AUSTRALIAOS

DECISION INFRASTRUCTURE FOR AUSTRALIAN INSTITUTIONS

australiaos.com.au

CLASSIFICATION | RELEASED—DECISION SUPPORT

JURISDICTIONAL EXPOSURE ASSESSMENT · NO.001

The Compellability *Gap*

In Commonwealth Cloud Assurance

REFERENCE	DATE	CLASSIFICATION	VERSION
AOS-CMP-2026-001-v1.1	6 July 2026	Released	1.1

Contents

1. Scope

This assessment examines two Australian Government instruments, the Foreign Ownership, Control or Influence Risk Assessment Guidance and the Hosting Certification Framework, and puts one question to each. Does the instrument, as published, test whether a certified or cleared provider can be lawfully compelled by a foreign government to disclose the data it holds. Amazon Web Services appears throughout as a worked example, because it is a provider that Home Affairs certifies at the Framework's highest tier and would also route out of the FOCI assessment at its first question. It is an exhibit of how the instruments treat a class of provider. It is not the subject.

The assessment rests on the public record alone. The instruments' own published text, the providers' own published statements, the government's own certification registers, and primary corporate filings. Every claim can be checked against a source a reader can open, and where a step is inference rather than record it is marked as inference. The finding that follows is deliberately narrow. It does not say Australian Government data is being taken. It says the two instruments relied on to guard against that possibility do not ask the question that would catch it.

(The full statement of what this assessment does not claim is held at Section 7, Bounds.)

---

2. Finding

The Australian Government relies on two instruments to assure the sovereignty of the cloud providers it procures, the Foreign Ownership, Control or Influence Risk Assessment Guidance and the Hosting Certification Framework. Both are administered by the Department of Home Affairs. Neither tests whether a certified provider can be lawfully compelled by a foreign government to disclose or hand over the data it holds. A United States owned provider is routed out of the FOCI assessment at its first question, because its owner sits inside the Five Eyes, before the compulsion question in Section 2 is reached. That same provider can hold the Framework's highest tier, Strategic, the level the Framework presents as its strongest assurance of sovereignty.

The gap is not that these instruments overlook foreign compulsion. The FOCI guidance acknowledges that allied governments can lawfully compel vendors, and it offers criteria for judging whether that compulsion is lawful. But it weighs the lawfulness of the foreign demand, not the exposure that demand creates for the Australian customer, and it routes a Five Eyes owned provider out of the assessment before even that weighing is applied. The Hosting Certification Framework, for its part, certifies ownership and control without

testing compellability at all.

The consequence is narrow and it is documented on the government's own record. A provider reachable under the United States CLOUD Act can clear both instruments and stand certified as sovereign. Not because either instrument tested foreign compulsion and cleared it, but because a lawful demand and an unlawful one end the same way, with the customer's data in a foreign government's hands, and neither instrument measures that.

---

3. The two instruments and their one owner

The first is the Foreign Ownership, Control or Influence Risk Assessment Guidance, published by the Department of Home Affairs. It gives organisations a repeatable method to identify whether a technology vendor is subject to foreign ownership, control, or influence, and to weigh the security risk that follows. It does not sit in isolation. Under the Protective Security Policy Framework, PSPF Direction 001-2024, issued by the Secretary of the Department of Home Affairs, requires the Commonwealth entities the Framework binds to identify and manage FOCI risk in technology procurement. The Direction sets the obligation but does not prescribe how it is met, and Home Affairs publishes this guidance as its own method for meeting it. So the requirement to assess FOCI is mandatory, the tool the department offers to satisfy it is this one, and nothing requires an entity to reach past it for a method that asks more.

The second is the Hosting Certification Framework, also administered by the Department of Home Affairs. It certifies hosting and cloud providers against enhanced privacy, sovereignty, and security requirements, so that government customers can identify providers cleared to hold their data. It has three levels. Strategic is the highest, described by the Framework as its highest level of assurance and available only to providers that let the government specify ownership and control conditions. Assured sits beneath it. Uncertified is the floor. What sets Strategic apart from the tiers below is precisely that ownership and control condition, which is the sovereignty dimension of the Framework itself.

Both are administered by the same department. One decides whether a vendor is safe to engage on the ground of foreign ownership. The other certifies whether a provider is cleared to host government data. For the specific question of which foreign owned providers may be trusted with that data, these two are the Commonwealth's targeted instruments. The finding that follows concerns what that method, held in a single set of hands, never asks.

4. The FOCI exit

Section 1 of the guidance opens the vendor review with a single question about ownership, and the answer to that one question decides whether the assessment goes on or stops. It asks:

> "Is the beneficial owner of the vendor from a Five Eyes country (Australia, Canada, New Zealand, UK, and United States)?"
>
> *Home Affairs, Foreign Ownership, Control or Influence Risk Assessment Guidance, Section 1 (Intent). Reproduced under CC BY 4.0.*

The routing off that one question is the whole of it:

> "If YES, consider cyber security hygiene risks posed by the vendor (see the ASD's Australian Cyber Security Centre guidance on"Identifying Cyber Supply Chain Risks"). If NO, go to Section 2."
>
> *Home Affairs, Foreign Ownership, Control or Influence Risk Assessment Guidance, Section 1 (Intent). Reproduced under CC BY 4.0.*

Section 2 is where the compulsion question actually sits:

> "There is a risk of a foreign government compelling the vendor to provide access to its private data to the government or its national security agencies (indicated by policies, legal frameworks, or public reports)?"
>
> *Home Affairs, Foreign Ownership, Control or Influence Risk Assessment Guidance, Section 2 (Vendor jurisdiction hazard), first question. Reproduced under CC BY 4.0.*

Directly beneath the ownership branch, the instrument carries a note of its own making:

> "Note – there are many non-Five Eyes countries whose interests, values and systems of government align with Australia's. Organisations may wish to expand the list of countries in this section for future assessments, informed by previous responses to Section 2."
>
> *Home Affairs, Foreign Ownership, Control or Influence Risk Assessment Guidance, Section 1 (Intent). Reproduced under CC BY 4.0.*

The drafters have written into the guidance itself that the ownership gate is drawn coarsely.

The consequence is structural, not incidental. A United States owned provider answers yes at the first question. It is routed to cyber hygiene and the assessment closes before

Section 2 is reached, so the compulsion question, which the instrument does contain, is never put to that provider. The provider does not pass the compulsion test. It is routed past it, by the nationality of its owner. A CLOUD Act exposure falls outside the FOCI assessment not because the assessment weighed it and cleared it, but because ownership ends the assessment one question before it would be asked.

---

5. The contradiction

Take the provider FOCI has just routed past the compulsion question and put it to the second instrument. Amazon Web Services holds certification under the Hosting Certification Framework at the Strategic level, the Framework's highest, and AWS states this itself. Strategic is the tier Home Affairs reserves for providers cleared under the strongest ownership and control conditions the Framework sets, the tier that carries its highest assurance of sovereignty.

Now read who that provider is, on the record. The entity that contracts with Australian customers, Amazon Web Services Australia Pty Ltd (ACN 605 345 891), is on AWS's own legal record an affiliate of Amazon Web Services, Inc., and since November 2021 the reseller of AWS cloud services to Australian accounts. It is a local storefront. Amazon's own filing with the United States Securities and Exchange Commission lists Amazon Web Services, Inc. as a Delaware company, wholly owned by Amazon.com, Inc. So the service the local entity resells, the infrastructure that runs it, and the corporate parent that controls it are American. Amazon Web Services, Inc. is a United States company, and a United States company is reachable under the CLOUD Act, which lets United States authorities compel a provider to produce data in its possession, custody, or control regardless of the country the data sits in. Local incorporation and an Australian region do not shift that reach, because the reach follows the parent, not the postcode.

Both facts stand on the government's own record, for one named provider. The first instrument routed it past the compulsion question because its owner is American. The second certified it Strategic, its highest assurance of sovereignty, with that same American ownership in plain view. The provider that could not be asked whether a foreign government can compel it is the provider the Framework holds out as most sovereign.

And it is not one provider, or two. The Hosting Certification Framework's own published register of certified service providers lists, at the Strategic tier in its cloud services, Amazon Web Services, Google Australia, Microsoft Azure, Oracle Australia, and IBM Australia. Each the Australian presence of a United States-incorporated parent: Amazon.com, Alphabet, Microsoft, Oracle, and IBM. Each certified against the same foreign law the tier

exists to assure against, and each listed by its Australian Regions, the residency stamp earning the sovereignty grade the incorporation cannot support. Five of the majors at the highest tier is not the shape of a slip in a single certification. It is the shape of a design applied evenly to a whole class.

The two instruments do not cover each other. One would expect the certification to catch what the intake screen missed, one layer answering for the other. It does not. FOCI declines to reach the compulsion question, and the Framework awards its highest tier without asking it either. The check that should have caught the gap repeats it instead, on the same providers, from the same hand.

---

6. The geometry

Two instruments assure the provider a Commonwealth entity wants to trust with its data, and a third program is the last place a careful reader looks for the question they miss. Each asks something real, and each asks the right thing for the threat it was built to face. FOCI, the intake screen, asks whether the owner is hostile. The Hosting Certification Framework, the certification, asks whether the ownership can shift beneath the government after it has committed. CI Fortify, the resilience program released by the Australian Signals Directorate, asks whether the entity can keep delivering its services if the provider is lost. Three genuine risks, three instruments doing the work they were designed to do.

Now set one provider against all three. A United States owned hyperscaler. FOCI asks whether the owner is hostile, finds a Five Eyes ally, and routes it out at the first question before Section 2 can test compulsion. The Framework asks whether the ownership can shift, takes the condition that lets government hold the owner in place, and awards Strategic, its highest tier. CI Fortify asks whether the service can be survived if lost, and offers isolation and rebuild for the day it goes dark. Every instrument returns a clean answer. Not hostile, ownership held, loss survivable. On the government's own record the provider stands sovereign, assured three times over.

And the question that actually governs reach is put by none of them. Not whether the owner is hostile, not whether ownership shifts, not whether the service can be lost, but whether the owner, allied and accepted and still delivering, can be lawfully ordered by its own government to hand the data over. FOCI carves that question out by ownership before Section 2 can raise it. The Framework certifies the ownership and never raises it. CI Fortify prepares for the service being taken away and has no answer for the service being turned while it stays. The question does not slip through one instrument. It falls

through the seam where all three meet, because each faces a different direction, and lawful compulsion of an allied provider stands in the one direction none of them watches.

Picture a walled city with three defences it is proud of. A gate that checks every traveller's colours against the enemy's standard. A treasury sealed with the city's finest lock, certified proof against any thief. A siege store deep enough to outlast the supply road being cut for a season. Each defence is real and each is well made. Then the conqueror comes. He wears the colours of an ally, so the gate waves him through by its own rule. He never touches the lock, because the city's own certified locksmith opens the treasury for him, the locksmith answering to the ally's crown. He never cuts the road, he keeps the grain moving the whole time, and folded into the manifest is a lawful order from his own king to carry a copy of everything back out. The city was never undefended. It was defended in three directions and open in the fourth, and the fourth was the only one he needed. The gate checked for the wrong flag. The lock guarded the wrong hand. The siege store answered the wrong loss.

That is the finding drawn whole. A provider reachable under the CLOUD Act is not certified sovereign despite this gap. It is certified sovereign because the instruments that define sovereignty in Commonwealth cloud assurance each face a real and different threat, and lawful compulsion by an allied government stands in the blind quarter where none of them look.

---

7. Bounds

This assessment examines the design of two Commonwealth instruments and one program. It does not assess the conduct of any provider or any government entity, and it alleges no wrongdoing by either.

It makes no allegation against Amazon Web Services, Google, or any provider named. That a provider holds Strategic certification, and that a United States company is reachable under United States law, are ordinary and lawful facts. No provider is said to have breached an obligation, acted improperly, or done anything beyond holding a certification it was awarded and standing subject to the laws of its jurisdiction, as every company does.

It makes no claim that any particular Australian Government dataset or system is held with any particular provider, at any tier, or in any location. Those placements are not on the public record and none is asserted here. The named providers appear as worked examples of how the instruments treat a class of provider, not as evidence of where any

data sits.

It does not allege that the CLOUD Act has been invoked, or that any Australian Government data has been compelled, disclosed, or accessed. The subject is legal reachability, a standing property of jurisdiction, not any event. Reachability is a blocked fire exit. This assessment reports the blocked exit. It does not report a fire, and it does not claim one has occurred.

It alleges no illegality and no dereliction by any party, including the Department of Home Affairs. FOCI routing a Five Eyes owner to cyber hygiene, and the Framework awarding Strategic certification, are each the instrument operating exactly as written. The subject is the design, not a failure to follow it.

Two boundaries are held throughout. The ownership and control conditions of the Strategic tier are named in public, but their operative terms sit in a Deed of Certification that is not public, so this assessment states only what the Framework publishes and characterises nothing behind it. And the FOCI guidance is the method Home Affairs offers for meeting its Direction, not the method the Direction compels, so the finding concerns what results when the department's own offered instrument is used as designed, not any claim that an entity is forced into that result.

The finding, held to its narrowest, is this. It does not say Australian Government data is being taken. It says the instruments relied upon to guard against that possibility do not test the one question that would surface it. The gap named here is a gap in the assurance. It is not, and is not claimed to be, a gap in any outcome.

References

Alphabet Inc. 2026, *Form 10-K for the fiscal year ended 31 December 2025 (cover page, state or other jurisdiction of incorporation: Delaware)*, US Securities and Exchange Commission, viewed 6 July 2026, https://www.sec.gov/Archives/edgar/data/1652044/000165204426000018/goog-20251231.htm.

Amazon.com, Inc. 2022, *Form 10-K for the fiscal year ended 31 December 2021, Exhibit 21.1 (List of Significant Subsidiaries)*, US Securities and Exchange Commission, viewed 6 July 2026, https://www.sec.gov/Archives/edgar/data/0001018724/000101872422000005/amzn-20211231xex211.htm.

Amazon Web Services n.d., *AWS Australia FAQs*, Amazon Web Services, viewed 6 July 2026, https://aws.amazon.com/legal/awsau/.

Amazon Web Services n.d., *Hosting Certification Framework* [AWS Security Blog], Amazon Web Services, viewed 6 July 2026, https://aws.amazon.com/blogs/security/tag/hosting-certification-framework/.

Australian Business Register n.d., *Amazon Web Services Australia Pty Ltd, ABN 63 605 345 891, ACN 605 345 891*, ABN Lookup, Australian Government, viewed 6 July 2026, https://abr.business.gov.au/.

Australian Signals Directorate 2025, *CI Fortify*, Australian Cyber Security Centre, Australian Government, viewed 6 July 2026, https://www.cyber.gov.au/business-government/secure-design/operational-technology-environments/ci-fortify.

Clarifying Lawful Overseas Use of Data Act 2018 (US), Pub. L. No. 115-141, div. V, codified in part at 18 USC 2713.

Department of Home Affairs n.d., *Foreign Ownership, Control or Influence Risk Assessment Guidance*, Australian Government, viewed 6 July 2026, https://www.homeaffairs.gov.au/nat-security/files/foci-risk-assessment-guidance-without-appendices.pdf.

Department of Home Affairs 2024, *PSPF Direction 001-2024: Managing Foreign Ownership, Control or Influence Risks in Technology Assets*, Protective Security Policy Framework, Australian Government, viewed 6 July 2026, https://www.protectivesecurity.gov.au/publications-library/direction-001-2024-managing-foreign-ownership-control-or-influence-risks-technology-assets.

Department of Home Affairs n.d., *Hosting Certification Framework: Certified Service Providers*, Australian Government, viewed 6 July 2026, https://www.hostingcertification.gov.au/certified-service-providers.

Department of Home Affairs n.d., *Hosting Certification Framework: Framework*, Australian Government, viewed 6 July 2026, https://www.hostingcertification.gov.au/framework.

Google Cloud n.d., *HCF Australia Compliance*, Google, viewed 6 July 2026, https://cloud.google.com/security/compliance/hcf-australia.

International Business Machines Corporation 2026, *Form 10-K for the fiscal year ended 31 December 2025 (cover page, state or other jurisdiction of incorporation: New York)*, US Securities and Exchange Commission, viewed 6 July 2026, https://www.sec.gov/Archives/edgar/data/51143/000005114326000010/ibm-20251231.htm.

Microsoft Corporation 2025, *Form 10-K for the fiscal year ended 30 June 2025 (cover page, state or other jurisdiction of incorporation: Washington)*, US Securities and Exchange Commission, viewed 6 July 2026, https://www.sec.gov/Archives/edgar/data/78

9019/000095017025100235/msft-20250630.htm.

Oracle Corporation 2026, *Form 10-K for the fiscal year ended 31 May 2026 (cover page, state or other jurisdiction of incorporation: Delaware)*, US Securities and Exchange Commission, viewed 6 July 2026, https://www.sec.gov/Archives/edgar/data/1341439/000119312526277521/orcl-20260531.htm.

The five Strategic-tier cloud majors named in Section 5, Amazon (Amazon Web Services, Inc.), Alphabet, Microsoft, Oracle, and IBM, are each traced to a primary SEC filing for their state of incorporation rather than carried by the certifier's register alone.

End of document.