Horizon 2 of the 2023–2030 Australian Cyber Security Strategy

[redacted]

[redacted]

Executive Summary

I welcome the opportunity to contribute individually to the development of Horizon 2 of the 2023–2030 Australian Cyber Security Strategy. My perspective reflects more than 16 years of experience in cyber leadership across various countries and sectors, and as highly skilled and certified security professional working directly with Australian organisations at the forefront of transformation.

Australia's cyber security future requires more than compliance uplift. It requires ambition. Horizon 2 must position Australia to thrive in an era of systemic fragility, accelerating AI adoption, and geopolitical volatility. We must be prepared not only to withstand attacks, but to adapt, recover, and innovate in the face of disruption.

This submission advances six recommendations that emphasise resilience, transparency, and foresight. Each is grounded in lessons from practice and global experience, with the goal of shaping a strategy that is pragmatic today but anticipatory of tomorrow's risks.

I fully support the world-leading initiative led by the Department of Home Affairs and am confident that my contribution will add meaningful value to its success.

Overview of Recommendations

This submission addresses selected Horizon 2 consultation questions where practical implementation detail can lift outcomes for Australian Government agencies and private businesses.

The summary table maps each recommendation to consultation questions, states the core proposal, and the intended benefit. The detailed sections then expand each item with context, a short case example, and clear outcomes.

This paper deliberately avoids restating well-established practices (e.g. awareness campaigns, baseline hygiene) or duplicating input already gathered through existing collaborations. The aim of this paper is to provide **targeted, pragmatic insights** that will help shape Horizon 2 implementation in ways that deliver real benefit to Australia.

Recommendation	Questions	Core Proposal	Intended Benefit
National Resilience Index	Q3, Q4, Q36	Publish an annual index of resilience outcomes (detection, containment, recovery times) across sectors	Creates transparency, builds accountability, and focuses investment on outcomes
Red Team by Design	Q6, Q24, Q27, Q31	Embed government-endorsed adversarial testing as part of national resilience exercises	Validates defences under real-world attack conditions, not just compliance
AI Safety and Assurance Baseline	Q19, Q20, Q33, Q34	Establish mandatory safety, auditability, and accountability requirements for AI systems	Protects against systemic harms from uncontrolled AI adoption
Cyber Transparency for Citizens	Q10, Q11, Q12	Require public disclosure of incident response effectiveness and recovery performance	Builds public trust and market discipline in resilience
Geopolitical Stress Testing	Q25, Q26, Q30	Simulate scenarios of global fragmentation, sanctions, and supply chain disruptions	Prepares Australia for systemic shocks beyond cybercrime
Talent Exchange Program	Q40, Q41, Q42	Create reciprocal placements between government, industry, and academia	Builds shared expertise and breaks down silos

Contents

National Resilience Index

Consultation Questions: Q3, Q4, Q36

Context

Most reporting today focuses on activity (audits completed, staff trained) rather than resilience outcomes. Without transparency on actual detection and recovery capability, the nation cannot track progress.

Recommendation

Publish an annual **National Cyber Resilience Index** reporting on key outcome metrics such as detection times, containment success rates, and service continuity during incidents.

Case Example

In healthcare, two operators with identical compliance scores showed radically different resilience in a ransomware attack: one resumed services in 48 hours, the other took weeks. An index would spotlight such differences and direct resources where most needed.

Intended Benefit

- Focuses investment on outcomes, not artefacts
- Creates transparency and accountability across sectors
- Enables government to prioritise interventions based on measurable gaps

Red Team by Design

Consultation Questions: Q6, Q24, Q27, Q31

Context

Tabletop exercises test process, but adversaries exploit technology, people, and integrations in practice. Without adversarial stress testing, hidden weaknesses remain.

Recommendation

Make red teaming a standard element of national cyber resilience programs. Establish a register of cleared red team providers and ensure findings feed into ACSC advisories.

Case Example

A financial services firm passed compliance audits but failed a red team test within 72 hours due to weak vendor integrations. Red team validation revealed blind spots that paperwork missed.

Intended Benefit

- Validates resilience under real attack conditions
- Improves cross-sector learning by sharing findings beyond single organisations
- Builds credibility in national capabilities

AI Safety and Assurance Baseline

Consultation Questions: Q19, Q20, Q33, Q34

Context

Agentic AI systems introduce novel risks: autonomous decision-making, opaque supply chains, and systemic vulnerabilities. Current frameworks lack enforceable guardrails.

Recommendation

Establish a national baseline for AI safety, requiring:

- Auditability of training data and model decisions
- Explicit accountability for outcomes of AI-enabled systems
- Integration of AI resilience into SOCI and privacy obligations

Case Example

A government agency piloting AI-based decision support discovered bias in its outputs only after complaints surfaced. A pre-deployment assurance baseline would have prevented reputational and operational damage.

Intended Benefit

- Protects citizens and operators from systemic AI risks
- Positions Australia as a global leader in safe AI deployment
- Reduces long-term liability for organisations adopting AI

Cyber Transparency for Citizens

Consultation Questions: Q10, Q11, Q12

Context

Citizens bear the impact of outages and breaches but receive little visibility into organisations' true resilience. Transparency builds both trust and market discipline.

Recommendation

Mandate public disclosure of incident recovery times and resilience metrics for operators of critical services.

Case Example

In the utilities sector, one operator restored service in hours while another took weeks. Public reporting would incentivise improvement and allow citizens to understand resilience capacity.

Intended Benefit

- Builds trust through openness
- Creates market incentives for resilience uplift
- Informs citizens of the reliability of essential services

Geopolitical Stress Testing

Consultation Questions: Q25, Q26, Q30

Context

Cyber strategy often assumes stable geopolitical supply chains, yet global fragmentation could cut off access to hardware, software, or cloud services overnight.

Recommendation

Introduce scenario-based stress tests simulating sanctions, trade disruptions, and regional conflicts that impact digital supply chains.

Case Example

During global chip shortages, Australian operators faced delays in critical system recovery due to unavailable hardware. A stress-testing framework would have prepared contingency plans in advance.

Intended Benefit

- Prepares Australia for systemic shocks beyond traditional cybercrime
- Strengthens sovereign capability by exposing dependencies
- Reduces recovery delays from unforeseen global events

Talent Exchange Program

Consultation Questions: Q40, Q41, Q42

Context

Australia's workforce challenge is not just numbers but siloed experience. Government, industry, and academia often lack shared understanding of each other's constraints.

Recommendation

Establish a national cyber talent exchange program enabling reciprocal placements across sectors, supported by security clearances and secondment frameworks.

Case Example

In Singapore, the Cybersecurity Associates and Technologists (CSAT) program places mid-career professionals into industry and government rotations, producing talent fluent in both domains.

Intended Benefit

- Builds shared expertise and mutual trust
- Creates flexible, experienced talent pools
- Reduces the "experience gap" between sectors

Conclusion

Australia's Horizon 2 strategy must not only close today's gaps but anticipate tomorrow's systemic risks. By focusing on resilience outcomes, embedding adversarial testing, governing AI safely, preparing for geopolitical shocks, and elevating accountability to boards, Australia can lead globally in shaping a cyber strategy that is credible, transparent, and future-ready.

I submit these recommendations as an individual practitioner who has worked across government, industry, and international contexts. My perspective is shaped by both operational lessons and strategic foresight, and I stand ready to contribute further to Horizon 2's development and implementation.