The Hosting Certification Exemption

REFERENCE	AOS-HCE-2026-001
VERSION	1.0
DATE	11 August 2026
CLASSIFICATION	Released
DIRECTOR	Brunel Al-Bijwaie

Verification. This document is published with a verification record at australiaos.com.au/verify/AOS-HCE-2026-001, which lists every source with its retrieval time and SHA-256, and states the SHA-256 of this file. To confirm this copy is unaltered, recompute the file's SHA-256 and compare it with the value on the verification record. AustraliaOS Pty Ltd, ABN 69 697 049 291.

Contents

Executive summary

An Australian instrument asks what foreign law can compel a supplier to do. The Security of Critical Infrastructure (Critical infrastructure risk management program) Rules require a responsible entity to identify, for each major supplier, "in relation to FOCI risks—legislative or other legal requirements to which the supplier is subject to". That is the compellability question, asked as a *must*, in a binding legislative instrument.

It is asked of nine classes of asset. Critical broadcasting, domain name system, electricity, energy market operator, freight infrastructure, freight services, gas, liquid fuel, water. **A critical data storage or processing asset — the class defined by reference to services provided to the Commonwealth — is not among them.** The obligation is an *enhanced* requirement, imposed only on the responsible entity for an asset specified in section 4A(1) of the Rules, and the data class sits in section 4(1) instead, which carries the *baseline* requirements. So for the class that holds government data, the compellability question has never been asked.

That is a gap in the Rules, and it exists independently of anything else in this assessment.

Section 30AB(4) of the *Security of Critical Infrastructure Act 2018* then does something separate. Where an entity holds a certificate of hosting certification (strategic level), and a critical infrastructure asset "or a part of" one is used "in connection with" the provision of any certified service, and the entity is the responsible entity, "this Part does not apply to the asset". The whole of Part 2A falls away — including the baseline risk-management program, and with it the material risk the Rules specify at section 6(d): "the storage, transmission or processing of sensitive operational information outside Australia". A submitter told the Parliamentary Joint Committee on Intelligence and Security exactly this in February 2022, naming that same risk.

The framework's own operative document, published in March 2021, said the Certification Framework "will also work in conjunction with" the powers and provisions protecting critical infrastructure, and treated those provisions as cumulative with certification rather than displaced by it. **The framework's stated posture was conjunction. The provision enacted substitution.** The framework was speaking of an earlier Bill and cannot have been speaking of a provision that did not yet exist — a limit this assessment states before it argues from the quotation, not after.

What replaces Part 2A is an annual report under Part 2AA, given to the Secretary or a relevant Commonwealth regulator, setting out the reason the asset is covered by the exemption. **No such report is public. This practice has read none and cannot.** This assessment therefore compares instruments. It does not, and cannot, compare practice.

This is not a claim that Parliament was misled, that the exemption is unexplained, or that any department,

official, provider or submitter acted wrongly. The rationale is stated in the explanatory memorandum and is quoted here in full. Nor is it a claim that any certified provider is subject to foreign compulsion. No entity is named in connection with any such claim.

Section 1: Scope, method, and what is contestable

What this assessment does

It compares two instruments. On one side, what the critical infrastructure regime requires of a responsible entity, and of whom. On the other, what the hosting certification framework says it requires, in the framework's own words. Between them sits section 30AB(4) of the *Security of Critical Infrastructure Act 2018*, which switches the first off for assets connected to services certified under the second.

Every factual assertion in this document is tied to a source pinned by SHA-256 in the register of the companion scoping case, listed on the verification record with its retrieval time. Where an assertion rests on an inference across provisions rather than on a quotation, it says so at the point it is made.

Citation convention

Page references to the framework's operative document are given as **printed page, with the PDF page in parentheses**. The document's printed numbering begins three leaves into the file, so the two never coincide, and a citation that does not say which it means cannot be checked.

Quotation

A quotation that elides a qualification is a misquotation. Every ellipsis in this document has been checked against its full passage, and no words are removed that change what the passage asserts. Where a submission or a report qualifies a proposition this assessment relies on, the qualification is quoted with it, in the same sentence, rather than being answered later.

Two quotations here span a page break in their source. Both were checked against page images rather than against an extracted text layer, because a text layer is no authority for where a sentence breaks.

Currency

Both live pages of the scheme, captured on 11 August 2026 at 08:01 UTC, carry the same notice: "The Hosting Certification Framework is currently undergoing reform. The Department will pause the HCF Certification registration of prospective service providers and HCF Certified providers seeking supplementary assessment effective from 3 November 2025 until HCF reforms have been completed." The operative framework document this assessment reads against is the March 2021 version, which is what the scheme published as at that date. Every observation here is as at 11 August 2026. **A reform that addresses what is observed would**

not make the observations wrong; it would make them historical, and this practice would record that.

The first contestable step: the Direction and the guidance

This assessment treats the Foreign Ownership, Control or Influence Risk Assessment Guidance as the method by which an entity meets PSPF Direction 001-2024. **That is an inference, and it is contestable.** The Direction requires a process "in accordance with Department of Home Affairs guidance" and does not name the guidance; the guidance does not name the Direction. Neither document names the other. What turns on it: if the Direction is met by some other method, the observation that the mandatory protective-security assessment is framed as ownership, control and influence rather than compellability does not follow from these two documents, and that step should be read as not made out.

Notice, and a standing invitation

No notice was served before this assessment was published. Every source it relies on is a public legal instrument or a public parliamentary record; no finding is adverse to any party; and nothing in it is a matter a party could correct from information this practice does not already hold. The practice's notice protocol is unchanged and continues to apply to assessments carrying adverse findings about identifiable parties from register data.

The invitation stands in its place, and it does not expire. Any party who considers a passage of this document misread — a provision, a submission, a report, or its own published material — is invited to say so at any time. Any correction received will be recorded, and where it bears on a finding it will be published, together with what the document said before it.

Every observation is as at the capture dates stated on the verification record. A source that has changed since its capture has not made the observation wrong; it has made it historical, and this practice would record that.

The second contestable step: section 51 declarations

Part 2A can also be applied to a particular asset by a ministerial declaration under section 51 of the Act. **Whether any such declaration has been made in relation to any asset discussed here cannot be determined from public sources, and this assessment does not assert that none exists.**

A declaration is available only where the Minister is satisfied there would be a risk if it were publicly known that the asset is a critical infrastructure asset; section 51(5) provides that it is not a legislative instrument, so it appears in no register; and disclosing the fact that an asset has been declared is an offence under section 45.

That secrecy is not an accident of drafting, and the point is the committee's rather than this practice's. The fifth of the nine principles at paragraph 3.49 of the Parliamentary Joint Committee on Intelligence and Security's September 2021 report — the same paragraph the explanatory memorandum invokes for the exemption — recommended that "the currently drafted secrecy around declarations of assets as SoNS under proposed section 52B of the SOCI Bill, and current section 51 of the Act, be amended to require that such

declarations only be confidential if the Minister is satisfied on reasonable grounds, that there is a significant risk of harm to Australia's defence or national security as a result of the disclosure of the regulatory status of the asset" (printed pp 46–47). The Act's endnotes record that section 51 was amended by Act No 124 of 2021 and Act No 33 of 2022; the confidentiality of a declaration remains.

Two further things follow from the provisions themselves, and this assessment states both. Section 51(1)(a) permits a declaration only where the asset "is not otherwise a critical infrastructure asset", which an asset answering section 12F already is. And section 30AB(2) makes the declaration limb subject to the hosting certification exemption. **This document says undeterminable as to whether any declaration exists. It never says none. It says what the provisions would do if one did.**

Section 2: The case against this assessment

This section states the case against what follows, before what follows is stated. Each item is sourced and none is answered here. Where an item is met later, it is met beside the claim it bears on, not in an endnote.

The measure has a stated rationale, and it is not obscure

The explanatory memorandum to the Bill that inserted section 30AB says at paragraph 142: "Subsection (4) was not included in the 2020 Bill. Consistent with recommendation 7 and paragraph 3.49 of the PJCIS report, this exemption is inserted to minimise the regulatory overlap between the critical infrastructure risk management program obligation and the HCF in response to feedback received from the data storage and processing sector."

At paragraph 146 it describes the measure as "the recognition of the HCF as a suitable alternate framework to the critical infrastructure risk management program obligation".

Nothing in this assessment claims the exemption is unexplained. The reason is stated, on the record, in the ordinary way.

The exemption is narrower than it first reads

The same explanatory memorandum says at paragraph 143, spanning printed pages 32 and 33: "While the exemption under subsection (4) is intended to minimise the regulatory overlap between the critical infrastructure risk management program obligation and the HCF, it will not apply to all facilities held by a responsible entity. Responsible entities for assets in the data storage and processing sector will still be required to comply with any rules made under Part 2A for facilities that do not hold a certificate of hosting certification (strategic level) under the HCF."

A responsible entity is not exempted wholesale. Only facilities used in connection with certified services are reached. Any reading of this assessment that treats a certified provider as outside Part 2A altogether is a misreading of the provision and of this document.

Something replaces what is removed

Part 2AA substitutes an annual report. It is not nothing, and this assessment does not say it is.

The submitter this assessment relies on said most risks are covered

Submission 5 to the 2022 inquiry, which identified the offshore-information risk, said at paragraph 5.3: "Although many of the specified material risks are reflected in the HCF, there are some that are not". **The submitter's position was that most are reflected.** This assessment claims the one it names, not the set.

The same submission said at paragraph 5.2: "It is reasonable to exempt such service providers from Part 2A given the HCF involves a similar risk management process. However, this should not be done through primary legislation until the HCF is itself formalised in legislation or regulation or at least incorporated into the Protective Security Policy Framework." **The objection was to method and timing, not to principle.**

One of the two submissions cited at paragraph 2.77 is not relied on here

The 2022 report's footnote 50 cites two submissions at paragraph 2.77. **Submission 12 does not mention the hosting certification framework, and this assessment therefore does not count it as support for anything.** Its own concern — that the data storage and processing industry faced "duplicative and inconsistent obligations", partially addressed by the Government's stated intention "to minimise any duplication or unnecessary burden, and to de-conflict requirements" — supports the exemption's stated rationale rather than this assessment's reading of it. **Submission 12 is not a witness for this assessment**, and the reader should discount any impression that two submitters stand behind the point made in Section 8. One does.

The framework was speaking of an earlier Bill

The framework's operative document names the Security Legislation Amendment (Critical Infrastructure) Bill 2020. That Bill became Act No 124 of 2021. Part 2A and section 30AB came from a later Act, No 33 of 2022. **The framework's "in conjunction with" cannot have been about the provision that later displaced it.** This is the answer a department will give, and it is given here, before the quotation is used.

For the same reason, the framework's operative document predates section 30AB and could not have disclosed it.

The construction of section 30AB(2) is contestable

This assessment reads section 30AB(2) as subordinating the declaration limb in subsection (1) to the exemption in subsection (4). A department could reasonably read subsection (2) as ordering the subsections without displacing a specific ministerial determination. **That reading is not refuted here**, and the assessment's second limb is stated as conditional on the construction rather than as settled law.

The nil returns come from documents that do not claim to be exhaustive

Where this assessment reports that a term does not appear in the framework's document or on the scheme's pages, that is a search result over a document which does not purport to enumerate what it tests. It is weaker than a nil return from a closed statutory list, and it is labelled as such at each use.

What has not been read

No report made under Part 2AA has been read, and none can be. The reports go to the Secretary or a relevant Commonwealth regulator and are not published. This caps the comparison permanently: the assessment compares instruments, never practice.

Section 3: What the regime asks

Claim. One binding Commonwealth instrument asks what foreign law can compel a supplier to do, and it asks it of nine classes of asset.

The question, as asked

The *Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023*, in the compilation in force 10 June 2026, provide at section 10A(5) that the system or process a responsible entity must maintain "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; and
(d) the extent to which the matters in paragraphs (a), (b) and (c) together may present a material risk for the CI asset, or could exceed a maximum acceptable outage of the service or product provided by the supplier; and
(e) as far as reasonably practicable to do so—steps to minimise or eliminate material risks and mitigate the relevant impact of the hazard on the CI asset.

Paragraph (a) is the compellability question. It is not framed as ownership, and it is not framed as location. It asks what law reaches the supplier. It is a *must*. Paragraph (d) shows what it is for: the answer feeds a determination of material risk to the asset.

Of whom it is asked

Section 10A(4) imposes the obligation: "A responsible entity for a CI asset **specified in subsection 4A(1)** must establish and maintain a system or process in the entity's CIRMP to assess the risks associated with an existing or proposed major supplier for the CI asset."

Section 4A(5) confirms the character of that obligation, listing the *enhanced* CIRMP requirements as the matters specified in sections 6A, 8A, 8B, 8C, 9A, **10A** and 11A.

Section 4A(1) is the list: "For the purpose of paragraph 30AH(2)(b) of the Act, the following CI assets are specified to be subject to enhanced CIRMP requirements: (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."

Nine classes. **This is a closed list introduced by "the following CI assets are specified", so the absence of a class from it is an inventory nil, not an inference.** It would be falsified by an amendment adding a class.

Analysis. The Commonwealth does ask the compellability question in a binding instrument, as an obligation rather than as guidance. Any assessment claiming that Australian law nowhere asks it is wrong, and this one does not claim it. What matters is the reach of the asking.

Recommendation 1. *To the Department of Home Affairs.* The record establishes that the compellability question is asked of nine asset classes and not of the class defined by reference to services provided to government. It does not establish why. **What would establish it is a statement, in the explanatory statement to any future amendment of the Rules or in the Department's published guidance, of the basis on which the enhanced requirements were confined to those nine classes.** This recommendation asks for the reasoning to be published; it does not assert that the current position is wrong.

Section 4: The class that holds government data

Claim. The class of asset defined by reference to services provided to government sits inside the regime and outside the question.

What the class is

The class is not assets holding Commonwealth data. It is assets the provider knows are used wholly or primarily to provide a data storage or processing service, relating to business critical data, to a Commonwealth, State or Territory end-user. That distinction is the Act's, not this assessment's, and it is carried wherever the class is described below.

Section 12F(1) of the Act provides that an asset is a critical data storage or processing asset if:

(a) it is owned or operated by an entity that is a data storage or processing provider; and
(b) it is used wholly or primarily to provide a data storage or processing service that relates to business critical data and that is provided by the entity to an end-user that is: (i) the Commonwealth; or (ii) a body corporate established by a law of the Commonwealth; or (iii) a State; or (iv) a body corporate established by a law of a State; or (v) a Territory; or (vi) a body corporate established by a law of a Territory; and
(c) **the entity knows that the asset is used as described in paragraph (b)**; and
(d) the asset is not a critical infrastructure asset that is covered by a paragraph of subsection 9(1) (other than paragraph 9(1)(d)).

That the regime applies to it

It does. Section 4(1) of the Rules specifies, for paragraph 30AB(1)(a) of the Act, thirteen classes, of which paragraph (c) is "a critical data storage or processing asset". Part 2A therefore applies, and the baseline critical infrastructure risk management program obligation applies with it.

That the question does not reach it

Section 4(1) and section 4A(1) are different lists doing different work. The data class appears in the first and not in the second. The vendor assessment at section 10A is imposed only on the responsible entity for an asset in the second.

This is an inference across three provisions of one instrument — section 4(1)(c), section 4A(1) and section 10A(4) — and it is stated as one. Read together, they mean that the obligation to identify the legislative or

other legal requirements to which a major supplier is subject has never applied to a critical data storage or processing asset.

Analysis. This is a gap in the Rules, and it exists whether or not any exemption is ever claimed by anyone. It is not caused by section 30AB(4), and this assessment does not say it is. An asset in this class that holds no certificate at all is still outside the compellability question.

Recommendation 2. *To the Department of Home Affairs.* Nothing on the record establishes that a critical data storage or processing asset is less exposed to foreign legal compulsion than a critical water asset or a critical gas asset. **What would establish the current allocation as considered rather than incidental is a published statement of the risk basis for it** — for instance in the explanatory statement accompanying any amendment to section 4A(1), or in the Department's guidance on the enhanced requirements. The recommendation is for disclosure of the basis, not for a change to the allocation.

Section 5: What the framework asks

Claim. The framework's operative document defines its own central concept as ownership and control, and says the critical infrastructure provisions will operate alongside it.

The framework's own definition

The *Hosting Certification Framework – March 2021* (version 2) resolves the meaning of its central term on its first printed page:

> For clarity, sovereignty refers to the ability of the government to specify and maintain stringent ownership and control conditions.

(printed p 1, PDF p 4). The sentence appears in a passage explaining that "sovereign" had been read as excluding any level of foreign investment, an interpretation the document sets aside as making any publicly listed provider ineligible for the higher certification level.

This is the pivot of the comparison, and it is a quotation, not a characterisation. The framework was not asked by this practice what it tests. It says what it tests.

What the document does not use

In the same 30-page document (printed pp 1–27, PDF pp 4–30), the string "ownership" occurs 40 times, "control" 40 and "foreign" 19, while *jurisdiction*, *compel*, *offshore*, *onshore*, *located*, *FOCI* and *beneficial* each return nil, as does *law*, including *laws* and *lawful*.

The method, stated so that the count can be repeated: text extracted with `pdftotext -layout`, de-hyphenated across line breaks, whitespace normalised, counted case-insensitively as substrings. A word-boundary count returns "ownership" 39; the difference is a single table-layout join in the text layer where "mid" and "ownership" abut, and the occurrence is genuine.

This nil is about the compellability concept, not about legal references generally. The document names the *Foreign Acquisitions and Takeovers Act 1975*, the *Foreign Acquisitions and Takeovers Regulation 2015*, the Commonwealth Procurement Rules and the Security Legislation Amendment (Critical Infrastructure) Bill 2020. It is a document that cites statutes. It does not use the vocabulary of legal compulsion.

This is a nil return from a document that does not purport to enumerate exhaustively what it tests. It corroborates the definition quoted above. It does not substitute for it.

What the framework said about the critical infrastructure regime

The limit on what follows, before what follows. The passage quoted below is from a document dated March 2021, which names the Security Legislation Amendment (Critical Infrastructure) Bill 2020. That Bill became Act No 124 of 2021. Section 30AB was inserted by a later Act, No 33 of 2022. **The framework was therefore not speaking of Part 2A, and cannot have been speaking of the exemption.** What the passage establishes is the framework's stated posture toward the critical infrastructure regime — that the two would operate together — and nothing about a provision that did not then exist. Read it for the posture, and not for the provision.

With that limit stated, the document says, under its own heading "Protecting Critical Infrastructure and Systems of National Significance" (printed p 8, PDF p 11):

> The Certification Framework will also work in conjunction with the powers and provisions of the Government's 2020 Cyber Security Strategy, including those regarding protecting Critical Infrastructure and Systems of National Significance (CI/SoNS), and once legislated, those provisions stipulated in the Security Legislation Amendment (Critical Infrastructure) Bill 2020, which was introduced into Parliament on 10 December 2020.

The posture is not confined to that sentence. The document treats those provisions as cumulative with certification. A breach of certification, it says, may result in a provider becoming uncertified and "triggering remediation provisions under this Framework, **as well as** the provisions of the PSPF, FIRB or, once legislated, the Security Legislation Amendment (Critical Infrastructure) Bill 2020 (CI/SoNS)" (printed p 13, PDF p 16). The Bill appears as a row in the document's Table 4 comparison of certification requirements, alongside the PSPF and FIRB (printed p 16, PDF p 19).

Analysis. Two propositions, each on the face of a published document. The framework's concept of sovereignty is ownership and control. The framework expected the critical infrastructure provisions to apply alongside certification, not instead of it. Neither is a characterisation by this practice, and the comparison that follows is therefore not one imposed on the framework from outside — it is the relationship the framework itself described, confined to the posture and not extended to a provision that post-dates it.

Recommendation 3. *To the Department of Home Affairs, as administrator of the framework.* The framework's published material states a posture of conjunction and does not state what certification now does to the application of Part 2A. **What would resolve the divergence is a published statement, in the reformed framework, of the relationship between certification and Part 2A as it now stands** — whether conjunction, substitution, or something else. The recommendation asks for the current position to be stated, not for it to be changed.

Section 6: What the exemption does

Claim. Section 30AB(4) removes the whole of Part 2A from an asset connected to a certified service, and Part 2AA substitutes an annual report.

Its limit, first

As set out in Section 2, the explanatory memorandum states at paragraph 143 that the exemption "will not apply to all facilities held by a responsible entity", and that responsible entities in the sector "will still be required to comply with any rules made under Part 2A for facilities that do not hold a certificate of hosting certification (strategic level) under the HCF" (printed pp 32–33). Everything below is confined to facilities within the exemption's reach.

The provision

Section 30AB(4) provides:

> If: (a) an entity holds a certificate of hosting certification (strategic level) that relates to one or more services; and (b) the certificate was issued under the scheme that is: (i) administered by the Commonwealth; and (ii) known as the hosting certification framework; and (c) a critical infrastructure asset, **or a part of** a critical infrastructure asset, is used **in connection with** the provision of **any of those services**; and (d) the entity is the responsible entity for the asset; **this Part does not apply to the asset.**

Four features are on the face of it. The exemption attaches to the asset. It reaches part of an asset. It turns on a connection to a service rather than on anything about the asset itself. And it imposes no continuing condition beyond holding the certificate.

What the Act says about the scheme

Neither "certificate of hosting certification (strategic level)" nor "hosting certification framework" is defined in the Act. The scheme is identified only as the one "known as" that name and administered by the Commonwealth. **The word "hosting" occurs exactly twice in the Act, both inside section 30AB(4).** The Act has a definitions section, at section 5, and neither term appears in it — so this is an inventory nil, not a document nil.

The same count carries a second consequence. Because "hosting" appears nowhere else in the Act, **no provision addresses what becomes of the exemption if the certificate lapses, is suspended or is revoked.**

This assessment reports that silence. It does not claim the exemption survives revocation, and it does not claim it does not.

What "this Part does not apply" removes

Part 2A carries the risk-management program obligation. Section 30AC requires a responsible entity to adopt and maintain a critical infrastructure risk management program. Section 30AH(1)(b)(i) states the purpose: to "identify each hazard where there is a material risk that the occurrence of the hazard could have a relevant impact on the asset".

Section 30AH(8) provides that "[t]he rules may provide that a specified risk is taken to be a material risk for the purposes of this section", and section 6 of the Rules is made for that subsection. Two of its paragraphs bear directly on an asset in this class:

> (d) the storage, transmission or processing of sensitive operational information outside Australia, which includes: (i) layout diagrams; (ii) schematics; (iii) geospatial information; (iv) configuration information; (v) operational constraints or tolerances information; (vi) data that a reasonable person would consider to be confidential or sensitive about the asset
>
> (f) impact to the availability, integrity, reliability or confidentiality of the data storage system holding business critical data

Section 6 is not among the enhanced requirements listed at section 4A(5). Both are therefore baseline, and both reach a critical data storage or processing asset.

The chain is an inference across provisions and is stated as one: section 30AB(4) removes Part 2A; Part 2A contains sections 30AC and 30AH; the Rules' material risks are specified for section 30AH(8); so the exemption removes the obligation to which those material risks attach, including the offshore-information risk at section 6(d).

What replaces it

Section 30AQ requires an entity that was, at any time in a financial year, the responsible entity for one or more assets covered by section 30AB(4), (5) or (6) to give a report within 90 days after the end of the financial year, to the relevant Commonwealth regulator or otherwise to the Secretary. The report must set out "the reason why those assets are covered by" the exemption and, if a hazard had a significant relevant impact during the period, identify the hazard and evaluate the effectiveness of any mitigating action.

Analysis. The removal is of an obligation with a specified content; the substitution is of a report with a different specified content. Whether the substitute delivers what the obligation did is not answerable from these instruments, and is not answered here — **no Part 2AA report is public and this practice has read none.** What can be said is what each instrument requires on its face, and the offshore-information material risk at section 6(d) is required by one and not mentioned in the other.

Recommendation 4. *To the Department of Home Affairs.* Nothing on the record establishes what the

Part 2AA reporting substitute delivers in practice, because no report is public. **What would establish it is publication, in the Department's annual reporting or in aggregate form, of the number of Part 2AA reports received in respect of section 30AB(4) and the categories of hazard identified in them** — without identifying any entity or asset. The recommendation asks for aggregate visibility, not for disclosure of any entity's report.

Recommendation 5. *To the Department of Home Affairs.* The Act does not state what becomes of the exemption if a certificate ceases to be held. **What would establish the position is an express provision, or published guidance, on the effect of lapse, suspension or revocation of a certificate on the application of Part 2A to an asset previously covered by section 30AB(4).**

Section 7: The declaration route

Claim. The one route by which the compellability question could reach an asset outside the nine classes is unavailable for an asset in this class, and on one reading is subordinated to the exemption in any event.

The route

Section 4A(2) of the Rules applies the enhanced requirements to a CI asset that is "(a) specified in subsection (1); or **(b) covered by paragraph 30AB(1)(b) of the Act**". Section 4(3)(b) does the same for the baseline requirements.

Paragraph 30AB(1)(b) of the Act covers an asset where "both: (i) the asset is the subject of a declaration under section 51; and (ii) the declaration determines that this Part applies to the asset". Section 51(2A)(b) empowers the Minister to make that determination.

So a ministerial declaration is a live route into the enhanced requirements, including the vendor assessment at section 10A(5)(a), for an asset that is not in the nine classes.

Why it closes for this class

Section 51(1) permits a declaration only if, among other conditions:

> (a) the asset is **not otherwise a critical infrastructure asset**; and (b) the asset relates to a critical infrastructure sector; and (c) the Minister is satisfied that the asset is critical to: (i) the social or economic stability of Australia or its people; or (ii) the defence of Australia; or
>
> (iii) national security; and (d) there would be a risk to: (i) the social or economic stability of Australia or its people; or (ii) the defence of Australia; or (iii) national security; if it were publicly known that the asset is a critical infrastructure asset.

An asset answering section 12F is otherwise a critical infrastructure asset. **The declaration route is therefore unavailable for it.** This is an inference across two provisions and is stated as one.

Why the second limb is needed, and why it is conditional

The first limb does not cover the field. An asset that does not answer section 12F — because the knowledge condition at section 12F(1)(c) is not met, for instance — is not otherwise a critical infrastructure asset, and a declaration is available for it.

For that asset, section 30AB(2) is what matters. It provides that "Subsection (1) has effect **subject to** subsections (3), (4), (5) and (6)". Subsection (1) contains the declaration limb. Subsection (4) is the hosting certification exemption.

On the plain reading, where the conditions in subsection (4) are met, Part 2A does not apply notwithstanding a declaration that it does. That is a construction of one provision, and it is labelled as a construction.

What the explanatory memorandum says about subsection (2)

The construction above is not this practice's invention. The explanatory memorandum to the Bill that inserted section 30AB states at paragraph 139, in full:

> Subsection 30AB(2) provides that the application provision in subsection (1) is subject to the exemptions listed in subsections (3), (4), (5) and (6).

The memorandum's own headings style those subsections as exemptions: "Subsection 30AB(3)—Exemption (delayed commencement)" and "Subsection 30AB(4)—Exemption (where a critical infrastructure asset is certified strategic under the hosting certification framework)".

What "subsection (1)" contains, on the memorandum's account, is set out at paragraph 129. Part 2A applies to a critical infrastructure asset "if either of the following apply":

> the asset is specified in the rules (made by the Minister under section 61 of the SOCI Act, paragraph (1)(a)), or
>
> the asset is subject to a declaration under section 51 of the SOCI Act (being a private declaration that an asset is a critical infrastructure asset) and the declaration determines that Part 2A applies to the asset under new paragraph 51(2A)(b) (paragraph (1)(b), see also item 70).

So the subsection the memorandum says is subject to the exemptions is, on the memorandum's own account, the subsection containing the declaration limb.

What that does not settle

Three things, and this assessment states all three rather than resting on the memorandum.

The memorandum is not the enacted text. It states what the government told Parliament the provision does. Whether a court would adopt that reading is not a question this assessment answers.

The memorandum speaks generally. Paragraph 139 addresses subsection (1) as a whole. It nowhere addresses the case this section is concerned with — a declaration under section 51 and a strategic-level certificate bearing on the same asset. It states the relationship between the subsections, not what happens when the two collide.

Explanatory material supporting a construction is not the construction being settled. A department could still read subsection (2) as ordering the subsections without displacing a specific ministerial determination. What can be said is that such a reading sits against what the memorandum told Parliament, not that it is

foreclosed.

The second limb therefore remains conditional on the construction, and the field is not presented as closed. What has changed is that the construction is now stated with the government's own explanatory account beside it, rather than as a bare reading a department is invited to reject.

Analysis. Between them the two limbs account for assets in this class and assets outside it. Neither accounts for both, and the second is conditional. What the section establishes is that the confidential ministerial mechanism is not a straightforward answer to the gap identified in Section 4 — not that it could never operate.

Recommendation 6. *To the Department of Home Affairs.* The explanatory memorandum states the general relationship between subsection (2) and the exemptions. Nothing on the record establishes how that relationship is applied where a declaration under section 51 and a certificate under the framework would both bear on the same asset. **What would establish it is a statement of the Department's construction of section 30AB(2) in relation to paragraph 30AB(1)(b)**, in published guidance or in response to this assessment. The recommendation asks for the reading to be stated; it does not assert that this assessment's reading is correct.

Section 8: How the exemption came about

Claim. The record of the exemption's origin is short, and what it contains is quoted here in full, including the parts that cut against this assessment.

What the explanatory memorandum said

Paragraphs 142 and 146 are set out in Section 2 and are not repeated. Paragraph 143, the limit on the exemption's reach, is set out there and in Section 6.

What the committee recommended

The explanatory memorandum invokes recommendation 7 and paragraph 3.49 of the Parliamentary Joint Committee on Intelligence and Security's September 2021 report. Recommendation 7 reads, at paragraph 3.50: "The Committee recommends that the remaining non-urgent elements of the current Security Legislation Amendment (Critical Infrastructure) Bill 2020 not recommended for inclusion in Bill One, be deferred and amended into a separate Bill (Bill Two) in line with the principles outlined in paragraph 3.49."

Paragraph 3.49 sets out nine principles. They concern definitions, alignment to international standards, rights of reply, foreign investment review processes, the secrecy of declarations, protected information exchange, merits review in two respects, and the breadth of immunities. **None concerns hosting certification**, and the report contains no occurrence of "hosting", "hosting certification" or "HCF".

What that does and does not show. It is a nil return over a document that does not purport to enumerate every matter its authors considered, so it establishes what the report records and not what the committee turned its mind to. **A recommendation to defer non-urgent elements to a second Bill is capable of accommodating a measure the report does not name**, and the memorandum's invocation of it is consistent on its face. This assessment records the contents of the two documents and draws no inference from the difference between them.

What the 2022 committee said

The report on the Bill that inserted section 30AB describes the measure, in its account of the Bill, as "Recognition of the Digital Transformation Agency's Hosting Certificate Framework (HCF) as a risk-management process similar to the critical infrastructure risk management program—by excluding responsible entities from the critical infrastructure risk management program obligation when an asset, or part of an asset, they are responsible for is 'certified strategic' under the HCF".

Separately, at paragraph 3.38: "The Committee accepts the Department's assertions that existing mature risk management programs that sophisticated entities currently have in place will satisfy the Part 2A requirements and that the flexibility in the rules will allow for that to be realised. The distinct recognition of existing compliance with systems such as those required by APRA, of under the HCF, or even sophisticated ISO 31000 compliant programs will allow for entities to attest compliance or make the requisite adjustments to existing mechanisms."

These are two passages in two places. The second is about mature risk management programs generally, and mentions the framework in the sentence following the acceptance. It is not a finding about the framework alone, and it is not presented as one here.

What the submissions said

Submission 5 was made by Macquarie Telecom Group Limited, which the Australian Business Register records as having held that entity name from 9 December 2004 until 31 May 2023, and as being named Macquarie Technology Group Limited from that date. It is named below as at the date of its submission. The submission, dated 24 February 2022, said at paragraph 4.8: "However, the HCF is not equivalent to the SOCI regime and is at best only a partial substitute to the SOCI Act given that the HCF: is not grounded or specified in any legislation or formal regulatory instrument; does not apply to data storage or processing for corporate Commonwealth entities or state and territory government entities; does not require any reporting of cyber incidents (like Part 2B of SOCI Act); and does not provide for government (ASD) intervention and technical assistance in the event of a major cyber security incident (like Part 3A of the SOCI Act)."

At paragraph 5.3, in full: "The Committee should note that the HCF exemption would have some drawbacks. In particular, a service provider certified under the HCF would not be required to address any of the 'material risks' that the Minister may specify for the purposes of new subsection 30AH(8). These are set out in the draft Security of Critical Infrastructure (Critical infrastructure risk management program) Rules 2022 (the draft Rules), which has been published as Attachment C to the Explanatory Memorandum to the Bill. **Although many of the specified material risks are reflected in the HCF, there are some that are not**, such as risks associated with 'the storage, transmission or processing of sensitive operational information outside Australia'."

The paragraph speaks of the draft Rules of 2022. The provision it names survives in the compilation in force 10 June 2026, at section 6(d), which is the provision set out in Section 6 above.

The point this assessment makes about section 6(d) was made by a submitter to the committee four years ago, with the same provision named. It is recorded here as the submitter's, not as this practice's. And the submitter's qualification travels with it: most of the specified material risks were, in the submitter's view, reflected in the framework.

The submitter appears on the framework's Strategic-tier certified-provider list, which this practice has separately assessed. That is a fact about the record and is stated once, without inference.

Submission 12, and why this assessment does not rely on it

The 2022 report states at paragraph 2.77: "Item 32 of the SLACIP Bill proposes amending the definition of a data storage or processing service provider to only those storing 'business critical data' as defined in the SOCI Act. Macquarie Telecom and others submit that this narrowing of the asset definition will leave providers that store other crucial government data vulnerable and potential reliance on the Commonwealth's hosting certification framework (HCF) for risk management program coverage may leave gaps in coverage."

Submission 12 was made on 1 March 2022 by the UNSW Allens Hub for Technology, Law and Innovation, which its own home page describes as having been "an independent community of scholars based at UNSW Sydney that operated from 1 November 2017 until 1 June 2024". It is named here as at the date of its submission.

Submission 12 contains no occurrence of "hosting", "HCF" or "certification", and this assessment therefore does not count it as support for anything. What it does say at page 4 is a different point: "We noted that the amendment to 12F significantly broadened the application of section 12F assets, some of which are only incidental to the processing of data. We expressed concern that the broadened definitions would raise practical issues with implementation and cost to industry, which would eventually be passed on to consumers. The retention of the 'wholly or primarily' limiting factor, and the addition of the 'business critical' requirement, does keep the definition narrower, although this may raise issues around interpretation of these requirements."

Its adjacent concern runs with the exemption's rationale rather than against it: "Our concerns that the data storage or processing industry was at high risk of duplicative and inconsistent obligations has been partially addressed", welcoming the Government's stated intention "to minimise any duplication or unnecessary burden, and to de-conflict requirements for entities with assets which fall within more than one definition of critical infrastructure asset."

This is a statement about what this assessment relies on, and nothing more. Submission 12 is not a witness for this assessment, and no part of what follows rests on it.

Analysis. The published record of the exemption's origin consists of a paragraph of explanatory memorandum, a description in a committee report, an acceptance of departmental assertions about mature risk programs generally, and two submissions of which one addressed the measure directly. The committee recommendation the memorandum invokes does not mention hosting certification, for the reasons and with the limits set out above. **That is what the record contains; it is not a criticism of anyone's conduct, and no inference about anyone's state of mind is drawn from it.**

Section 9: Disclosure, and the dates that qualify it

Claim. The framework's published material does not disclose the effect of strategic-level certification on the application of Part 2A, and the dates explain part of that silence.

What the published material says

Neither the operative March 2021 document nor either of the two live scheme pages captured on 11 August 2026 states that strategic-level certification affects the application of Part 2A of the Act. Neither page contains "Part 2A", "30AB", "Security of Critical Infrastructure", "critical infrastructure" or "risk management program".

This is a nil return over documents that do not purport to be exhaustive, and it is weaker than an inventory nil. It establishes what a reader of the scheme's published material would not learn from it. It does not establish that no departmental material anywhere states the position.

The dates

The operative document is dated March 2021. The Bill it names became Act No 124 of 2021, assented 2 December 2021. Section 30AB was inserted by Act No 33 of 2022; the Act's endnotes record it as added by that Act, with no amendment to it recorded since.

The March 2021 document could not have disclosed a provision inserted in 2022. That answers the silence in the operative document entirely.

It does not answer the silence on the live pages, which carry a current reform notice and are revisable at any time. That is the narrower observation, and it is the only one made here.

Analysis. A provider reading the framework's published material learns what certification requires. It does not learn that certification bears on the application of a Part of the Act. Whether that matters depends on who the audience for the scheme's pages is taken to be — a question this assessment does not answer.

Recommendation 7. *To the Department of Home Affairs.* The scheme's published material does not state the relationship between certification and Part 2A. **What would resolve it is a sentence on the scheme's published pages, or in the reformed framework, stating the effect of a strategic-level certificate on the application of Part 2A.** This follows from Recommendation 3 and is the narrower, immediately actionable form of it.

Section 10: Limits, and what would falsify each claim

This section states what this assessment cannot establish, and what would show each of its claims to be wrong.

What it does not claim

1. It does **not** claim Parliament was misled.
2. It does **not** claim any provider, department, official, committee or submitter did anything wrong.
3. It does **not** claim the exemption is unexplained. The rationale is quoted in full.
4. It does **not** claim no Australian instrument asks the compellability question. One does, as a *must*.
5. It does **not** claim a section 51 declaration has or has not been made in relation to any asset.
6. It does **not** claim the framework is inadequate as a hosting certification. It states what the framework says it tests, and what terms are absent from its document.
7. It does **not** claim the exemption leaves an asset unregulated. Part 2AA substitutes an annual report.
8. It does **not** claim the exemption covers everything a certified provider holds. Facilities not used in connection with certified services remain covered.
9. It does **not** claim Submission 12 supports any part of this assessment.
10. It does **not** claim the framework concealed the exemption, or was silent about the critical infrastructure regime. It named the Bill three times and predates section 30AB.
11. It does **not** claim government data holdings sit outside the SOCI scheme. They are inside it as a defined class.
12. It does **not** claim any certified provider is subject to foreign compulsion, or that any data has been accessed.
13. It does **not** claim to know what any Part 2AA report contains.
14. It does **not** claim its construction of section 30AB(2) is the only available reading.

The permanent limit

No report made under Part 2AA has been read, and none can be from public sources. This assessment compares what instruments require. It does not compare what is done. Every conclusion here is about instruments, and any reading of it as a conclusion about practice is a misreading.

What would falsify each claim

Claim	Falsified by
The compellability question is confined to nine classes	An amendment adding the data class to section 4A(1) of the Rules
The question has never reached the data class	Any provision, in any compilation, imposing section 10A on an asset specified in section 4(1)
Neither key term is defined in the Act	The terms appearing in section 5 or elsewhere in a compilation
No provision addresses lapse or revocation	Any such provision in a compilation
The framework's document defines sovereignty as ownership and control	A different definition elsewhere in the same document
The framework said the regimes would work in conjunction	Nothing on the present record; it is a quotation
The scheme's published material does not disclose the Part 2A effect	Any framework or scheme material stating it
The declaration route is unavailable for this class	A reading of section 51(1)(a) permitting declaration of an asset already within section 12F
Section 30AB(2) subordinates the declaration limb	A departmental or judicial construction to the contrary — this is a construction, not settled law
Submission 12 does not make the proposition footnoted to it	Any passage in Submission 12 asserting reliance on the framework or gaps arising from it

Section 11: Recommendations

Each recommendation follows from a claim in this assessment. **None asserts that the current position is wrong.** Each states what is not established on the record and what would establish it.

#	To	What is not established	What would establish it
1	Department of Home Affairs	Why the enhanced requirements, including the compellability question, were confined to nine asset classes	A published statement of the basis, in an explanatory statement to any future amendment of the Rules or in departmental guidance
2	Department of Home Affairs	That the allocation of the data class to baseline rather than enhanced requirements was considered rather than incidental	A published statement of the risk basis for the allocation
3	Department of Home Affairs	The current relationship between certification and Part 2A, given the framework's stated posture of conjunction	A statement of the relationship in the reformed framework
4	Department of Home Affairs	What the Part 2AA reporting substitute delivers, no report being public	Publication, in aggregate and identifying no entity or asset, of the number of Part 2AA reports received in respect of section 30AB(4) and the hazard categories identified

#	To	What is not established	What would establish it
5	Department of Home Affairs	What becomes of the exemption if a certificate lapses, is suspended or is revoked	An express provision or published guidance on the effect of lapse, suspension or revocation
6	Department of Home Affairs	How section 30AB(2) is read where a section 51 declaration and a certificate would both bear on one asset	A statement of the Department's construction of section 30AB(2) in relation to paragraph 30AB(1)(b)
7	Department of Home Affairs	The effect of a strategic-level certificate on Part 2A, for a reader of the scheme's published pages	A sentence to that effect on the scheme's published pages or in the reformed framework

End of document.