The jurisdictional basis of sovereignty

KITBAGS RESPONSE TO THE JOINT SELECT COMMITTEE ON ARTIFICIAL INTELLIGENCE



Kitbag

ENTERPRISE EVOLVED

Table of Contents

The Jurisdictional Basis Of Sovereignty 5

1. About the author 5

2. Introduction 5

2.1 What is meant by artificial intelligence 5

2.2 The opportunity and the confidence gap 6

3. The jurisdictional basis of sovereignty 8

4. Addressing the Terms of Reference 9

4.1 The opportunity and national resilience 9

4.1.1 Two legitimate paths 9

4.1.2 Reshoring and robotics 10

4.1.3 Resilience as the test 10

4.1.4 Distribution and adoption 11

4.1.5 Reversing a dependency 12

4.2 Building and retaining sovereign capability 12

4.2.1 A tiered sovereignty classification 13

4.2.2 A Deed of Sovereignty 14

4.2.3 The supply problem 15

4.2.4 Weighting and international practice 15

4.2.5 Trade obligations 16

4.3 Data sovereignty and domain-specific models 17

4.3.1 The opportunity 17

4.3.2 The opportunity can be built and then lost 17

4.3.3 The second sovereign data asset 17

4.3.4 Control of weights and the open-weight model pathway 19

4.4 Workforce and skills 20

4.5 Adoption, transparency and accountability 21

4.5.1 The existing regime asks a different question 21

4.5.2 Why procurement data cannot answer it either 22

4.6 Supply chains and critical infrastructure 23

4.7 Governance before the point of action 23

5. Applying the framework in practice 25

6. Summary of Recommendations 25

7. Conclusion 28

Appendix A: Recommendations and the problem each address 29

Appendix B: Sovereignty scoring table 31

Appendix C: Related submissions 32

Appendix D: What Commonwealth AI transparency statements disclose 2

Executive Summary

Background

Artificial intelligence is an economic question for Australia before it is a technological one. The gains anticipated over the coming decade will be captured in application rather than invention, in the industries where Australian operating knowledge is the scarce input and in AI driven automation to repatriate critical supply chains.

Whether the benefits are realised turns on a question the Commonwealth does not ask, being 'who can lawfully compel the entity that operates the capability'?

Data residency describes where information is stored. Sovereignty describes who can access and withdraw it.

Problem

Australia is acquiring a dependency it cannot see, cannot price and cannot easily reverse.

The United States, China and India each have laws that can compel companies domiciled in their countries to hand over Australian data. A contract signed in Australia cannot override a law passed overseas. A supplier bound by one of these laws must comply with it even when the data resides in an Australian data centre and even when the contract with the Commonwealth says otherwise.

The United States has the CLOUD Act, China has its National Intelligence Law and India has section 69 of its Information Technology Act 2000. The problem is not what these companies intend to do, it is what their home governments can lawfully order them to do.

The data these laws can reach is not limited to names and records. It includes the *operating logic* that makes an Australian business or agency competitive: how a mine schedules its equipment, how a farm manages its planting cycle, how an agency reaches its decisions. When a foreign government can compel a company to hand over that knowledge, it can transfer the source of Australia's competitive advantage directly to industries inside its own economy. In June 2026 a single United States government decision cut off everyone outside the United States from two leading AI models for nineteen days.

Australia signed the United States-led Pax Silica declaration in December 2025 and in August 2026 the United States Studies Centre, supported by the US Consulate here in Australia argued that Australia *cannot build its way out of dependency* on the United States and should instead negotiate access terms, what it called *managed dependency*. China distributes capable open-weight models free into markets it does not otherwise reach, using training data that cannot be independently verified. India holds equivalent legal reach over data as both.

The Commonwealth cannot currently say who can compel the entities running its AI capability. Of 73 government transparency statements reviewed in September 2026, none state whether inference is processed onshore, whether the Commonwealth holds the model weights, or whether any foreign jurisdiction has legal reach over the supplier.

A second exposure sits beneath that and no current instrument classifies it as data. Before an AI capability can act inside an agency, it must be given the agency's own operating logic: its System of Work. When that layer is configured inside a foreign-controlled platform, it leaves with the platform. The agency cannot fully account for what its AI may do and cannot change vendor without rebuilding that logic from the ground up.

Once that logic is inside a foreign-controlled platform, two outcomes become inevitable and neither requires hostile intent. The first is commodification. The operating logic gets wrapped into an API call and priced as a subscription. What was a competitive advantage now becomes a use case available to everyone. The second is replacement. Using that operating logic and applying compute at a scale no incumbent can match, the platform replicates an entire industry's function and delivers it faster and cheaper. The industry itself becomes redundant.

This exposure does not arrive through a single visible decision. It arrives through licence extensions and feature additions inside platforms agencies already hold. Each individual step is defensible. Nobody is assessing the cumulative position. Technology is the largest procurement category across Australian government, and contracts worth approximately $27 billion reach their end dates during 2026.

Solution

Thirteen recommendations follow, directed at two outcomes. Jurisdictional exposure should be scored before a capability is bought. An agency or enterprise should hold its own System of Work under Australian law. Each can be delivered through instruments the Commonwealth already holds and none requires a new agency. Three warrant action first, because each resides inside an existing process and the first closes a window that shuts during 2026.

- Recommendation 1 makes legal domicile the test of sovereignty and applies a tiered classification at the point of purchase. Conditions set at the 2026 renewals cost nothing and capability bought without them carries the exposure for the life of the contract.
- Recommendation 11 adds four disclosure fields to the transparency statements agencies already publish, turning an existing compliance exercise into a national picture of jurisdictional exposure at close to no cost.
- Recommendation 12 is within the committee's own gift. Asking each portfolio how much of its AI capability is operated by entities subject to foreign compulsion and publishing who could answer would establish a position no submitter can.

1. About the author

Kitbag Consulting is a veteran-owned Canberra firm with over eighteen years of management consultancy experience across the national security, public and private sectors. The firm builds sovereign operating capability for complex organisations and the work is operations-led rather than technology-led. It begins by modelling how an organisation decides and delivers, converts that into an operating logic the organisation owns and only then determines what technology should execute it. The firm has done this for Commonwealth agencies and for businesses carrying the same problem at commercial scale, including the design of AI governance and operating frameworks for organisations adopting the technology at pace.

One conclusion from that work frames this submission: the System of Work described above is what determines whether artificial intelligence scales or merely accumulates dependency. An AI capability cannot act until it is told what the organisation permits, who may decide what and within what limits. Where that logic is held as an asset, each new capability is configured against it and adoption compounds. Where it is not, every deployment encodes the logic again inside whichever platform is being implemented, so the organisation scales its dependency rather than its capability.

2. Introduction

This submission addresses paragraphs (a) to (h) and (l) of the terms of reference, together with a matter raised under paragraph (n).

2.1 What is meant by artificial intelligence

This submission adopts the Commonwealth's own definitions. The Technical standard for government's use of artificial intelligence takes the OECD definition of an AI system, being a machine-based system that infers from its input how to generate predictions, content, recommendations or decisions, together with the ISO/IEC 22989 definitions of an AI model and of machine learning and the NIST definition of generative AI.

Those definitions describe what a system does rather than who holds it or who can withdraw it. Six categories are in use across the Commonwealth and each sits differently on the second question.

- Predictive and analytical models trained on an agency's own data.
- Generative models accessed as a service, where the Commonwealth holds access rather than the capability.
- Open-weight models run on the agency's own infrastructure, where the weights are held and provenance is the governing question.
- Agentic systems that take actions and transact with agents in other organisations, addressed by Recommendation 8.
- Embedded AI arriving inside a platform already licensed, never procured or recorded as AI.
- Robotics and industrial automation, which leave the control software and operating data with whoever built the line.

No agency or business currently uses all six. Each draws on a different combination according to what it does, so the exposure that matters is set by the categories an organisation actually relies on rather than by the full list. A small business using a generative model as a service faces a different question from an agency training predictive models and using automations on its own data.

What the six share is the second question, who can lawfully compel the entity that operates the capability. Recommendation 1 turns on that question rather than on which type of AI was bought.

2.2 The opportunity and the confidence gap

The Productivity Commission anticipates productivity gains from AI of approximately $116 billion over the coming decade, with other estimates considerably lower[1]. Value from the general purpose technology will accrue to the country that applies it well rather than to the country that invents it. Australia is positioned to apply it well. The industries in which this country already competes globally, being resources, agriculture, health and medical research and defence sustainment, are data-rich industries in which Australian operating knowledge is the scarce input.

Artificial intelligence and robotics change the economics of industries Australia was priced out of decades ago.

Half of Australians regularly use artificial intelligence in one or more of the forms described above. Thirty-six per cent are willing to trust it and thirty per cent consider that the benefits outweigh the risks, the lowest result recorded across the forty-seven countries surveyed.[2]

The prevailing debate offers two responses; adopt quickly because the cost of falling behind is high or to proceed slowly until the risks are better understood. The first response is now being argued in its strongest form. In August 2026 the United States Studies Centre published Sovereignty through managed dependence, which holds that Australia cannot build its way out of dependency on the United States, that sovereign compute at scale is inefficient and likely infeasible and that the task is to secure favourable access terms rather than to hold capability. Australia is already party to the United States-led Pax Silica declaration, signed in December 2025 as one of seven original signatories.

Australians are pursuing the first while holding the second, which produces adoption without confidence. Adoption of that character reverses at the first significant failure and an economy does not compound gains from a technology its population is prepared to abandon.

The choice is not between the frontier and falling behind. Open-source inference models can handle around 98 per cent of the work that generates value inside any organisation. The frontier is for edge cases roughly two per cent of use where the task genuinely cannot be done any other way.

Treating frontier models as the default rather than the exception is what manufactures the dependency the first response accepts as unavoidable. It is a procurement habit, not a technical requirement.

[1] Productivity Commission, Harnessing data and digital technology, interim report, August 2025.

[2] Gillespie, N., Lockey, S., Ward, T., Macdade, A. and Hassed, G. (2025). Trust, attitudes and use of artificial intelligence: A global study 2025. The University of Melbourne and KPMG.

Open-weight models that Australian organisations own, inspect and adapt deploy now, at known cost, under Australian law. That is what allows adoption at speed. When a capability operates under rules Australian institutions have set, in a jurisdiction the public can reach, its failures can be corrected rather than endured. That supplies the confidence now missing.

Sovereignty is the term for that condition as it lets Australia adopt quickly and keep the value of adoption here.

For the 2% of edge cases, United States-led Pax Silica declaration will suffice for now.

3. The jurisdictional basis of sovereignty

The US CLOUD Act compels US companies to provide access to data and systems under their control wherever those systems sit, whatever the contract says and whether or not the Australian counterparty has consented.[3] China's National Intelligence Law imposes an equivalent obligation, with no opt-out and no carve-out available through a subsidiary.[4] A vendor cannot override either obligation. The contract does not supersede the law the vendor answers to.

Australian law does not extinguish these obligations. It coexists with them and where they conflict the vendor's home jurisdiction prevails. The governing question for a Commonwealth AI contract is therefore not which terms apply but *which jurisdiction controls the relationship*. Data residency tells you where information sits. Sovereignty tells you who can compel its production, alter its availability or withdraw the service.

Encryption under Australian control is a genuine complementary safeguard and a Commonwealth-held key can stop a foreign government reading data even if it compels access to the system storing it. It is not a substitute for jurisdictional control. Where the vendor or its parent holds the keys or can be compelled to assist in decrypting what it stores, the technical control follows the same jurisdiction as the contract and fails at the same moment the legal one does.

Risk assessment that ignores the political disposition of a vendor's home jurisdiction and the instruments that jurisdiction holds over the vendor, is assumption management presented as due diligence.

One objection may be anticipated, namely that treating a treaty ally in the same frame as a strategic competitor is misjudged. Australia receives intelligence, defence technology and computing capability from the United States on terms extended to very few countries and nothing here proposes weakening that relationship. The argument does not rest on the disposition of any government. It rests on the existence of the instrument. A compulsion power operates whatever the state of the relationship, survives changes of administration and is exercised in the interests of the country holding it.

The June 2026 export control directive described in section 4.3.2 was issued by Australia's closest security partner and applied to every Australian user by operation of nationality. Alliance is a reason to expect an instrument to be used carefully, not a reason to assume it will never be used.

Jurisdiction also bears on public confidence. A person affected by an automated decision can ask an Australian agency to explain it and the agency answer to the courts, the Ombudsman and this Parliament. None of those avenues reaches an entity operating outside Australian jurisdiction. Accountability that stops at the edge of the platform is not accountability the public can rely on.

[3] Clarifying Lawful Overseas Use of Data Act 2018 (US CLOUD Act), 18 U.S.C. § 2713

[4] People's Republic of China, National Intelligence Law (2017), Articles 7 and 14.

4. Addressing the Terms of Reference

4.1 The opportunity and national resilience

Artificial intelligence is a general purpose technology and value from such technologies accrues where they are applied, not where they are invented. Australia is unlikely to lead in building frontier foundation models and does not need to. The opportunity in paragraphs (a) to (d) sits at the application layer, in the sectors where Australia already holds comparative advantage and, in the sectors, where the cost structure that drove them offshore no longer holds.

Australian mining shows the pattern. Autonomous haulage, automated rail and remote operations centres run at scale here, built on Australian operating knowledge of Australian conditions. The same logic extends across the sectors named in paragraph (c). Agricultural robotics and yield modelling draw on more than a century of observational data. Advanced manufacturing gains from AI-directed process control and robotics at the small production volumes typical of Australian industry, where flexibility is worth more than scale. Health and medical research hold population-scale longitudinal data few countries can assemble. Financial services hold decades of transaction, credit and superannuation data under Australian law, an advantage in fraud detection and credit-risk modelling that a system trained on a foreign market does not carry. Defence sustainment and logistics cannot be run from offshore in a contingency. In each case the model is a component and the advantage lies in the domain knowledge, the data and the operating logic wrapped around it.

4.1.1 Two legitimate paths

Sovereign capability does not require building everything here. It requires that capability operating in Australia answering to Australian law. Two paths follow.

The first is to build domestically where the data advantage already exists, as it does in agriculture, resources, health and defence sustainment. Capability of that kind can be built at a fraction of frontier cost and the intellectual property, profits and skills stay onshore. These are the predictive and analytical models trained on an agency's own data, the first of the six categories in section 2.1. Of the six they carry the least jurisdictional exposure because the data and the model both stay onshore.

The second is to import what cannot practicably be built here, on conditions that keep it within Australian jurisdiction: inference processed onshore, the operating logic held under Australian law separately from the imported component and control of the model weights themselves wherever the supplier’s structure allows it. Proprietary frontier suppliers rarely allow it, which is why Recommendation 6 defaults domain-specific capability to small models that are open-weight or Australian-made instead. Capability governed on these terms is a national asset. The same capability taken as a service, with the operating logic inside a foreign-controlled platform, is a dependency that surfaces only when it is withdrawn. Recommendations 1, 5 and 6 give effect to that distinction.

4.1.2 Reshoring and robotics

The opportunity is not confined to sectors where Australia already leads. Several industries left this country because labour cost and production scale determined competitiveness and Australia could offer neither. Automation changes those terms. On an AI-directed and robotically operated line the decisive inputs are energy, land, capital, proximity to the customer and the engineering skill to run the system, which Australia holds or can hold. Paragraph (c) puts robotics alongside artificial intelligence and names new industries and exports, so the question is squarely before the committee.

Australia has a stronger base for this than is generally assumed. Australian mining is among the most automated heavy industry in the world and the knowledge behind autonomous haulage, automated rail and remote operations centres was developed here for conditions found here. Robotics integration, systems engineering, remote operations and the maintenance of autonomous fleets are the disciplines that food processing, pharmaceutical production, critical minerals processing and defence manufacturing all require. Capability proven in Australian conditions is also exportable to countries facing the same problems, which is how a domestic application layer becomes a trade position rather than an exercise in import substitution.

What is largely absent is the manufacture of the robotics themselves, so automating an Australian production line generally means importing a foreign one, with the control software, the service relationship and the accumulated operating data held offshore. Treating robotics and industrial automation as a sovereign manufacturing opportunity rather than an input to be purchased would place the intellectual property, the profits and the engineering workforce onshore and would draw on the skills the Commonwealth is already funding through defence industrial investment. A robotic production line operated through a foreign-controlled platform is a dependency installed inside Australian industry rather than beside it and reshoring on those terms returns the jobs while leaving the control where it was. Recommendation 2 applies the same test to automation that Recommendation 1 applies to artificial intelligence.

> Recommendation 2: Apply the AI sovereignty classification to robotics and industrial automation. Assess robotics and automated production lines using the same jurisdictional criteria applied to AI, establishing the controlling entity's domicile at the point of purchase. Update industry and defence policies to recognise domestic robotics integration and manufacturing as sovereign industrial capability.

4.1.3 Resilience as the test

Resilience is the capacity to keep operating when something upstream fails and it yields a test an agency can apply. If this supplier, this model or this jurisdiction became unavailable tomorrow, what would stop working, for how long and what would restore it? Few Commonwealth agencies could answer today and the answer measures exposure better than any statement of intent.

Applied to a case the test resolves quickly. Take an agency using a frontier model through an interface to triage incoming correspondence. What stops working is triage, immediately and completely.

The inference is not the only thing that stops. The operating logic stops with it, the understanding of how that task is performed, because it sat inside the platform rather than with the agency. Held centrally that logic survives and another model can be re-tasked to it.

How long it stops is unknown to the agency, because the duration is set by a foreign government and a foreign company. What restores it is a decision the agency has no part in, or a fallback to manual processing at a volume the agency stopped staffing for. That is an argument for knowing the answer before deploying the model, not against using it.

On that test the economic argument and the sovereignty argument converge. Capability held under Australian jurisdiction survives a foreign policy change, an export control decision or a commercial withdrawal. Capability rented from a foreign platform is productive until it stops.

Containerised open-weight models are the resilient case. A model held in the agency's own container cannot be switched off from outside the country, so capability of that kind rather than capability rented from a platform is what should carry the industrial and economic output the country depends on.

4.1.4 Distribution and adoption

Paragraphs (b) and (d) ask about spreading benefits across the suburbs and regions and about adoption by smaller businesses. The evidence on the second is clear about what holds adoption back. Across the December 2025 to February 2026 quarter, 43 per cent of Australian small and medium enterprises reported some level of AI adoption. That figure counts any reported use rather than structured adoption, so it measures how many businesses have touched the technology rather than how many have built it into how they work, a distinction the measurement gap below makes plain.

Of those not adopting, around 65 per cent cited distrust of AI decision-making or a preference to keep humans in control of their processes and the National AI Centre reports that finding as consistent across business sizes and geographies.[5] Cost and access did not lead. Trust did.

The measurement gap is itself informative. The Australian Bureau of Statistics puts AI use among small and micro businesses far lower than the Centre's figure, because the two are measuring different things.[6] A great many businesses are using AI tools without having decided to adopt AI, which is the same pattern visible at national scale in section 2.2. Use is running ahead of confidence at every level of the economy.

A small business owner deciding whether to let a system draft advice to a customer or price a job is asking who is accountable when it goes wrong and whether the tool will still be there in six months. Those are questions about jurisdiction and recourse rather than capability. A domestic application layer operating under Australian law can answer both, because the supplier is reachable, the obligations are Australian and the recourse is real. An offshore service cannot, whatever its technical merits.

On distribution, applied AI in agriculture, resources and manufacturing is regional because the domain expertise sits where the industry sits. The manufacture and integration of robotics would locate on the same logic, near the mines, farms and processing plants that run them. Compute and inference capacity can also sit outside the major cities, where energy, transmission and network connectivity bind before talent does. Those constraints sit outside this committee's terms of reference and will determine whether the regional opportunity in paragraph (b) is realised.

[5] National AI Centre, AI adoption insights, December 2025 to February 2026, ai.gov.au.

[6] Australian Bureau of Statistics, Business Characteristics Survey 2024-25, released June 2026

4.1.5 Reversing a dependency

Any sovereignty position attracts the same objection, which is that the dependency is already built and cannot be undone. Australian vehicle manufacturing is the example usually reached for and it misleads. Rebuilding car production means rebuilding plants, tooling and supplier networks. The inputs to AI capability are data, model weights and people.

European governments have already reversed comparable dependencies within short timeframes and at bounded cost. Schleswig-Holstein moved its entire state administration off Microsoft Exchange and Outlook within six months,[7] and Germany's OpenDesk, a state-backed alternative to Microsoft 365, is now available across government.[8] Both are national capability decisions rather than procurement decisions, taken because the alternative was permanent dependency on a foreign jurisdiction.

Reversal costs money and takes years and success depends on executive commitment sustained across electoral cycles rather than on the technology itself, as Munich's abandoned LiMux migration shows. The cost rises the longer a dependency runs, because the agency's operating logic accumulates inside the platform while its own understanding of that logic erodes. Retention costs less than recovery. Recommendation 9 follows, because an agency that cannot describe its exit path has not established whether recovery is available to it.

> Recommendation 9: Require a credible exit path for major AI and platform investments prior to approval, tested against a defined dependency scenario. Mandate that agencies state what would stop working if the supplier, the model or its jurisdiction became unavailable, for how long and what would restore it, alongside where operating logic will be held, what would be required to substitute the capability and what specific assets the agency would retain if the supplier relationship ended.

4.2 Building and retaining sovereign capability

The binding constraint was not investment or talent. Until 31 August 2026 the Commonwealth had no accepted method for identifying a sovereign supplier and so no mechanism to prefer one. The Digital Transformation Agency has since adopted sovereignty as one of six principles governing Coordinated Contracting Arrangements, testing whether a seller or its parent may be subject to foreign compulsion, requiring transparency over jurisdictional and operational control and asking for measurable sovereignty and resilience outcomes.[9]

That is close to the test this submission proposes and Kitbag's own submission to the consultation that produced it is listed at Appendix C. What it does not yet do is apply beyond Coordinated Contracting Arrangements, which are one procurement vehicle among many. Recommendation 1 asks the committee to see that the same discipline reach every AI and cloud procurement, not only the panels the principle currently covers.

Suppliers describe themselves as sovereign based on Australian hosting, Australian staffing, local incorporation or certification against a security standard. Each claim is true as far as it goes and none answers who can lawfully compel the supplier.

[7] Schleswig-Holstein state government open-weight model and digital sovereignty programme.
[8] OpenDesk, assembled by ZenDiS, the German Centre for Digital Sovereignty
[9] Digital Transformation Agency, Coordinated Contracting Arrangement principles, announced 31 August 2026

Without an agreed test an evaluation team has no defensible basis for choosing between competing claims, so the safest course is to disregard them and decide on price and functionality. Australian sovereign capability is not being outcompeted so much as rendered invisible at the point of evaluation.

One option is to give the tiered classification a hard ownership floor in the Commonwealth Procurement Rules, so that a supplier cannot be treated as Australian sovereign at Tier 1 unless it is at least 51 per cent Australian-owned.

4.2.1 A tiered sovereignty classification

We proposed a four-tier classification to the Digital Transformation Agency's consultation on coordinated contracting arrangements, listed at Appendix C. It positions a supplier on two axes, being sovereign control in its legal, operational and jurisdictional dimensions and Australian economic contribution measured through employment, research, small business participation and profits retained onshore.[10]

- Tier 1, fully Australian sovereign. Australian-owned, holding intellectual property, profits and operating logic onshore under Australian law, with local workforce and engineering across the full stack, no foreign jurisdictional exposure and an auditable build chain.
- Tier 2, Australian-owned with foreign collaboration. Australian-owned and governed, with accountability anchored in Australian law, where a multinational collaboration introduces some dependency. An infrastructure partnership carries materially less risk than deep model or intellectual property integration.
- Tier 3, foreign entity with an Australian subsidiary. A foreign parent whose intellectual property and operating logic remain subject to foreign jurisdiction, delivering onshore benefit through local operations, employment and tax. Eligibility should turn on confirmation that inference is processed onshore, on supply chain disclosure and on a Deed of Sovereignty.
- Tier 4, fully foreign with no Australian benefit. No substantive local entity, workforce or economic contribution, with data, logic, intellectual property and profits held offshore. The operational kill switch sits outside Australian jurisdiction. Eligibility should require exceptional justification and mandatory safeguards.

Figure 1 shows how the axes combine. A supplier moves up the vertical axis as more of its legal, operational and jurisdictional control sits in Australia and across the horizontal axis as more of its economic activity does, which is why suppliers reach the same tier by different routes. The preferred zone in the upper right marks the position the Commonwealth should be creating suppliers for. It is thin because nothing in the current framework rewards occupying it.

[10] World Economic Forum, 'Digital Sovereignty' (2025/2026), weforum.org.

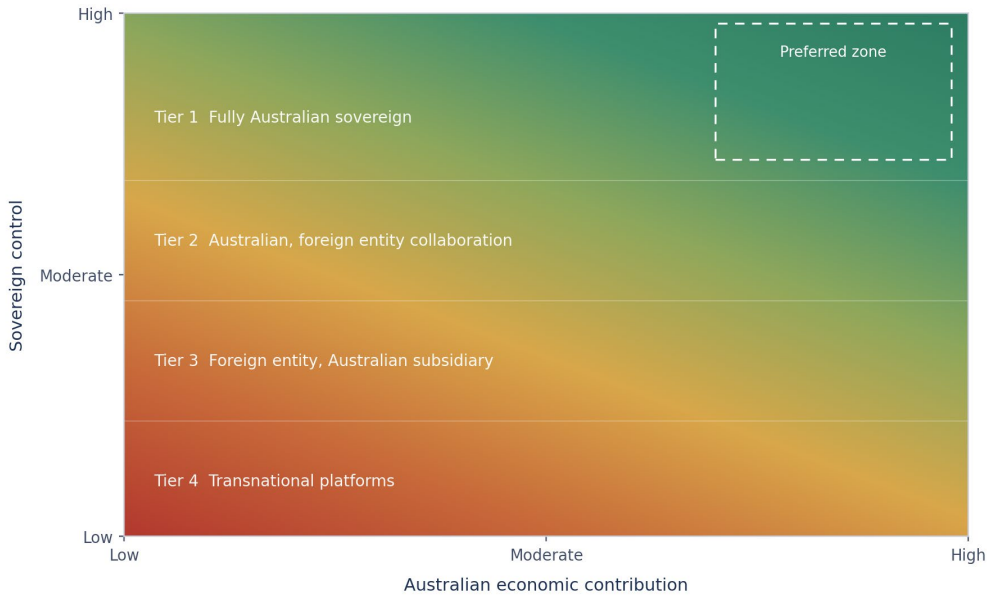


Figure 1: Sovereignty assessment matrix, sovereign control against Australian economic contribution

A scoring table supports the classification, allocating sixty per cent to sovereign control and forty per cent to Australian economic contribution. Absence of foreign jurisdictional exposure carries the heaviest weight at twenty per cent, followed by onshore operating logic at eighteen. Contract value adjusts the threshold, so a supplier acceptable at Tier 2 for a thirty million dollar contract may need Tier 1 safeguards at two hundred million. Applied at the point of purchase, this converts an unverifiable marketing claim into a graded attribute. The full table is at Appendix B.

Recommendation 1: Implement a tiered sovereignty classification for AI and cloud procurements. Assess sovereignty based on the legal domicile of the supplier, its operating entity and its ultimate parent company and the foreign jurisdictions to which each may be subject, rather than the location in which data or infrastructure is held. Apply this tiered classification at the point of purchase to establish sovereign characteristics before contractual commitment.

4.2.2 A Deed of Sovereignty

Accepting Australian terms and conditions does not extinguish a supplier's obligations to its home jurisdiction. Where terms and conditions govern the commercial relationship, the deed governs the sovereign one, setting out which obligations sit with the Australian entity, which sit with a foreign parent and how conflicts resolve.

For Tier 2 arrangements the deed preserves accountability at the Australian layer while acknowledging the partnership. For Tier 3 it becomes a condition of eligibility, binding the supplier to identify, disclose and allocate its jurisdictional exposure. Structural risk does not disappear. The deed makes it visible, named and auditable, within existing Australian contract law and without new legislation.

Recommendation 4: Incorporate a Deed of Sovereignty into Commonwealth AI contracts. Require suppliers to identify and warrant every foreign jurisdiction under which they, or their parent entities, may be compelled to produce data, modify a service, or suspend access and to notify the Commonwealth immediately if that compulsion occurs. Mandate that suppliers notify the Commonwealth of any change to this jurisdictional exposure and provide meaningful business continuity and redress where delivery is disrupted by foreign action, on the Commonwealth's own determination of what is essential to service delivery rather than the suppliers.

4.2.3 The supply problem

An objection follows immediately. If few Australian suppliers sit at Tier 1 across the full stack, an agency applying the classification finds nothing to buy and reverts to price and functionality. The objection describes the present market accurately. Australian suppliers holding intellectual property, engineering and profits onshore across an entire AI stack are uncommon and in some categories they do not exist. The classification is not proposed on the assumption that supply is already there. It is proposed because supply follows demand and demand is presently expressed in a way that gives no supplier a reason to build here.

A firm choosing where to domicile its intellectual property, where to place its engineers and whether to hold its own model weights currently gains nothing in a Commonwealth evaluation by choosing Australia. Signalling that those choices will be scored consistently changes the calculation for the next firm making it. The classification makes the attribute visible and the weighting makes it worth having. Neither creates a supplier overnight and both change what a supplier is building toward.

In the interim the framework still does useful work. It grades Tier 3 arrangements against each other, which is where most Commonwealth AI procurement will sit for some years and it distinguishes a foreign supplier processing inference onshore under a Deed of Sovereignty from one that does neither.

4.2.4 Weighting and international practice

Neither instrument changes the outcome of an evaluation in which sovereignty carries no weight. New Zealand took the direct route, requiring agencies to apply a minimum weighting for economic benefit above defined thresholds.[11] An Australian supplier currently competes on price and functionality against suppliers whose sovereignty disadvantage is never scored.

Others have reached similar conclusions. Switzerland rejected Palantir for sensitive military applications because exposure to United States jurisdiction created an unmitigable sovereignty risk and has moved to reduce its reliance on Microsoft across government. Germany and France go further still, mandating domestic jurisdiction over government technology and a certified sovereign cloud standard respectively.[12] Australia risks becoming an outlier through misidentifying where sovereignty resides.

[11] New Zealand Government Procurement Rules, 5th edition, Rule 8 (Economic benefit to New Zealand). See procurement.govt.nz.
[12] Swiss Armed Forces internal risk assessment (December 2024), reported by Republik and netzpolitik.org (December 2025)

Recommendation 3: Embed a mandatory sovereignty weighting in value-for-money assessments. Update evaluation guidance under the CPRs to include a sovereignty weighting, aligning with the New Zealand precedent that establishes a mandatory minimum weighting for economic benefit.

4.2.5 Trade obligations

A weighting of this kind must sit within Australia's procurement commitments. The WTO Agreement on Government Procurement, the Australia United States Free Trade Agreement and comparable instruments each require national treatment for covered suppliers above threshold. New Zealand's Rule 8 is subject to the same constraint through the Australia New Zealand Government Procurement Agreement and a symmetrical Australian rule would carry the same qualification in reverse.[13]

What we propose is not a nationality preference. A jurisdictional exposure test asks which legal instruments can compel a supplier and the answer turns on the supplier's corporate structure and legal position, not on the passport of its owners. A United States company that holds its model weights in Australia, processes inference onshore and accepts a Deed of Sovereignty scores better under this framework than an Australian-incorporated reseller whose capability is a foreign platform in a local wrapper. That result is the intended one and it is not available to a rule that discriminates by nationality.

Where a criterion does bite in a way that affects covered suppliers, the frameworks already provide for it. The Commonwealth Procurement Rules permit departure from the competitive rules for measures necessary to protect essential security interests. Both parties to AUSFTA exempted procurement critical to national security. Australia negotiated exceptions on accession to the Government Procurement Agreement to preserve flexibility in the national interest. Continuity of a capability the Commonwealth cannot operate without and the ability of a foreign government to withdraw it, are security questions on any ordinary reading.

The narrower and better practice writes the criterion as a capability requirement. An agency that requires model weights to be held onshore, inference to be processed in Australia and jurisdictional exposure to be disclosed has specified what it is buying. Any supplier able to meet those terms may bid, whatever its domicile. Suppliers that cannot meet them have disclosed something the Commonwealth needs to know.

Recommendation 5: Update the Commonwealth Procurement Rules (CPRs) for imported AI capability. Where AI capability cannot practicably be built domestically, condition its acquisition on the strongest combination of safeguards a supplier can offer onshore inference processing, operating logic retained under Australian law and, where the supplier's structure allows it, Commonwealth control of the model weights. Proprietary frontier suppliers will rarely offer control of their weights; where that is the case, Recommendation 6 sets out the alternative. Require major AI investment proposals assessed through the Digital and ICT Investment Oversight Framework to explicitly identify where sovereign control sits.

[13] Commonwealth Procurement Rules, paragraph 2.6, permitting departure from the rules for measures necessary to protect essential security interests and Appendix A exemptions.

4.3 Data sovereignty and domain-specific models

Paragraph (f) pairs data sovereignty with the opportunity in narrow domain-specific models trained on Australian data. The pairing is correct. It should not be assumed that the second delivers the first.

4.3.1 The opportunity

Australia holds data no other country can assemble, being longitudinal population health data through Medicare and the Pharmaceutical Benefits Scheme, defence personnel and sustainment records, agricultural and climate observation spanning more than a century, court and legislative records and the administrative records of a federated system of government. A model trained on them can outperform a general purpose model in the domains where Australia leads and the data binds before the compute does. Capability of this kind is buildable within this parliament, at a fraction of the cost of competing at the frontier.

4.3.2 The opportunity can be built and then lost

A model is not sovereign because its training data was Australian. Sovereignty requires that the entity building, hosting and operating it cannot be compelled by a foreign government and that the Commonwealth holds the model weights. On current settings a sovereign model built on Australian public data can be operated by an entity subject to the instruments in section 3 and the value created from national data assets accrues to a foreign-controlled platform.

On 12 June 2026 the United States Department of Commerce directed the suspension of access to two frontier AI models by any foreign national, three days after their release. The developer disabled the models worldwide to avoid breaching the order. Access resumed on 1 July after the controls were lifted, an outage of nineteen days.[14] Every Australian user was a foreign national for the purposes of that order. No Australian contract, no local incorporation and no local relationship changed the outcome. The sanctioning of International Criminal Court personnel in February 2025 followed the same pattern, with the chief prosecutor losing access to Microsoft cloud services.[15] No contract was breached in either case and no data left its jurisdiction of storage. The capability stopped being available.

The obvious reply is that the episode was brief and no Australian institution suffered lasting harm. Nineteen days measured the duration of one decision rather than the reach of the power. The length was set in Washington on grounds Australia could not have influenced and nothing in the mechanism limits the next suspension to nineteen days. An agency running a citizen-facing service cannot plan around an outage of unknown length. The question for the committee is what the same directive would cost over a quarter, or against a capability embedded in payments, health or border processing.

4.3.3 The second sovereign data asset

Data sovereignty is usually understood to concern corpora, being the records an agency holds and the models trained on them. A second asset matters as much, being the operating logic of the agency itself.

[14] Anthropic, 'Statement on the US government directive to suspend access to Fable 5 and Mythos 5' (12 June 2026), anthropic.com/news/fable-mythos-access; CNBC (30 June 2026).

[15] US Executive Order 14203 (6 February 2025), sanctions on International Criminal Court personnel.

That logic is how an agency decides, expressed as sequencing, approval authorities, delegations, policy associations and the conditions under which one path is taken rather than another.

It is at risk because nothing classifies it as data. An agency knows where its records are held. It rarely knows where its operating logic is held, because that logic exists as configuration inside whichever platform was most recently deployed, never as a dataset. Where the platform is foreign controlled, the encoded logic of how a Commonwealth agency exercises authority sits under a foreign jurisdiction and no data sovereignty assessment detects it, because the assessment looks for records.

The pattern is familiar to anyone who has rebuilt one. When an agency deploys a case management, payments or personnel platform, its assessment criteria, delegation thresholds, escalation paths and exception handling are configured into the vendor's system during implementation. Some of it derives from legislation and policy. Much of it is practice that was never written down anywhere else. Five years on, the authoritative statement of how that agency decides exists only inside the configuration and the people who could reconstruct it have moved on. Our own work reconciling the personnel systems of the three services was exactly this exercise.

AI accelerates this. A model configured to draft, triage, recommend or decide must be given the agency's logic to function and the transfer happens as a condition of the capability working at all. It is a sovereignty event, invisible in every framework that governs it.

That asset also determines whether artificial intelligence can be scaled at all. An agency holding its System of Work[16] explicitly can point successive capabilities at the same rules, delegations and boundaries, so each deployment inherits the accountability established by the last. An agency that does not must reconstruct that logic every time and leave it inside the platform that executes it, so the estate grows while the capability does not compound and the exit path narrows with each addition. Recommendation 7 gives the layer a procurement category within the Australian Government Architecture so that it can be bought, held and governed as an asset, in the place the Commonwealth's own architecture already reserves for it.

Figure 2 sets out the layers of an AI capability and the jurisdiction that controls each. The marked layer is the one an agency either holds or gives away.

[16] Australia First True System of Work- DOLIUM.AI

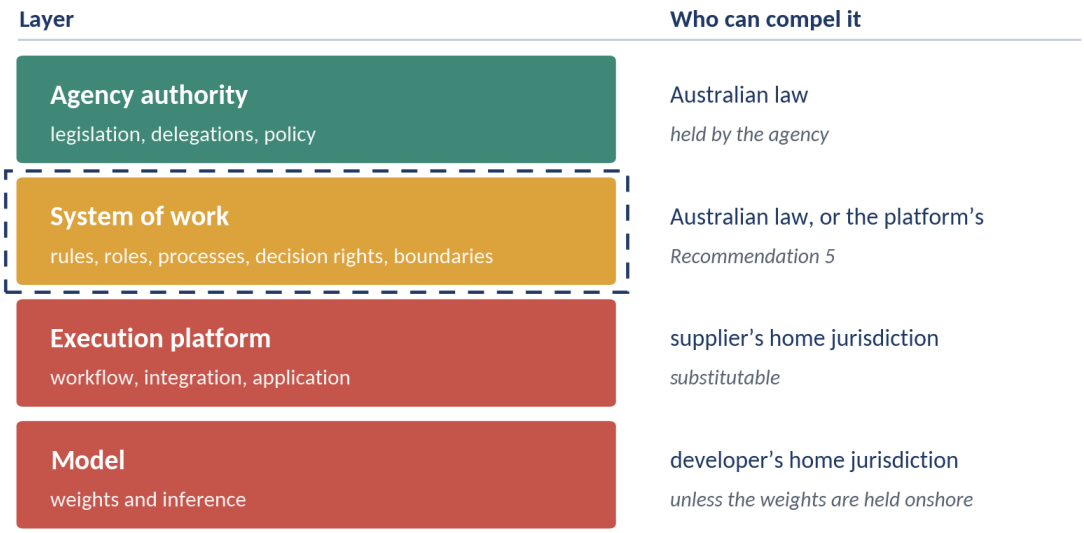


Figure 2: Where sovereignty is decided in an AI capability, by layer and by the jurisdiction that controls it

Recommendation 7: Hold an agency's operating logic within the Australian Government Architecture, as a distinct procurement category within existing marketplace arrangements. Recognise an agency's operating logic as a sovereign asset held separately from the systems and staff that execute it, embedded in the Architecture over the long term rather than inside whichever platform currently executes it. Require the layer holding an agency's rules, roles, processes and boundaries to be held under Australian law and structurally separated from the underlying AI models.

4.3.4 Control of weights and the open-weight model pathway

The practical question is whether the Commonwealth holds the weights or holds access to them, which is the difference between owning a capability and renting one. In June 2026 organisations depending on interface access lost the capability by a decision taken in another country. Organisations running open-weight models on their own infrastructure did not, because there was nothing for a foreign directive to withdraw.

Open-weight models fine-tuned on Australian domain data are therefore the most direct route to Tier 1 capability available today. They can be hosted onshore, inspected, retained indefinitely and operated regardless of any decision by an original developer. For most applications contemplated in paragraph (f), the capability gap against frontier models is narrow and closing while the sovereignty gap between holding weights and holding access is absolute. Frontier scale is not the requirement domain-specific capability is often assumed to need; a small model, whether an open-weight model fine-tuned onshore or one built in Australia from the outset, can match a narrow task without inheriting either the cost or the exposure of a frontier system. Recommendation 6 makes that combination, open-weight or Australian-made, the default in that case.

Open-weights model are not categorically preferable. Frontier capability is real and some applications need it. One inversion should concern the committee.

Open-weights model reduce compellability risk while raising provenance risk, because several of the most widely used open-weight families come from developers domiciled in the People's Republic of China and training corpora are generally not published and cannot be independently verified. Sovereignty on this pathway depends on provenance assessment and supply chain integrity, which connects to section 4.6.

Recommendation 6: Default to small, open-weight or Australian-made models for domain-specific capability. Frontier-scale capability is not required for most domain-specific tasks. For AI capabilities built on Australian data, agencies should default to small language models that are either open-weight and held and operated onshore, or developed in Australia, rather than defaulting to a frontier model accessed as a service. Subject these deployments to strict provenance assessments and supply chain disclosures regarding the model developer.

4.4 Workforce and skills

The Commonwealth already knows what happens when capability is bought rather than held. Expenditure on IT temporary personnel rose from roughly $289 million in 2022-23 to more than $808 million in 2025-26, with contract numbers rising from 436 to 1,104, while internal ICT and digital headcount grew by about 45 per cent over a comparable period and most agencies continued to report critical ICT skills shortages.[17] Buying more capability and building more of it have not closed the gap, because where the work sits determines where the skill accumulates.

Where the Commonwealth buys from an Australian-owned supplier, the specialist skills developed on that engagement stay in the Australian economy. The engineers and practitioners who learn how AI behaves in the Australian legislative and governance context remain available to the next agency. Where the Commonwealth buys the same capability from a foreign-parented supplier, delivery may be excellent while the skills accrue to a global talent pool.

This is a retention question before it is a training question. Skills follow the work, so the composition of the Commonwealth's supplier base shapes the domestic AI workforce a decade from now more directly than any training program. Where an agency procures from a supplier that cannot deliver retention by structure, vendor-neutral skills transfer is a reasonable condition and the ratio of vendor-specific to vendor-neutral training shows whether an arrangement builds capability or consolidates dependency. That is the substance of Recommendation 10. The skills that matter most are those required to build and govern the agency's own operating logic and decision authorities, which survive a change of model, a repricing or an export control decision. Product certifications do not.

Recommendation 10: Condition relevant AI procurements on vendor-neutral skills transfer. Where an agency procures AI capability from a supplier that is structurally unable to retain specialist skills within the Australian economy, require vendor-neutral training conditions covering maintenance, personnel, functionality and the resourcing needed to bring the capability in-house or re-source it to another supplier. The vendor should be obliged to train Commonwealth staff directly, not merely document the capability.

[17] Australian Public Service Commission, State of the Service reports, which have identified critical ICT skills shortages across most federal agencies since 2023. Analysis of AusTender data by The Canberra Times, July 2026.

4.5 Adoption, transparency and accountability

The deficiency lies not in how agencies use AI once acquired but in the fact that the Commonwealth cannot say what it has bought or from whom, in the sense that matters for sovereignty.

4.5.1 The existing regime asks a different question

A mandatory disclosure regime already exists. Under version 2.0 of the Policy for the responsible use of AI in government, agencies must designate accountable officials, publish and annually review a transparency statement, maintain a register of in-scope use cases with an accountable owner for each and complete an impact assessment before deployment.[18] None of this should be duplicated.

These instruments describe what an agency does with AI, being which use cases exist, who owns them and how risks are managed. They do not describe what the agency depends on. An agency can hold an accountable official, a current transparency statement, a complete use case register and a finalised impact assessment for every deployment and still be unable to say whether the model underneath can be withdrawn or compelled by a foreign government. Nothing in the mandatory requirements asks, so nothing in the published statements answers.

That is not a theoretical objection and we tested it. Between 1 and 2 September 2026 we attempted to read every AI transparency statement published by a Commonwealth entity, working from the central register the Digital Transformation Agency maintains. We retrieved and coded 73 of the 99 statements sought, against five questions fixed before reading. 28 identify a specific system or product, in almost every case Microsoft 365 Copilot. Two identify the legal entity operating a capability and in both cases that entity is itself a Commonwealth one. None states whether inference is processed in Australia. None states whether the Commonwealth holds the model weights or accesses the model as a service. None mentions foreign jurisdiction, extraterritorial law or compellability in any form.

No agency is at fault in that result. Every statement we read complies with the Standard, because the Standard does not ask any of those questions. The gap is in the requirement rather than in the compliance, which is why it cannot be closed by asking agencies to try harder and why Recommendation 11 is drafted as an additional field rather than a new obligation. Appendix D lists every statement, its address and the date we read it, so the committee can verify the finding or repeat the exercise.

The architecture exists, agencies are resourced to comply and the reporting cadence is established. One additional field, as set out in Recommendation 11, would convert an existing compliance exercise into a national picture of jurisdictional exposure at close to no cost.

Recommendation 11: Require expanded disclosure in AI transparency statements. For each material AI capability, the Standard for AI transparency statements should require disclosure of the legal domicile of the operating entity and its ultimate parent, whether inference is processed onshore and whether the Commonwealth holds or merely accesses the model weights.

[18] Digital Transformation Agency, Policy for the responsible use of AI in government, version 2.0, effective 15 December 2025,

4.5.2 Why procurement data cannot answer it either

AusTender records the contracting entity, the value, the method and the category. It does not record the legal domicile of that entity, the domicile of its parent or whether the capability is delivered from a platform controlled outside Australia. Those fields do not exist, so no analysis of published contract notices can produce a picture of jurisdictional exposure. The determining variable was never captured.

Commonwealth AI capability also arrives through standalone contracts, extensions to existing software licences, cloud consumption arrangements and features delivered inside platforms an agency already holds. Only the first is identifiable as an AI procurement. The rest enter the estate reported against the category of the original arrangement and invisible as AI. Exposure accumulates through extension, not competition. Each decision is defensible. Nobody assesses the cumulative position.

There is also a limit on what the Commonwealth can compel after the fact. When the Senate sought material from PwC, the global entity declined on the basis that it belonged to the international firm rather than the Australian one.[19] A domestically owned supplier carries no equivalent conflict.

The deeper consequence is dependency. As an agency configures its decision rules and workflows into a platform it does not control, its own understanding of that logic erodes and substitution becomes hard regardless of whether a comparable product exists. GovERP was wound back after roughly three hundred and ninety million dollars and decommissioned in January 2025. The Queensland Health payroll replacement required over two thousand five hundred customisations to encode the department's pay rules, at a rectification and operating cost the Commission of Inquiry put near one point two billion dollars.[20] AI reproduces this pattern faster, with a foreign jurisdictional dimension the earlier programs did not carry.

The committee is better placed than any submitter to establish the current position. Finance holds contract-level data beyond what is published and agencies hold their own licence records. Recommendation 12 asks the committee to put that question to each portfolio and to publish which agencies were able to answer. The gaps will be informative. Appendix D shows how little the published record can answer on its own.

> Recommendation 12: Audit current sovereign AI exposure across portfolios using the tiered sovereignty classification in Recommendation 1. The committee should write to each portfolio to classify its current AI capability against that scale, including where a change in a supplier's ownership, control or jurisdiction has altered its tier since contract and publish which agencies were able to answer.

[19] Australian Senate Finance and Public Administration References Committee, PwC Australia inquiry (2023 to 2024). PwC

[20] Digital Transformation Agency, GovERP Reuse Assessment (August 2024). See also Queensland Health Payroll System Commission of Inquiry, Final Report, The Honourable Richard N Chesterman AO RFD QC (31 July 2013).

4.6 Supply chains and critical infrastructure

Australian AI capability depends on a small number of foreign-controlled model providers, a small number of hyperscale cloud platforms and a concentrated data centre market. One foreign legal or commercial decision can therefore affect many Australian entities at once, including entities with no contractual relationship to each other and no visibility of their shared dependency. Assessments conducted entity by entity will not detect a correlated exposure of that kind.

The Security of Critical Infrastructure Act framework addresses supply chain risk through obligations on responsible entities to identify and mitigate hazards. Where the hazard is the legal domicile of an upstream provider, the responsible entity cannot mitigate it. It can only choose a different provider and that choice is made at procurement. The obligation and the point of control sit with different parties at different times, which is what Recommendation 13 addresses. We set this out at greater length in our submission to the Department of Home Affairs on the Tranche 2 reforms, listed at Appendix C.

Foreign interference risk here is not confined to covert activity. The exercise of foreign law over a supplier is overt, lawful in the jurisdiction concerned and generally not disclosable to the Australian customer, which places it outside the frame of most foreign interference assessments. We invite the committee to treat it as a distinct category of risk.

> Recommendation 13: Amend the Security of Critical Infrastructure (SOCI) Act framework. Formally recognise the legal domicile of an upstream provider as a hazard that a responsible entity cannot mitigate post-contract. Place the regulatory obligation to assess this hazard at the point of procurement.

4.7 Governance before the point of action

Two developments in August 2026 show how seriously the demand for governance is taken. South Australia announced the first Australian royal commission into artificial intelligence, commencing 1 October 2026 and reporting by 1 July 2027.[21] In the same week the Australian AI Safety Institute released its first publication, on risks and controls for multi-agent systems.[22] Its central finding is that control erodes as agents interact across organisational boundaries. A collection of safe agents does not make a safe collection of agents and once agents interact across boundaries no single organisation can see or control the whole. Both point to the same requirement, which is whether the use of AI can be bounded and made visible.

The market has met the demand for capability and left the demand for control behind. What governs AI products mostly operates after the event, monitoring outputs, filtering content or logging activity once the capability has acted. Many organisations deploying AI today cannot state what rules their AI operates under, what it is permitted to do or how to demonstrate afterwards what it did and why.

[21] Government of South Australia, Royal Commission into Artificial Intelligence, announced August 2026.

[22] Gradient Institute, Risks and controls for multi-agent systems, commissioned by the Australian AI Safety Institute and published by the Department of Industry, Science and Resources, August 2026.

Monitoring, filtering and logging serve a purpose without governing anything. Governance means defining the rules a capability must follow and enforcing them at the point of action. For any AI supporting a decision that affects a person, an agency should be able to state what its AI is permitted to do and demonstrate that it did only that.

That rigour need not be uniform. The Policy already requires an impact assessment before deployment and that assessment already produces a risk rating.[23] Recommendation 8 asks that this existing rating set how tightly a capability is bound, rather than creating a second, parallel assessment: a low-risk administrative task can operate under lighter rules than a decision that affects a person's entitlements or liberty. The instrument already exists. What is missing is the link between the rating it produces and the rules an agency then enforces.

Recommendation 8 should be read with three qualifications. It does not require constraining a model's internal behaviour, which is beyond present capability. It constrains what a system is permitted to do with a model's output, being which actions, it may take, against which records, under whose authority and within what limits. Those constraints sit outside the model, so they work with a general purpose model an agency did not build and cannot inspect.

The second qualification is scope. Rules of this kind bind well where authority and process are already defined in legislation, delegations or policy, which describes most Commonwealth decision-making. They bind poorly where a judgement is genuinely open and an agency should not pretend otherwise by encoding a rule that does not exist.

The recommendation therefore addresses decisions affecting a person, not an AI use case.

The third is cost. The work is in articulating the rules rather than in the technology and agencies that have mapped their delegations and processes will find much of it already done. An agency unable to state what its AI may do generally cannot state what its staff may do either.

The second limb of Recommendation 8 extends the principle across agency boundaries, where the Safety Institute report locates the sharpest loss of control. The report frames tiers of agent governance by the minimum level of governance in place between interacting agents, which is exactly the variable an agency loses once its agents transact with agents it does not govern. A shared and inspectable layer lets each agency keep authority over its own rules while their agents interact within limits all of them can see. That arrangement cannot be assembled retrospectively from separate monitoring regimes.

Recommendation 7 connects this to section 4.2.3. Rules held inside the same foreign-controlled platform that executes them leave the agency without governance in any meaningful sense. Holding that layer under Australian law, within the Australian Government Architecture and separately from the underlying models, lets an agency change model, change vendor or lose access to without losing the constraints on its AI. Kitbag works in this area. The recommendation stands independently of any supplier.

[23] Digital Transformation Agency, Artificial intelligence impact assessment tool and accompanying guidance, digital.gov.au.

Recommendation 8: Require rules-based governance for AI supporting decisions affecting a person, scaled to the risk rating in the agency's existing impact assessment. For any AI capability supporting such a decision, define what the AI is permitted to do, make those rules machine-readable and enforce them before the point of action, with the rigour of enforcement set by that existing risk rating rather than a new assessment. Where AI operates across agency boundaries, require each agency to retain authority over its own rules while a shared and inspectable layer allows agents to interact within limits every participating agency can see.

5. Applying the framework in practice

Two qualifications apply to any agency putting this framework into practice.
Sovereignty carries a cost. A Tier 1 supplier may charge more, offer narrower functionality or bring delivery risk a hyperscale platform does not. The framework makes that trade-off visible and leaves the choice with the agency. An agency that knowingly accepts jurisdictional exposure to obtain a capability it cannot otherwise get has made a defensible decision. An agency that acquires the same exposure unknowingly has made no decision at all. Domicile answers a specific question, being who can compel a supplier. It is not a proxy for security, quality or capability and the classification filters alongside existing security and capability assessment rather than replacing either. A Tier 1 result confirms freedom from foreign legal compulsion; it does not excuse a supplier, sovereign or otherwise, from the assessment every supplier must still pass.

6. Summary of Recommendations

The opportunity sits where artificial intelligence is applied, in the sectors where Australia already leads and in the sectors this country was priced out of and can now credibly re-enter. Sovereignty over that capability turns on the legal domicile of whoever operates it. Both the market and the Commonwealth's own frameworks leave that question unasked.

Rules of that kind are set in procurement. The legal domicile of the entity that builds, hosts and operates a capability determines who can compel it and that domicile is fixed the moment an agency sign. The timing favours action. Technology is the largest procurement category across Australian government and contracts worth roughly $27 billion reach their end dates during 2026.[24] Sovereignty conditions applied at renewal cost nothing and that window is open now.

- **Recommendation 1:** Implement a tiered sovereignty classification for AI and cloud procurements. Assess sovereignty based on the legal domicile of the supplier, its operating entity and its ultimate parent company and the foreign jurisdictions to which each may be subject, rather than the location in which data or infrastructure is held. Apply this tiered classification at the point of purchase to establish sovereign characteristics before contractual commitment.
- **Recommendation 2:** Apply the AI sovereignty classification to robotics and industrial automation. Assess robotics and automated production lines using the same jurisdictional criteria applied to AI, establishing the controlling entity's domicile at the point of purchase. Update industry and defence policies to recognise domestic robotics integration and manufacturing as sovereign industrial capability.

[24] Awarded Tenders analysis of AusTender and state and territory procurement portals, February 2026.

- **Recommendation 3:** Embed a mandatory sovereignty weighting in value-for-money assessments. Update evaluation guidance under the CPRs to include a sovereignty weighting, aligning with the New Zealand precedent that establishes a mandatory minimum weighting for economic benefit.
- **Recommendation 4:** Incorporate a Deed of Sovereignty into Commonwealth AI contracts. Require suppliers to identify and warrant every foreign jurisdiction under which they, or their parent entities, may be compelled to produce data, modify a service, or suspend access and to notify the Commonwealth immediately if that compulsion occurs. Mandate that suppliers notify the Commonwealth of any change to this jurisdictional exposure and provide meaningful business continuity and redress where delivery is disrupted by foreign action, on the Commonwealth's own determination of what is essential to service delivery rather than the suppliers.
- **Recommendation 5**: Update the Commonwealth Procurement Rules (CPRs) for imported AI capability. Where AI capability cannot practicably be built domestically, condition its acquisition on the strongest combination of safeguards a supplier can offer onshore inference processing, operating logic retained under Australian law and, where the supplier's structure allows it, Commonwealth control of the model weights. Proprietary frontier suppliers will rarely offer control of their weights; where that is the case, Recommendation 6 sets out the alternative. Require major AI investment proposals assessed through the Digital and ICT Investment Oversight Framework to explicitly identify where sovereign control sits.
- **Recommendation 6:** Default to small, open-weight or Australian-made models for domain-specific capability. Frontier-scale capability is not required for most domain-specific tasks. For AI capabilities built on Australian data, agencies should default to small language models that are either open-weight and held and operated onshore, or developed in Australia, rather than defaulting to a frontier model accessed as a service. Subject these deployments to strict provenance assessments and supply chain disclosures regarding the model developer.
- **Recommendation 7:** Hold an agency's operating logic within the Australian Government Architecture, as a distinct procurement category within existing marketplace arrangements. Recognise an agency's operating logic as a sovereign asset held separately from the systems and staff that execute it, embedded in the Architecture over the long term rather than inside whichever platform currently executes it. Require the layer holding an agency's rules, roles, processes and boundaries to be held under Australian law and structurally separated from the underlying AI models.
- **Recommendation 8:** Require rules-based governance for AI supporting decisions affecting a person, scaled to the risk rating in the agency's existing impact assessment. For any AI capability supporting such a decision, define what the AI is permitted to do, make those rules machine-readable and enforce them before the point of action, with the rigour of enforcement set by that existing risk rating rather than a new assessment. Where AI operates across agency boundaries, require each agency to retain authority over its own rules while a shared and inspectable layer allows agents to interact within limits every participating agency can see.

- **Recommendation 9**: Require a credible exit path for major AI and platform investments prior to approval, tested against a defined dependency scenario. Mandate that agencies state what would stop working if the supplier, the model or its jurisdiction became unavailable, for how long and what would restore it, alongside where operating logic will be held, what would be required to substitute the capability and what specific assets the agency would retain if the supplier relationship ended.
- **Recommendation 10**: Condition relevant AI procurements on vendor-neutral skills transfer. Where an agency procures AI capability from a supplier that is structurally unable to retain specialist skills within the Australian economy, require vendor-neutral training conditions covering maintenance, personnel, functionality and the resourcing needed to bring the capability in-house or re-source it to another supplier. The vendor should be obliged to train Commonwealth staff directly, not merely document the capability.
- **Recommendation 11:** Require expanded disclosure in AI transparency statements. For each material AI capability, the Standard for AI transparency statements should require disclosure of the legal domicile of the operating entity and its ultimate parent, whether inference is processed onshore and whether the Commonwealth holds or merely accesses the model weights.
- **Recommendation 12:** Audit current sovereign AI exposure across portfolios using the tiered sovereignty classification in Recommendation 1. The committee should write to each portfolio to classify its current AI capability against that scale, including where a change in a supplier's ownership, control or jurisdiction has altered its tier since contract and publish which agencies were able to answer.
- **Recommendation 13:** Amend the Security of Critical Infrastructure (SOCI) Act framework. Formally recognise the legal domicile of an upstream provider as a hazard that a responsible entity cannot mitigate post-contract. Place the regulatory obligation to assess this hazard at the point of procurement.

Every recommendation can be delivered through instruments the Commonwealth already holds, being the Commonwealth Procurement Rules, standard contract templates, the Standard for AI transparency statements, existing marketplace arrangements and existing industry policy settings. None requires a new agency. None requires primary legislation, except Recommendation 7 if the obligation is to bind entities beyond the Commonwealth and Recommendation 13 if the Security of Critical Infrastructure Act is to be amended. Recommendation 12 is within the committee's own gift. Table 1 maps each recommendation to the instrument that would deliver it and to the terms of reference it answers.

Table 1: Enabling Instrument

Rec.	Delivered through	Terms of reference
1	Commonwealth Procurement Rules; evaluation guidance; marketplace arrangements	(e), (l)
2	Industry policy settings; Commonwealth Procurement Rules	(c)
3	Commonwealth Procurement Rules, value for money	(e)
4	Standard Commonwealth contract templates	(e), (l)
5	Commonwealth Procurement Rules; Digital and ICT Investment Oversight Framework	(e), (f)
6	Commonwealth Procurement Rules; agency capability requirements	(f)

Table 1: Enabling Instrument		
Rec.	**Delivered through**	**Terms of reference**
7	Marketplace arrangements and contract templates, with legislation if extended beyond the Commonwealth	(e), (f)
8	Policy for the responsible use of AI in government	(h), (n)
9	Digital and ICT Investment Oversight Framework	(e), (h)
10	Standard Commonwealth contract templates	(g)
11	Standard for AI transparency statements; AusTender	(h)
12	The committee	(h)
13	Security of Critical Infrastructure Act 2018, as amended	(l)

Table 1: Recommendations, delivery instrument and terms of reference

7. Conclusion

Sovereignty is a legal and structural condition, not a contractual one. A supplier's domicile determines the jurisdiction that follows it through the door. An agency's operating logic is a sovereign asset and must be governed as one. Procurement is the most direct instrument the Commonwealth holds to act on any of it.

The economic case and the sovereignty case are one case. The gains anticipated over the coming decade will be realised in application, in the industries where Australian operating knowledge is the scarce input and, in the industries, automation now allows this country to re-enter. Whether they are retained here depends on who holds the capability that produces them, because value follows the entity that owns the model, the operating logic and the relationship with the customer. Australia has reached a global position before by being early and disciplined in a narrow field. Every country now confronting the same dependency is a market for capability built on these terms.

Sovereignty can be lost through accumulated deference as readily as through any single decision. The procurement decisions being made now will define the exposure Australian institutions carry for the next decade and they are being made while this committee settles its work program.

Australians are adopting artificial intelligence faster than they trust it. That gap will not close by slowing adoption or by asking the public to feel differently. It closes when the capability being adopted operates under rules Australian institutions have set, in a jurisdiction the public can reach, on terms that can be inspected and enforced. Every recommendation here is directed at that outcome and at the economic position that follows from it. Kitbag Consulting would welcome the opportunity to appear before the committee.

Appendix A: Recommendations and the problem each address

Table 2 sets out each recommendation against the problem it addresses and what it changes in practice. Section 6 carries the recommendations in full and Table 1 maps each one to the instrument that would deliver it.

Table 2: Recommendations and the problem each address

Rec.	The problem	Recommendation	What it does
1	Sovereignty is not assessed before contract, so domicile is fixed the moment an agency sign.	Implement a tiered sovereignty classification for AI and cloud procurements.	Makes jurisdictional exposure a scored attribute before contractual commitment, so an agency knows which tier it is buying.
2	Automating a production line usually means importing a foreign one, so the control software, service relationship and operating data sit offshore.	Apply the AI sovereignty classification to robotics and industrial automation.	Extends the same test to physical automation, so a robotic line is assessed on who controls it rather than on price and function alone.
3	Sovereignty carries no weight in evaluation, so an Australian supplier competes on price against suppliers whose disadvantage is never scored.	Embed a mandatory sovereignty weighting in value-for-money assessments.	Gives sovereignty a score in evaluation, so an Australian supplier's advantage is counted rather than ignored.
4	A supplier cannot override the compulsion power of its home jurisdiction and the Commonwealth is not told when that power is used.	Incorporate a Deed of Sovereignty into Commonwealth AI contracts.	Puts the supplier's jurisdictional exposure on the contract record and obliges it to disclose when that exposure changes or is exercised.
5	Capability that cannot be built here is taken as a service, with nothing retained under Australian law.	Update the Commonwealth Procurement Rules for imported AI capability.	Sets the minimum terms on which imported capability may be bought, so the Commonwealth retains something where a supplier cannot offer everything.
6	Access to a frontier model can be withdrawn by a foreign directive, whereas there is nothing to withdraw from weights an agency holds.	Default to small, open-weight or Australian-made models for domain-specific capability.	Shifts the default for domain work from a rented model to a held one, so there is nothing for a foreign directive to withdraw.
7	An agency's operating logic exists as configuration inside whichever platform was last deployed, is classified as data nowhere and leaves with the platform.	Hold an agency's operating logic within the Australian Government Architecture, as a distinct procurement category.	Creates a place to buy and hold the operating logic as an asset, so it survives a change of model or vendor.
8	Most AI governance operates after the event, so agencies cannot state what their AI is permitted to do or demonstrate that it did only that.	Require rules-based governance for AI supporting decisions affecting a person, scaled to the risk rating in the agency's existing impact assessment.	Converts an existing risk rating into enforceable limits on what an AI may do, checked before the action rather than after it.
9	Reversal costs rise every year a dependency runs and few agencies can say what would stop working if a supplier or jurisdiction became unavailable.	Require a credible exit path for major AI and platform investments prior to approval, tested against a defined dependency scenario.	Forces the dependency question to be answered before money is approved rather than after a capability stops.
10	Buying capability rather than holding it leaves the skill with the supplier. IT contractor spends rose from $289 million to $808 million while shortages persisted.	Condition relevant AI procurements on vendor-neutral skills transfer.	Obliges the supplier to build Commonwealth capability as a condition of sale, so the skill accumulates onshore.
11	The Standard does not ask about jurisdiction, onshore inference or control of weights, so no published statement answers.	Require expanded disclosure in AI transparency statements.	Turns a compliance task agency already perform each year into a national picture of jurisdictional exposure.
12	AusTender does not record supplier domicile, so no submitter can establish the Commonwealth's current exposure.	Audit current sovereign AI exposure across portfolios using the tiered classification in Recommendation 1.	Establishes the Commonwealth's current position, which no submitter can establish from published data.

Table 2: Recommendations and the problem each address			
Rec.	**The problem**	**Recommendation**	**What it does**
13	Where the hazard is an upstream provider's legal domicile, the responsible entity cannot mitigate it and the point of control sits at procurement.	Amend the Security of Critical Infrastructure Act framework.	Moves the obligation to where it can be acted on, being the procurement decision rather than the operating entity.

Appendix B: Sovereignty scoring table

The table below supports the four-tier classification described in section 4.2.1 and is reproduced from our submission to the Digital Transformation Agency on coordinated contracting arrangements. Each criterion is scored zero, five or ten and weighted to a total of one hundred. Sovereign control accounts for sixty per cent of the total and Australian economic contribution for forty. Contract value adjusts the threshold a supplier must meet rather than the weighting itself.

Table 3: Proposed four-tier classification

Criterion	Weight	What it assesses
No foreign jurisdictional exposure	20%	Whether the supplier, its operating entity or its ultimate parent can be compelled under foreign law such as the US CLOUD Act. Physical location is not legal protection.
Onshore operating logic	18%	Whether the structured logic governing decisions, workflows and authority is held under Australian law rather than as configuration inside a foreign-controlled platform.
Australian ownership	12%	Whether a foreign parent holds a controlling interest. A Deed of Sovereignty mitigates this exposure for foreign-parented suppliers but does not replicate Australian ownership.
Data and inference localisation	10%	Whether inference processing is confirmed onshore, not only data storage. Many platforms route inference through offshore capacity.
Australian workforce and research	14%	Whether engineers and researchers are employed in Australia rather than a sales presence alone. Skills developed here stay in the Australian economy.
Intellectual property retained in Australia	12%	Whether operational ontologies and institutional logic persist as Australian-owned assets, independent of any single model or vendor.
Profits retained onshore	8%	Whether economic returns are anchored in Australia rather than flowing to a foreign parent.
Australian SME participation	6%	Whether the supply chain includes Australian small and medium enterprises against defined thresholds.
Total	100%	Sovereign control sixty per cent. Australian economic contribution forty per cent.

Appendix C: Related submissions

Two earlier submissions develop parts of this argument at greater length. Both are provided with this submission and may be published with it.

Kitbag Consulting, submission to the Digital Transformation Agency on coordinated contracting arrangements, June 2026. Sets out the four-tier sovereignty classification, the scoring table at Appendix B and the proposed System of Work procurement category.

Kitbag Consulting, submission to the Department of Home Affairs on the Tranche 2 reforms to the Security of Critical Infrastructure Act 2018, 31 July 2026. Addresses cyber security incidents involving automated systems and artificial intelligence and the position of operators and managed service providers.

SHAPING THE FUTURE OF AI FOR AUSTRALIA

INNOVATION. SOVEREIGNTY. GROWTH.

Australian Government

Kate Chaney MP

FEDERAL MEMBER FOR CURTIN



Kitbag

ENTERPRISE EVOLVED

SUBMISSION

Shaping the Future of AI for Australians

Discussion Paper by Kate Chaney MP, May 2026

Submitted by Kitbag Consulting

June 2026

About This Submission

The Honourable Kate Chaney's discussion paper is the most comprehensive AI policy produced by an Australian parliamentarian to date. It names real harms, proposes funded institutions and confronts the question of economic sovereignty that most AI policy frameworks deliberately avoid. We welcome the paper and the invitation to respond to its four consultation questions.

- Are there risks or opportunities the paper has missed?
- Are there policies that should be pursued but are not included?
- Are there design, implementation or trade-off details that deserve more attention?
- Are there directions proposed with which we disagree?

Our response aims to substantively advance this national AI discussion and is grounded in our experience across digital sovereignty, procurement and innovation. It addresses each consultation question, proposes additional policies and details implementation pathways to achieve the objectives set out in the Honourable Kate Chaney's discussion paper.

Background

Understanding AI

Before addressing the discussion paper, it is important to establish a clear understanding of the forms of AI that bear on the policy questions raised.

- **Generative AI (GenAI).** The most visible form currently. Large language or frontier models generate text, code, images and synthetic data from natural language prompts. The dominant enterprise use cases are content generation, summarisation, code assistance and customer-facing chatbots.
- **Predictive AI.** The older, more mature category. Machine learning models trained on historical data to forecast outcomes like demand, churn, fraud and equipment failure. It has delivered genuine return on investment in tightly scoped domains where data quality is high and the decision being influenced is well-defined. The persistent problem is that most organisations built these models in isolation, disconnected from the decision architecture they were supposed to inform.
- **Agentic AI.** At the forefront of evolution and the form the market is moving toward fastest, while understanding least. AI agents that can plan, take actions, use tools and execute multi-step tasks with minimal human intervention. The deployment risk is significant: an agent operating inside a process with no codified decision logic, no authority structure and no governance framework will either stall or cause damage. This is the form of AI that most directly exposes the absence of a System of Work.
- **Small Language Models (SLMs).** The intelligent counterpoint to the LLM arms race. Purpose-built, domain-specific models that run with lower compute cost, reduced latency and critically inside a defined operational boundary. The practical architecture

pairs SLMs for process and query automation with LLM firewalls at both ends. The SLM knows the operating context; the LLM does not need to.

- **AI Governance and GRC Tooling.** The emerging fifth category and the one where the market faces the most acute and least-solved problem. Boards and regulators are demanding accountability for AI decisions. The EU AI Act[1] and Australia's voluntary AI Safety Standard[2] are creating compliance obligations that most platforms are architecturally incapable of meeting, because they have no codified record of what operating logic drove what decision under whose authority.

Where Does Your Data and IP Go?

The question of what happens to organisational data when it enters an AI platform operates across four compounding layers. Each layer compounds the next and contractual exclusions do not provide architectural protection.

- **Layer 1 — What the AI vendor does with your input.** When you submit content to a commercially hosted AI platform, whether OpenAI, Google Gemini, Microsoft Copilot or similar, that content is transmitted to and processed on infrastructure owned and operated by a foreign-headquartered corporation. What happens to it after that depends entirely on the terms of service and the deployment model in use.
- **Layer 2 — Jurisdictional exposure.** This is the legal dimension that most organisations have not confronted. The US CLOUD Act (2018)[3] grants US authorities the power to compel US-headquartered technology companies to produce data stored anywhere in the world, including in Australian data centres, without the knowledge or consent of the Australian Government or the data owner. Jurisdiction follows the vendor's corporate domicile, **not** the physical location of the data. An organisation feeding sensitive operational content into any US-headquartered AI platform is operating under a legal regime where a foreign government has a lawful pathway to compel disclosure of that content. That is the current legal position, not a theoretical risk. Chinese national security legislation creates a parallel mechanism. The National Intelligence Law (2017) and the Data Security Law (2021)[4] require Chinese entities and nationals, including companies with Chinese ownership structures, development teams or supply chain dependencies, to cooperate with state intelligence work on demand. India's Information Technology Act 2000 (Section 69)[5] similarly empowers the Indian government to compel interception, monitoring or decryption of information on national security grounds. The relevant question is not where the vendor is headquartered but where ownership, development capability and supply chain sit.
- **Layer 3 — The model training signal problem.** Beyond contractual data use, there is an architectural risk that receives almost no attention in enterprise AI discussions. When organisations feed their processes, decision logic, workflow structures and operational content into AI tools at scale, they generate a rich signal about how their

---

[1]Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (AI Act).
[2]Australian Government, Department of Industry, Science and Resources, Voluntary AI Safety Standard (2024).
[3]Clarifying Lawful Overseas Use of Data (CLOUD) Act, Pub. L. No. 115-141, 132 Stat. 348 (2018).
[4]People's Republic of China, National Intelligence Law (2017), Art. 7; Data Security Law (2021), Art. 36.
[5]Information Technology Act 2000 (India), s 69, as amended by the Information Technology (Amendment) Act 2008.

organisation works. Even where individual inputs are not retained, the aggregate signal shapes model behaviour and in some deployment architectures influences fine-tuning. The operating intelligence of the organisation is being extracted through use, regardless of what the terms of service say about training data. Data residency policies address where data sits at rest. They do not address what the act of using a foreign-owned AI platform does to the confidentiality of operating logic over time.

- **Layer 4 — Loss of competitive or policy advantage.** When an organisation loads its ways of working into a third-party AI platform, it is not simply configuring software. It is exporting its institutional knowledge: the accumulated decisions, sequencing logic, approval hierarchies, policy associations and operational heuristics that represent how that organisation actually functions at its best. That operating logic is competitive and policy-sensitive IP, reflecting years of refinement that no procurement process can replicate and no organisational chart can document. Feeding it into platforms governed by foreign jurisdiction, foreign commercial incentives and opaque training pipelines is the institutional equivalent of publishing your playbook. The consequence is not theoretical: eroded competitive advantage in commercial markets, compromised policy differentiation in government and operating logic that can be pattern-matched, replicated or turned against you. The question is not whether your data is sovereign. It is whether your ways of working are.

Overall Assessment

The paper is right in its central diagnosis: Australia's passivity on AI policy is not neutrality but a dangerous default that hands our future to overseas technology companies and the oligarchies that run them. The 18-policy framework is well-structured, covers the right terrain and is largely correct in direction.

Our overarching observation is that the paper is stronger on what to do than on how to make it stick. Several policies identify the right outcome but leave unresolved the enforcement architecture, the sovereignty mechanism or the design choice that will determine whether the policy delivers or becomes another announcement without consequence. Our submission focuses on those gaps.

Response

Question 1: Risks and Opportunities the Paper Has Missed

Missing Risk: AI in Government Procurement and the Operational Sovereignty Gap

The paper's most significant omission is the role of government procurement as both a risk vector and a policy lever. The Digital Transformation Agency's Coordinated Contracting Arrangements govern how the Australian Public Service acquires AI, cloud and digital services, but under the current framework no weighting is applied to sovereign risk. As set out in the Background to this submission, that risk operates across four compounding layers: data handling, jurisdictional exposure, the model training signal problem and the migration of operating logic into foreign-owned platforms.

Each layer compounds the next and contractual exclusions do not provide architectural protection. Jurisdiction follows the vendor's corporate domicile, not the location of the data. Sustained use of a foreign-owned platform extracts operational intelligence regardless of what the terms of service say about training data. When an organisation's ways of working are encoded inside a platform it does not own, the institutional memory required to operate without that platform erodes until substitution becomes structurally impossible.

The paper calls for taxing AI companies, regulating data centres and requiring transparency from frontier developers. None of these levers reaches the four-layer exposure described above. We recommend adding Policy 19, as set out below in response to Question 2, and reforming the CCA suitability assessment framework to incorporate a digital sovereignty tier. This would require frontier AI developers to demonstrate that Commonwealth data inference occurs within Australian jurisdiction, under Australian law and within a governed operational boundary, as a condition of whole-of-government contract eligibility.

Missing Opportunity: Australia as a Sovereign AI Export Market

The paper frames AI opportunity primarily through domestic productivity and research investment and does not address the export opportunity that Australia's geopolitical position makes available. This gap is most acute across the Indo-Pacific, where nations with comparable concerns about foreign technology dependence are actively seeking alternatives to US and Chinese AI systems but have limited credible options between them.

Australia's stable democracy, strong rule of law, Five Eyes membership and established middle-power relationships across the region are structural competitive advantages for sovereign AI export that no other nation in the Indo-Pacific can fully replicate. Countries that would not trust a US platform with sensitive operational data and would not consider a Chinese platform under any circumstances represent a genuine and largely uncontested market for Australian-built AI operating under Australian legal and governance frameworks.

The National AI Missions framework should explicitly pursue this opportunity rather than leave it unaddressed. Sovereign AI export is not simply a commercial proposition; it is a foreign policy instrument and a mechanism for extending Australian governance standards and rule-of-law principles into a region where the alternative is a default toward either US platform dependency or Chinese state-adjacent technology. The paper's silence on this front represents a missed strategic opportunity that compounds with each year the market develops without an Australian position in it.

Missing Opportunity: Defence and National Security AI

The paper is silent on AI in defence and national security contexts. This is understandable given classification constraints but represents a significant structural omission in a framework intended to be comprehensive. AUKUS Pillar II[6] explicitly includes AI as a capability domain, establishing a trilateral commitment to developing and fielding advanced AI-enabled military capabilities. The Australian Institute for Safety and Innovation's mandate, as described in the paper, does not appear to encompass classified or defence-adjacent AI systems, creating a visible gap between the civilian AI governance framework and the defence AI investment being made simultaneously under a separate architecture.

Whether this gap is intentional, reflecting a deliberate decision to address defence AI through classified policy instruments, or an omission that leaves defence AI development without adequate civilian governance oversight should be made explicit. If the former, the paper should say so. If the latter, a separate classified policy track with defined interface points to the civilian framework should be recommended. Leaving the question unaddressed in a national AI strategy invites the assumption that defence AI operates outside the governance principles the paper otherwise establishes, which is not a position Australia should allow to stand by default.

Question 2: Policies That Should Be Pursued but Are Not Included

Policy 19: Reform Government Procurement to Apply a Sovereign AI Lens

[6]AUKUS Joint Leaders Statement, 13 March 2023; AUKUS Pillar II Advanced Capabilities includes AI/ML, autonomous systems and electronic warfare.

As described above, the CCA suitability assessment framework should be reformed to apply a tiered sovereignty assessment to AI implementation. We propose a four-tier scale reflecting the WEF's sovereignty dimensions, moving CCA assessment from binary eligibility to a graduated framework that rewards Australian-controlled capability and applies proportionate scrutiny to foreign dependency risk.

TIER 1	**Fully Australian Sovereign — Preferred** Australian-owned entity; IP, profits and operating logic retained onshore under Australian law. Local workforce, R&D and engineering across the full AI stack, not just sales presence. No foreign jurisdictional exposure; auditable build chain and model training practices. Data, GPU inference, model weights and application layer all onshore. Streamlined CCA assessment.
TIER 2	**Australian-Owned, in Collaboration with a Multinational — Preferred with Conditions** Australian-owned and governed; primary accountability anchored in Australian law. Collaboration with a multinational introduces some foreign dependency; the nature and extent of that dependency determine positioning within this tier. Sovereign control rating varies: infrastructure partnership carries less risk than deep model or IP integration. A Deed of Sovereignty (formalised via MOU between the Australian entity and the DTA) is recommended where multinational collaboration creates material jurisdictional exposure, delineating which obligations sit with the Australian entity and which with the foreign partner.
TIER 3	**Multinational with Australian Subsidiary — Conditional** Foreign parent entity; IP and operating logic subject to foreign jurisdiction (e.g. US CLOUD Act). Some onshore economic benefit through local operations, employment and tax contribution. GPU inference path must be confirmed onshore, not routed through offshore AI factories. Eligible subject to local benefit commitments, supply chain disclosure and Deed of Sovereignty.
TIER 4	**Fully Foreign Entity, No Australian Benefit — High Scrutiny** No substantive local entity, workforce or economic contribution to Australia. Data, logic, IP and profits held offshore; full CLOUD Act and foreign regulatory exposure. Operational kill switch sits outside Australian jurisdiction. CCA eligibility requires exceptional justification and mandatory sovereign safeguards.

Tier 1 and Tier 2 sellers receive streamlined or preferential assessment. Tier 4 sellers face enhanced conditions or exclusion. Positioning within each tier is determined by the nature of the seller's arrangement; sovereign control and economic contribution are assessed across both axes.

Australia would not be alone in applying procurement as a sovereignty lever. France's SecNumCloud framework[7] requires cloud services used for sensitive government workloads to be certified under French and EU law, with ownership and control conditions that effectively exclude foreign-controlled providers from the most sensitive tiers. Crucially, it is not a ban; it is a tiered framework that channels procurement toward sovereign options while retaining access to foreign vendors for lower-sensitivity workloads. The result is a market signal that has accelerated investment in French-owned cloud capability without closing France off to global technology. Germany mandates domestic jurisdiction over government

[7]Agence nationale de la sécurité des systèmes d'information (ANSSI), Référentiel d'exigences SecNumCloud, v3.2 (2022). See https://www.ssi.gouv.fr/secnumcloud.

IT. Canada introduced a digital sovereignty procurement framework in late 2024.[8] The EU's Gaia-X initiative[9] invests in federated sovereign infrastructure.

The risk of inaction is not hypothetical. Comparable democracies are actively shaping their technology markets through procurement policy. Australia's absence from that cohort is not a neutral position; it is a decision, a dangerous default, to leave sovereign capability development to market forces that have no particular interest in producing it.

Policy 20: A Mandatory AI Register for High-Risk Government Decisions

A public register of automated decision-making systems, as proposed under Policy 12, addresses only the most visible tier of AI deployment. The four-layer sovereignty risk identified in Question 1 cannot be managed through a register scoped to ADM systems alone. The more consequential exposure sits in the layers beneath visible decisions: in how AI is being used to inform, prepare and shape the judgements that precede any formally automated outcome.

Responsible AI deployment inside complex organisations operates across three distinct layers, each of which creates sovereign exposure of a different character. The outermost is the frontier model tier, platforms connected to the global AI ecosystem carrying the full jurisdictional and training signal risks described above. These tools must be air-gapped from organisational knowledge. The second layer is the internal agent, a Small Language Model operating against a retrieval-augmented generation architecture that interrogates internal policy, practice, procedure and systems. Properly deployed, this layer keeps decision-makers informed without exporting institutional knowledge beyond the organisation's sovereign boundary. The third layer is agentic AI: systems that interrogate ways of working and deliver automation of transactional processes without meaningful human involvement at the point of execution.

A register limited to the third layer leaves the first two unaccountable and the four-layer risk unaddressed. The register must span all three deployment tiers. It should require disclosure of: the AI system used and its developer; the sovereignty tier under which it is deployed and whether inference occurs onshore under Australian law; the layer of deployment (frontier productivity, internal decision support or agentic automation); what human oversight is in place and at what point in the decision chain it operates; and the volume of decisions influenced or made. Agencies should further be required to demonstrate that a governed System of Work providing structural accountability across all three tiers is in place as a condition of deploying AI at any layer. Without that scope, the DDOC and the ADM framework remain supervisory in name only.

Question 3: Design, Implementation and Trade-Off Details That Deserve More Attention

Policy 1: AISI Governance, Not Just Funding

The paper identifies the risk that the AISI will be caught up in the bureaucracy and politics of government but does not resolve it. Funding the AISI to $100 million annually while leaving it housed within the Department of Industry, Science and Resources creates a structural tension: the AISI is expected to provide independent technical assessments of AI models developed by companies with active lobbying relationships with the same minister to whom the AISI ultimately answers.

---

[8]Treasury Board of Canada Secretariat, Direction on the Secure Use of Commercial Cloud Services: Security Policy Implementation Notice (SPIN) 2023-01, updated 2024.
[9]Gaia-X Association AISBL, Gaia-X Architecture Document (2023). See https://gaia-x.eu.

The design question that deserves more attention is what governance model protects the AISI's technical independence. Options worth considering include:

- A statutory authority model with an independent board, fixed-term appointments and a published methodology for model assessments, insulating assessments from ministerial direction.
- A hybrid structure with a protected technical core that publishes findings without ministerial clearance, alongside a policy advisory function that operates through normal departmental channels.
- An explicit provision, modelled on the Australian Bureau of Statistics Act, prohibiting ministerial direction on the content of technical assessments.

The $100 million commitment is welcome. The AISI must be built to survive a change of government.

Policy 14: What Compels Frontier AI Developers to Comply?

The mandatory transparency and incident reporting scheme is correct in intent. The design gap is leverage and it is a gap that narrows over time. The paper notes that California requires large AI developers to publish safety frameworks and pre-deployment reports[10] and that Australia has no equivalent. It proposes one. What it does not address is what happens if a frontier AI developer domiciled outside Australia simply does not comply. Australia has no power to override the domestic legislation of a foreign jurisdiction. Where a developer's home jurisdiction actively conflicts with Australian transparency expectations, compliance cannot be assumed and cannot be compelled through disclosure obligations alone.

The only period in which Australia holds meaningful leverage is before dependency is established. Market access, data centre approvals, CCA eligibility and participation in government procurement are conditions a developer needs at the point of entry. Once a platform is embedded in government operations, the threat of exclusion becomes progressively less credible. Agencies that have reshaped their processes around an incumbent platform cannot easily substitute it and vendors understand this. Lock-in does not happen by accident; it is the commercial logic of the model.

The transparency obligations in Policy 14 must therefore be enforced as conditions of market entry, not as ongoing reporting requirements that assume a cooperative relationship. A developer that does not meet them should be ineligible for Commonwealth contracts and CCA participation from the outset. Attempting to impose compliance after embedding has occurred cedes the only leverage Australia has.

The structural answer to this compliance risk is not solely regulatory; it is architectural. A three-layer deployment model, with frontier platforms air-gapped from organisational knowledge, an internal Small Language Model interrogating policy and procedure within a sovereign boundary and agentic automation operating only against sanctioned ways of working, limits the exposure that non-compliant vendors can create. When organisational knowledge, decision logic and operating process are governed inside a sovereign System of Work rather than encoded in a foreign-owned platform, the consequences of vendor non-compliance shrink materially. The organisation retains its institutional intelligence regardless of what the vendor does or does not disclose. Sovereignty is not contingent on the vendor's cooperation because the operating logic was never ceded to them in the first place. This is the architecture that makes Policy 14's intent achievable in practice, not as a substitute for

[10]California Senate Bill 1047, Safe and Secure Innovation for Frontier Artificial Intelligence Models Act (2024); Assembly Bill 2013 (2024) requiring AI transparency reports.

the compliance framework but as the foundation that ensures Australia is not structurally dependent on its enforcement.

Policies 17 and 18: Timelines Are the Test of Seriousness

The paper's gas industry analogy is its most important political argument. Australia missed the window to design a fair returns mechanism into its gas industry before companies locked in their investments and lobbying positions. The paper correctly argues that we are in the pre-lock-in period for AI and that the window to signal an incoming framework is now open.

The critical trade-off is between getting the design right and moving fast enough to retain leverage. The paper calls for consultation on both the data centre obligations and the taxation mechanism. Consultation is appropriate but the paper should specify a clear timeline. The government should publicly announce within six months that binding data centre obligations and an AI tax framework are coming, regardless of whether the design is finalised. The design process should complete within twelve months. The framework should be enacted within twenty-four months.

Amazon's $20 billion data centre commitment[11] and Microsoft's broader $25 billion global commitment[12] are already in progress. The construction timelines for these facilities are three to five years. The window to impose binding conditions before the physical infrastructure is locked in is measured in months, not years.

The Microsoft MOU is a case in point.[13] The commitment to invest $5 billion in Australian data centre infrastructure, create 1,900 jobs over five years and deliver AI skilling to 300,000 Australians is presented as a landmark sovereign partnership. In some respects it is: the investment is real, the jobs are welcome and the skilling commitment addresses a genuine gap. But the MOU is **not** legally binding. Microsoft has no obligation enforceable under Australian law to deliver any of it. There are no penalties for non-performance, no clawback provisions and no independent verification mechanism. If Microsoft's global strategic priorities shift, Australia has no recourse. A commitment announced at a press conference is not the same as a condition of market access. This is precisely the gap that converting the Data Centre Expectations into binding obligations (Policy 17) and establishing a mandatory returns mechanism (Policy 18) are designed to close. The MOU model should be the floor, not the ceiling: a signal of good faith from industry that the government then has an obligation to formalise into enforceable terms before the infrastructure is built and the leverage is gone.

Closing Remarks

The Chaney discussion paper is a serious and timely contribution to a debate that has been dominated by either uncritical enthusiasm for AI's potential or unfocused anxiety about its risks. Its strength lies in naming specific harms, proposing specific institutions and confronting the question of who captures the economic value of AI, a question that most policy frameworks deliberately avoid.

This submission has aimed to be constructive in that spirit. We have identified gaps in the paper's risk analysis, proposed two additional policies grounded in practical implementation

---

[11]Amazon Web Services, "AWS to Invest $20 Billion in Australia," AWS News Blog, 5 May 2024.

[12]Microsoft, "Microsoft to invest $3 billion in AI and cloud infrastructure in Australia," Microsoft News Centre Australia, 2 May 2024. The $25 billion figure reflects the global commitment announced concurrently.

[13]Australian Government, Department of Industry, Science and Resources, "Microsoft MOU: Partnership for Australia's AI Future" (2024). The MOU is a statement of intent and does not create legally binding obligations enforceable under Australian law.

experience and offered design refinements to strengthen the enforcement architecture of existing proposals. Across each area, our consistent concern is the same: good policy intent is not sufficient without the institutional architecture and timeline discipline required to make it stick.

Australia is not short of AI policy discussion. What it has lacked is the political will to convert that discussion into enforceable frameworks before dependency is established and leverage is lost. The window is open. The decisions made in the next two years will determine whether Australia enters the AI era as a sovereign participant or a dependent consumer. The policies in this paper are the right starting point. What happens next will be determined not by the technology but by whether government chooses to act before that window closes.

About Kitbag Consulting

Founded in 2008, Kitbag is a Canberra-based consultancy delivering strategic, operational and sovereign digital solutions to government and industry. Eighteen years of sustained delivery across Defence, national security and federal agencies. Services span governance, risk, procurement advisory, programme management and operational modelling. Australian-owned, self-funded and non-aligned. Kitbag won the Telstra Best of Business Award in the ACT in 2025.

By 2023, three forces converged: Big Four misconduct had damaged the sector's credibility; AI was eroding demand for traditional advisory services; and Kitbag's core modelling work was tethered to Defence enterprise software that had become technically fragile and constraining. With no viable alternative in the market, Kitbag established KB Technology and developed DOLIUM, a sovereign and globally first System of Work purpose-built for the AI era, self-funded to remain mission-driven. DOLIUM won the 2025 ACT iAwards for Excellence in Innovation.

Kitbag is the driving influence in establishing the Parliamentary Friends of Digital Sovereignty, a multipartisan parliamentary group uniting parliamentarians and sovereign-industry around a single proposition: that Australia must own, control and build upon its critical digital infrastructure, data and IP rather than cede that capability and competitive

Australian Government
Digital Transformation Agency

COORDINATED CONTRACT AGREEMENTS SUBMISSION TO ENABLE AUSTRALIA'S SOVEREIGN STRATEGY

STRONGER ECONOMY.
GREATER RESILIENCE.
SUSTAINABLE FUTURE.



Kitbag
ENTERPRISE EVOLVED

Suitability Assessment Framework for Coordinated Contracting Arrangements

Submitted by Kitbag Consulting and KB Technology

In response to: DTA Discussion Paper, June 2026 | Questions 2, 3, 4 and 5

About This Submission

This submission is made by Kitbag Consulting and KB Technology, an accredited Australian Early-Stage Innovation Company (ESIC) building digital capability in Australia, in response to the DTA's discussion paper on seller eligibility for coordinated contracting arrangements (CCAs). We provide views on Questions 2, 3, 4 and 5.

Preliminary Position: Australian Jurisdictional Risk

The US CLOUD Act[1] compels US companies to provide access to data and systems under their control regardless of where those systems are physically located, regardless of what the contract says and regardless of whether the Australian counterparty has consented. The vendor cannot override that obligation even if it wanted to. The contract does not supersede the law the vendor answers to.

China's National Intelligence Law[2] carries an equivalent obligation. Article 7 requires any Chinese organisation or citizen to support, assist and cooperate with national intelligence work. Article 14 grants Chinese intelligence agencies the authority to demand cooperation from any relevant institution. There is no opt-out provision, no contractual carve-out and no mechanism by which a Chinese-domiciled or Chinese-controlled entity can refuse a request from the state. This obligation follows the vendor into every relationship, regardless of where the subsidiary is incorporated, where the servers are located, or what the contract says.

A contract governed by Australian law does not extinguish these obligations. It coexists with them and when they conflict, the vendor's home jurisdiction prevails. Multinational vendors frequently promote sovereign cloud offerings based on physical data location. Physical location does not resolve jurisdictional exposure. In 2025, Switzerland formally rejected Palantir for sensitive military applications[3] not on capability grounds, but because the company's exposure to US jurisdiction meant Switzerland could not guarantee long-term sovereign control of its government data. Switzerland has also moved to restrict Microsoft as the predominant office suite across government operations[4] for the same reason. They are the considered conclusions of a neutral nation with a long history of institutional risk management.

[1] Clarifying Lawful Overseas Use of Data Act 2018 (US CLOUD Act), 18 U.S.C. § 2713. Requires US-based technology companies to produce data stored outside the United States when served with a valid US legal process, regardless of where that data is physically located.

[2] People's Republic of China, National Intelligence Law (2017), Articles 7 and 14. Requires any Chinese organisation or citizen to support and cooperate with state intelligence work; no contractual carve-out or subsidiary structure can override this obligation.

[3] Swiss Armed Forces internal risk assessment (December 2024), reported by Republik and netzpolitik.org (December 2025). The 20-page evaluation concluded Palantir's US jurisdiction created an unmitigable sovereignty risk and recommended considering alternatives.

[4] Swiss federal and cantonal authorities, 2025–2026. A government feasibility study confirmed open-source replacement of Microsoft 365 is viable, citing US CLOUD Act exposure as a primary concern. See: lenews.ch and swissinfo.ch (April 2026).

The question governing a Commonwealth Contract for Capability is therefore not simply which terms and conditions apply. It is which jurisdiction controls the relationship when those frameworks conflict. A vendor domiciled in a foreign jurisdiction who accepts Australian T&Cs has not resolved that conflict.

The deeper risk is operational, not contractual. The problem is not simply that AI tools are foreign built. It is that the logic encoding how an organisation functions, how decisions are made, tasks executed and authority exercised, increasingly resides in platforms beyond Australian legal control. When government agencies embed their operational logic in foreign platforms, three structural vulnerabilities follow.

Kill Switch Risk

When the US sanctioned the chief prosecutor of the International Criminal Court, he lost access to his Microsoft cloud account overnight.[5]. Parts of national capability can be rendered inoperable by legal decisions taken in a foreign jurisdiction in which Australia has no standing and no recourse.

On 13 June 2026, the US administration-imposed export controls on Anthropic's Fable 5 and Mythos 5 models, cutting off access for every non-US user worldwide. Anthropic complied immediately. There was no warning, no transition period, and no Australian legal mechanism to prevent it or seek redress. Organisations that had embedded those models into their operations lost access overnight and critically, so did those operating through Anthropic's own Australian subsidiary. No local structure, no local contract, and no local relationship could override a directive from the foreign parent's home government. Australia had no standing, no vote and no recourse. It is the precise scenario this submission has sought to address: the strategic and operational exposure created when Australian institutions embed their workflows in foreign-controlled AI platforms whose continued availability is subject to legal, political and commercial decisions made in another country, in another interest, under another flag.[6]

Corporate Veil Risk

Multinational vendors answer to their global headquarters and foreign regulators. The PwC Australia scandal[7] illustrated this directly when the Senate sought critical information, PwC International refused on the basis that the material belonged to the global entity. A domestically owned vendor has no such conflict. Its obligations are singular and Australian.

Dependency shadow

Over time, agencies reshape their processes around dominant platforms and internal understanding of operational logic erodes. When substitution becomes necessary due to sanctions, policy divergence or strategic realignment the obstacle is not finding a comparable tool. It is restoring the sovereign capability that was allowed to atrophy. That restoration is expensive, slow and politically difficult precisely because the dependency was never formally acknowledged as a risk.

---

[5] US Executive Order 14203 (6 February 2025), sanctions on International Criminal Court personnel. Following the order, the ICC chief prosecutor lost access to Microsoft cloud services; the ICC subsequently migrated away from Microsoft to open-source alternatives, illustrating how foreign legal action can render organisational capability dependent on a foreign vendor's compliance decisions.

[6] Axios, 'Trump administration blocks foreign access to Anthropic's most powerful AI' (12 June 2026); ABC News, 'Trump administration forces Anthropic to pull models worldwide' (13 June 2026).

[7] Australian Senate Finance and Public Administration References Committee, PwC Australia inquiry (2023–2024). PwC International declined to provide documents to the Senate and ATO on the basis that material belonged to the global entity, not the Australian firm.

The answer is not better contract terms. It is selecting vendors whose legal domicile, operating infrastructure and accountability framework are subject to Australian law without qualification where no foreign statute exists to override what the contract says, and no foreign government holds a legal instrument compelling access to Australian operational systems.

There is no avoiding the fact that the geopolitical environment in which these procurement decisions are made is not stable and it is not improving. Commercial relationships are increasingly being weaponised as instruments of state leverage through tariffs, technology access restrictions, the threat of platform withdrawal and through legal compulsion mechanisms that were always present but are now being actively exercised.

Procurement risk assessment that does not account for the political disposition of a vendor's home jurisdiction and the instruments that jurisdiction holds over the vendor's obligations to Australian clients is not risk assessment. It is assumption management dressed as due diligence.

The decisions being made in procurement today will define the exposure Australian organisations carry for the next decade. The geopolitical environment demands that those decisions be made with full awareness of what jurisdiction follows the vendor through the door.

> *Australia is not alone. Germany mandates domestic jurisdiction over government IT*[8]. France enforces SecNumCloud[9]. Gaia-X[10] invests in federated sovereign infrastructure. Canada introduced a digital sovereignty procurement framework in late 2025[11]. Not moving in a comparable direction risk positioning Australia as an outlier not for lack of capability, but for misidentifying where sovereignty now resides.

[8] BSI IT-Grundschutz framework; German Federal Government cloud strategy. The state of Schleswig-Holstein migrated 40,000+ workstations to open-source software, achieving over €15 million in annual savings.

[9] ANSSI SecNumCloud qualification framework (France), ssi.gouv.fr. Sets mandatory sovereignty requirements for cloud providers serving sensitive French government data, including that operational control not be subject to non-EU legal jurisdiction.

[10] Gaia-X, European federated data infrastructure initiative, gaia-x.eu (est. 2019, Germany and France). Aims to create a sovereign, interoperable European cloud ecosystem reducing dependency on non-European technology providers.

[11] Government of Canada, Digital Sovereignty Framework, Treasury Board Secretariat (November 2025); Buy Canadian procurement policy framework (December 2025). The Framework outlines procurement and technical controls to strengthen institutional control over federal government data and systems. See: canada.ca

Question 2 — Terms and conditions

> *What risks or challenges does accepting government terms and conditions (rather than seller T&Cs) create for sellers and how could those challenges be addressed?*

Our Position

Kitbag Consulting and KB Technology accepts government terms and conditions as a baseline requirement. The risks and challenges of doing so are real but addressable provided the framework distinguishes between sovereignty terms, which are non-negotiable and commercial mechanics, which can be adapted proportionately to a seller's structure and risk profile. The tier framework below provides that mechanism.

Sovereignty Terms and Conditions

Sovereignty terms exist because Australian law cannot compel a foreign vendor's home government. Accepting Australian T&Cs on jurisdiction and data governance is the minimum condition for calling an arrangement sovereign. That condition applies regardless of vendor origin. The goal is not to exclude foreign vendors categorically but to ensure Australian options receive a fair hearing and that Australia's digital sovereignty is actively encouraged and protected. As Assistant Minister Charlton observed at UTS, Australian options are currently losing by default, not by merit.

Acceptance of Australian government sovereignty terms on jurisdiction, data governance and accountability to Australian law should be a condition of eligibility, not a starting position for negotiation. A seller's resistance to these terms is itself a sovereignty signal. It typically reflects an unwillingness to submit to Australian legal jurisdiction, a preference for contract terms drafted to protect foreign corporate interests, or a structural inability to separate Australian operations from the global policy frameworks their parent entity operates under. These are not administrative concerns; they are indicators of where control of the relationship resides.

For sellers subject to the US CLOUD Act[12] or comparable extraterritorial instruments, accepting Australian government terms on jurisdiction and data governance is the minimum necessary condition for the arrangement to function as described. The CLOUD Act compels US-incorporated companies to produce data held under their control regardless of where it is physically stored, regardless of what the contract says and regardless of whether the Australian counterparty has been notified or consented. An Australian contract that coexists with that obligation does not resolve, only defers the jurisdictional question. The terms the government accepts as sovereign protection may, in practice, be subordinate to a foreign statute the vendor cannot override even if it chooses to.

That baseline is not a burden to be negotiated away. It is the minimum condition for calling the arrangement sovereign. The jurisdictional dimension of this question is addressed in our preliminary position above.

[12] Clarifying Lawful Overseas Use of Data Act 2018 (US CLOUD Act), 18 U.S.C. § 2713. Requires US-based technology companies to produce data stored outside the United States when served with a valid US legal process, regardless of physical location.

Commercial Terms and Conditions

We acknowledge that genuine operational challenges exist, particularly for sellers whose global structures were not designed around Australian procurement requirements. Liability exposure, IP provisions affecting global product deployment and conflicts with international compliance certifications are real friction points. These are not sovereignty issues; they are commercial ones, and they are addressable through standard contract negotiation practices.

Introducing the tier framework

Not all sellers present the same risk profile and a procurement framework that treats them identically will either exclude capable local suppliers through unnecessary friction or expose government to jurisdictional risk by applying the same flexibility to foreign-controlled entities. The tier framework set out in Question 3 addresses this by calibrating sovereign accountability to structural risk. It recognises that an Australian-owned business operating entirely under Australian law is a fundamentally different proposition from a transnational entity whose parent is subject to foreign government compulsion. The degree of commercial flexibility available under T&C negotiations should reflect that difference.

The World Economic Forum[13] defines digital sovereignty as the ability to have control over your own digital destiny the data, hardware and software that you rely on and create. International accounting standards[14] define *Control* of an economic resource meaning the ability to direct the use of the economic resource and obtain the economic benefits that flow from it. *Control* also includes the ability to prevent others from directing the use of and obtaining the benefits from the resource.

The WEF identifies multiple dimensions including data sovereignty, operational sovereignty, technical sovereignty and legal sovereignty. Critically, its 2026 framing rejects the false choice between sovereignty and openness: sovereignty means balancing strategic self-reliance with intelligent partnerships, not isolationism

Applying this to T&Cs, we propose a tiered framework that gives procurement specialists a mechanism to assess the risk profile of foreign entities, while preserving the underlying principles of sovereignty terms across all tiers and allowing commercial mechanics to be adapted proportionately. The goal is an Australian procurement function that does not just assess foreign risk but actively champions domestic capability.

Tier 1 — Australian-owned, subject only to Australian law These sellers face the least friction. Their structures are already aligned with government requirements and government T&Cs should apply with minimal adaptation.

Tier 2 — Australian-owned in collaboration with a foreign entity friction may arise where multinational arrangements introduce conflicting obligations. Commercial terms may be adapted proportionately to the nature and depth of the collaboration. A Deed of Sovereignty can help delineate which obligations sit with the Australian entity and which with the foreign partner, preserving sovereign accountability while acknowledging operational reality.

[13] World Economic Forum, 'Digital Sovereignty' (2025/2026), weforum.org. Defines digital sovereignty as "the ability to have control over your own digital destiny — the data, hardware and software that you rely on and create."

[14] IFRS Conceptual Framework for Financial Reporting (2018), paragraph 4.20, International Accounting Standards Board. Defines control as the present ability to direct the use of an economic resource and obtain the economic benefits that flow from it.

Tier 3 -- Foreign entity with Australian subsidiaries A defined set of commercial carve-outs may be negotiated where genuine conflicts with global structures exist, subject to disclosure to the relevant agency and approval. These carve-outs apply to commercial mechanics only, not to jurisdiction, data governance, or accountability provisions.

Tier 4 — Transnational Platforms/Sellers Government T&Cs apply in full as a condition of eligibility. Their jurisdictional exposure is precisely the risk the T&Cs are designed to manage and no commercial carve-out resolves that underlying problem.

Introducing the Deed of Sovereignty

The Deed of Sovereignty is a proposed instrument to address a structural limitation in current procurement frameworks: that accepting Australian T&Cs does not extinguish a foreign vendor's obligations to its home jurisdiction. A contract governed by Australian law coexists with, but does not override, the statutory obligations a vendor carries by virtue of its domicile. Where those obligations conflict, the vendor's home jurisdiction prevails. No commercial negotiation resolves that. The Deed works by making sovereign accountability an explicit, standalone commitment, delineating which obligations sit with the Australian entity, which sit with the foreign partner, and how conflicts between them are resolved. It operates at a different layer from standard T&Cs: where T&Cs govern the commercial relationship, the Deed governs the sovereign one. It is designed to operate within existing Australian contract law and deed instrument precedent, requiring no new legislative framework to implement. For Tier 2 arrangements, where an Australian-owned entity collaborates with a multinational, the Deed provides the mechanism to preserve sovereign accountability at the Australian layer while acknowledging the operational reality of the partnership. For Tier 3 arrangements, it functions as a condition of eligibility, a binding commitment that jurisdictional exposure has been identified, disclosed, and allocated. It does not eliminate foreign jurisdictional risk where that risk is structural. What it does is make that risk visible, named, and governed, shifting it from an assumed condition of the arrangement to an explicit and auditable obligation.

The Distinction in Practice

The framework above draws a clear line: commercial terms can be adapted to build a workable, sustainable supplier relationship. Sovereignty terms cannot. This distinction allows government to engage pragmatically with the market without compromising the accountability and jurisdictional integrity that Australian procurement policy is designed to protect.

Question 3 — Broader economic benefits & public reporting

> *Thinking about the broader economic benefits that CCA sellers may provide to the Australian economy, what offerings are commercially reasonable from your perspective and what should be included in public reporting to provide transparency whether planned economic benefits have been achieved?*

Our Position

The PGPA and the Commonwealth Procurement Rules should embed a sovereignty weighting into the value for money evaluation, following New Zealand's precedent of a legislated minimum 10% weighting on sovereign capability. The case for doing so is economic as much as strategic. The existing SSA structure has defaulted to sellers already holding significant government presence, which in practice are large foreign multinationals that use transfer pricing and intra-group arrangements to repatriate profits to their parent jurisdictions. Commonwealth expenditure that appears to support domestic capability is in substantial part flowing offshore. A sovereignty weighting distinguishes between spending that circulates within the Australian economy and spending that does not. Value for money with a sovereignty dimension should therefore be the organising principle that separates genuine economic contribution from contractual window-dressing.

The independent review of the government's Single Seller Arrangements found that while the arrangements have driven reported savings of $1.6 billion, realised discounts are "hard to quantify", actual license use has "limited visibility", and some arrangements operate as simple commercial transactions rather than genuine strategic partnerships between government and industry. The review also found inconsistency between seller terms and government policy on cyber and local industry participation. The CCA suitability assessment framework is the mechanism to address those shortcomings and this submission offers a structured approach to doing so.[15].

What Is Commercially Reasonable to Expect

The following are reasonable baseline expectations of any CCA seller, calibrated to their sovereignty tier (see scale below):

- Investment in Australian operations across the full AI lifecycle, data infrastructure, GPU/inference, foundation models, applications and governance not just sales and account management presence.
- Full supply chain and jurisdictional disclosure: where model weights and operational logic are held, which foreign entities have legal access and whether the company is subject to instruments such as the US CLOUD Act, which compels US companies to grant access to data regardless of where it is physically stored.
- Data localisation for Commonwealth data as a baseline, including GPU inference onshore. Many transnationals route inferences through global AI factories; a user's request, potentially with attached Commonwealth data, is processed offshore even where storage is local. This must be explicitly confirmed and reported.
- Architectural separation between execution infrastructure (which can be globally shared) and operational ontology the logic encoding how an agency functions, complies and exercises authority. That layer must remain under Australian ownership and jurisdiction.

[15] Joseph Brookes, 'Govt agencies may team up on large tech procurements', InnovationAus (13 June 2026), innovationaus.com.

- Meaningful Australian SME subcontracting, with defined minimum thresholds as a share of contract value.
- Open-architecture or interoperability commitments ensuring the government can substitute execution layers without losing institutional knowledge operational IP must accumulate as a sovereign asset, not a platform dependency.

Proposed Sovereignty Scale for CCA Assessment

We propose the DTA adopt a four-tier sovereignty scale as a core assessment tool, reflecting the WEF's four sovereignty dimensions. The scale moves CCA assessment from binary eligibility to a graduated framework that rewards Australian-controlled capability and applies proportionate scrutiny to foreign dependency risk. Positioning within each tier is determined by two axes: sovereign control (legal, operational and jurisdictional) and Australian economic contribution (employment, R&D, SME participation, profits retained onshore).

Proposed Australian Economic Sovereignty Scale for CCA Sellers

TIER 1	**Fully Australian sovereign — preferred** ▲ Preferred • Australian-owned entity; IP, profits and operational logic retained onshore under Australian law. • Local workforce, R&D and engineering across the full AI stack — not just sales presence. • No foreign jurisdictional exposure; auditable build chain and model training practices. • Data, GPU inference, model weights and application layer all onshore.
TIER 2	**Australian-owned, in collaboration with a Foreign Entity — preferred with conditions** ▲ Preferred with conditions • Australian-owned and governed; primary accountability anchored in Australian law. • Collaboration with a multinational introduces some foreign dependency the nature and extent of that dependency determine positioning within this tier. • Sovereign control rating varies infrastructure partnership carries less risk than deep model or IP integration. • Deed of Sovereignty recommended where multinational collaboration creates material jurisdictional exposure.
TIER 3	**Foreign Entity with Australian subsidiary — conditional** ► Conditional • Foreign parent entity; IP and operational logic subject to foreign jurisdiction (e.g. US CLOUD Act). • Some onshore economic benefit through local operations, employment and tax contribution. • GPU inference path must be confirmed onshore — not routed through offshore AI factories. • Eligible subject to local benefit commitments, supply chain disclosure and Deed of Sovereignty.

TIER 4	**Fully Foreign Entity, no Australian benefit — high scrutiny** ▼ High scrutiny • No substantive local entity, workforce, or economic contribution to Australia. • Data, logic, IP and profits held offshore; full CLOUD Act and foreign regulatory exposure. • Operational kill switch sits outside Australian jurisdiction. • CCA eligibility requires exceptional justification and mandatory sovereign safeguards.

Tier 1 and Tier 2 sellers receive streamlined assessment. Tier 4 sellers face enhanced conditions or exclusion. Positioning within each tier is determined by the nature of the seller's arrangement, sovereign control and economic contribution are assessed across both axes.

Sovereignty Scoring Table

The World Economic Forum defines digital sovereignty as the ability to have control over your own digital destiny the data, hardware and software that you rely on and create. This scoring table operationalises that definition for CCA procurement assessment across two axes: sovereign control (60% of total score) and Australian economic contribution (40% of total score).

Score each criterion 0 (no / fully foreign), 5 (partial / conditional), or 10 (yes / fully Australian). Multiply each score by its weight to calculate the weighted contribution, then sum all contributions for the final sovereignty score out of 100. Contract value should also be considered: a vendor who qualifies at Tier 2 for a $30M contract may require Tier 1 safeguards at $200M, because the strategic dependency created by a larger arrangement amplifies every jurisdictional risk.

Criterion	Weight	Score (0 / 5 / 10)	Weighted score	Max possible	Notes
No foreign jurisdiction exposure US CLOUD Act, extraterritorial legal exposure. Physical location is not legal protection foreign governments can compel access to data regardless of where it is stored.	20%			20	CLOUD Act, extraterritorial legal exposure
Onshore operational logic the structured logic governing decisions, workflows and authority is a sovereign asset. When embedded in foreign platforms it becomes subject to foreign subpoena, sanction, or commercial change.	18%			18	Decision logic, workflows, governance
Australian ownership Domestic vendors have no conflict of interest between Australian obligations and foreign parent obligations. A Deed of Sovereignty can partially mitigate but not fully replicate this for foreign-parented vendors.	12%			12	No foreign parent with controlling interest
Data & inference localisation GPU inference processing must be confirmed onshore, not just data storage. Many platforms route inference through global AI factories, processing Commonwealth data offshore.	10%			10	GPU inference confirmed onshore

Criterion	Weight	Score (0 / 5 / 10)	Weighted score	Max possible	Notes
Australian workforce & R&D Skills and knowledge that develop within Australian-owned businesses stay within the Australian economy. This retention is structural and compounds over time it is the sovereign workforce dividend.	14%			14	Engineers, researchers not just sales
IP retained in Australia Operational ontologies and institutional logic must persist as Australian-owned assets, independent of any single model or vendor. IP held offshore migrates sovereignty with the platform.	12%			12	No IP transfer to foreign parent
Profits retained onshore Economic returns flowing to a foreign parent signal misaligned long-term interest. Onshore profit retention indicates the vendor's commercial future is anchored in Australia.	8%			8	Tax and financial returns in Australia
SME subcontracting CCA arrangements represent collective buying power at scale. Directing that power toward vendors with Australian SME supply chains multiplies sovereign economic benefit beyond the primary contract.	6%			6	Defined Australian SME thresholds
Total sovereignty score	**100%**		**/100**	**100**	

Tier guidance: 75–100 = Tier 1 (fully Australian sovereign) | 55–74 = Tier 2 (Australian, foreign entity collaboration) | 28–54 = Tier 3 (foreign entity with Australian subsidiary) | 0–27 = Tier 4 (transnational platforms). Contract value may lower the effective score threshold for higher tiers.

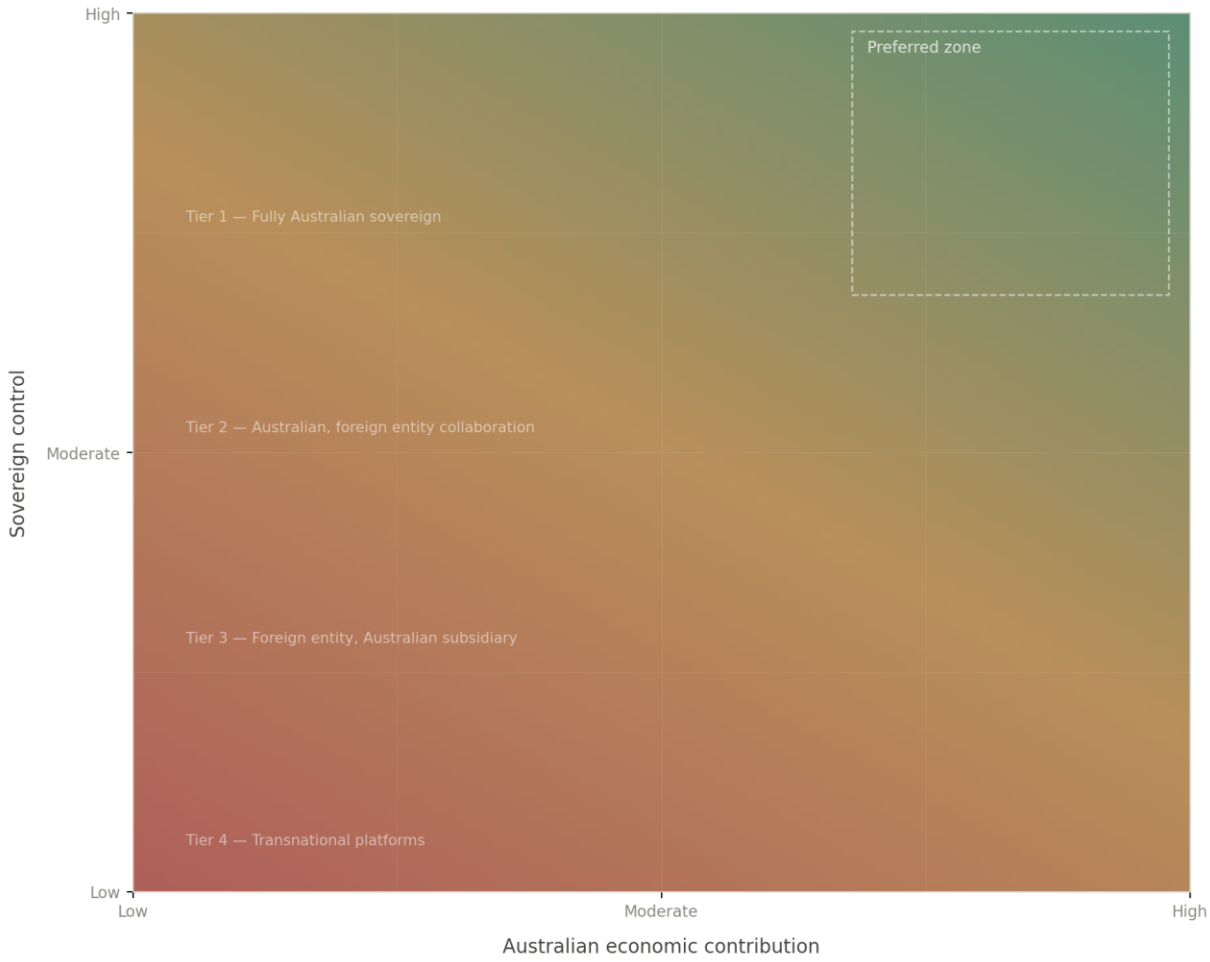


Figure 1: CCA seller sovereignty assessment matrix — sovereign control vs Australian economic contribution

What Should Be Publicly Reported

Annual reporting by CCA sellers, published on BuyICT, should cover:

- Total Australian spend including full supply chain breakdown
- Local employment by role type, distinguishing engineering and R&D from sales and support
- Australian SME subcontracting volumes as a percentage of contract value
- Sovereignty tier classification and any changes during the reporting period
- GPU inference path disclosure confirmation that Commonwealth data inference is processed onshore.
- Jurisdictional exposure summary: which foreign legal instruments apply to the seller's data and operational logic
- Deed of Sovereignty status where applicable
- Nature and extent of any multinational collaboration arrangements (for Tier 2 sellers)
- Progress against any sovereign capability commitments made at CCA establishment

We further recommend the DTA introduce a sovereignty maturity indicator distinguishing sellers who are contractually compliant from those who actively reduce the government's structural dependency on foreign-controlled digital infrastructure.

Question 4 — Digital skills & workforce development

> *What could CCA sellers do to help the public sector achieve the government's digital skills objectives? Consider short, medium and long-term objectives, as well as the opportunity to leverage a CCA to achieve outcomes for the government at scale rather than solely with individual agencies.*

Our Position

The DTA should distinguish between two fundamentally distinct workforce dynamics depending on seller sovereignty tier. For Tier 1 and Tier 2 sellers Australian-owned businesses employing Australians the question is not about training obligations. It is about the natural economic dividend of sovereign capability: skills, institutional knowledge and specialist AI expertise that develop within these businesses stay within the Australian economy. That retention is structural, not contractual. It compounds over time. When government procures from an Australian-owned business, it is investing in an ecosystem where the talent, the IP and the accumulated operational knowledge all remain here.

For Tier 3 and Tier 4 sellers, the dynamic is reversed. Skills developed in their engagements flow to global teams. IP accumulates offshore. The Australian economy receives a service, not a capability. For these sellers, explicit training and labour development obligations are not optional extras, they are the partial offset for the sovereign value that their structure cannot deliver by default.

> *Minister Charlton's observation that competitive advantage in AI now sits between the base model and the end product has a direct workforce implication: the skills that matter most are not those required to operate a vendor's interface, but those required to build and govern the layer above it — the agency's own operating logic, decision authorities and knowledge structures.*

Tier 1 And Tier 2 Sellers: Sovereign Skill Retention

The CCA framework should recognise and reward the structural workforce dividend that Tier 1 and Tier 2 sellers deliver. When government awards a CCA to an Australian-owned business, it is:

- Retaining specialist AI skills within the Australian economy rather than exporting them to a foreign parent's global talent pool
- Building a domestic base of engineers, researchers and practitioners who understand the Australian operating context the legislative environment, governance requirements and policy constraints that foreign models fundamentally lack
- Creating conditions for skills to compound: the more Australian businesses build AI for Australian government, the deeper and more capable the local talent ecosystem becomes
- Reducing long-term dependency on foreign expertise for the maintenance, governance and evolution of critical government systems

For Tier 2 sellers, the extent of this dividend depends on the nature of the multinational collaboration. Where the collaboration is at the infrastructure or execution layer, the core skill and knowledge retention benefit remains intact. Where it extends to IP or model development, the DTA should seek disclosure of where that knowledge resides.

The DTA should reflect this structural benefit explicitly in the sovereignty tier weighting it is the difference between an AI investment that builds national capability and one that rents it.

Tier 3 And Tier 4 Sellers: Explicit Development Obligations

For sellers who cannot deliver sovereign skill retention by structure, the CCA framework should require explicit labour and skills development commitments as a condition of eligibility, assessed across three horizons:

- **Short-term:** Free or heavily subsidised access to broadly transferable digital skills training, available whole-of-government rather than negotiated agency by agency. Aligned to Skills Framework for the Information Age frameworks (SFIA) and APS Professions standards not product certifications. Must include AI governance literacy: how to evaluate supplier sovereignty claims, audit supply chains across the AI stack layers, assess CLOUD Act exposure and govern deployed models.
- **Medium-term:** Co-design of nationally recognised, portable micro-credential pathways with the APS Academy, TAFE, or universities in cloud architecture, data engineering, cybersecurity, agentic AI governance and operational logic design. Capability that survives a model deprecation, vendor repricing, or foreign export control decision.
- **Long-term:** Structural knowledge transfer: open documentation standards, interoperability commitments and transition support ensuring institutional logic stays with the agency, not the platform. The goal is an APS that can substitute any execution layer or model without loss of operational knowledge. Sovereignty cannot be restored on demand. It must be designed in from the start.

What Should Be Publicly Reported

We recommend the DTA requires CCA sellers to report annually on:

- For Tier 1 and Tier 2 sellers: Australian headcount growth, role types created and R&D investment as evidence of the sovereign skill retention dividend. For Tier 2 sellers, disclosure of where knowledge generated through multinational collaboration resides.
- For Tier 3 and Tier 4 sellers: total training hours delivered, split by vendor-specific versus vendor-neutral content the ratio is a direct indicator of whether sellers are building sovereign capability or consolidating ecosystem dependency.
- Number of APS staff trained, by agency and role level and nationally accredited qualifications or micro-credentials delivered.
- Training content mapped against APS Professions standards and SFIA frameworks.

Question 5 — Other matters for the DTA's consideration

Are there any other matters that you consider should be included when the DTA is determining the principles for CCAs? Please feel free to provide your feedback or add your views.

Sovereign Systems of Work as a Mandatory CCA Procurement Category

The preceding answers concern the sellers an agency contracts. We close on the layer beneath that relationship, which the framework does not yet address: an agency's own operating logic, meaning the decisions, sequencing, approval authorities and policy associations that constitute how it functions. This logic exists independently of any system, and historically it has lived in legislation, policy, delegations, procedure and the experience of staff. When an agency undertakes a large platform deployment, an enterprise resource planning system or, increasingly, an artificial intelligence capability, a codified version of that logic is configured into the vendor's system. Where that layer sits inside a foreign-controlled platform, the dependency carries the jurisdictional exposure set out in our response to Question 3.

Beyond the issue of sovereignty, as an agency's operating logic accumulates inside a configured platform which it does not control, and the originating knowledge is not deliberately retained as a separable asset, the agency progressively loses the ability to operate, audit or replace that platform without the vendor. This dependency is well documented in Australian government, and its cost is a matter of public record. The whole-of-government GovERP program, which sought to standardise corporate systems across roughly one hundred agencies on a single enterprise platform, was wound back after expenditure the Minister for Finance described as almost $400 million, and was decommissioned in January 2025.[16] The Queensland Health payroll replacement required over 2,500 system customisations to encode the department's pay rules, affected the pay of tens of thousands of staff, and was estimated by the subsequent Commission of Inquiry to cost in the order of $1.2 billion to rectify and operate over eight years.[17]The Department of Defence is presently consolidating around five hundred applications onto a single enterprise resource planning platform at a cost valued in the billions, a program still in delivery.[18] These programs differ in their particulars, and together they show one pattern: once an organisation's operating logic is concentrated inside a large enterprise platform, substitution becomes slow, expensive and difficult to reverse.

The protection against this is architectural, and we describe it here as a sovereign System of Work. It is a layer that holds an agency's operating logic above and separate from the systems that execute it, under the agency's own ownership and Australian jurisdiction. Its value lies in what that separation makes possible. Execution-layer systems, whether an enterprise resource planning module, an artificial intelligence model or a productivity tool, can be substituted without the operating logic being lost alongside them. The logic itself remains inspectable and governable, which is the condition on which accountable AI deployment depends. The institutional knowledge of how the agency functions is retained as a sovereign asset rather than dispersed among vendors and consultants, and interoperability across systems is preserved because the logic connecting them is held in one governed place.

[16] Digital Transformation Agency, *GovERP Reuse Assessment* (August 2024), dta.gov.au. Finance Minister Katy Gallagher described the program as a costly flop based on "naive ideas about the ability to standardise complex corporate systems" after expenditure of approximately $390 million.

[17] Queensland Health Payroll System Commission of Inquiry, Final Report, The Honourable Richard N Chesterman AO RFD QC (31 July 2013), healthpayrollinquiry.qld.gov.au.

[18] Department of Defence, Defence Enterprise Resource Planning Program, defence.gov.au. Program consolidating approximately 500 legacy applications onto SAP S/4HANA; still in delivery.

The sequence in which this layer is established determines whether it protects anything. To preserve sovereignty over their operating logic, agencies should have a sovereign System of Work in place before they undertake large technology transformations such as enterprise resource planning deployments and artificial intelligence initiatives. Where the layer exists first, those subsequent procurements draw from and reference the agency's own logic, and the vendor systems are configured from it and do not become its only record. Where the layer is absent, each major platform reconstructs the operating logic inside itself, and command of that logic is conceded by default, one deployment at a time.

This points to a specific role for the framework. We recommend the DTA recognise the System of Work as a defined capability within the Australian Government Architecture, so that major enterprise resource planning and artificial intelligence investments, assessed through the Digital and ICT Investment Oversight Framework, are expected to demonstrate that the agency retains a sovereign operating-logic layer. We further recommend the DTA establish a System of Work category within the existing Software and ERP Marketplace, so that sovereign options in this category receive a structured procurement pathway rather than being assessed indirectly, if at all, through procurements scoped around other systems.

Recognised this way, the System of Work is both an architectural foundation and a procurement consideration in its own right. The framework can continue to assess sellers system by system, leaving the more consequential question of who commands an agency's operating logic unasked. The alternative is to make that question explicit, and to give agencies a sovereign means of answering it before their operating logic is committed to systems they do not control.

Closing Remarks

The tier framework, the sovereignty scoring table, the Deed of Sovereignty, the reporting requirements and the Systems of Work procurement category proposed in this submission are not independent measures. They are a single argument made at five levels: that sovereignty is a legal and structural condition, not a contractual one; that the vendor's domicile determines the jurisdiction that follows them through the door; that operational logic is a sovereign asset that must be governed as such; and that the CCA framework is one of the most direct instruments available to make Australian capability the default rather than the exception.

Sovereignty is not a passive state. It can be lost through accumulated deference as surely as through any single decision. The decisions being made in procurement today will define the exposure Australian organisations carry for the next decade. The framework should be designed to find Australian capability and to keep it here.

Appendix D: What Commonwealth AI transparency statements disclose

Method- The Digital Transformation Agency maintains a central register of the AI transparency statements Commonwealth entities publish under the Policy for the responsible use of AI in government. Working from that register, we sought the statement of every entity listed, together with four departments that publish a statement without appearing on it, giving 99 statements sought. We retrieved 73 and coded each against five questions settled before any statement was read:

- Does it name a specific AI system, product or vendor?
- Does it identify the legal entity operating that capability, or its ultimate parent?
- Does it state whether inference is processed in Australia?
- Does it state whether the Commonwealth holds the model weights or merely accesses the model as a service?
- Does it mention foreign jurisdiction, extraterritorial law or compellability in any form?

A general assurance about security, privacy or data residency was not counted as an answer to the third, fourth or fifth question, because none of those assurances identifies who can compel the supplier.

Limits- A statement recorded as not retrieved is not a statement that does not exist. In almost every case the address is known and the page could not be read from our environment. Those rows are excluded from the counts rather than counted as omissions. Seven entities disclose that they use no AI at all; those are marked with an asterisk, since their silence on the later questions means something different from a genuine gap. One entity, the Department of Defence, publishes AI policy settings but no transparency statement we could locate.

Codes are Y for yes and N for no.

The abbreviated column headings are systems, entity, onshore, weights and jurisdiction.

Table 4: Commonwealth AI transparency statements coded against five questions

Entity and statement address	Sys	Ent	On	Wt	Jur
Administrative Review Tribunal www.art.gov.au/ai-transparency-statement	—	—	—	—	—
Attorney-General's Department www.ag.gov.au/about-us/accountability-and-reporting/attorney-generals-department-artificial-intelligence-transparency-statement	—	—	—	—	—
Australian Federal Police www.afp.gov.au/news-centre/feature/artificial-intelligence-ai-transparency-statement	N	N	N	N	N
Australian Financial Security Authority www.afsa.gov.au/about-us/accountability-and-reporting/ai-transparency-statement	N	N	N	N	N
Australian Institute of Criminology www.aic.gov.au/about-us/artificial-intelligence-ai-transparency-statement	N	N	N	N	N
Australian Law Reform Commission www.alrc.gov.au/about/corporate-information/ai-transparency-statement	Y	N	N	N	N
Australian Transaction Reports and Analysis Centre www.austrac.gov.au/about-us/corporate-information-and-governance/reports-and-accountability/austrac-artificial-intelligence-transparency-statement	N	N	N	N	N
Federal Court of Australia www.fedcourt.gov.au/about/corporate-information/ai-statement	N	N	N	N	N
National Anti-Corruption Commission www.nacc.gov.au/ai-transparency-statement	N	N	N	N	N
Office of Parliamentary Counsel www.opc.gov.au/sites/default/files/2025-02/AI Transparency Statement OPC_0.pdf	N	N	N	N	N
Office of the Australian Information Commissioner* www.oaic.gov.au/about-the-OAIC/our-corporate-information/oaic-ai-transparency-statement	N	N	N	N	N

Table 4: Commonwealth AI transparency statements coded against five questions					
Entity and statement address	**Sys**	**Ent**	**On**	**Wt**	**Jur**
Office of the Commonwealth Ombudsman www.ombudsman.gov.au/about/ai-transparency-statement	N	N	N	N	N
Office of the Director of Public Prosecutions www.cdpp.gov.au/about-us/ai-transparency-statement	N	N	N	N	N
Office of the Inspector-General of Intelligence and Security	—	—	—	—	—
Office of the Special Investigator www.osi.gov.au/policy-responsible-use-ai-government-ai-transparency-statement	—	—	—	—	—
Bureau of Meteorology	—	—	—	—	—
Clean Energy Regulator cer.gov.au/about-us/our-policies/artificial-intelligence-transparency-statement	Y	N	N	N	N
Climate Change Authority www.climatechangeauthority.gov.au/artificial-intelligence-transparency-statement	N	N	N	N	N
Department of Climate Change, Energy, the Environment and Water www.dcceew.gov.au/about/commitment/information-public-data/ai-transparency-statement	—	—	—	—	—
Great Barrier Reef Marine Park Authority* www2.gbrmpa.gov.au/artificial-intelligence-ai-transparency-statement	N	N	N	N	N
Asbestos and Silica Safety and Eradication Agency www.asbestossafety.gov.au/ai-transparency-statement	Y	N	N	N	N
Australian Skills Quality Authority www.asqa.gov.au/about-us/governance-and-accountability/artificial-intelligence-ai-transparency-statement	N	N	N	N	N
Department of Employment and Workplace Relations www.dewr.gov.au/artificial-intelligence-dewr/dewr-ai-transparency-statement	—	—	—	—	—
Fair Work Commission www.fwc.gov.au/about-us/artificial-intelligence-transparency-statement	—	—	—	—	—
Office of the Fair Work Ombudsman www.fairwork.gov.au/sites/default/files/2025-02/fwo-ai-transparency-statement.pdf	N	N	N	N	N
Safe Work Australia www.safeworkaustralia.gov.au/about-us/corporate-publications-and-resources/ai-transparency-statement	N	N	N	N	N
Seafarers Safety, Rehabilitation and Compensation Authority	—	—	—	—	—
Australian Electoral Commission www.aec.gov.au/About_AEC/Publications/files/AEC-AI-Transparency-Statement.pdf	Y	Y	N	N	N
Department of Finance www.finance.gov.au/about-us/artificial-intelligence-ai-transparency-statement	Y	N	N	N	N
Digital Transformation Agency www.dta.gov.au/ai-transparency-statement	Y	N	N	N	N
Future Fund Management Agency www.futurefund.gov.au/en/About-us/access-to-information/parliamentary-and-statutory-reporting	N	Y	N	N	N
Independent Parliamentary Expenses Authority	—	—	—	—	—
Parliamentary Workplace Support Service	—	—	—	—	—
Services Australia www.servicesaustralia.gov.au/automation-and-artificial-intelligence-transparency-statement	—	—	—	—	—
Australian Centre for International Agricultural Research www.aciar.gov.au/artificial-intelligence	Y	N	N	N	N
Australian Trade and Investment Commission www.austrade.gov.au/en/site-information/ai-transparency	Y	N	N	N	N
Department of Foreign Affairs and Trade dfat.gov.au/about-us/corporate/artificial-intelligence-ai-transparency-statement	Y	N	N	N	N
Aged Care Quality and Safety Commission www.agedcarequality.gov.au/about-us/corporate-documents/ai-transparency-statement	—	—	—	—	—
Australian Radiation Protection and Nuclear Safety Agency www.arpansa.gov.au/about-us/corporate-publications/arpansas-artificial-intelligence-transparency-statement	N	N	N	N	N
Cancer Australia	—	—	—	—	—
Department of Health, Disability and Ageing www.health.gov.au/about-us/corporate-reporting/our-commitments/ai-transparency-statement	Y	N	N	N	N
National Blood Authority* www.blood.gov.au/nbas-ai-transparency-statement	N	N	N	N	N
National Health and Medical Research Council www.nhmrc.gov.au/about-us/accountability-and-reporting/artificial-intelligence-ai-transparency-statement	Y	N	N	N	N
National Health Funding Body	—	—	—	—	—

Table 4: Commonwealth AI transparency statements coded against five questions					
Entity and statement address	**Sys**	**Ent**	**On**	**Wt**	**Jur**
www.publichospitalfunding.gov.au/about-us/corporate-governance/ai-transparency-statement					
Office of the Inspector-General of Aged Care www.igac.gov.au/resources/artificial-intelligence-ai-transparency-statement	—	—	—	—	—
Organ and Tissue Authority* www.donatelife.gov.au/ai-transparency-statement	N	N	N	N	N
Professional Services Review www.psr.gov.au/artificial-intelligence-ai-transparency-statement	—	—	—	—	—
Sport Integrity Australia www.sportintegrity.gov.au/about-us/corporate/governance/ai-transparency	Y	N	N	N	N
Department of Industry, Science and Resources www.industry.gov.au/publications/artificial-intelligence-transparency-statement	N	N	N	N	N
Geoscience Australia www.ga.gov.au/about/corporate-documents/ai-transparency-statement	Y	N	N	N	N
IP Australia www.ipaustralia.gov.au/About-us (AI Transparency Statement, PDF)	Y	N	N	N	N
Net Zero Economy Authority* www.netzero.gov.au/artificial-intelligence-transparency-statement	N	N	N	N	N
Australian Communications and Media Authority	—	—	—	—	—
Australian Transport Safety Bureau www.atsb.gov.au/ai-transparency-statement	—	—	—	—	—
Department of Infrastructure, Transport, Regional Development, Communications and the Arts www.infrastructure.gov.au/about-us/artificial-intelligence-transparency-statement	Y	N	N	N	N
National Archives of Australia www.naa.gov.au/about-us/who-we-are/accountability-and-reporting/artificial-intelligence-ai-transparency-statement	N	N	N	N	N
National Capital Authority* www.nca.gov.au/nca-artificial-intelligence-ai-transparency-statement	N	N	N	N	N
Department of Parliamentary Services www.aph.gov.au (Department of Parliamentary Services, AI Transparency Statement)	N	N	N	N	N
Department of the House of Representatives www.aph.gov.au (Department of the House of Representatives, AI transparency statement)	Y	N	N	N	N
Department of the Senate www.aph.gov.au (Department of the Senate, AI transparency statement)	Y	N	N	N	N
Parliamentary Budget Office	—	—	—	—	—
Australian National Audit Office www.anao.gov.au/work/corporate/anaos-artificial-intelligence-transparency-statement	—	—	—	—	—
Australian Public Service Commission www.apsc.gov.au/about-us/accountability-and-reporting/transparent-use-ai-commission	—	—	—	—	—
Department of the Prime Minister and Cabinet www.pmc.gov.au/about-us/accountability-and-reporting/corporate-reporting/artificial-intelligence-transparency-statement	N	N	N	N	N
National Indigenous Australians Agency www.niaa.gov.au/artificial-intelligence-ai-transparency-statement-2026	Y	N	N	N	N
Office of the Official Secretary to the Governor-General www.gg.gov.au/sites/default/files/2025-02/OOSGG AI transparency statement 2025.pdf	N	N	N	N	N
Workplace Gender Equality Agency www.wgea.gov.au/about/governance/AI-transparency-statement	N	N	N	N	N
Australian Institute of Family Studies aifs.gov.au/compliance-reporting/ai-transparency-statement	N	N	N	N	N
Department of Social Services www.dss.gov.au/doing-business-us/corporate-policies/artificial-intelligence-ai-transparency-statement	N	N	N	N	N
Domestic, Family and Sexual Violence Commission www.dfsvc.gov.au/resources/our-ai-transparency-statement	N	N	N	N	N
NDIS Quality and Safeguards Commission* www.ndiscommission.gov.au/about-us/corporate-reports/ai-statement	N	N	N	N	N
Australian Bureau of Statistics www.abs.gov.au/about/legislation-and-policy/ai-transparency-statement	N	N	N	N	N
Australian Competition and Consumer Commission www.accc.gov.au/about-us/accc-role-and-structure/governance-and-accountability/artificial-intelligence-ai-transparency-statement	N	N	N	N	N
Australian Office of Financial Management www.aofm.gov.au/about/compliance-reporting/artificial-intelligence-transparency-statement	—	—	—	—	—

Table 4: Commonwealth AI transparency statements coded against five questions					
Entity and statement address	**Sys**	**Ent**	**On**	**Wt**	**Jur**
Australian Prudential Regulation Authority www.apra.gov.au/apras-ai-transparency-statement	Y	N	N	N	N
Australian Securities and Investments Commission www.asic.gov.au/about-asic/what-we-do/how-we-operate/accountability-and-reporting/artificial-intelligence-transparency-statement	N	N	N	N	N
Australian Taxation Office www.ato.gov.au/about-ato/commitments-and-reporting/information-and-privacy/ato-ai-transparency-statement	Y	N	N	N	N
Commonwealth Grants Commission www.cgc.gov.au/about-us/accountability-and-reporting/artificial-intelligence-transparency-statement	—	—	—	—	—
Department of the Treasury treasury.gov.au/the-department/accountability-reporting/ai-transparency-statement	Y	N	N	N	N
Inspector-General of Taxation taxombudsman.gov.au/wp-content/uploads/2026/03/AI-transparency-statement-March-2026.pdf	Y	N	N	N	N
National Competition Council ncc.gov.au/about/statutory_andrequired_reporting	N	N	N	N	N
Office of the Auditing and Assurance Standards Board www.auasb.gov.au/about-auasb/artificial-intelligence-ai-transparency-statement	Y	N	N	N	N
Office of the Australian Accounting Standards Board aasb.gov.au/about-the-aasb/artificial-intelligence-ai-transparency-statement	Y	N	N	N	N
Productivity Commission www.pc.gov.au/ai-transparency	Y	N	N	N	N
Royal Australian Mint www.ramint.gov.au/sites/default/files/2025-04/royal_australian_mint_ai_transparency_statement.pdf	N	N	N	N	N
Australian Digital Health Agency www.digitalhealth.gov.au/about-us/policies-privacy-and-reporting/artificial-intelligence-transparency-statement	Y	N	N	N	N
Australian Institute of Health and Welfare www.aihw.gov.au/about-us/our-governance/ai-transparency-statement	N	N	N	N	N
Healthdirect Australia www.healthdirect.gov.au/artificial-intelligence-transparency-statement	Y	N	N	N	N
Food Standards Australia New Zealand www.foodstandards.gov.au/about-us/corporate-information/ai-transparency-statement	N	N	N	N	N
National Offshore Petroleum Safety and Environmental Management Authority www.nopsema.gov.au/about/ai-transparency-statement	N	N	N	N	N
Commonwealth Scientific and Industrial Research Organisation www.csiro.au/en/about/Policies/Artificial-Intelligence-Statement	N	N	N	N	N
Screen Australia www.screenaustralia.gov.au/corporate-documents/policies/ai-transparency-statement	Y	N	N	N	N
National Library of Australia www.library.gov.au/visit/about-us/corporate-information/corporate-strategies/artificial-intelligence-ai-transparency	N	N	N	N	N
Australian Maritime Safety Authority www.amsa.gov.au/about-us/who-we-are/ai-transparency-statement	N	N	N	N	N
Infrastructure Australia www.infrastructureaustralia.gov.au/transparency-statement-use-artificial-intelligence-ai	N	N	N	N	N
Department of Home Affairs www.homeaffairs.gov.au/commitments/files/ai-transparency-statement.pdf	N	N	N	N	N
Department of Agriculture, Fisheries and Forestry www.agriculture.gov.au/about/reporting/obligations/AI-transparency-statement	N	N	N	N	N
Department of Education www.education.gov.au/about-department/corporate-reporting/artificial-intelligence-ai-transparency-statement	—	—	—	—	—
Department of Defence no statement located	—	—	—	—	—