The Question Not in the Set

REFERENCE	AOS-ACD-2026-001
VERSION	1.1
DATE	15 August 2026
CLASSIFICATION	Released
DIRECTOR	Brunel Al-Bijwaie

Version 1.1, 15 August 2026. This assessment examines two question sets in one published guidance document. It rests entirely on that document's own text, read at page-image resolution. **Page citations give the printed page number. In this document the printed page number and the PDF page position are the same, verified on every one of the twenty pages that carries a printed page number** — pages 4 to 23. Pages 1 to 3 and page 24 carry none, so there is nothing on them to check. **No parenthetical PDF position is carried.**

Version note

This is v1.1, published 15 August 2026. It is a correction to v1.0 of 15 August 2026. **One sentence changes. No finding moves, no count moves, and nothing else in v1.0 is withdrawn or qualified.**

Where	What changed	Why
Section 1, the paragraph on earlier work	The sentence "It is cited for one thing only: that the question is one Commonwealth assurance material has not put before" is replaced. It now cites that earlier assessment for its own finding about the two instruments it examined, and for nothing wider	`AOS-CMP-2026-001` finds that **two named instruments** — the Foreign Ownership, Control or Influence Risk Assessment Guidance and the Hosting Certification Framework, both administered by the Department of Home Affairs — do not test whether a certified provider can be lawfully compelled by a foreign government. **It makes no claim about Commonwealth material at large, and this document was not entitled to cite it for one**

How it was found. In the course of verifying an unrelated claim about the Information Security Manual, `AOS-CMP-2026-001` was read again against the documents citing it. **The defect exists independently of that work.**

What no check caught, recorded because it bears on how much the checks are worth. The corrected sentence does not quote `AOS-CMP-2026-001`. **It is a citation whose scope exceeded its source, and no check in this practice reads a citing sentence against what the cited document holds.** The full account is in `CORRECTIONS-REGISTER.md`.

v1.0 remains published at its own address with its own hash, and both versions resolve.

1. Scope

This assessment examines the vendor question sets in *Opportunities for AI in cyber defence*, published by the Australian Signals Directorate on 27 May 2026 and last updated on 12 August 2026. The guidance was co-sealed by the Canadian Centre for Cyber Security, the New Zealand National Cyber Security Centre and the United Kingdom National Cyber Security Centre. It runs to 24 printed pages and carries two appendices of questions for organisations to put to vendors, at pp 18 to 20 and pp 21 to 22.

The question this assessment puts is narrow. **One of those question groups is headed "Data protection and sovereignty". Does the guidance, in that group or anywhere else, ask which state can require a vendor to produce the data it holds?**

The domain, stated before the finding rather than after it. Printed pages 4 to 24 were read — the whole of the document's body, its appendices, a page carrying no text at p 23, and its closing page. Pages 1 to 3 are the cover, a blank verso and the table of contents, and carry no text bearing on the question. **Both appendices and the Supply chain subsection were read at page-image resolution, as was every other page from which this assessment quotes.** Where this assessment says the guidance does not ask something, it means it across those pages and says so.

The guidance states how it is to be regarded, on its final page. **The sentence is quoted because an assessment of a document should record how that document describes the standing of what it says, and for no other reason. No inference is drawn from it in either direction** — it is not offered as an explanation of what this assessment finds, and it is not offered as evidence against one.

> "The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances."
>
> *Australian Signals Directorate, Opportunities for AI in cyber defence, printed p 24, Disclaimer.*

The document states its own audience at printed p 4:

> "This guidance supports cyber defenders, such as Chief Information Security Officers and senior security leaders who are responsible for cyber security strategy, operations and risk outcomes."

(The full statement of what this assessment does not claim is held at Section 8, Bounds. It is not an afterthought, and a reader who reads only the finding should read that section with it.)

---

2. Finding

The guidance closes with two appendices of questions for organisations to put to vendors. One group in the first appendix is headed **"Data protection and sovereignty"**, and its opening explanatory line directs the reader to "customer data sovereignty obligations".

Three questions sit under that heading. They ask how sensitive data is handled and protected during processing; what data is retained, reused or used to retrain models; and which jurisdictions process or store customer data. The third gives its reason as cross-border or regulated data constraints.

None of the three asks which state can require the vendor to produce the data it holds. Nor does any other question in either appendix. Appendix A carries eight question groups and twenty-two questions; Appendix B carries eight groups and sixteen questions; **both were read end to end at page-image resolution and neither puts the question in any form.**

The one other place the guidance addresses data sovereignty is a bullet in the Supply chain subsection, which asks that organisations understand how data is **accessed, used and handled** across the AI supply chain, to ensure alignment with data sovereignty requirements. **That is a question about handling. It is not a question about reach.**

The consequence is narrow and it is a consequence about a record. A question set that names data sovereignty as its ground asks **where** the data is, and does not ask **whose law reaches the vendor holding it**. Location and legal reach are different questions, and a vendor can answer the first completely while the second remains open: data held in Australia by an operator answerable to another state's law satisfies the question that is asked and leaves untouched the one that is not.

This is not a gap of the kind the practice has recorded before, and the difference matters. Where an instrument routes a provider past a question it contains, the question exists and is never reached. **Here nothing routes past the question, because there is nothing to route past.** The question is not in the set.

What makes that a finding rather than an ordinary limit of scope is that the group names the ground. A document may leave out anything it did not set out to cover. **This group is headed "Data protection and sovereignty" and its explanatory line invokes sovereignty obligations**, and the three questions beneath it ask about handling, retention and location.

---

3. What the question sets are for

The guidance states the purpose of each appendix in its own words. Appendix A, at printed p 18:

> "Appendix A provides a set of questions to help organisations assess the security, reliability and maturity of AI capabilities offered by vendors. These questions are designed to distinguish engineered, production-ready solutions from those relying on automation, assumptions, or emerging features."
>
> *Printed p 18, Appendix A: Cyber security questions for AI vendors.*

And Appendix B, at printed p 21:

> "Appendix B provides structured questions to help organisations evaluate the effectiveness, reliability and operational fit of AI capabilities in cyber security. The focus is on ensuring AI delivers

> measurable outcomes while remaining secure, transparent and aligned with organisational risk requirements."
>
> *Printed p 21, Appendix B: AI capability questions for cyber security vendors.*

Both are addressed to an organisation deciding whether to engage a vendor. Each question is followed by a short explanatory line, set as a sub-bullet, giving the reason for asking it. Those explanatory lines are quoted throughout this assessment because they state what the guidance says each question is for.

---

4. The sovereignty group, in full

The group appears in Appendix A at printed p 19, under the heading **"Data protection and sovereignty"**. It has three questions, each with its explanatory line, and all three are set out here:

The first question, and beneath it the explanatory line the guidance gives for asking it:

> "How is sensitive data handled, stored and protected during AI processing?"
>
> "Ensure alignment with internal policies, regulatory requirements and customer data sovereignty obligations"

The second:

> "What data is retained, reused, or used to retrain models and under what conditions?"
>
> "This helps identify unintended data exposure or long-term privacy risks"

And the third:

> "Which jurisdictions process or store customer data, including through third-party AI services?"
>
> "This is critical for organisations with cross border or regulated data constraints"
>
> *All six passages: printed p 19, Appendix A, Data protection and sovereignty. Read at the page image.*

What each asks. The first asks about handling and protection — the treatment of data during processing, measured against the organisation's own policies and its regulatory and sovereignty obligations. The second asks about retention and reuse, and gives its reason as data exposure and privacy risk. **The third asks about location: which jurisdictions data is processed or stored in, including through third parties.** Its stated reason is cross-border or regulated data constraints.

The third is the one that comes closest and it is worth being precise about what it does. It asks where the data goes. A vendor answering it fully would name the countries in which processing and storage occur, its own and its subcontractors'. **That answer would not disclose which state could require the vendor to produce the data**, because a state's reach over a company does not follow only from where that company keeps its data.

---

5. What Appendix B contains, and what it does not

Appendix B carries **eight question groups and sixteen questions**: security outcomes and effectiveness; scope, assumptions and constraints; handling uncertainty and error; transparency and auditability; security of the AI system; data use and protection; integration and operational fit; and resilience and recovery.

It contains no question about data location, jurisdiction or legal reach at all. Its data group, headed "Data use and protection" at printed p 22, asks two questions:

> "What operational data does the AI access, and how is access minimised?"
>
> "Limiting data access reduces exposure and supports least privilege principles"
>
> "Is any customer data reused beyond its original purpose, including for model tuning?"
>
> "Clear boundaries on data use reduce long-term privacy, confidentiality and legal risk"
>
> *All four passages: printed p 22, Appendix B, Data use and protection.*

The phrase "legal risk" in the second explanatory line concerns the boundaries of data use. It is recorded here because it is the nearest thing in either appendix to the register of the question this assessment is about, and because a reader scanning either appendix for legal language would find it and should know what it attaches to.

---

6. The supply chain bullet

Outside the appendices, the guidance addresses data sovereignty once, in the Supply chain subsection under "Securely adopting AI", at printed p 15. Among the things organisations should do:

> "understand how organisational data is accessed, used and handled across the AI supply chain to ensure alignment with data sovereignty requirements and to determine which types of AI solutions are most suitable"
>
> *Printed p 15, Securely adopting AI, Supply chain.*

Access, use, handling, and alignment with requirements. The bullet directs an organisation to understand what happens to its data as it moves through the supply chain, and to use that understanding to choose between kinds of AI solution. **It does not direct the organisation to establish whose law reaches the parties handling the data.**

The nearest passage anywhere else is in the Governance subsection on the same page, which asks organisations to:

> "define and enforce policies governing what data AI tools may access, how data may be used and where outputs may be transmitted"
>
> *Printed p 15, Securely adopting AI, Governance.*

That concerns the organisation's own policy about transmission. It is a rule the organisation makes for itself, not an enquiry into another state's authority over a vendor.

---

7. The reading, and what it establishes

Printed pages 4 to 24 were read. The Introduction and Audience (p 4); the evolving landscape, including the spectrum of AI use, agentic AI, and malicious use (pp 5–6); the six ISM functions of Govern, Identify, Protect, Detect, Respond and Recover (pp 7–12); Securely adopting AI, including human oversight, system protection and sandboxing, secure system integration, governance, supply chain, testing and assurance, and Secure by Demand (pp 13–16); the Conclusion and Further information (p 17); Appendix A (pp 18–20); Appendix B (pp 21–22); a page carrying no text (p 23); and the closing page (p 24).

No passage in those pages puts the compellability question in any form. That is established by the reading, and it is bounded by it.

A term census was run and it is not the evidence. It is recorded because a reader may ask, and because it agreed with the reading in both extraction modes: `compel`, `compellable`, `compulsion`, `lawful access`, `legal process`, `disclosure order`, `warrant`, `subpoena`, `production order`, `foreign law` and `Cloud Act` each occur **zero times**, and **`jurisdiction` occurs once in 24 pages** — in the question quoted at Section 4.

A count of that kind can be correct and still worthless, which is why it is not relied on. This case has already produced one near miss of exactly that species: the guidance page renders "third-party" with a non-breaking hyphen where the PDF uses an ordinary one, so a search of the page for the sovereignty question with an ordinary hyphen returns nothing at all. **The question is there. The search is what fails.**

---

8. Bounds

This assessment examines two question sets in one published guidance document. **It makes no finding about the Australian Signals Directorate, about the Australian Cyber Security Centre, or about any of the three co-sealing agencies.** No person is named and none is the subject of any finding.

It does not say the guidance is wrong, or that it should not be followed. The questions it contains are questions about matters the guidance identifies, and whether the set as a whole is well made is not a question this assessment reaches or answers.

It does not say the omission was deliberate. No claim is made about intent, awareness, or how the document was drafted. **The finding is that a question is not on the record, not that anybody failed to put it there.**

It does not say any AI vendor is compellable, and it names no vendor. The question this assessment says

is not asked is a question about legal reach. **This assessment does not answer it, in any direction, about anyone.** Whether any particular vendor could be required by any particular state to produce data is outside the scope of this document and is not asserted here.

It is bounded to the Australian publication. The guidance names three co-sealing agencies. **No partner-hosted version of it was located**, across five search routes: a general search on the title with all three agencies; a title search restricted to the partner domains; a subject search restricted to the New Zealand domains; a search of the whole web for the appendix's own distinctive question text, which a co-sealed version would carry whatever it were titled; and the document itself, which carries no joint advisory number to search on. **That establishes that no partner version was found. It does not establish that none exists, and nothing is said here about what any partner version contains.**

Two limits on method are held throughout. First, this assessment relies on one document. It does not draw on the Information Security Manual, on any of the publications the guidance cites, or on any external account of vendor practice. Where the guidance says something, this assessment records that it says it, and no further. Second, **every absence recorded here was established by reading the pages where the proposition would sit, at page-image resolution, and is bounded by those pages.**

The relationship to earlier work in this practice, stated so it is not mistaken for a repetition of it. `AOS-CMP-2026-001` examined two Commonwealth instruments — the Foreign Ownership, Control or Influence Risk Assessment Guidance and the Hosting Certification Framework — and found that neither tests whether a certified or cleared provider can be lawfully compelled by a foreign government to disclose the data it holds. **That assessment's reasoning is not repeated here and this document does not depend on it.** It is cited for that finding and no more: for what those two instruments do not test, and not for any proposition about Commonwealth material at large. **The instrument examined here is of a different kind — those are instruments government operates, this is guidance offering questions for an organisation to put to a vendor — and the finding takes its shape from that difference**, which is set out at the end of Section 2.

The finding, held to its narrowest, is this. **It does not say that an organisation following this guidance would fail to discover which state can reach its vendor** — an organisation may ask a vendor anything it wishes, and many will. **It says that on this instrument's record, in a question group that names data sovereignty as its subject, the question is not put.** The gap named here is a gap in a question set. It is not, and is not claimed to be, a gap in any outcome.

References

Australian Signals Directorate 2026, *Opportunities for AI in cyber defence*, Australian Cyber Security Centre, Canberra, first published 27 May 2026, last updated 12 August 2026, viewed 15 August 2026, https://www.cyber.gov.au/business-government/secure-design/artificial-intelligence/opportunities-for-ai-in-cyber-defence.

AustraliaOS 2026, *The Compellability Gap in Commonwealth Cloud Assurance*, AOS-CMP-2026-001, v1.2, viewed 15 August 2026, https://australiaos.com.au/verify/AOS-CMP-2026-001.

Source pins

The assessed document was retrieved on 15 August 2026 and pinned by SHA-256. Every quotation in this assessment was read from that pinned copy at page-image resolution.

Ref	Artefact	SHA-256
A-GUID-1	*Opportunities for AI in cyber defence*, PDF, 24 pages	`bf1ac3624676e11df2cd9694a869c4b938a28e7d4cab371e0e07172f35470e6b`
A-GUID-2	The guidance page, HTML as served	`96b45d5e2130f8962ce741d9f8c06f0b93e0db00a040261276e7d7def8f0796b`

Both artefacts are independently archived at the Internet Archive and both captures were seen to resolve. The archived PDF was fetched raw and hashes to the same value struck above, so a reader can check every quotation against a third-party copy without relying on this practice's archive or on the publisher's site remaining unchanged.

The HTML and the PDF carry the same body text, including both appendices in full. One difference was found and it is typographic: the page sets "third-party" with a non-breaking hyphen where the PDF uses a plain one.

End of document.