AustraliaOS Pty Ltd

The Jurisdiction Gap

The second supplement stated that the exclusion of critical data storage or processing from the enhanced risk-management tier is unexplained. It is explained, in the instrument that supplement cited. A correction, and a third supplement to submission AOS-AIDC-2026-001 to the Senate inquiry into artificial intelligence and data centres.

REFERENCE	DATE	CLASSIFICATION	CORRECTS
AOS-AIDC-2026-001-SUPP-03	August 2026	Public	AOS-AIDC-2026-001-SUPP-02

Copyright © 2026 AustraliaOS Pty Ltd. ABN 69 697 049 291. Decision support, not statutory authority. Signed by Brunel Al-Bijwaie, Director.

Contents

01 Purpose of this supplement 4
02 What was lodged 4
03 What the record says 4
04 The corrected position 5
05 Why the earlier statement was wrong 6
06 What does not change 7
Appendix A. Sources 9

01 Purpose of this supplement

This supplement corrects the second supplement. It withdraws a finding and replaces it with a narrower one. No recommendation is added, withdrawn or qualified.

The correction is this. The second supplement, lodged in August 2026, stated that the exclusion of critical data storage or processing assets from the enhanced risk-management tier is unexplained, and that no reason for it is published anywhere this practice had located. **A reason is published. It is in the instrument that supplement itself cited, in three places, and a departmental response to the question of asset-class scope is in the same instrument.** None of the four passages names the excluded class, which is why a search for the class's name did not find them.

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

02 What was lodged

The second supplement's section 04 is headed "The exclusion is unexplained, and it was raised". It closes:

> 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.[1]

The finding rested on a count, reported in the same section: the explanatory statement to the amending instrument "runs to 64 pages; the phrase 'data storage' does not appear in it."[2]

That count is correct, and has been re-established for this supplement by reading all 64 pages as page images rather than as extracted text.[3]

03 What the record says

The explanatory statement carries a Statement of Compatibility with Human Rights at Attachment B, and an *Addendum to the 2022 Regulation Impact Statement* at Attachment C, pages 30 to 64. Both are part of the instrument as registered.

The Statement of Compatibility gives the reason, at printed page 23:

> The Amendment Rules aim to strengthen these obligations further by introduc-

[1] AOS-AIDC-2026-001-SUPP-02, section 04 and Recommendation D1. See Appendix A, item 1.
[2] AOS-AIDC-2026-001-SUPP-02, section 04 and Recommendation D1. See Appendix A, item 1.
[3] Explanatory Statement to F2026L00701, all 64 pages. See Appendix A, item 2.

Copyright © 2026 AustraliaOS Pty Ltd. ABN 69 697 049 291. Decision support, not statutory authority. Signed by Brunel Al-Bijwaie, Director.

> ing further, enhanced security obligations for critical infrastructure assets in sectors that Australia's intelligence agencies have identified are most at risk.[4]

The same page then lists the nine asset classes to which the enhanced obligations apply.[5]

The Addendum gives it again, at printed page 36:

> The proposed amendments to the CIRMP Rules are intended to increase risk management requirements for asset classes that pose the greatest potential consequences for Australia's national security and economic stability. These amendments align with assessments by the National Intelligence Community (NIC), which have identified sectors and asset classes as at elevated risk.[6]

The Addendum states, at printed page 38, the only class-specific justification the instrument offers. Some classes are outside the enhanced tier because another regime already reaches them:

> In some cases, asset classes not captured by the enhanced CIRMP Rules are subject to alternative regulatory frameworks that impose comparable obligations. This includes asset classes regulated under:[7]

The four named are the *Aviation Transport Security Act 2004*, the *Maritime Transport and Offshore Facilities Security Act 2003*, APRA Prudential Standard CPS 230 — Operational Risk Management, and the Defence Industry Security Program.[8]

And the Addendum answers the scope question at printed page 54, in a table of consultation themes. Against the theme "Asset-class scope and proportionality", the policy design response is:

> Enhanced obligations remain limited to nine specified asset classes identified as higher risk.[9]

04 The corrected position

The second supplement's finding does not survive. What replaces it is narrower, and it is set out here so that the committee can see exactly what is and is not established.

[4] Explanatory Statement to F2026L00701, Attachment B, printed page 23. See Appendix A, item 2.

[5] Explanatory Statement to F2026L00701, Attachment B, printed page 23. See Appendix A, item 2.

[6] Explanatory Statement to F2026L00701, Attachment C, section 1.2, printed page 36. See Appendix A, item 2.

[7] Explanatory Statement to F2026L00701, Attachment C, section 1.3, printed page 38. See Appendix A, item 2.

[8] Explanatory Statement to F2026L00701, Attachment C, section 1.3, printed page 38. See Appendix A, item 2.

[9] Explanatory Statement to F2026L00701, Attachment C, Table 11, printed page 54. See Appendix A, item 2.

Copyright © 2026 AustraliaOS Pty Ltd. ABN 69 697 049 291. Decision support, not statutory authority. Signed by Brunel Al-Bijwaie, Director.

First, the selection is explained, and the explanation rests on assessments that are not public. The instrument attributes the choice of the nine classes to the National Intelligence Community and to what Australia's intelligence agencies have identified.[10][11] This supplement says nothing about the content or quality of those assessments. It observes only that the reason given cannot be checked against a published standard, because the standard is not published.

Second, the one published class-specific justification does not reach this class. Where the instrument explains an exclusion by pointing to another regime, it names four.[12] Critical data storage or processing assets fall under none of them, and the class is not named anywhere in the 64 pages.[13]

Third, the response to the scope question names no class. It records that the enhanced obligations remain limited to the nine identified as higher risk,[14] addresses no particular class that was not selected, and responds to no submitter.

The accurate statement is therefore not that the exclusion is unexplained. It is that the exclusion is **explained by reference to an unpublished assessment, and falls outside the only published class-specific justification the instrument gives.**

05 Why the earlier statement was wrong

The search that produced the earlier finding looked for the excluded class. It counted occurrences of "data storage" in the explanatory statement, found none, and treated the absence as the absence of a reason.

That could not have worked. The instrument explains the selection positively — by stating why the nine classes were chosen — and a document that explains a choice that way need never name what it left out. A search for the excluded thing's name cannot see a reason expressed in terms of the things included.

Two of the four passages sit in attachments to the explanatory statement. **The practice should have read the attachments.** They are part of the registered instrument, they were in the file it had retrieved and pinned, and nothing prevented it from reading them.

[10] Explanatory Statement to F2026L00701, Attachment B, printed page 23. See Appendix A, item 2.

[11] Explanatory Statement to F2026L00701, Attachment C, section 1.2, printed page 36. See Appendix A, item 2.

[12] Explanatory Statement to F2026L00701, Attachment C, section 1.3, printed page 38. See Appendix A, item 2.

[13] Explanatory Statement to F2026L00701, all 64 pages. See Appendix A, item 2.

[14] Explanatory Statement to F2026L00701, Attachment C, Table 11, printed page 54. See Appendix A, item 2.

Copyright © 2026 AustraliaOS Pty Ltd. ABN 69 697 049 291. Decision support, not statutory authority. Signed by Brunel Al-Bijwaie, Director.

06 What does not change

This correction withdraws no recommendation and qualifies none. A stated reason for selecting nine asset classes does not address whether a tenth should be added, so the correction in sections 03 to 05 leaves every recommendation where it was.

But one of them has a limit, and this practice states it here rather than leaving it to be found.

Recommendation D1 asked that subrule 4A(1) of the CIRMP Rules, or the application of rule 10A, be extended to critical data storage or processing assets and critical telecommunications assets.[15] Both provisions sit inside Part 2A of the Security of Critical Infrastructure Act 2018. Subrule 4A(1) is made "for the purposes of paragraph 30AH(2)(b) of the SOCI Act",[16] and rule 10A is made "for paragraph 30AH(1)(c) of the SOCI Act".[17] Section 30AH is a provision of Part 2A.[18]

Section 30AB(4) provides that where an entity holds a certificate of hosting certification at the strategic level, and a critical infrastructure asset or a part of one is used in connection with the certified services, and the entity is the responsible entity for the asset, "this Part does not apply to the asset".[19] **A rule made for the purposes of section 30AH therefore does not reach an asset that section 30AB(4) has taken outside Part 2A.**

So D1 as drafted would reach a critical data storage or processing asset only where the exemption does not apply — where the responsible entity holds no strategic-level certificate, or the asset is not used in connection with the certified services. Where all of section 30AB(4)'s conditions are met, extending subrule 4A(1) would not reach the asset. **The critical telecommunications limb of D1 is unaffected**, because those assets enter the risk-management regime through a different instrument.[20]

Recommendation D2 operates where D1 does not. It asks for the jurisdictional question on the approved annual report form "for both Part 2A and Part 2AA reporting",[21] and Part 2AA is the reporting regime that applies to an asset covered by section 30AB(4).[22] The gap D1 leaves is the gap D2 was drafted across.

[15] AOS-AIDC-2026-001-SUPP-02, section 04 and Recommendation D1. See Appendix A, item 1.
[16] Explanatory Statement to F2026L00701, Attachment A, printed page 7. See Appendix A, item 2.
[17] Explanatory Statement to F2026L00701, Attachment A, printed page 18. See Appendix A, item 2.
[18] Security of Critical Infrastructure Act 2018, Compilation No. 9 (C2026C00213), compilation date 4 June 2026, sections 30AB(4), 30AH and Part 2AA. See Appendix A, item 6.
[19] Security of Critical Infrastructure Act 2018, Compilation No. 9 (C2026C00213), compilation date 4 June 2026, sections 30AB(4), 30AH and Part 2AA. See Appendix A, item 6.
[20] AOS-AIDC-2026-001-SUPP-02, section 04 and Recommendation D1. See Appendix A, item 1.
[21] AOS-AIDC-2026-001-SUPP-02, section 04 and Recommendation D1. See Appendix A, item 1.
[22] Security of Critical Infrastructure Act 2018, Compilation No. 9 (C2026C00213), compilation date 4 June 2026, sections 30AB(4), 30AH and Part 2AA. See Appendix A, item 6.

Copyright © 2026 AustraliaOS Pty Ltd. ABN 69 697 049 291. Decision support, not statutory authority. Signed by Brunel Al-Bijwaie, Director.

A narrowed replacement for D1 is not attempted here. Reaching an exempt asset means either amending section 30AB(4) itself — which D1 was narrowed specifically to avoid, because it would require legislation — or working through Part 2AA. That is a question of design, not a correction, and a correction document is the wrong place to answer it. It is recorded as owed.

One consequence for Recommendation C, stated no further than the provision supports. Section 30AB(4) speaks of "a critical infrastructure asset, or a part of a critical infrastructure asset", and is not limited by asset class.[23] Recommendation C asks that the Act's critical asset definitions be extended to AI infrastructure; any class so added would come within reach of section 30AB(4) on the same terms as the classes already there. **Nothing further is claimed**, and C is not withdrawn or qualified.

Recommendations D3, and A, B, E and F of the original submission, are untouched.

What this supplement does not claim. Stated on its face, because a correction can be misread as more than it is:

1. That the National Intelligence Community assessments are wrong, absent, or improperly relied on. They are not public and nothing is asserted about them.
2. That the exclusion of critical data storage or processing was deliberate, or that it was an oversight. Neither is established and neither is inferred.
3. That any department, official or provider acted wrongly. The Department published a reason; the observation concerns what the reason reaches.
4. That Parliament was misled.
5. That the alternative frameworks named at page 38 are, or are not, adequate for the classes they cover. The instrument names them; this supplement assesses none of them.
6. That the published consultation record is complete. It is the subset the Department chose to publish, as the second supplement recorded.
7. That the practice's earlier statement was made carelessly. Its cause is stated in section 05 and nothing beyond that is claimed.

One further matter, recorded and not pursued. Items 12 and 14 of the second supplement's Appendix A cite two of this practice's published assessments by address without their hashes, and both are documents capable of revision. The citations in this supplement carry hashes.

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

[23] Security of Critical Infrastructure Act 2018, Compilation No. 9 (C2026C00213), compilation date 4 June 2026, sections 30AB(4), 30AH and Part 2AA. See Appendix A, item 6.

Copyright © 2026 AustraliaOS Pty Ltd. ABN 69 697 049 291. Decision support, not statutory authority. Signed by Brunel Al-Bijwaie, Director.

Appendix A. Sources

1. AOS-AIDC-2026-001-SUPP-02, as lodged in this inquiry, section 04 and Recommendation D1.
2. Explanatory Statement to the Security of Critical Infrastructure Legislation Amendment (Enhanced Critical Infrastructure Risk Management Program) Rules 2026 (LIN 26/075, F2026L00701), authorised version registered 9 June 2026, 64 pages, including Attachments B and C. Retrieved 5 August 2026; every page read at image resolution 13 August 2026. https://www.legislation.gov.au/F2026L00701/2026-06-09/2026-06-09/es/original/pdf
3. AOS-HCE-2026-001 v1.1, SHA-256 f4ad8bb3e087cccf…, published with verification record. https://australiaos.com.au/verify/AOS-HCE-2026-001
4. AOS-HCF-2026-001, SHA-256 7ac47464508b5656…, published with verification record. https://australiaos.com.au/verify/AOS-HCF-2026-001
5. AOS-CMP-2026-001, SHA-256 54801ebc3b299397…, published with verification record. https://australiaos.com.au/verify/AOS-CMP-2026-001
6. Security of Critical Infrastructure Act 2018, Compilation No. 9 (C2026C00213), compilation date 4 June 2026, sections 30AB(4), 30AH, and Part 2AA (section 30AQ). https://www.legislation.gov.au/C2018A00029/latest/text

End of supplement.

Copyright © 2026 AustraliaOS Pty Ltd. ABN 69 697 049 291. Decision support, not statutory authority. Signed by Brunel Al-Bijwaie, Director.