AustraliaOS

australiaos.com.au

AustraliaOS Pty Ltd
Decision infrastructure
for Australian institutions

# Telstra CLOUD Act Assessment

A jurisdictional exposure assessment of an Australian critical telecommunications carrier under the Security of Critical Infrastructure Act 2018.

| REFERENCE | DATE | CLASSIFICATION | VERSION |
| --- | --- | --- | --- |
| AOS-TEL-2026-001-v1.7 | May 2026 | Public | 1.7 |

Contents

## 01 Doctrine

Doctrine fixes the statutory and legal boundaries within which this assessment is made.

### Telstra is a SOCI responsible entity

Telstra operates under carrier licences held by Telstra Limited (ACN 086 174 781, licence 582) and Telstra Corporation Limited (ACN 051 775 556, licence 1) under the Telecommunications Act 1997 (Cth); Telstra Group Limited (ASX:TLS, ABN 56 650 620 303) is the listed holding company of the group. The licensee carrier entities are responsible entities for critical telecommunications assets under the Security of Critical Infrastructure Act 2018 (Cth). In this assessment, "Telstra" refers to the Telstra group; statutory obligations attach to the relevant operating entity within the group.

The Enhanced Response and Prevention Act 2024 received Royal Assent on 29 November 2024. Schedule 5 commenced 4 April 2025. From that date the Telecommunications Sector Security Reforms regime under Part 14 of the Telecommunications Act ceased. The all hazards security setting of the SOCI Act applies.

The Telecommunications Security and Risk Management Program Rules 2025 took effect on the same date. They impose a written risk management program obligation on all carriers including Telstra. They impose increased cyber security framework requirements relative to the cross sector rules.

The Minister for Home Affairs holds direction power over Telstra under the SOCI Act. The Minister can direct Telstra to do, or not do, a specified thing reasonably necessary to reduce or eliminate a security risk.

### The CLOUD Act reaches covered providers regardless of data location

The Clarifying Lawful Overseas Use of Data Act 2018 inserted 18 USC 2713. Section 2713 requires a provider of electronic communication service or remote computing service subject to US jurisdiction — including by incorporation — to preserve, back up, or disclose customer data on US legal process. The obligation applies regardless of whether the data is located within or outside the United States.

Reach attaches to a covered provider through US jurisdiction; for the US incorporated vendors assessed here, incorporation is the operative basis. It does not attach to the location of the data. A US incorporated provider holding Telstra workload data in Sydney is within the reach of a US warrant served in the United States (CLAIM F).

The Australia United States CLOUD Act Agreement was made under section 2523, signed on 15 December 2021, certified by the US Attorney General under section 2523(b), and brought into force on 30 January 2024 through a formal exchange of diplomatic notes.

It governs reciprocal access between Australian and United States authorities. Operationally, it works through the International Production Order framework in Schedule 1 to the Telecommunications (Interception and Access) Act 1979: Australian orders are reviewed and transmitted by the Australian Designated Authority within Home Affairs, the US Department of Justice performs the same function for the United States, and orders under the Agreement must not intentionally target persons in the receiving country. Article 10 of the Agreement states that it is without prejudice to, and shall not affect, other legal authorities and mechanisms for obtaining electronic data from covered providers. The Agreement therefore does not narrow whatever Section 2713 obligation a covered US provider owes to US legal process, and it does not create one where the statutory conditions are not met (CLAIM G; ANALYSIS B).

**PSPF and ISM are the reference baseline**

The Protective Security Policy Framework sets policy expectations for Commonwealth entities. The Information Security Manual sets technical control baselines for Australian Government information systems. Neither binds Telstra directly outside contracted Government work. Both apply where Telstra carries Commonwealth, Defence, or intelligence customer data, and both are the reference standard against which any future SOCI direction will be measured.

**Doctrine position**

Telstra carries an enforceable all hazards risk management obligation under the SOCI Act.

Foreign legal access exposure created by US incorporated vendors holding Telstra workload data is a risk within the all hazards definition. It is statutory. It is named. It is not theoretical.

The CLOUD Act Agreement does not remove the exposure. It administers it.

Final decisions on vendor selection and operational use remain with Telstra. This assessment produces a decision posture, not a substitute for internal governance.

## 02 Case context

Telstra Group Limited (ABN 56 650 620 303) is the case subject. The assessment scope is the foreign legal access exposure created by US incorporated vendor dependencies in Telstra's operational AI and cloud workloads, measured against the all hazards risk management obligation that attaches to Telstra as a responsible entity for critical telecommunications assets under the SOCI Act and the TSRMP Rules 2025. The exposure is operational, not hypothetical. Telstra's Connected Future 30 strategy, announced 27 May

2025, names AI as a strategic driver of customer experience and network operations, and the production deployment of Microsoft Azure OpenAI for customer facing AI was jointly disclosed by Telstra and Microsoft on 7 February 2024.

## 03 Assessment summary

The assessment reviewed Telstra's public vendor partnership disclosures, identified US incorporated providers handling Telstra workload data, assessed each named vendor against the Section 2713 conditions, with reach found to attach, to be conditional, or not to attach depending on whether the vendor operates as a covered provider holding Telstra data, and tested the resulting exposure against the SOCI Act all hazards risk management framework as augmented by the TSRMP Rules 2025. The vendor footprint that drove the assessment comprises Microsoft Azure OpenAI for "Ask Telstra" and "One Sentence Summary" production customer service AI; AWS hosting Nokia IMS in a resiliency trial, initially for Voice over LTE with expansion under way to broader network services; the seven year Telstra Accenture AI joint venture and the Silicon Valley AI Hub with named ecosystem partners AWS, Databricks, and Microsoft; and the Red Hat, Dell, and Cisco autonomous network proof of concept of 2 March 2026.

## 04 Risk posture and decision

**Risk posture: High.**

**Decision: Conditional Continuation with Mandatory Sovereign Migration Pathway.**

The High posture is driven by the concentration of Telstra's most strategically significant AI and network workloads on US incorporated providers whose exposure to US legal jurisdiction is not removed by the Australia US CLOUD Act Agreement. Azure OpenAI, operational and powering customer facing AI at scale, is a hosted service holding Telstra data, placing it within Section 2713 reach on a covered provider characterisation that is reasonable but contestable (ANALYSIS A). AWS features in a Voice over LTE resiliency trial, a network layer function, where whether Section 2713 attaches depends on whether AWS holds Telstra data in that role, a question the source register does not resolve (ANALYSIS C). The Accenture seven year JV and Silicon Valley Hub embed Telstra's foundational AI architecture in an ecosystem whose collaboration partners are themselves US incorporated. The exposure is structural across the AI strategy, not isolated to a single workload.

Conditional Continuation rather than Cease is warranted because the SOCI framework is calibrated for risk management, not vendor prohibition. The TSRMP Rules 2025 require a written all hazards risk management program; they do not require a sovereign only operating posture (CLAIM D). The source register establishes no Australian incorporated

production grade equivalent to Azure OpenAI, and abrupt cessation would itself create availability risk for the VoLTE resilience function and the customer service AI workloads.

Mandatory Sovereign Migration Pathway is warranted because continued operation without a migration commitment converts a managed risk into an accepted standing exposure. The Minister for Home Affairs holds direction power under the SOCI Act (CLAIM E), and the absence of a migration pathway materially weakens any defence against a future direction. The pathway is the condition that keeps the posture defensible.

## 05 Decision basis

The residual risk after current controls is the standing capacity of US legal process, served on Microsoft, AWS, or any other US incorporated provider in the assessed footprint, to compel disclosure of Telstra workload data held by that provider, where it holds such data, regardless of where the data is physically located. Section 2713 reach attaches to a covered provider by country of incorporation, not by the location of the data (CLAIM F). The Australia US CLOUD Act Agreement, in force since 30 January 2024, administers reciprocal access through the International Production Order framework; by its own Article 10 it is without prejudice to other legal authorities and mechanisms for obtaining electronic data from covered providers, so it does not extinguish whatever Section 2713 obligation a covered provider owes (CLAIM G; ANALYSIS B).

A lower posture would be appropriate on two changes: an Australian incorporated production grade alternative for the Azure OpenAI workload is adopted for any workload involving Commonwealth, Defence, or intelligence customer data; and the AWS Voice over LTE deployment is mirrored or replaced by an Australian controlled equivalent. [GAP: source register does not establish whether such Australian incorporated production grade alternatives currently exist for the specific Azure OpenAI workload functions in production at Telstra.]

## 06 Primary decision drivers

**1. Microsoft Azure OpenAI dependency for production customer service AI.** Telstra and Microsoft jointly disclosed on 7 February 2024 the deployment of “Ask Telstra” and “One Sentence Summary” on Azure OpenAI Service — Ask Telstra trialled with about 200 contact centre agents from mid 2023, One Sentence Summary trialled with 100 agents in 2023 — expanding across contact centre and store teams through 2024. Microsoft Corporation is Washington incorporated, and as the operator of the hosted Azure OpenAI service that processes this data it is the kind of provider Section 2713 reaches (ANALYSIS A). Exposure is workload class; the source register does not establish what specific data classes flow through.

**2. AWS dependency for Voice over LTE network resilience.** On 19 February 2024 Telstra, AWS and Nokia announced a hybrid network architecture resiliency trial of Nokia's IMS software on AWS — initially for Voice over LTE resilience, with expansion under way beyond VoLTE toward the full scale of network provided services. Amazon.com Inc is Delaware incorporated. Network resilience at this layer is a production-relevant function, so a trial of this scope involving a US incorporated provider is a potential exposure surface rather than a peripheral experiment. The source does not establish whether the trial progressed to production, whether AWS holds Telstra data in this role, or its current status. The assessment treats the production-versus-trial scope as unresolved and flags the involvement as a potential exposure pending further disclosure (ANALYSIS C).

**3. Accenture seven year AI joint venture and Silicon Valley Hub.** The JV announced 15 January 2025 was finalised in February 2025 and commenced operations in April 2025, with Telstra committing approximately AUD 700 million over the seven year term (CLAIM J; CLAIM Y). The venture is 60 per cent owned by Accenture and 40 per cent by Telstra (CLAIM V), is staffed in part through 726 roles affected within Telstra's Data and AI teams across Australia and India (CLAIM Z), and consolidates Telstra's vendor support from 18 data and AI providers down to two JVs, Quantium Telstra and the Accenture venture (CLAIM X) — a deepening of dependency concentration at the centre of Telstra's AI architecture. Telstra states that it retains control over its data and AI strategy and roadmap, which the JV helps deliver (CLAIM W); retained strategy control does not of itself determine where the data sits or which entity holds it. The 13 May 2025 Silicon Valley Hub names AWS, Databricks, and Microsoft as ecosystem partners, and connects with Accenture teams in Sydney, Melbourne, and Bangalore through Accenture Connected Innovation Centers (CLAIM K). Accenture plc is Irish incorporated. The operating entity of the JV is not identified in the public announcements. An ASIC Connect search conducted 10 June 2026 (terms: Telstra Accenture; Accenture Telstra; Telstra; Accenture; Quantium Telstra) found the precedent joint venture registered under the parents' combined names — Quantium Telstra Pty Ltd, ACN 664 366 885, registered 8 December 2022 (CLAIM BB) — but no equivalent registration for the Accenture JV. The operating entity is therefore either registered under an unannounced name, registered outside Australia, housed within an existing Accenture subsidiary, or contractual in form; exposure through the JV remains conditional pending entity level disclosure. An Australian registration, if located, would specify rather than resolve the exposure question: with majority foreign ownership, possession, custody, or control reach through the parent remains a live question regardless of the JV's place of incorporation.

**4. Red Hat, Dell, and Cisco autonomous network proof of concept.** On 2 March 2026 Telstra disclosed a proof of concept demonstrating an AI-enabled self-healing network

capability, in collaboration with Red Hat, Dell Technologies and Cisco. Red Hat, LLC is a Delaware-formed limited liability company; Dell Technologies Inc. and Cisco Systems, Inc. are Delaware-incorporated corporations. A self-healing, self-optimising capability of this kind operates at the network management layer rather than on customer communications data. These are infrastructure and software vendors rather than communications or computing service providers holding Telstra data, so Section 2713 reach does not attach to them in the way it may to a hosted-service provider; the exposure they create is of a different kind. As US-incorporated vendors operating at the network management layer, they fall within the standing reach of US export-control and sanctions law (ANALYSIS E), which gives the US government the capacity to restrict what they may supply and support. That exposure is contingent rather than active: most items require no licence to most destinations, Australia is an allied participant in the multilateral export-control arrangements, and no current restriction is in force. The exposure here is to the supply and operational continuity of the network-management capability, conditional on future US action, not to compelled disclosure of communications data.

**5. Absence of a sovereign equivalent for the production AI workload.** [GAP: source register does not establish the existence or non-existence of an Australian incorporated production grade alternative to Azure OpenAI for Telstra's customer service AI workloads.] Treated as an operating environment fact pending verification. The absence claim is testable through direct vendor disclosure or a structured market scan, and the appropriate response is verification rather than assumption.

**6. SOCI Minister direction power as a residual mitigation.** The Minister for Home Affairs holds direction power over Telstra under the SOCI Act and can direct Telstra to do, or not do, a specified thing reasonably necessary to reduce or eliminate a security risk (CLAIM E). The power is not a substitute for Telstra's own risk management program. It is the residual instrument the Commonwealth retains.

## 07 Required conditions

The overall posture decision is recorded as RECOMMENDATION A: Conditional Continuation of the current US-incorporated provider footprint, paired with a Mandatory Sovereign Migration Pathway for production AI workloads. The following seven conditions operationalise that posture.

1. Maintain an Australian incorporated alternative or air gapped equivalent for any production AI workload involving Commonwealth, Defence, or intelligence customer data. The condition is asset class scoped, not vendor blanket. (RECOMMENDATION B)

2. Quarterly re-assessment of the foreign legal access exposure surface under the TSRMP Rules 2025 cyber security framework, recorded in Telstra's written risk management program. (RECOMMENDATION C)
3. No standing US incorporated vendor privileged access to network management plane workloads. Operational access time bound, ticketed, and revocable. (RECOMMENDATION D)
4. Mandatory disclosure to the relevant Commonwealth customer of any vendor change that materially alters the foreign legal access surface for that customer's data. (RECOMMENDATION E)
5. Approval gating on any expansion of the Azure OpenAI footprint into protected Commonwealth workloads, with the gating decision held outside the operating business unit. (RECOMMENDATION F)
6. Documented Section 2713 disclosure handling protocol covering Telstra's actions if a US incorporated vendor receives US legal process for data containing Telstra workload material. (RECOMMENDATION G)
7. Nomination of a sovereign migration target for the production AI workload class, with a stated target date and a disclosure pathway consistent with the all hazards risk management obligation. (RECOMMENDATION H)

The binding obligation behind these conditions is Telstra's all hazards risk management program under the SOCI Act and the TSRMP Rules 2025; APRA's Prudential Standard CPS 230 does not bind Telstra, which is not an APRA regulated entity. As a cross regime benchmark, however, the pathway contents required by condition 7 — a nominated target, a stated date, and a disclosure pathway — mirror what Australia's prudential regulator already codifies for the entities it does regulate: CPS 230 requires provider exit and transition planning for material service providers, assessment of geographic location and concentration risk before entering a material arrangement, and prior notification to the regulator of any material offshoring arrangement, including where data or personnel relevant to the service will be located offshore (CLAIM AA). A sovereign migration pathway with a named target and date is therefore not an extraordinary demand on a critical telecommunications carrier; it sits within the established envelope of Australian regulatory expectations for managing material service provider risk.

## 08 Review value

The assessment is reviewable. The evidence base is the Telstra-Sources.md source register, every claim is traceable to a public source, and the gaps are flagged inline rather than papered over. The reviewing authorities are Telstra's own SOCI risk management program owners, any Commonwealth customer with contractual or statutory entitlement

to review the foreign legal access exposure of services provided to it, and the Minister for Home Affairs in the exercise of the direction power.

The assessment is not a substitute for legal advice on 18 USC 2713 application to specific data flows. It is not a substitute for Telstra's own SOCI risk management program. It is not a directive. Final decisions on vendor selection and operational use remain with Telstra. Final statutory direction remains with the responsible Minister. The assessment produces a decision support artefact. Its value is reviewability, not authority.

End of document.