scyne

Submission by Scyne Advisory to Horizon 2 of the

Australian Cyber Security Strategy 2023-2030 Discussion Paper

Date

29 August 2025

scyne

Contents

Executive Summary

Who we are

1 Whole of State Cyber Operating Model

Our response to the question: *Are there initiatives or programs led by State or Territory governments you would like to see expanded or replicated across other levels of government?*

2 Foreign Ownership, Control & Influence Advice

Our response to the question: *What additional guidance do you or your organisation need to manage foreign ownership, control or influence risks associated with technology vendors?*

3 Artificial Intelligence Standard Testing Framework

Our response to the question: *What guidance can government provide to support the safe and responsible uptake of critical and emerging technologies?*

4 Cyber Crisis Simulation Learnings

Our response to the question: *Are the roles and responsibilities of government and industry clear for cyber security in a conflict or crisis scenario? What activities, such as cyber crisis simulation exercises, could Government undertake to make you feel better prepared to respond in a cyber conflict or crisis?*

Key Contacts

Expert Advisory Board
2023-30 Australian Cyber Security Strategy
c/- Department of Home Affairs
Australian Government

29 Augu st 2025

Department of Home Affairs,

We appreciate the opportunity to provide feedback on the Commonwealth Cyber Security Policy Consultation Package. As Australia's largest dedicated public purpose advisory firm, Scyne Advisory specialise in supporting our government institutions to build more resilient, secure, equitable and prosperous communities. Supporting Australia in becoming one of the world's most cyber secure nations by 2030 is closely aligned with our purpose as a company.

Scyne Advisory is proudly Australian owned and operated, with a clear focus on protecting Australian interests. We are conflict-free from the for-profit private sector, ensuring that our advice is always impartial and aligned with the public good. Our team of nearly 1,000 public purpose specialists brings together expertise from diverse fields, harnessing technology and innovation to tackle complex challenges and deliver the best solutions for our government clients.

Given our unique position and industry perspective, we have selected a small number of questions to respond to where we feel our insights will be more impactful. Four of the senior leaders in our national Cyber practice have provided their insights into four questions most aligned with our areas of expertise and day-to-day work. These leaders include:

- [redacted], outlining how State and Territory governments are unlocking collaboration and significant cyber improvements through whole of government cyber operating models;
- [redacted], exploring our experience in supporting Commonwealth departments assess FOCI risks;
- [redacted], discussing building trust in emerging technologies and addressing AI sentiment; and
- [redacted], outlining our learnings from running dozens of cyber crisis simulations across all levels of government.

Our submission reflects our deep understanding of the current challenges faced by government departments and agencies in navigating the cyber threat and we trust will provides meaningful insights into strengthening the Commonwealth Cyber Security Uplift approach.

Yours sincerely,

[redacted]

Who we are

Scyne is proudly Australian owned and operated, with a clear focus on protecting Australian interests. We are conflict-free from the for-profit private sector and bring independent, impartial advice and solutions to our clients. This unique position ensures our work is always aligned to the public good.

We are a trusted partner across federal and state governments, bringing deep experience in supporting agencies to strengthen their cyber resilience. We have a clear understanding of the complex challenges facing the public sector, and equally, we see the immense potential that can be achieved by tackling these challenges.

We are deeply familiar with the threats confronting Australia today. Our insights are drawn directly from assisting government agencies in managing ongoing cyber risks. This experience gives us a practical understanding of the threat environment, and the steps needed to protect vital public functions against emerging challenges.

> The mission of our Cyber practice is to increase public trust and participation in government digital services; a key driver in improving Australia's productivity, equality, resilience and prosperity.
>
> We bring scale and expertise across all phases of cyber transformation covering advisory and assurance, AI & data governance, workforce & skills transformation, technology implementation and ongoing security operations.

Whole of State Cyber Operating Models

Are there initiatives or programs led by State or Territory governments you would like to see expanded or replicated across other levels of government?

Governments worldwide are grappling with the escalating threat of cyber incidents as they attempt to navigate the increasingly complex landscape of digital vulnerabilities. However, the interconnected nature of government operations and their underlying infrastructure adds a further level of complexity when compared to private sector companies that largely need to only worry about themselves. Australia's state governments represent large, sprawling ecosystems of hundreds of departments and agencies, often connected by shared infrastructure and hamstrung by constrained cyber budgets.

For the past decade, most state government departments and agencies have largely tried to 'go it alone' on cyber security, which has undermined two notable advantages our state governments have:

1. The ability to easily share scarce cyber resources and consume central services for economies of scale; and

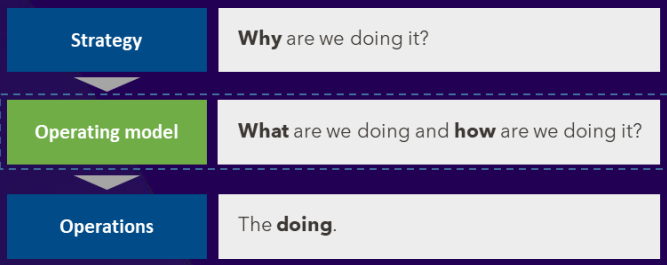
2. The considerable purchasing power of operating as a single conceptual entity at this scale.

This presents significant opportunity for aligning around a shared, **whole-of-state cyber operating model** to drive collaboration and generate budget savings.

Recently, Scyne has worked with a number of the state governments on whole-of-state cyber operating models, from concept and design right through to implementation of at-scale central and federated cyber services. We are now seeing the significant impact of these operating models coming online and the noticeable improvement in coordination and quality of state cyber capabilities, and we believe a similar initiative would have the same impact at a Commonwealth level.

The context for change

In simple terms an operating model provides the bridge between strategy and the day-to-day operations:



There are a range of current challenges across Australian state governments in managing cyber security:

- **Fragmented approaches to cyber security:** As state departments and agencies are individually governed, cyber security is often managed in silos without a statewide view of the most important information and services, and how to best protect them.
- **Ineffective collaboration and ways of working across the cyber workforce:** There is currently a lack of clarity, consistency and effectiveness in cyber risk management practices which results in agencies being unaware of the risk they carry and their responsibilities.
- **Aged legacy technology:** Many departments are hosting legacy technologies, sometimes 20+ years old, that continue to provide vital citizen services and are increasingly vulnerable to cyber attacks. However, security and replacement of these assets are still largely managed by individual departments/agencies.

These same challenges are prominent in the Commonwealth departments and agencies, with the added complexity of what role the Commonwealth should play in supporting the states, territories and private sector with cyber services and capabilities for the overall protection of the country.

Whole of State Cyber Operating Models

Whilst most states have now formed a central cyber security capability to tackle whole-of-state challenges, there are significant hurdles for these teams in driving meaningful whole-of-state change. This commonly includes a lack of clarity on the roles and responsibilities between agencies and the centralised functions, and the services provided by the central cyber capability. This is causing either duplication of effort, or more concerningly, actions not being taken.

In addition to duplication of effort, an unclear view of the roles and responsibilities of agencies and central cyber teams hinders the government's ability to operate as a cohesive group with a strong collegiate culture. Without a clear overarching view of what is being done, who is responsible and what the gaps are, it has been found that agencies may assume that central teams and/or suppliers are providing more protection against cyber incidents than is the case. This could consequently have an impact on the government's ability to detect and respond to cyber incidents in a timely and coordinated manner.

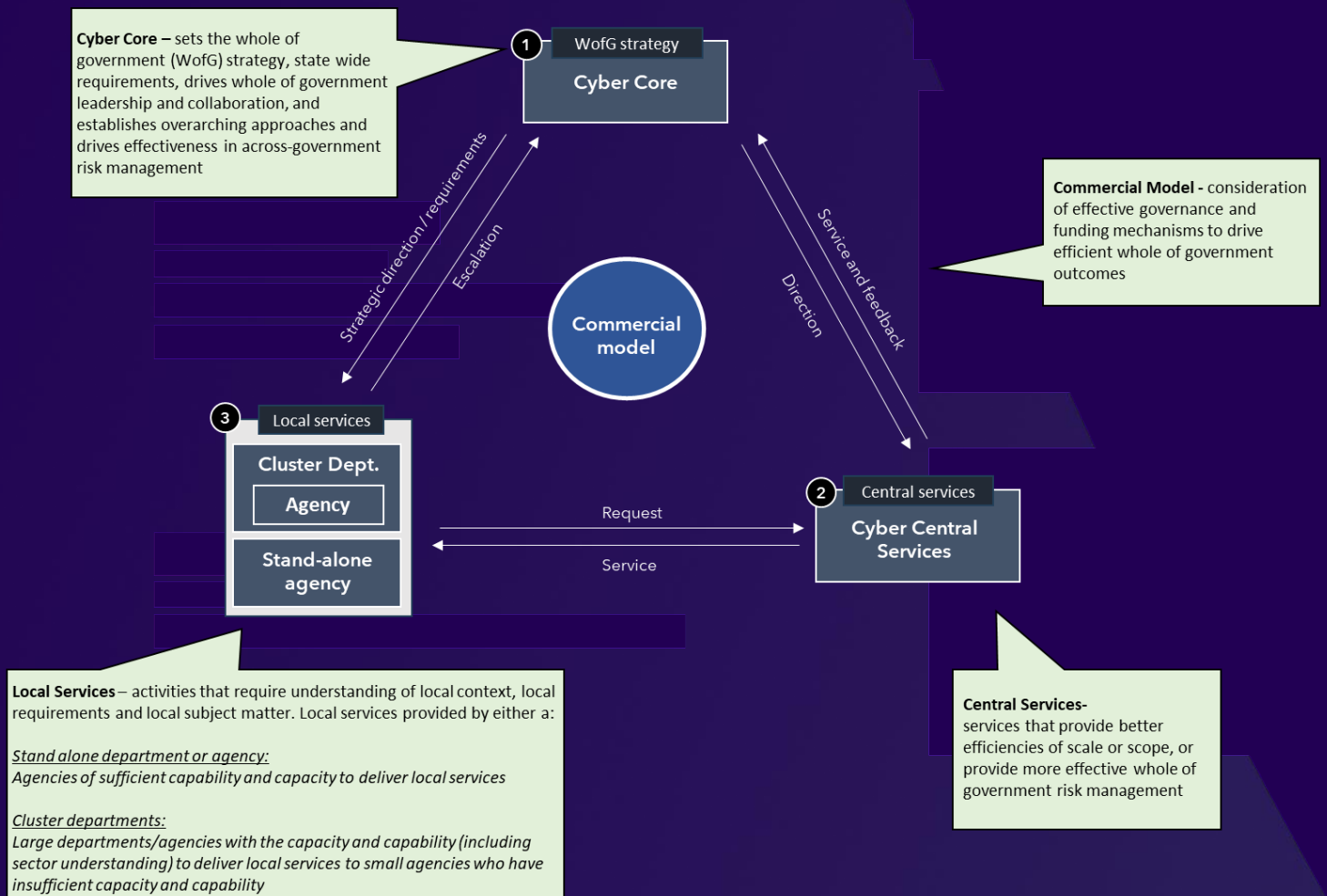
Operating model architecture and roles

To address current challenges, Scyne has been supporting state governments with a methodological approach to the design of key elements of a future state Whole of Government Cyber Security Operating Model. The objectives of these programs are to:

1) Drive clarity on the roles and responsibilities of stakeholders (including across government and third parties) in providing cyber security services

2) Drive efficiency and effectiveness in the way cyber security services are delivered by relevant stakeholders (including across government and third parties)

The basic operating model architecture defines three (3) layers (Core, Central, and Local) and is illustrated below.



Whole of State Cyber Operating Models

Defining the future state

With this basic architecture in mind, defining a whole of government cyber operating model then follows a sequential process.

1) Cyber activities taxonomy

This requires summarising the high level key cyber activities that happen day-to-day in securing the state. This is best informed by the state's current cyber security framework (e.g. VPDSF, SACSF, etc.), legislation and central directives.

2) Design principles

A set of principles are defined to inform clarity in the allocation of cyber security services activities. Common principles include:

- Cyber Core defines key strategic considerations that impact whole-of-government including strategy, requirements, governance and major investment. **This means clarity and consistency of direction and requirements.**
- Common activities and services are performed centrally at scale. **This means avoided duplication of common activity.**
- Activities that strengthen whole-of-government risk management relating to systems of state significance are managed centrally. **This means greater visibility of critical assets.**
- Activities that require local context, or relate to local requirements, or require sector-related subject matter are provided locally. **This means agencies are provided the appropriate level of relevant support locally aligned to their requirements.**

3) Delineate roles and responsibilities

Each activity in the taxonomy is run through a decision tree based on the design principles, resulting in that activity being allocated to a layer in the operating model (i.e. Core, Central Services, or Local Services).

4) Define RACIs for each activity in the taxonomy

Applying the design principles to each activity also defines the RACI across each cyber domain within the taxonomy. This is done collaboratively with cyber leaders from across the state government to appropriately challenge and reach consensus for the accountability and responsibility of each cyber activity within the model.

5) Define and implement service catalogues

Filtering the aggregated RACIs on the 'responsibility' column ultimately then defines the service catalogue for each later in the operating model. This provides clarity for each layer in terms of their responsibilities in making the model work, and where to target investment and capability maturity. Across the states this is typically resulting in:

- **Cyber Core** focusing on the cyber strategy and requirements, governance structures and leadership culture, and the rolled-up view of the highest cyber risks for the state.
- **Cyber Central Services** focusing on cyber capabilities that can optimise the deployment of scarce resources or deliver economies of scale cyber services such as threat intelligence, attack surface management, and third-party risk insights.
- **Local Services** focusing on activities that require local context or sector specific subject matter expertise such as risk management, platform security, or security operations.

Why replicate or expand this approach?

The states that have embraced a whole of government cyber operating model are already seeing significant benefits. Common feedback includes:

- Less conflict and more collaboration, as every organisation is clear on their role in the operating model and the cyber capabilities, they need to invest in.
- Ease in approving cyber investment funding, as any budget bids for cyber capability that don't align with the operating model are simply rejected.
- Commonality across governance models in agencies and in cyber role descriptions across the state, driving more respectful and aligned cyber communities.
- Better alignment with the technology trend around platform consolidation, which aligns with the increased delivery of central cyber services and cluster/portfolio department shared services.

Whole of State Cyber Operating Models

- Better partnerships with industry due to more predictable and stable spend into a set of well-defined capabilities, rather than the patchwork of often small and duplicative procurements that currently dominate the market.

An Australian cyber operating model

The challenges experienced by the states and territories resonate at the Commonwealth level too, where collective general cyber maturity has remained stubbornly slow. And whilst there are governance arrangements in place for interactions between the Commonwealth and state/territory cyber teams such as the Cyber Incident Management Arrangements (CIMA), these largely revolve around sharing threat intelligence and responding to incidents once they've happened.

The states and territories are getting themselves organised now, and commonality is forming in their structures, cyber service catalogues and ways of working. Whilst the Commonwealth has made significant and much needed progress on the legislative policy front, its role in supporting states and territories outside of central incident coordination remains unclear.

In the meantime, we continue to have individual cyber security frameworks and policies on a state-by-state basis which still differ significantly from the Commonwealth standards. In a game where the weakest link in the chain is where the attack will come from, our chains are not even joined together. The need to comply with a patchwork of cyber frameworks also increases the cost of service delivery for organisations that partner with federal, state and territory government entities.

As stated above, an operating model traditionally follows the strategy to answer the question of 'what are we doing and how are we doing it?' We would like to see the Commonwealth emulate the significant progress the states are making around cyber operating models, if anything to be clear about the role it will play and the services it will provide in the collective defence of our government institutions.

2 Foreign Ownership, Control or Influence Advice

What additional guidance do you or your organisation need to manage foreign ownership, control or influence risks associated with technology vendors?

Australia's economy is built on globally integrated supply chains. While these deliver efficiencies, they also introduce systemic risk, particularly where suppliers are subject to foreign ownership, control and influence (FOCI) that could be leveraged to compromise national security, data sovereignty or the integrity of essential services.

The Australian Government has taken important steps in recognising this threat. **The Protective Security Policy Framework (PSPF)** [1] forms the foundational set of protective security standards for Australian Government entities to implement. The **Technology Vendor Review Framework** [2] provides a structured, risk-based model for evaluating technology vendors, particularly in critical and government contexts. These approaches are complemented by guidance from the Australian Signals Directorate (ASD) on **cyber supply chain security** [3], and broader **Critical Technology Supply Chain Principles** [4], which promote transparency, trust and resilience.

However, as these frameworks and guidance mature, many organisations lack clear operational guidance, tools and scalable mitigation models. This is an opportunity to support embedding consistent and proactive FOCI risk management processes.

Understanding FOCI Risk in the Australian Security Landscape

FOCI risk goes beyond direct foreign ownership. Risk can occur through less transparent or indirect channels, such as overseas subsidiaries or foreign legal jurisdictions requiring access to data or systems, no matter location.

Strategic influence is another parameter to consider. Third-party supplier decision-making may be indirectly influenced by foreign state interests. Suppliers may have interests aligned with foreign governments, compromising supply chain integrity.

Manufacturing and design may introduce hardware or software vulnerabilities. Every interaction with suppliers introduces inherent cyber risks; they may be unintentional but can still be exploited.

Many modern service delivery models rely on outsourced or offshore resources. This may lead to exposure of offshore access, remote administration, or non-sovereign data hosting[5]. This can introduce overseas jurisdictional exposure, potentially without transparency.

Real-World Example: Microsoft's "Digital Escort" Model and FOCI Risk Exposure

For nearly a decade, Microsoft operated a low-profile "digital escort" program to support sensitive U.S. Defence Department cloud systems while relying on foreign engineers, including those based in China. Since these engineers were not permitted to access sensitive data directly, Microsoft employed U.S.-based personnel with security clearances to act as intermediaries. These escorts received instructions from overseas experts and executed commands on government systems, often without fully understanding their technical implications. While intended as a workaround for clearance restrictions, the model created an indirect channel of influence that introduced a significant FOCI risk.

1 Australian Government Protective Security Policy Framework Guidelines, Department of Home Affairs, 2025 https://www.protectivesecurity.gov.au/system/files/2025-07/pspf-release-2025.pdf
2 Technology Review Vendor Framework, Department of Home Affairs, 2024 https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/technology-and-data-security/technology-vendor-review-framework
3 Identifying Cyber Supply Chain Risks, Australian Signals Directorate, 2024, https://www.cyber.gov.au/resources-business-and-government/maintaining-devices-and-systems/outsourcing-and-procurement/cyber-supply-chains/identifying-cyber-supply-chain-risks
4 Critical Technology Supply Chain Principles, Department of Home Affairs https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/critical-technology-supply-chain-principles
5 Guidelines for Procurement and Outsourcing, Information Security Manual, https://www.cyber.gov.au/sites/default/files/2025-07/05.%20ISM%20-%20Guidelines%20for%20procurement%20and%20outsourcing%20%28June%202025%29.pdf

Foreign Ownership, Control & Influence Advice

Real-World Example (Cont.)

Security experts and former officials later raised concerns that the escort model could enable foreign adversaries to insert malicious code or manipulate systems without detection. Despite Microsoft's assurances that audit logs and oversight controls were in place, some former Department leaders were unaware the program existed, revealing a lack of transparency and oversight. This case highlighted how global workforce models, even those technically compliant, could unintentionally bypass safeguards meant to protect sensitive government data from foreign influence [6].

Key Insights

Drawing on our experience supporting governments with FOCI risk management, several observations emerge:

- **Limited Maturity in FOCI Risk Governance:** Despite growing awareness, agencies exhibit underdeveloped frameworks for identifying, assessing, and mitigating FOCI risks. There is fragmented accountability, insufficient visibility into foreign influence vectors and a lack of sustained mitigation strategies, leaving critical vulnerabilities unaddressed.

- **Disjointed Treatment of FOCI and Supply Chain Risk:** FOCI risks are frequently siloed from broader supply chain risk management efforts. Effective resilience requires foreign influence considerations be embedded across the supply chain lifecycle, from vendor onboarding to decommissioning, to ensure comprehensive coverage and early detection.

- **Downstream Supply Chain Influence:** Sub-tier suppliers and service providers often possess or exert control over essential components, systems, or data flows without adequate scrutiny. These hidden dependencies can compromise FOCI controls and introduce latent risks that evade traditional oversight mechanisms.

- **Misalignment Between Procurement and Cyber Security Functions:** A recurring operational gap exists between procurement teams, who typically prioritise cost and functionality, and cyber security stakeholders, whose input is often solicited too late in the acquisition process. This disconnect results in incomplete vendor risk assessments and missed opportunities to preemptively address FOCI-related concerns.

- **Need for Continuous Monitoring and Automation:** FOCI risk management cannot rely on static, point-in-time assessments. Dynamic monitoring enabled by automation and advanced analytics is essential to maintain situational awareness of ownership changes, geopolitical shifts, and emerging threats across the supply chain ecosystem.

- **Broadening the Scope of FOCI Risk Posture:** A robust FOCI strategy must extend beyond ICT supply chains to encompass non-digital assets, including operational technologies, physical infrastructure, and support services. This holistic view ensures that all vectors of foreign influence are considered in risk mitigation planning.

- **Many agencies do not have funding or access to suitably qualified or experienced personnel to manage FOCI risks on an ongoing basis.** FOCI risk management requires sustained resourcing to support continuous monitoring, vendor reassessments and responding to emerging threats.

Key Recommendations

The Australian Government has the opportunity to take an enabling role to ensure industry can effectively identify and mitigate FOCI risks, particularly where capability gaps exist or the procurement lifecycle is complex:

- The Australian Government has made positive inroads to protect Agencies through the Technology Vendor Review Framework. However, this is not a publicly accessible version of this framework. By releasing a **simple and available version of the framework** will enable industry to apply consistent risk assessment processes, without the need to access sensitive data.

- To reduce complexity and promote adoption, the Australian Government **should integrate FOCI considerations into existing cyber security frameworks.** Embedding these controls into widely adopted standards such as the PSPF, the Information Security Manual (ISM) and ISO27001 will streamline implementation and consistency in approach.

- **Create and maintain a centralised database of vendors** assessed for elevated FOCI risks to reduce duplicated vetting across government and industry.

Foreign Ownership, Control & Influence Advice

- Provide model procurement clauses **within established Government panels** that address FOCI concerns such as offshore data access, subcontractor transparency, and ownership change notifications, to assist organisations in formalising FOCI protections, even with limited legal resources.
- **Provide clear and consistent guidance on reporting suspected foreign influence or interference** through technology vendors. This includes defined risk thresholds, escalation pathways, and protections for vendors acting in accordance with good FOCI practice. This approach creates timely and appropriate responses in the reporting process.
- **Strengthen international coordination on vendor risk management and FOCI intelligence** sharing by actively engaging with trusted international partners[7] engaging with trusted partners such as Five Eyes alliance (United States, United Kingdom, Canada and New Zealand), as well as the European Union, Japan and regional allies through ASEAN or APEC forums, Aligning with global best practices and regulatory approaches, such as the EU Digital Operational Resilience Act (DORA)[8] and UK supply chain policies, will enhance Australia's visibility of emerging threats and support consistent cross-border supply chain efforts.

Strengthening Internal Controls

While the Australian Government provides essential oversight and regulatory frameworks to manage FOCI risks, it is equally important for industry to take proactive steps internally, through governance, education, and ongoing monitoring, to strengthen their own FOCI risk posture.

Control mechanisms can include:

1. Adopt automation tools to screen for FOCI risks.
2. Incorporate FOCI risk clauses into contracts, such as data location, subcontractor transparency, and termination clauses based on changes in foreign control.
3. Align the Procurement and Cyber Security teams on FOCI responsibilities.
4. Conduct FOCI risk analysis over the lifecycle of the vendor, not just at procurement but at regular phases throughout engagement.
5. Provide relevant training and awareness, not just for those responsible for immediate FOCI risks, but throughout the organisation.
6. Align internal practices with national cyber security standards by applying ISM/PSPF/Essential Eight as a baseline and address FOCI considerations within governance processes and risk assessments.
7. Develop internal policies for identifying, escalating, and reporting suspected foreign influence or interference in relation to vendors.
8. Ensure there is an accurate inventory of all ICT systems across the entity to ensure that cyber security and FOCI risks can be properly tracked and assessed.

7. Department of Defense looks to collaborate on technology supply chain with 'Five Eyes' allies, https://connect.na.panasonic.com/blog/toughbook/dod-looks-to-collaborate-on-technology-supply-chain-with-five-eyes-allies
8. Digital Operational Resilience Act: https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/digital-operational-resilience-act-dora
9. UK Critical Imports and Supply Chains Strategy: https://www.gov.uk/government/publications/uk-critical-imports-and-supply-chains-strategy

3 Promote trust and enable innovation with emerging technology

What guidance can government provide to support the safe and responsible uptake of critical and emerging technologies?

As an organisation dedicated to public good projects, our work around **data and AI governance** span's digital identity, national infrastructure, consumer data rights, artificial intelligence, and safety frameworks. While our internal review of the consultation identified a broad range of opportunities on this topic, including governance, transparency, interoperability, risk management, and community engagement, we have chosen to focus the response to this question on four areas we believe are most critical to national interest and public trust.

These are:

1. Building public trust and addressing AI sentiment
2. Infrastructure and data ecosystems,
3. Developing skills and talent
4. Encouraging commercialisation and widespread adoption.

Together, these pillars form a cohesive strategy for enabling safe, inclusive, and economically beneficial technology deployment across Australia. We also outline key national security risks associated with emerging technologies, particularly AI, and recommend targeted government interventions to mitigate these risks while fostering innovation.

Building Public Trust and Addressing AI Sentiment

Public trust is a strategic asset in the deployment of emerging technologies. In Australia, recent surveys show **that only 36% of Australians[10] feel confident that AI will be used responsibly** by government and industry. In a global study, only 30% of Australians believed AI's benefits outweigh the negatives, compared to 73% globally[11]. This trust deficit is exacerbated by opaque decision-making, limited public understanding, and growing concerns about bias, surveillance, and job displacement.

These concerns are shared across both metropolitan and regional communities. In urban centres, fears about algorithmic bias, misinformation, and the erosion of privacy are prominent. In regional areas, these are compounded by historical underinvestment in infrastructure and services, and a perception that technology is imposed rather than co-developed.

To address these issues, government must take a proactive and inclusive approach to public engagement. This includes embedding **public awareness campaigns** in support of AI adoption in government service delivery. Awareness campaigns accompanying new or improved AI-enabled government services should:

- Explain the purpose and benefits of AI in government services in plain language.
- Address common misconceptions and fears, including those related to surveillance and automation.
- Promote ethical safeguards and government oversight to reassure the public that AI is being introduced responsibly.

Campaigns should be delivered through multiple channels and tailored to different demographics, including culturally and linguistically diverse communities. They should also include interactive formats such as webinars, community forums, and digital learning modules to reach a wide audience and encourage dialogue.

Government leadership is crucial to shift the narrative towards trust and opportunity. To build trust at the local level, government should support community-led pilots and transparent engagement processes. For example, in Orange, NSW, the local council's co-design of a sensor-enabled waste system with residents led to higher public acceptance and improved outcomes[12].

10. AI Trust in 2025: What Australians think and how businesses can build it - Agile Insights
11. KPMG, Trust, attitudes and use of artificial intelligence, Trust, attitudes and use of artificial intelligence
12. Orange Case Study – Local Government NSW December 2014 - orange-waste-project-orange.pdf

Promote trust and enable innovation with emerging technology

Highlighting AI's role in solving everyday problems is key. Many Australians already unknowingly benefit from AI through use of commonplace technologies including spam filters and navigation apps with little controversy. In Dubbo[13] and Wagga Wagga[14], AI-powered "smart city" solutions such as irrigation systems that adjust to soil moisture and air quality sensors for bushfire smoke have demonstrated that AI can be a practical, non-threatening tool. These examples show that when AI is deployed to meet local needs, it is more likely to be embraced.

Government should also expand AI literacy programs in regional areas. The CSIRO's "Introduction to AI" micro skills course[15], which offers **one million free AI training scholarships**, is a strong start. Ensuring that regional Australians have equal access to these programs, through local TAFEs, libraries, and community centres, will help demystify AI and empower communities to engage with it confidently.

Finally, ethical safeguards must be visible and reassuring. Voluntary standards, transparent labelling of AI-generated content and AI-supported decision-making, and public oversight mechanisms should be promoted nationally. This includes funding local councils and agencies to run AI pilots with ethical review and community consultation, ensuring that diverse voices shape the rollout of emerging technologies.

Infrastructure and Data Ecosystems: Foundations for Safe Tech Uptake

Emerging technologies like artificial intelligence (AI) require robust infrastructure and trusted data ecosystems. Without equitable access to high-speed internet, smart devices, and reliable power, the benefits of AI and other technologies risk being unevenly distributed, deepening divides between metropolitan and regional communities. A recent ASPI report[16] highlights that "cloud infrastructure, such as undersea cables, is now a strategic national asset. Its security, interoperability and governance are becoming critical tests of sovereignty and trust."

The **government's Digital Economy Strategy 2030** identified significant gaps in broadband access, particularly in regional and remote areas. While the expansion of the National Broadband Network (NBN) and the Regional Connectivity Program have begun to address these disparities, more targeted investment is needed to support "last-mile" connectivity including wireless broadband for farming districts and low-earth-orbit satellite internet for remote communities. These investments are not just about inclusion; they are essential for enabling regional innovation and ensuring national resilience.

Government should also support shared digital infrastructure such as public Wi-Fi, local data networks, and smart utility platforms, that lower the barrier for SMEs and startups to deploy technology in both regional and urban areas. Local councils can be empowered to lead these initiatives, with federal support for planning, procurement, and training.

Cyber security is another critical pillar. The Australian Cyber Security Centre reported **a 23% increase in cyber incidents in 2023**, many targeting critical infrastructure and AI systems. As technologies become more autonomous and integrated into essential services, the potential for malicious exploitation grows. Government should strengthen cyber security capabilities across public and private sectors, including through threat modelling, incident response planning, and workforce development.

The convergence of cloud and 5G technologies is accelerating risk exposure. ASPI warns that "The expanded reliance on cloud infrastructure and 5G networks creates a significantly larger attack surface for cyber adversaries"[7]. This reinforces the need for secure-by-design principles and coordinated threat intelligence sharing.

13. Smart Irrigation Management for Parks and Cool Towns – Digital NSW November 2022 - Smart Irrigation Management for Parks and Cool Towns | Digital NSW
14. How smart cities can improve air quality – Green City Times - IoT Tech for Air Quality in Smart Cities | Green City Times
15. One million 'Introduction to AI' scholarships available to Australians – CSIRO March 2024 - One million 'Introduction to AI' scholarships available to Australians – CSIRO
16. Hyperscale cloud and shared security in the Indo-Pacific - Hyperscale cloud and shared security in the Indo-Pacific: Views from The Strategist

Promote trust and enable innovation with emerging technology

Data governance is equally vital. Many organisations lack the tools and frameworks to share data safely and effectively. Concerns around **data sovereignty**, especially when sensitive Australian data is stored offshore, have prompted calls for stronger national standards. The Consumer Data Right (CDR) initiative has made progress in enabling secure data sharing, but uptake remains limited outside the financial sector.

To support innovation while protecting privacy, government should **promote privacy-preserving technologies** such as federated learning, differential privacy, and synthetic data generation. These approaches allow data to be used for training AI models without exposing individual records, enabling safe collaboration across sectors.

A cautionary example is the rollout of **the My Health Record** platform. While the system offers significant potential for improving health care outcomes through greater availability of clinically relevant data, early missteps in consent management and transparency led to public backlash and reduced participation. This case highlights the importance of building trust through clear governance, opt-in models, and robust privacy protections. It also underscores the need for government to lead by example in deploying emerging technologies responsibly.

Government-held datasets, such as geospatial, environmental, and health data, should be made available in standardised formats to support innovation. For example, anonymised agricultural data could help farmers use AI for precision farming, while open transport data could support smart mobility solutions in cities. Public-private data partnerships, supported by clear governance frameworks, can unlock new opportunities for both economic and social benefit.

Finally, infrastructure planning must consider climate resilience and sustainability. As data centres and digital services expand, their energy and water demands must be managed responsibly. Government guidance should include standards for energy efficiency, renewable integration, and water conservation particularly in regions facing resource constraints.

By investing in inclusive infrastructure and trusted data ecosystems, government can ensure that the benefits of emerging technologies are not just concentrated in metropolitan centres but deployed to solve real problems across the country. This approach supports innovation, strengthens national security, and ensures that all Australians- regardless of location- can benefit from the digital transformation.

Developing Skills and Talent for the Emerging Tech Revolution

Australia's ability to harness emerging technologies depends on a skilled, adaptable, and diverse workforce. Yet current indicators suggest a widening gap between demand and supply. The National Skills Commission reports that demand for AI and data science roles has grown by 38% over the past two years, while the available talent pool remains constrained. Without targeted support, this gap risks undermining Australia's competitiveness and deepening digital inequality- particularly between metropolitan and regional communities.

The projected growth of AI-related jobs- from 33,000 today to 200,000 by 2030- must be matched by a coordinated national effort to build capability across all regions and sectors. This includes both high-skill roles in AI development and broader digital literacy for the general workforce.

Government should expand tertiary education and vocational training in priority fields such as AI, cyber security, data analytics, and digital ethics. This expansion must include regional centres, with funding for TAFEs and universities to offer relevant courses locally. Micro-credentials and online learning platforms should be tailored to regional contexts, supported by digital access, mentoring, and flexible delivery models.

Programs like the CSIRO's AI scholarships[4] must be actively promoted in regional areas, with local delivery partners to ensure uptake. Similarly, industry PhDs and apprenticeships should be extended to regional industries- such as agriculture, mining, and tourism- where emerging technologies can have transformative impact. These programs should be designed to support cross-disciplinary learning, integrating technical, legal, and social dimensions of technology.

Promote trust and enable innovation with emerging technology

Case studies from South Australia's Australian Institute for Machine Learning (AIML)[15] show how strategic clustering of research and industry can create local tech ecosystems. AIML has attracted global companies and fostered startups by aligning academic excellence with commercial opportunity. Government should replicate this model in regional centres, supporting innovation precincts that bring together education, industry, and community. For example, a regional AI hub focused on AgTech could drive job creation and skills development in farming communities.

Skilled migration programs should also be leveraged to address immediate gaps. The Global Talent Visa and upcoming National Innovation Visa can be used to attract experts to regional areas, supported by incentives such as housing, relocation assistance, and community integration programs. These placements should be aligned with local industry needs and supported by regional employers and councils.

Digital literacy must be embedded in schools and community programs across Australia. Coding clubs, STEM grants, and AI competitions should be scaled to reach under-resourced schools and communities, ensuring that the next generation of Australians- regardless of location- is tech-savvy and innovation-ready. This includes targeted outreach to underrepresented groups, including women, Indigenous Australians, and culturally and linguistically diverse communities.

Finally, government should incentivise continuous learning across the workforce. Subsidies for professional development, tax deductions for training, and employer-led upskilling programs can help mid-career professionals adapt to technological change. Specific support should be provided to SMEs and older workers, who may face greater barriers to accessing training.

By investing in skills and talent development nationally and equitably, government can ensure that Australia has the human capital to lead in emerging technologies. This approach supports innovation, inclusion, and resilience- ensuring that all Australians can participate in and benefit from the digital transformation.

Encouraging Commercialisation and Widespread Adoption

Australia has world-class research capabilities but continues to face challenges in translating innovation into commercial success. The Global Innovation Index ranks Australia 25th in innovation outputs, despite being 10th in inputs- highlighting a persistent gap between research and real-world impact. This gap is particularly acute in regional areas, where startups and SMEs often face greater barriers to accessing capital, customers, and technical expertise.

To realise the full benefits of emerging technologies, government must foster an environment that supports innovation, responsible commercialisation, and widespread adoption across all regions. This includes targeted support for early-stage ventures, streamlined regulatory pathways, and stronger public-private partnerships.

Programs like the AI Adopt Program[16] have shown promise in helping SMEs integrate AI into their operations. Expanding these programs to target regional businesses- through local chambers of commerce, councils, and business incubators- can help scale adoption. For example, an AI Adoption Centre in a regional town could offer consultations, training, and pilot funding tailored to local industries such as agriculture, logistics, or tourism.

Government procurement can also be a powerful lever. By prioritising regional tech providers in public contracts and offering innovation sandboxes for regional pilots, government can stimulate local commercialisation. For instance, a regional council could trial an AI-powered scheduling tool for community services, with federal support and ethical oversight. These pilots not only improve service delivery but also create reference customers for local tech firms.

Case studies from regional NSW show that when local governments adopt smart technologies- such as sensor-enabled waste systems or AI-driven irrigation- they not only improve services but also demonstrate the viability of emerging technologies in non-metropolitan contexts. These examples should be documented and shared widely to inspire other regions and build momentum for adoption.

15. AIML – University of Adelaide, Dr Miguel Balbin, May 2025 - Case studies | Australian Institute for Machine Learning (AIML) | University of Adelaide
16. Funding for Artificial Intelligence (AI) Centres to help SMEs adopt AI technologies, Business.gov.au - Artificial Intelligence (AI) Adopt Program | business.gov.au

Promote trust and enable innovation with emerging technology

Financial incentives- such as patent box regimes and R&D tax concessions- should be accessible to regional innovators. Simplifying application processes and offering micro-grants can engage grassroots entrepreneurs. Additionally, regional innovation precincts can provide shared facilities, mentorship, and networking to help startups scale and connect with national and global markets.

To ensure widespread adoption, government should also address liability and insurance concerns that may deter businesses from using emerging technology. Clear guidance on legal responsibilities, risk management, and access to tailored insurance products will reduce uncertainty and encourage uptake.

Sector-specific guidance and best practice frameworks can further support adoption. For example, an "AI in Agriculture" guide could help farmers understand how to deploy AI for crop monitoring, yield prediction, and resource optimisation. Similarly, a "Small Business Guide to AI" could provide practical steps for integrating automation, customer analytics, and digital tools.

Finally, government should monitor adoption outcomes and adjust policy accordingly. Metrics such as SME participation in tech procurement, sandbox graduation rates, and regional startup growth can help track progress and identify areas for improvement.

By supporting commercialisation and adoption nationally and equitably, government ensures that emerging technologies contribute to balanced economic growth, improved public services, and a resilient innovation ecosystem. This approach enables Australia to not only invent but also scale and export solutions that reflect our values and strengths.

Conclusion

Australia stands at a pivotal moment in shaping the future of critical and emerging technologies. To ensure these technologies are adopted safely, responsibly, and inclusively, government leadership must be proactive and community-focused. Scyne's submission highlights four foundational areas, public trust, infrastructure, skills, and commercialisation, that together form a cohesive national strategy. By addressing public sentiment, strengthening digital foundations, building workforce capability, and supporting innovation pathways, Australia can unlock the full potential of technologies like AI while safeguarding national interests and ensuring equitable benefit across all regions.

Key Recommendations

- Embed AI awareness campaigns in AI-enabled government service delivery.
- Support voluntary standards, labelling of AI-generated content, and independent oversight mechanisms.
- Prioritise "last-mile" connectivity and shared infrastructure in regional and remote areas.
- Enhance national standards, promote privacy-preserving technologies, and support secure data sharing frameworks.
- Release anonymised government-held data in standardised formats to support innovation across sectors.
- Fund tertiary and vocational training in AI and emerging tech, including micro-credentials and regional delivery.
- Replicate successful models like AIML to foster local ecosystems and job creation.
- Use targeted visa programs to attract global talent to regional and priority sectors.
- Expand programs like AI Adopt, simplify grant processes, and offer micro-grants and pilot funding.
- Prioritise regional tech providers and create innovation sandboxes for real-world trials.
- Publish practical frameworks for industries such as agriculture, manufacturing, and small business.
- Track metrics such as SME participation, sandbox graduation rates, and regional startup growth.

4 Cyber Crisis Simulation Learnings

Are the roles and responsibilities of government and industry clear for cyber security in a conflict or crisis scenario? What activities, such as cyber crisis simulation exercises, could Government undertake to make you feel better prepared to respond in a cyber conflict or crisis?

Building Realistic Scenarios to Strengthen Government Resilience

Scyne has extensive experience conducting tailored cyber crisis simulations for federal and state government departments across a wide range of sectors.

No two-crisis scenarios are alike

Each exercise is designed to reflect the distinct risks facing the agency involved, with a focus on the vulnerabilities in their systems and the unique services they provide. This ensures scenarios are realistic and tests the areas that are most vital for the public.

Involving stakeholders across disciplines

Our approach goes beyond scenario writing. We engage stakeholders across all levels of the organisation, including senior leadership, emergency management teams and technical managers, to co-design exercises that are both feasible and challenging.

This process builds ownership and ensures that decision-making structures, escalation pathways and technical considerations are tested under realistic conditions.

What we have seen on the frontline, built into the scenario

Scyne's work is strengthened by our first-hand experience supporting government agencies with incident response. We bring a current and practical understanding of the threats organisations face.

These insights allow us to embed credible adversary behaviours into exercises that test how agencies respond to the challenges of today's threat landscape.

Decisions that only leaders can make

A core focus of our simulations is the role of leadership in a crisis. We emphasise the importance of tactical decision-making under pressure, understanding the systems leaders are accountable for and guiding their teams effectively.

Equally, we highlight the preparation that can be done before a crisis, helping agencies identify gaps, clarify roles and rehearse the decisions that will matter most when real incidents occur.

Key Recommendations

1. **Sponsor multi-agency cyber crisis exercises.**
   Sponsoring regular multi-agency exercises will help strengthen coordination between government departments and critical industries. These simulations provide a safe environment to test joint response procedures, identify interdependencies and uncover weaknesses in communication or decision-making. While individual departments often have matured internal processes, coordinating across multiple agencies can be far more difficult. By bringing different organisations together, government can raise the overall level of preparedness and ensure that when a real incident occurs, collaboration happens seamlessly rather than being improvised under pressure.

2. **Define the scope and limits of government support in a crisis**
   Organisations need clarity on what assistance they can expect from government during a major incident. This includes knowing what resources are available, how quickly they can be deployed and importantly, the limitations of this support. By setting out this information in advance, government can reduce uncertainty, enable departments and businesses to plan realistically and avoid duplication of effort during a crisis.

3. **Strengthen accountability by defining departmental and industry responsibilities.**
   Greater clarity is needed on the division of responsibilities during a cyber crisis. This includes confirming what obligations sit with government and what must be managed by departments and businesses themselves. Establishing this split in advance helps prevent confusion, ensures accountability is clear and allows each party to focus on the aspects of the response they are best placed to deliver.

Managing through cyber crisis – the lessons we've learned

Navigating a cyber crisis can be daunting, but preparation is key. Here are some pragmatic ways you can better prepare.

Understand the threat landscape

Executives must develop a clear understanding of the evolving cyber threat landscape. This includes recognising the most common attack vectors, such as ransomware, phishing, and insider threats, as well as emerging risks like supply chain vulnerabilities and AI-driven exploits. A strong grasp of these threats enables leaders to ask the right questions, allocate resources effectively, and make informed decisions about risk tolerance and mitigation strategies.

Plan for a cyber crisis

A robust cyber crisis plan should be viewed as an organisational strategic imperative, rather than understood as only an IT responsibility. The plan should clearly define roles and responsibilities across the executive team, outline decision-making protocols and include escalation paths for critical incidents. Having a **"who to call" list** of internal and external stakeholders such as legal counsel, communications leads, and cyber forensics experts ensures swift coordination. Pre-determined isolation pathways for critical systems can dramatically reduce response time and limit damage.

Regular training and simulations

Cyber readiness is not achieved through documentation alone; it must be tested. Executives should participate in regular tabletop exercises and live simulations that mimic real-world cyber incidents. These sessions help identify gaps in decision-making, communication, and technical response, while also building muscle memory for high-pressure scenarios. **Training should be tailored to executive roles**, focusing on strategic oversight, stakeholder engagement, and reputational risk management.

Establish clear communication channels

During a cyber crisis, communication can make or break the response.

Executives must ensure that transparent, timely and consistent messaging reaches employees, citizens, regulators and the media. **Pre-approved communication scripts**- developed in collaboration with legal and PR teams, help maintain control of the narrative and reduce the risk of misinformation. Internal channels should also be stress-tested to ensure they remain operational during a crisis.

Collaborate with experts

No organisation should face a cyber crisis alone. Building **trusted relationships with cyber security experts**, legal advisors and crisis communication specialists before an incident occurs is essential. These partners can provide surge capacity, technical expertise and strategic guidance when internal teams are stretched thin. Executives should also consider establishing retainer agreements or joining industry threat-sharing networks to stay ahead of emerging risks.

Board and executive alignment

Cyber security risk is a board-level issue. Executives must ensure that the **board is fully briefed** on the organisation's cyber risk posture, response protocols and strategic priorities. This includes alignment on sensitive topics such as the organisation's stance on ransomware payments, disclosure obligations, and regulatory engagement. Regular updates and joint participation in simulations help foster a shared understanding and unified response.

Continuous Improvement

Every cyber crisis- real or simulated- is an opportunity to learn. After the dust settles, executives should lead a structured post-incident review to capture lessons learned, assess the effectiveness of the response and identify areas for improvement. These insights should feed into updated playbooks, training programs and investment decisions. A **culture of continuous improvement** ensures the organisation becomes more resilient with each challenge.

Key Contacts

[redacted]