Thank you for the opportunity to contribute to the development of Horizon 2 of Australia's 2023–2030 Cyber Security Strategy. As the third major national cyber strategy, Horizon 2 marks a critical moment for strengthening Australia's resilience, competitiveness, and global leadership in the digital economy.

Amazon Web Services (AWS) commends the Department of Home Affairs (the Department) for its evidence-based, outcomes-driven approach. This philosophy of measuring what matters and working backwards from tangible results is one we share at AWS and apply in delivering secure, reliable, and innovative cloud services globally. We encourage the Department to use the Horizon 2 time period to bed down and evaluate initiatives commenced during Horizon 1 which have required industry to develop and implement regulatory programs.

We acknowledge the Department's leadership in advancing a truly "whole-of-nation" approach to cyber security and welcome the continued emphasis on co-designing solutions with industry. Horizon 2 presents an opportunity not only to strengthen protections for critical infrastructure and digital services, but also to enable trust, innovation, and long-term resilience across Australia's economy and society.

Regulatory Harmonisation and Streamlining

AWS supports the Department's commitment to harmonising and simplifying regulatory obligations while maintaining strong security outcomes. Today's overlapping frameworks can create duplication, confusion and complexity. For example, organisations must navigate disparate security requirements between the Digital Security Policy Framework (DSPF) and the Protective Security Policy Framework (PSPF), creating unnecessary complexity in implementing consistent security controls. This regulatory fragmentation extends to how organisations manage and protect identity information, with multiple frameworks governing the storage and handling of personal information. A unified approach to digital verification could enhance security and privacy by reducing the physical sharing and storage of identity documents, while enabling more efficient online service delivery and stronger participation in the digital economy. By consolidating requirements and modernising identity frameworks, Australia could free resources to focus on real-world risk mitigation and incident preparedness, while reducing compliance burden.

Cloud Security as a National Enabler

Secure cloud adoption is central to achieving Horizon 2's objectives. From AI innovation to resilient digital infrastructure, cloud provides the scalability, agility, and transparency required across all sectors of the Australian economy. Small businesses benefit from enterprise-grade security at accessible costs, while larger organisations gain the flexibility to innovate securely at scale. We caution against the introduction of data localisation mandates which can restrict access to cutting-edge security capabilities and lower enterprise resilience. Security depends on agile protective measures rather than mandated physical location, and global cloud providers benefit from collecting and analysing worldwide threat data to enhance protections for all customers. AWS welcomes the opportunity to co-develop a modern security compliance framework that reflects contemporary cloud architecture and ensures robust protections without constraining innovation for organisations of all sizes across every sector of the economy.

Emerging Technologies and AI Security

AWS supports a targeted, risk-based approach to regulating emerging technologies like AI, recognising both its transformative potential for enhancing security capabilities and the need for active appropriate governance. Drawing from global regulatory developments and implementation experience, we advocate for regulation that is necessary and effective, appropriate and balanced, implementable and maintainable, and which is consistently aligned with international standards to avoid fragmentation. AI presents significant opportunities to strengthen cyber defenses through advanced threat detection, automated response capabilities, and predictive security analytics. While harnessing these security benefits, frameworks should clearly identify high-risk use cases while enabling continued innovation in lower-risk applications. We believe there is substantial benefit in distinguishing between AI developers and deployers, with differentiated obligations that reflect their distinct roles and responsibilities in the AI ecosystem. Furthermore, we advocate for security assessment frameworks that are simple, clear, and accessible, ensuring that emerging technologies can flourish while maintaining robust security standards that remain relevant and up to date through regular review and industry consultation.

Incident Reporting and Information Sharing

We support the Department's work to refine incident reporting obligations. Establishing clear materiality thresholds and standardised timeframes will ensure focus on genuinely systemic risks while reducing duplicative reporting. Equally important is reciprocity: timely, actionable feedback from government to industry which will strengthen national resilience by ensuring lessons learned are shared across sectors. AWS applauds the industry consultation efforts of the National Cyber Security Coordinator and the Office of Cyber Security. Their collaborative and evidence-based approach to engagement with industry has grown confidence and stimulated genuinely beneficial consideration of best practices.

Leveraging Global Security Certifications

AWS strongly supports the Department's consideration of security certifications and mutual recognition schemes. Leveraging established frameworks such as ISO 27001, SOC 2, NIST, and IRAP will allow organisations across all technology sectors to build efficient, sustainable assurance models. We encourage pursuing mutual recognition of security certifications with trusted international partners. This would reduce duplicative assessments while maintaining high security standards and enabling faster adoption of secure technology solutions across the digital economy. This approach benefits not only cloud providers but also software developers, hardware manufacturers, managed service providers, and other technology vendors serving the Australian market.

Supporting Small and Medium Businesses

AWS recognises the critical importance of supporting small and medium businesses in their cyber security journey. We support government initiatives like the Small Business Cyber Security Resilience Service and propose enhancing these through cloud-based security solutions that are both accessible and cost-effective. Through our experience working with businesses of all sizes, we understand that cyber security resources must be practical, easy to implement, and scalable. We recommend developing clear, industry-specific guidance that helps small businesses understand and implement essential security controls without overwhelming technical complexity.

Threat Intelligence Sharing and Blocking

AWS supports Australia's development of a robust threat intelligence ecosystem. AWS's global security operations enable automated detection and response to cyber threats at scale. By converting threat insights into actionable security controls, AWS delivers automated protection through our services, helping to disrupt malicious actors and safeguard Australian organisations. This approach supports rapid operationalisation of security intelligence, facilitating automated remediation of threats to help protect critical systems and infrastructure. Our focus remains on delivering real-world security outcomes through technology that scales, helping to strengthen Australia's cyber resilience while maintaining the speed and agility needed in today's threat landscape. We support the development of automated threat blocking capabilities that can operate at scale and drive down Time to Resolution by leveraging cloud infrastructure to protect Australian organisations proactively.

Supporting National Priorities

AWS is committed to supporting Australia's broader national priorities through Horizon 2. We are actively building sovereign capability by investing in skills development, training, and knowledge-sharing with Australian cyber professionals. Our focus extends to enhancing the resilience of essential services by providing secure, scalable infrastructure for particularly health, education, and critical industries. Through regional engagement, AWS partners with governments and organisations across the Pacific to uplift collective cyber resilience and protect shared digital ecosystems. With trusted partners we are also deeply committed to international collaboration, working to harmonise incident reporting requirements and align security standards to reduce global regulatory fragmentation.

Conclusion

AWS welcomes the Department's comprehensive evaluation framework which considers both bottom-up and top-down perspectives. This approach will be crucial in ensuring Horizon 2 initiatives deliver measurable, real-world improvements to Australia's cyber security posture. We would recommend that Department establish an independent review group comprising representatives from the public, private and academic sectors to collect, analyse, review and report on outcomes achieved across Horizon 1 and recommend measurement goals for Horizon 2.

AWS looks forward to supporting the design of practical, risk-based security solutions across Horizon 2 that will help achieve Australia's ambition of becoming the world's most cyber secure nation by 2030.

Sincerely,

[redacted]