Australian Information
Industry Association

Australian Information Industry Association

Submission on

Consultation on developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy

5 September 2025

Introduction

The Australian Information Industry Association (AIIA) welcomes the opportunity to contribute to the Government's Horizon 2 Cyber Security Strategy Discussion Paper. Horizon 2 must build on the foundation of Horizon 1 by moving beyond isolated initiatives toward a more comprehensive and forward-looking approach to national cyber resilience. This means not only addressing today's threats, but also preparing for the systemic risks of tomorrow, ensuring that all Australians can operate safely and securely in the digital environment.

In this submission, we present industry perspectives and recommendations across key areas critical to Australia's cyber resilience in 2026–28 and beyond.

Factoring the Geostrategic Environment into Horizon 2 Planning

The Horizon 2 planning should be undertaken with full cognisance of the deteriorating global and regional geostrategic environment. The Discussion Paper notes that *"increasing tensions in our society, geopolitical competition and technological advances have created a multifaceted, cascading and compounding threat environment."* In practice, this means Australia is operating in an era of heightened cyber threat from state-aligned actors and sophisticated criminal groups. As great-power competition intensifies in the Indo-Pacific, we can expect more frequent and brazen cyber intrusions, espionage, and disruptive attacks targeting Australian networks for geopolitical ends.

By 2028 the cyber threat landscape will be materially different in scale and intensity. AIIA recommends that Horizon 2 explicitly integrate geostrategic risk assessment into cyber security planning and exercises. This involves closer cooperation between the cyber security industry, cyber security agencies and national security/defence intelligence to anticipate state-sponsored threats. It also means investing in resiliency for critical sectors against high-impact scenarios (for instance, power grid or financial system attacks linked to international conflict). The Government should ensure Horizon 2 initiatives (like expanded threat blocking under Shield 3 and critical infrastructure protections under Shield 4) are tested against scenarios of heightened geopolitical tension. This will help Australia build cyber defences that are not only strong in day-to-day threat conditions, but also capable of withstanding concerted campaigns by capable adversaries during periods of crisis.

Planning for Horizon 2 should explicitly acknowledge that Australia's cyber risk environment is worsening due to global strategic tensions. This acknowledgement must translate into concrete measures, such as more threat intelligence sharing with allies, scenario planning for geopolitical crises, enhanced defence of critical systems, and a posture of vigilance and proactive cyber defence that matches the evolving threat landscape.

Protecting Small Businesses and Not-for-Profits

Small and medium-sized enterprises (SMEs) and not-for-profit organisations (NFPs) are vital to Australia's economic and social fabric. They account for over 97 per cent of actively trading businesses and employ millions of Australians [1]. Despite this, they often lack the dedicated staff, financial resources, or technical expertise required to implement robust cyber defences. The result is a disproportionate exposure to cyber risks, where even a single successful attack can cause financial losses, reputational harm, and in some cases threaten business survival. For community organisations, a breach can also compromise sensitive client or donor information, undermining public trust.

To address this vulnerability, Horizon 2 must establish a scalable model that allows SMEs and NFPs to access essential security capabilities at low or no cost. Under such an approach, eligible organisations could draw on baseline protections such as managed firewalls, Security Operations Centre (SOC) services, vulnerability scanning, basic observability tools, and curated threat intelligence at a subsidised rate. Making these core capabilities more widely available would dramatically lift the minimum standard of security across the economy, ensuring that protection is not confined to large enterprises with the resources to invest heavily in cyber resilience.

A practical mechanism to achieve this is to leverage the Commonwealth's significant procurement power. The Commonwealth is one of the largest buyers of ICT products and services in Australia and can use this market influence to negotiate volume discounts or corporate-social-responsibility commitments from major vendors. Services purchased at scale by government can then be distributed to SMEs and NFPs at a fraction of the market cost. This creates efficiencies of scale, drives down costs, and ensures that critical protective services reach the long tail of smaller organisations that need them most.

Education, Collaboration and the Cyber Workforce

A sustainable and resilient cyber security posture cannot be achieved without a skilled workforce to design, implement, and maintain it. At present, Australia faces a shortage of cyber professionals. This shortage represents a critical bottleneck, and without adequate human capability, even the most advanced tools, policies, and frameworks will not be effectively executed. Horizon 2 must therefore prioritise strengthening cyber security skills development through deeper collaboration between education providers and industry, ensuring that the nation develops a larger, more diverse, and AI-capable workforce.Importantly, this effort must recognise the full range of cyber jobs and skills required. Cyber security is not a single occupation but an ecosystem of roles spanning

[1] Australian Small Business and Family Enterprise Ombudsman (ASBFEO), *Number of small businesses in Australia*, Small Business Data Portal, June 2024. Available at: https://www.asbfeo.gov.au/small-business-data-portal/number-small-businesses-australia

incident response, threat intelligence, architecture, secure software development, governance, risk and compliance, operations, and policy. A narrow focus on only the most visible roles, such as incident responders, risks leaving critical gaps in other areas that are just as essential to national resilience.

To address this, Horizon 2 should promote a coordinated national approach to skills development that covers every career entry point and transition pathway into cyber. This includes ensuring that school leavers, university graduates, and mid-career professionals can access clearly defined pathways into the full spectrum of cyber roles, supported by relevant training and accreditation. It also means aligning workforce planning with industry demand, so that efforts to fill skills shortages are distributed across all domains rather than concentrated in one or two high-profile fields. By adopting a holistic view of the cyber workforce, Horizon 2 can ensure that Australia builds not just more cyber professionals, but the right mix of capabilities across technical, operational, and strategic domains. This approach will strengthen resilience, reduce the risk of skills bottlenecks, and provide individuals with clearer opportunities to enter and progress within the sector.

Boosting education pathways

The pipeline begins in schools and universities. Horizon 2 should continue and expand initiatives that integrate cyber security into STEM curricula, raising awareness from an early age and promoting the sector as a dynamic, high-value career path. Programmes such as CyberTaipan provide excellent entry points by engaging secondary students in real-world cyber challenges. Similarly, tertiary scholarships for cyber-related degrees should be scaled to reach a wider pool of students. Crucially, industry participation is essential to keep course content relevant to evolving threats and technologies, ensuring that graduates are work-ready and aligned to the needs of employers.

Facilitating mid-career transitions and upskilling

Many successful cyber professionals come from non-traditional backgrounds. Veterans, engineers, and even individuals from unrelated disciplines have successfully retrained as cyber specialists. Horizon 2 should actively support such transitions through structured programmes that provide intensive training and mentorship. The AIIA recommends the establishment of cyber apprenticeships and cadetships targeted at workers in adjacent fields such as network engineering, software development, and data analysis.

The role of AI in the future workforce

Artificial Intelligence (AI) will transform many areas of workforce including cyber. The current skills gap is informed by the technology of recent years. As AI capability and adoption becomes more widespread, we need to ensure we are both addressing the skills needed to work in an AI-enabled future but also new areas in the governance, security and ethics implications of AI adoption across business more widely.

If Australia does not significantly expand its cyber workforce in the next few years, even the best strategies will falter in execution. Investment in people is as important as

investment in technology. Horizon 2 must ensure that Australia can attract, train, and retain its share of global cyber talent, and in doing so, secure the capabilities needed to protect the nation into the future

Advancing Australia's Privacy and Data Protection Laws

Robust privacy and data protection laws are a necessary complement to cyber security uplift. While cyber security initiatives reduce the risk of unauthorised access, privacy law sets the standard for how organisations collect, handle, and safeguard personal information. Horizon 2 must ensure that these two pillars are integrated, so that stronger privacy obligations are matched with practical tools and guidance to help organisations comply.

The Attorney-General's Department has concluded a comprehensive review of the Privacy Act 1988, with recommendations to bring the law into line with community expectations and international benchmarks. Horizon 2 should incorporate these reforms into the broader cyber security strategy, creating a consistent and mutually reinforcing framework. Clearer and stronger privacy obligations will encourage organisations to uplift their security posture and reduce the potential harms caused by large-scale breaches.

A central reform is the proposed removal of the small business exemption, which would mean that organisations with an annual turnover under $3 million would be subject to the Privacy Act's requirements. This change recognises that small businesses routinely handle sensitive customer data and that breaches affecting these entities can have impacts just as significant as those involving larger enterprises. The AIIA supports the removal of the exemption, however, acknowledges that this should be accompanied by adequate support for SMEs. This will balance the imperative for stronger privacy protections with the reality of resource constraints faced by small operators.

Threat Sharing and Blocking at Scale

Everyday Australians face an unprecedented volume of cyber threats, from phishing emails and scam texts to malware-laden websites and botnets. While individual vigilance remains important, the scale and sophistication of modern attacks mean that expecting every citizen to defend themselves is unrealistic. Instead, national-level measures that block threats "upstream" can provide baseline protection for millions of users simultaneously.

Telstra has already demonstrated leadership through its *Cleaner Pipes* initiative, which applies Domain Name System (DNS) filtering to block access to known malicious domains before they reach end users. The program has successfully intercepted vast quantities of scam messages and prevented malware infections, proving the effectiveness of proactive filtering. However, DNS filtering addresses only part of the threat. Cyber adversaries now exploit multiple points across the ecosystem, communications service providers, internet

service providers, web browsers, domain registrars, cloud platforms, and more. This fragmentation allows many attacks to slip through.

Horizon 2 should therefore commit to developing a national threat blocking strategy. Such a strategy would broaden and coordinate efforts across all layers of the internet ecosystem, ensuring that malicious traffic is identified and neutralised as early as possible. The goal should be to stop known threats at scale before they reach households, small businesses, or community organisations.

Update SOCI RMPs to Address Emerging Risks

Australia's Security of Critical Infrastructure (SOCI) Act framework has seen significant expansion in recent years, introducing obligations like mandatory reporting of cyber incidents and requiring critical infrastructure entities to maintain a Risk Management Program (RMP) covering cyber and other hazards. AIIA broadly supports these measures as vital for national security. However, one identified gap is the lack of explicit requirement for addressing post-quantum and AI-related risks in current RMP rules.

Critical infrastructure sectors typically have long asset lifespans and must anticipate future threats. We recommend that the Government update and refine Australia's critical infrastructure security regime (SOCI Act and associated rules) to address emerging risks, notably by including post-quantum cryptography and AI readiness in mandatory RMPs. This would ensure that Australia's operators are not only managing today's risks but are also actively preparing for the next wave of systemic challenges.

Importantly, we also need to allow for the adoption of AI to the benefit of cybersecurity. The opportunity for AI technologies to augment cybersecurity professionals, to automate time consuming and repetitive tasks, and to provide new AI and ML powered cybersecurity capabilities not previously possible needs to be recognised and supported. We need to be mindful that any proposed regulations and guidelines also do not overly restrict AI adoption to the detriment of security.

Preparing for Quantum Technologies

Advances in quantum computing pose a unique asymmetric risk to cyber security. A large-scale quantum computer in the hands of an adversary could render today's widely used encryption algorithms breakable, undermining the confidentiality of sensitive data. While such a machine may still be years away, the threat is not abstract or distant, and action is needed now to ensure our information remains secure in the future. Foreign actors can collect troves of encrypted communications or personal records now, with the intent to decrypt them once quantum capabilities mature. Horizon 2 should drive awareness and adoption of post-quantum cryptography across government, critical infrastructure and industry.

The 2021 AIIA whitepaper on Growing Globally Competitive Industries recommended that "[g]overnment needs to dedicate resources to identify the potential quantum-era security exposures across all departments and keep abreast of the developments in post-quantum cryptography standards, to implement solutions as they become available." The quantum threat may not fully materialise within the Horizon 2 timeframe, but the long lead time required for migration means that delay is not an option. Preparing now will ensure Australia's resilience when quantum capabilities reach maturity.

Managing the Two-Way Impact of AI on Cyber Security

AI is transforming the cyber security landscape in profound ways. It is simultaneously expanding the threat surface for attackers and providing powerful new tools for defence. AIIA considers it essential that Horizon 2 actively account for both dimensions of AI's impact, so Australia is prepared to manage AI-driven threats and to capitalise on AI-enabled security innovations.

AI as a driver of new and evolving threats
AI is enabling threat actors to increase the scale, speed, and sophistication of their operations. Malicious use of generative models to craft highly convincing phishing lures, deepfakes, and synthetic identities is lowering the barrier to entry for cybercrime and improving social engineering success rates. Adversaries can use AI to automate reconnaissance across vast attack surfaces, prioritise exploitable weaknesses, and fine-tune payloads that evade traditional signature-based detection. There is also a rising risk of data poisoning, model inversion, and prompt-based attacks that target organisations' own AI systems. AI is not only amplifying existing threats but also creating new attack vectors that are fast-moving and difficult to detect with legacy tooling.

AI as a force-multiplier for defence
On the positive side, AI is revolutionising cyber defence. Modern security operations increasingly rely on machine learning to sift large volumes of telemetry, detect anomalies, and surface weak signals that would be invisible to human analysts working alone. AI-driven analytics can correlate indicators across endpoints, networks, identity systems, and cloud platforms to predict likely attack paths and accelerate containment. Automated playbooks can triage common alerts, isolate compromised assets, and enrich incidents with context in near real time, allowing human operators to focus on complex investigation and response. When implemented safely and with proper oversight, AI can materially reduce attacker dwell time and improve the overall resilience of public and private systems.

Cyber Capacity Building in the Pacific Region

The AIIA strongly supports continued and expanded cyber capacity building in the Pacific as a core element of Horizon 2. Australia's longstanding development assistance in the Pacific, traditionally focused on physical infrastructure like roads, ports, and airports, must now extend into the digital realm. In the modern era, secure digital infrastructure is just as critical to regional stability and growth as transport or energy infrastructure.

Elevating cyber capabilities in the Pacific is not just an altruistic development goal, it is fundamentally in Australia's national interest. A more cyber-secure Pacific region directly enhances Australia's own security. Neighbouring countries with resilient networks are less likely to serve as backdoors or safe havens for cybercriminals and state-sponsored attackers targeting Australia. Conversely, if our Pacific partners remain vulnerable, hostile actors could exploit those weak links to threaten Australian systems.

Australia's ability to influence and shape the regional cyber and technology environment depends not only on domestic capabilities but also on strong diplomatic representation. The Ambassador for Cyber Affairs and Critical Technology plays a central role in advancing Australia's interests internationally, particularly in the Pacific. The Ambassador coordinates whole-of-government engagement on cyber capacity-building, advocates for an open, secure, and trustworthy cyberspace, and represents Australia in multilateral and bilateral forums where norms and standards are being debated. We recommend continued support for role of the Ambassador for Cyber Affairs and Critical Technology as a permanent and senior diplomatic position. The Ambassador should be tasked not only with maintaining regional partnerships and coordinating cyber capacity-building but also with ensuring that Australia's voice shapes global norms, standards, and governance arrangements for critical technologies. This continuity of representation will strengthen Australia's leadership, credibility, and influence in the Pacific and beyond.

Conclusion

Cyber security is now inseparable from Australia's economic prosperity, social wellbeing, and national security. Horizon 2 represents a crucial opportunity to accelerate progress, address emerging risks, and ensure that Australia keeps pace with global technological change. Horizon 2 must take decisive, forward-looking steps now to build the skills, infrastructure, partnerships, and governance frameworks that will underpin our resilience for decades to come. The AIIA and its members stand ready to work in partnership with Government to ensure that Australia remains a safe, trusted, and competitive digital nation.

We appreciate the inclusive approach of this statutory review and look forward to continued collaboration. Should you require further information, please contact Mr David Makaryan, Advisor, Policy and Media, at david@aiia.com.au.

Yours sincerely

Elizabeth Whitelock
Interim CEO, AIIA

***

About the AIIA

The AIIA is Australia's peak representative body and advocacy group for those in the digital ecosystem. Since 1978, the AIIA has pursued activities to stimulate and grow the digital ecosystem, to create a favourable business environment for our members and to contribute to Australia's economic prosperity. We are a not-for-profit organisation to benefit members, which represents around 90% of the over one million employed in the technology sector in Australia. We are unique in that we represent the diversity of the technology ecosystem from small and medium businesses, start-ups, universities, and digital incubators through to large Australian companies, multinational software and hardware companies, data centres, telecommunications companies and technology consulting companies