsible Minister and department already maintain.

02 The question is already written, in a rule made this year

The Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023, as amended with effect from 10 June 2026, provide at rule 10A that a responsible entity must maintain a vendor-assessment process, and that:

> (5) The system or process outlined in subsection (4) must identify, for each existing or proposed major supplier:
>
> (a) in relation to FOCI risks—legislative or other legal requirements to which the supplier is subject to; and
> (b) restrictions, sanctions or other impediments affecting the jurisdiction to which the entity may be subject to; and
> (c) the access, influence and control the supplier has over the CI asset in connection with the product or service the supplier provides; ...[2]

"FOCI" is defined in the rules as "foreign ownership, control or influence."[3] The citation is the authorised compilation: LIN 23/006, Compilation No. 2, F2026C00562, compilation

[1] AOS-AIDC-2026-001-v1.1, Recommendation D. See Appendix A, item 1.
[2] CIRMP Rules, Compilation No. 2 (F2026C00562), rule 10A(5). See Appendix A, item 2.
[3] CIRMP Rules, Compilation No. 2 (F2026C00562), rule 3 (definition of FOCI). See Appendix A, item 2.

date 10 June 2026.

Rule 10A carries a 24-month implementation period: under subrule 4A(6)(b), it does not apply to an asset that was already a critical infrastructure asset until the end of the period of 24 months after the amendment's commencement — that is, until the end of 10 June 2028 — and, for an asset that becomes a critical infrastructure asset later, until 24 months after it does.[4] This supplement relies on the obligation's drafting, not its commencement date: the question has been written into a Commonwealth rule, and nine asset classes are committed to answering it. Extending the rule now would bring the excluded classes inside the same implementation period rather than starting a later one.

What this establishes is narrow and checkable: the Commonwealth has already drafted the jurisdictional question. Paragraph 10A(5)(a) — the legal requirements a supplier is subject to — is the question the original submission asked to have asked. No new legislative concept is required.

03 It does not apply where government data sits

Rule 10A applies only to the asset classes specified in subrule 4A(1):

> (a) a critical broadcasting asset; (b) a critical domain name system; (c) a critical electricity asset; (d) a critical energy market operator asset; (e) a critical freight infrastructure asset; (f) a critical freight services asset; (g) a critical gas asset; (h) a critical liquid fuel asset; (i) a critical water asset.[5]

Critical data storage or processing assets are specified in rule 4(1), the baseline list, and do not appear in subrule 4A(1). Critical telecommunications assets appear in neither list: they enter the risk-management regime through the Security of Critical Infrastructure (Telecommunications Security and Risk Management Program) Rules 2025, whose supply-chain provision mirrors the baseline and carries no jurisdiction language.[6]

The one Commonwealth instrument that requires the jurisdictional question to be asked of suppliers does not apply to the asset classes that store and carry government data.

04 The exclusion is unexplained, and it was raised

The explanatory statement to the amending instrument (LIN 26/075, F2026L00701) runs to 64 pages; the phrase "data storage" does not appear in it.[7] The consultation paper of December 2025 displays the choice in a table — data storage or processing in the

[4] CIRMP Rules, Compilation No. 2 (F2026C00562), subrule 4A(6)(b). See Appendix A, item 2.

[5] CIRMP Rules, Compilation No. 2 (F2026C00562), subrule 4A(1). See Appendix A, item 2.

[6] Telecommunications SRMP Rules 2025, ss 5, 7 and 14; the supply-chain comparison is with rule 10 of the CIRMP Rules. See Appendix A, items 2 and 3.

[7] Explanatory Statement to F2026L00701. See Appendix A, item 4.

"subject to existing CIRMP" column — and explains only the classes outside the risk-management regime entirely, which are covered by alternative frameworks.[8] The department's published feedback summary for the exposure draft addresses implementation timeframes, grace periods and costs.[9]

The extension was asked for. Three published submissions to the consultations sought it: Good Ancestors Policy recommended in terms that the enhanced rules be extended to critical data storage or processing assets;[10] Global Shield Australia proposed the drafting itself — "insert: (j) a critical data storage or processing asset" — and noted the interaction with the Hosting Certification Framework exemption;[11] and SAP Australia, itself the responsible entity for a critical data storage or processing asset, argued that the excluded class is a cross-sector enabler on which the covered classes depend.[12]

No departmental response to those calls appears in the published record, and no reason for the exclusion is published in any document this practice has located. This supplement does not infer a reason and does not characterise the department's conduct. The observation is confined to the public record: the question was raised, and the published record does not answer it.

05 The attestation surface already exists

Section 30AG(2)(f) of the Security of Critical Infrastructure Act 2018 requires the annual report on a risk-management program, "if the entity has a board, council or other governing body," to be "approved by the board, council or other governing body, as the case requires."[13] The approved form — the Cyber and Infrastructure Security Centre's annual report web form — carries a personal declaration in attestation terms:

> I attest that this Annual Report provided by the Responsible Entity in relation to the Entity's CIRMP for its critical infrastructure asset(s) has been approved by that Responsible Entity's board, council or governing body, in accordance with section 30AG(2)(f) of the Security of Critical Infrastructure Act 2018.[14]

The form closes with an acknowledgement that knowingly providing false or misleading information to the Commonwealth is an offence under the Commonwealth Criminal

[8] Consultation paper (December 2025), Table 1. See Appendix A, item 5.
[9] Feedback summary, Exposure Draft of the enhanced CIRMP Rules. See Appendix A, item 6.
[10] Good Ancestors Policy submission, Recommendation 1. See Appendix A, item 7.
[11] Global Shield Australia submission. See Appendix A, item 8.
[12] SAP Australia submission. See Appendix A, item 9.
[13] Security of Critical Infrastructure Act 2018, s 30AG(2)(f). See Appendix A, item 10.
[14] CISC annual report form (Part 2A and Part 2AA), Section 1 attestation declaration. See Appendix A, item 11.

Code.[15]

The same form already asks four supplier questions that go beyond the statutory minimum: whether an alternate supply chain is identified for critical operations; whether major suppliers are required to undergo regular security audits, and how often; whether major suppliers are required to implement technical and operational controls protecting the entity's data; and whether suppliers are required to notify security incidents or data breaches.[16] None of the four reaches ownership, jurisdiction, incorporation or foreign legal reach.

What this establishes: the reporting surface exists, it is board-approved and attested, it already asks about suppliers, and adding one question to it is a form change.

06 The population this inquiry concerns is inside the form already

Section 30AB(4) of the Act exempts an asset from the risk-management regime where the responsible entity holds a certificate of hosting certification at the strategic level under the Hosting Certification Framework and the asset is used in connection with the provision of the certified services. Section 30AQ still requires those entities to submit a board-approved annual report, stating why the exemption applies.[17]

The approved form serves both regimes, and its selection list for exempt entities is the list of strategic-certified hosting services itself.[18] For those entities, the form asks the basis of the exemption and the statutory hazard statements; there is no supplier obligation behind it, because the risk-management program whose supplier machinery would generate one does not apply.

This is stated carefully, because it should not be overstated. The exemption is lawful and deliberate: certification at the strategic tier is the Framework's highest assurance, and Parliament chose to let it substitute for the risk-management program. The observation is only this: for the providers that hold certified government data, the substitute report asks nothing about suppliers, and the certified obligations that stand in place of the program are set out in a Deed of Certification that is not public.[19]

[15] CISC annual report form (Part 2A and Part 2AA), Section 5 acknowledgement. See Appendix A, item 11.
[16] CISC annual report form (Part 2A and Part 2AA), Section 3 supplier questions. See Appendix A, item 11.
[17] Security of Critical Infrastructure Act 2018, ss 30AB(4) and 30AQ. See Appendix A, item 10.
[18] CISC annual report form (Part 2A and Part 2AA), Part 2AA certified-services selection list. See Appendix A, item 11.
[19] AOS-CMP-2026-001 (the Deed of Certification is named as not public). See Appendix A, item 12.

07 The technical authority still stops at foreign ownership

On 5 August 2026 the Australian Signals Directorate, with the Australian Institute of Company Directors, published "Frontier AI cyber threat considerations for boards of directors." It asks boards three times to assess the foreign ownership, control or influence of their AI vendors, including in its threshold questions:

> Are we relying on vendors and service providers without sufficient governance and oversight, including an understanding of their foreign ownership, control or influence?[20]

The publication does not ask whether a provider can be lawfully compelled by a foreign government to act on data or capability it holds. A cyber-threat publication is not obliged to cover lawful process, and this supplement does not suggest it failed. The observation is about where the guidance stops: current Commonwealth guidance for boards reaches ownership and does not reach compellability. That boundary is the finding of this practice's published assessment of the Foreign Ownership, Control or Influence guidance,[21] and its published assessment of the Hosting Certification Framework's strategic tier identifies the certified population to which the boundary applies.[22]

08 Recommendations

Recommendation D of the original submission is narrowed to the following, each a single change to a single instrument:

Recommendation D1. Extend subrule 4A(1) of the Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023 — or the application of rule 10A — to critical data storage or processing assets and critical telecommunications assets.

Recommendation D2. Add to the approved annual report form, for both Part 2A and Part 2AA reporting, a question requiring the responsible entity to state whether the jurisdictional exposure of its major suppliers — the legislative or other legal requirements those suppliers are subject to — was considered.

The first is a rule amendment of a kind the Minister made on 10 June 2026; the second is a change to a form the department already maintains — its page states it was last updated on 17 June 2026. Neither requires legislation.

One further element would serve the committee, and it is proposed conditionally. The Hosting Certification Framework is under reform, with certification registrations paused

[20] ASD and AICD, Frontier AI cyber threat considerations for boards of directors. See Appendix A, item 13.
[21] AOS-CMP-2026-001. See Appendix A, item 12.
[22] AOS-HCF-2026-001. See Appendix A, item 14.

since 3 November 2025.[23] **Recommendation D3.** In concluding that reform, publish the ownership, control and supplier obligations that certification imposes — the operative terms now carried in the non-public Deed of Certification — so that the Part 2AA report of an exempt entity can be read against a public standard. This asks for publication of obligations, not their alteration.

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

09 Evidence base

Every instrument cited in this supplement was captured from its primary source, hashed, and pinned to a register on the date of capture. The Security of Critical Infrastructure Act 2018 was read from the authorised compilation C2026C00213 (Compilation No. 9, compiled 4 June 2026), captured 4 August 2026. The CIRMP Rules were read from the authorised compilation F2026C00562 (Compilation No. 2, compiled 10 June 2026), the amending instrument F2026L00701 and its explanatory statement from their authorised versions, and the Telecommunications SRMP Rules from F2025L00325, all captured 5 August 2026. The consultation papers, the departmental feedback summary and the published submissions were captured from the Department of Home Affairs' consultation pages on 5 August 2026. The CISC annual report form page, whose complete field schema is embedded in the page source, was captured on 5 August 2026 (the page states it was last updated 17 June 2026). The ASD–AICD publication was captured, page and PDF, on 5 August 2026, its first day of public availability. SHA-256 hashes and retrieval times for each capture are held in the practice's registers. The assessments cited — AOS-CMP-2026-001 and AOS-HCF-2026-001 — are published with verification records at the addresses in Appendix A.

Two limits are stated on the face of this supplement. What any entity actually reported in its annual reports is not public, so nothing here asserts that any entity has or has not considered jurisdiction. And the published submissions are the subset the department chose to publish, so the record of who raised the exclusion is necessarily partial.

Appendix A. Sources

1. AOS-AIDC-2026-001-v1.1, Recommendation D (as lodged in this inquiry).
2. Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023, Compilation No. 2 (F2026C00562), compilation date 10 June 2026, rules 3, 4, 4A and 10A. https://www.legislation.gov.au/F2023L00112/2026-06-10/2026-06-10/text/original/pdf
3. Security of Critical Infrastructure (Telecommunications Security and Risk Manage-

[23] Hosting Certification Framework, Framework page. See Appendix A, item 15.

ment Program) Rules 2025 (F2025L00325), sections 7 and 14. https://www.legislation.gov.au/F2025L00325/2025-03-11/2025-03-11/text/original/pdf

4. Explanatory Statement, Security of Critical Infrastructure Legislation Amendment (Enhanced Critical Infrastructure Risk Management Program) Rules 2026 (LIN 26/075, F2026L00701). https://www.legislation.gov.au/F2026L00701/2026-06-09/2026-06-09/es/original/pdf
5. Department of Home Affairs, Consultation paper: proposed amendments to enhance the CIRMP Rules (December 2025), Table 1. https://www.homeaffairs.gov.au/how-to-engage-us-subsite/files/consultation-on-enhancements-to-cirmp-rules/consultation-paper-proposed-amendments-enhance-cirmp.pdf
6. Department of Home Affairs, Feedback summary: Exposure Draft of the enhanced CIRMP Rules. https://www.homeaffairs.gov.au/how-to-engage-us-subsite/files/ministerial-directions-powers-and-exposure-draft/summary-exposure-draft-cirmp-rules.pdf
7. Good Ancestors Policy, submission to the enhanced CIRMP Rules consultation, Recommendation 1. https://www.homeaffairs.gov.au/how-to-engage-us-subsite/files/consultation-on-enhancements-to-cirmp-rules/good-ancestors-policy.pdf
8. Global Shield Australia, submission on the Exposure Draft of the enhanced CIRMP Rules. https://www.homeaffairs.gov.au/how-to-engage-us-subsite/files/ministerial-directions-powers-and-exposure-draft/GlobalShieldAustralia2.pdf
9. SAP Australia, submission on the Exposure Draft of the enhanced CIRMP Rules. https://www.homeaffairs.gov.au/how-to-engage-us-subsite/files/ministerial-directions-powers-and-exposure-draft/SAPAustralia.pdf
10. Security of Critical Infrastructure Act 2018, Compilation No. 9 (C2026C00213), compilation date 4 June 2026, sections 30AB(4), 30AG and 30AQ. https://www.legislation.gov.au/C2018A00029/2026-06-04/2026-06-04/text/original/pdf
11. Cyber and Infrastructure Security Centre, Responsible Entity Critical Infrastructure Risk Management Program Part 2A and Part 2AA — Annual Report (online form; page states last updated 17 June 2026). https://www.cisc.gov.au/resources/online-forms/responsible-entity-risk-management-program-annual-report
12. AOS-CMP-2026-001, published with verification record. https://australiaos.com.au/verify/AOS-CMP-2026-001
13. Australian Signals Directorate with the Australian Institute of Company Directors, Frontier AI cyber threat considerations for boards of directors (published 5 August 2026). https://www.cyber.gov.au/business-government/protecting-business-leaders/cyber-security-for-business-leaders/frontier-ai-cyber-threat-considerations-for-boards-of-directors
14. AOS-HCF-2026-001, published with verification record. https://australiaos.com.au

/verify/AOS-HCF-2026-001

15. Department of Home Affairs, Hosting Certification Framework, Framework page (reform notice; registrations paused from 3 November 2025). https://www.hostingcertification.gov.au/framework

End of supplement.