Submission to Horizon 2 of the 2023–2030 Australian Cyber Security Strategy

29 August 2025

CISO Tribe Members

- [redacted]
- [redacted]
- [redacted]

Executive Summary

This submission is respectfully provided to support the Australian Government's development of Horizon 2 under the 2023–2030 Australian Cyber Security Strategy. It represents the collective insights of senior Chief Information Security Officers from across critical sectors, including infrastructure, finance, energy, higher education, healthcare and technology. The views expressed herein respond to the consultation questions set out in Appendix A of the Horizon 2 Discussion Paper and offer constructive recommendations across the Strategy's six strategic "Shields".

Horizon 2 represents a critical opportunity to consolidate the foundational investments of Horizon 1 and elevate Australia's cyber resilience. This submission outlines a suite of practical, industry-informed recommendations aimed at enhancing national cyber maturity, economic competitiveness and international credibility.

We acknowledge the Department of Home Affairs and the National Cyber Security Coordinator for their commitment to consultative policy development and stand ready to provide further advice and operational insight as implementation progresses.

Overall Recommendation			
#	**Section**	**Observation**	**Recommendation**
1	Strategic Outlook for Horizon 2: Emerging Trends and Threats	Horizon 2 will be shaped by the rapid growth of artificial intelligence, edge computing, quantum-resilient cryptography, and increasing international cyber aggression. Australia's attack surface will continue to expand in parallel with the digital economy. Our collective cyber resilience will depend on proactive regulation, advanced risk forecasting and enhanced public-private coordination.	Establish a cross-jurisdictional foresight advisory group to monitor emerging technologies and cyber threats and inform strategic responses.
2	Strengthening Intergovernmental Collaboration: Scalable State and Territory Initiatives	We recommend scaling successful jurisdictional models nationally, such as the NSW Cyber Security Policy and Victoria's Cyber Resilience Strategy, which have proven effective in policy execution and operational uplift.	Empower the National Cyber Security Coordinator to drive consistent standards and reporting mechanisms across federal, state and territory governments to reduce complexity and enhance efficiency.
3	Evaluation and Continuous Improvement: Cyber Security Policy Evaluation Model	The Policy Evaluation Model is conceptually sound. However, more robust implementation will require consistent data sources across both public and private sectors.	Incorporate recovery time, trust and confidence indices, citizen satisfaction metrics and threat telemetry into the evaluation framework, supported by periodic public reporting.

Recommendations by Strategic Shield			
#	**Section**	**Observation**	**Recommendation**
Shield 1: Strong Businesses and Citizens			
1	Cyber Awareness Initiatives	Develop a sustained, centralised cyber security awareness campaign, drawing on behavioral science principles. Campaigns must be tailored for linguistic diversity, accessibility, and relevance to both metropolitan and regional communities.	• Create simplified, sector-agnostic cyber security control templates based on the Essential Eight and ISO standards.
2	Support for SMEs and Not-for-Profits (NFPs)	SMEs and NFPs are disproportionately under-resourced for implementing traditional frameworks.	• Establish a co-funded National Cyber Resilience Program for small entities, offering grants or rebates for basic cyber hygiene and preparedness activities
3	Ransomware and Insurance Market Gaps	Cyber insurance remains unaffordable for many entities, with policy complexity and lack of clarity on coverage.	• Promote co-designed reinsurance frameworks with industry to improve cyber insurance accessibility. Expand the Government’s ransomware guidance and deliver simulation exercises tailored for high-risk industries
4	Digital Inclusion and Identity Crime Support	Support programs must evolve to meet the rising demand for victim assistance and identity recovery.	• Expand multilingual and trauma-informed services for victims of cyber crime, with clear referral pathways and case management options.

Recommendations by Strategic Shield			
#	**Section**	**Observation**	**Recommendation**
Shield 2: Safe Technology			
5	Product Standards and Device Labelling	Introduce mandatory cyber security labelling for consumer smart devices, aligned with global initiatives (e.g. the US Cyber Trust Mark and EU Cyber Resilience Act).	• Scale national adoption of Software Bill of Materials (SBOMs) and secure-by-design procurement principles. • Ensure alignment with other regulatory requirements for regulated industries such as APRA CPS 230 in collaboration with the respective agencies.
6	Vendor Risk and Data Sovereignty	Implement a foreign influence and control disclosure framework for technology vendors servicing critical infrastructure and government.	• Strengthen vendor risk assessments within procurement frameworks.
7	Governance and Oversight of Autonomous AI Capabilities	Support the safe and transparent deployment of generative and agentic AI systems by promoting operational safeguards and human accountability without stifling innovation or burdening SMEs. This is an emerging threat vector that will affect Australian businesses and individuals, which is particularly dangerous due to the massive efficiencies and positive business impacts that may lead to security trade-	• Build on existing AI data security guidance by developing operational governance principles for AI systems that act autonomously or make decisions on behalf of users. • Promote human-in-the-loop oversight and adopt voluntary transparency standards for AI-driven actions, including step-up authentication for sensitive decisions, agent identity verification, action logging, and disclosure of autonomous capabilities. • Expand SME support programs to include practical guidance on GenAI risks, such as prompt injection, data leakage, and unintended autonomous behaviour. • Explore targeted regulatory levers in high-risk sectors to mandate human oversight and confirmation mechanisms

Recommendations by Strategic Shield			
#	Section	Observation	Recommendation
		offs without appropriate awareness and business/government oversight.	for AI-driven decisions, while preserving flexibility for innovation in general business contexts.
8	Federated Vendor Due Diligence Sharing via IRAP / similar Expansion	Expanding the proposed framework to include overseas vendors and a dynamic risk monitoring model would significantly enhance Australia's cybersecurity resilience and streamline supply chain management. This would enable the Australian government to leverage strong frameworks like IRAP for continuous vendor due diligence, moving beyond one-off, point-in-time assessments.	**<u>Extending the Framework to Overseas Vendors</u>** The government could consider leveraging existing, trusted overseas frameworks—such as **FedRAMP (U.S.)** or the **EU's ENISA certification scheme**—and treating them as an acceptable baseline for foreign vendors. • **Mutual Recognition Agreements:** Australia could establish agreements with international partners to formally recognize their government-accredited cybersecurity assessments. • **Assessment Mapping:** A standardized process would be developed to map controls from frameworks like FedRAMP or ISO 27001 to the IRAP controls. This would allow for a gap analysis, where only the unique Australian requirements would need to be addressed. • **Tiered Approach:** A tiered system could be implemented. For low-risk vendors, a recognized international certification might suffice. For high-risk or critical infrastructure providers, a full or hybrid IRAP assessment might still be required. **<u>Transitioning to Dynamic Risk Monitoring</u>** A major enhancement would be shifting from a static, point-in-time assessment to continuous, dynamic risk monitoring. This would provide real-time insights into a vendor's

Recommendations by Strategic Shield			
#	**Section**	**Observation**	**Recommendation**
			security posture, which is crucial in a rapidly changing threat landscape. • **Automated Data Feeds:** The centralized registry would be integrated with automated security tools that provide continuous monitoring of vendor assets. This could include vulnerability scanning, dark web monitoring, and threat intelligence feeds. • **Security Performance Metrics:** Vendors would be required to report on key security performance indicators (KPIs) through a secure dashboard. This could include patching cadence, incident response times, and employee training completion rates. • **Trigger-based Reassessment:** Instead of a rigid annual reassessment schedule, a new assessment would be triggered by significant events, such as a major security incident at the vendor, a change in their security architecture, or a drop in their security performance metrics. This ensures that due diligence is always current and relevant.
Shield 3: World-Class Threat Sharing and Blocking			
9	Threat Sharing Expansion	Support the creation and funding of sector-specific Information Sharing and Analysis Centers (ISACs), particularly for health, aged care, education and agriculture.	• Establish a Threat Intelligence Uplift Fund to enable ISAC formation and maturity. • Standardise deceptive warning and safe browsing overlays through ISP cooperation to prevent known malicious traffic.

Recommendations by Strategic Shield			
#	**Section**	**Observation**	**Recommendation**
Shield 4: Protected Critical Infrastructure			
10	SOCI Act Clarity and Proportionality	The Security of Critical Infrastructure (SOCI) Act is essential but currently burdensome in its application to smaller providers and complex infrastructure operators.	• Provide binding guidance and implementation toolkits to improve understanding and compliance. • Incentivise voluntary uplift in sectors not formally designated under the SOCI Act.
Shield 5: Sovereign Capabilities			
11	Cyber Workforce and Diversity	Address mid-career barriers and workforce participation from under-represented groups including women, First Nations Australians, veterans and neuro diverse individuals. Promote inclusive workforce development by supporting mid-career transitions, under-represented groups (e.g. women, First Nations Australians, veterans and neuro diverse individuals), and flexible entry pathways into cybersecurity roles.	• Develop a National Cyber Workforce Development Framework with formal certification pathways. • Further subsidies and expand hands-on entry level and intermediate TAFE first-party and private partnership cybersecurity courses for eligible residents/citizens. Look to capture this in the National Framework. • Expand micro-credential programs and conversion pathways from adjacent sectors (e.g. law enforcement, IT, risk, and audit). • Continue to avoid rigid professionalisation requirements, such as mandatory certifications to operate. This approach fosters broader workforce participation, retains skilled professionals, and strengthens Australia's sovereign cyber capability.
12	Research and Industry Collaboration	Align government, academia and industry research priorities through strategic co-investment and a national cyber research agenda.	• Fund collaborative Cyber Research Centers of Excellence across states to build sovereign capability in priority areas such as post-quantum cryptography, secure digital identity and AI assurance.

Recommendations by Strategic Shield			
#	Section	Observation	Recommendation
Shield 6: Resilient Region and Global Leadership			
13	Cyber Diplomacy and Deterrence Tools	We support the use of public attributions, sanctions and multilateral responses to malicious cyber activity. However, deterrence must be paired with regional cooperation and direct intervention capabilities.	• Expand the Cyber RAPID initiative to include operational deployment capabilities in coordination with regional allies. • Advocate for international standards alignment in identity assurance, AI governance and critical technology protection.