Microsoft

Developing Horizon 2 of the 2023 – 2030 Australian Cyber Security Strategy – Response to Policy Discussion Paper

Executive Summary

Microsoft welcomes the opportunity to respond to the Australian Government's consultation on Horizon 2 of the 2023-2030 Australian Cyber Security Strategy. Having operated in Australia for over 40 years, Microsoft is deeply committed to strengthening the nation's cyber capabilities to support national security and drive economic prosperity. We commend the Australian Government's global leadership on this important topic.

This consultation comes at a pivotal time, with the threat landscape continuing to evolve rapidly. Microsoft processes over 78 trillion security signals across the world each day, providing us with a unique vantage point on cyber security threats. We are witnessing an alarming rise in the complexity and scale of cyber threats[1], but also see tremendous potential for Australia to innovate and lead.

- The lines between nation state actors and cybercriminals are increasingly blurred, with nation states now using cybercriminals and their tools to launch attacks. Meanwhile, cybercriminals are operating with a level of sophistication once elusive outside of nation-state operations.
- The pace of nation-state sponsored cyber-attacks has escalated to the point where there is now effectively constant combat in cyberspace without any meaningful consequences to the attacker. Attacks on essential services and critical infrastructure have become dangerously normalised.
- We are witnessing a surge in ransomware, fraud and financially motivated cybercrime that is having widespread impacts, including on individuals, businesses and organisations of all sizes.
- We have entered the AI era. Just as governments and businesses are adopting AI technologies to improve the efficiency and effectiveness of their operations, so too are cybercriminal groups, nation-state threat actors and other adversaries – from deepfake-driven influence operations to automated phishing. Governments and businesses must also adopt AI technologies to avoid being outpaced.
- The quantum computing era is approaching fast. For decades, encryption algorithms have protected everything from personal passwords and private communications to the critical infrastructure that supports the global financial system. However, a sufficiently powerful quantum computer could one day render some encryption methods obsolete, threatening the confidentiality and integrity of data that underpins our digital lives. Malicious actors are already employing "harvest now, decrypt later" strategies.[2]

These insights underscore that defending against modern threats requires constant innovation and a collective approach to cyber defence across the broader economy and society.

[1] Microsoft Digital Defense Report (2024)
[2] Post-quantum resilience: building secure foundations

Microsoft

Australia enters Horizon 2 with strong foundations, including a mature cyber policy and regulatory framework. At the same time, the rapidly changing threat and technology environment means continued reform efforts will be essential to keep pace with evolving risks and opportunities and meet the ambitious goal to be a world-leader in cyber security by 2030.

Microsoft has provided feedback on a broad range of questions in the discussion paper, but we encourage the Australian Government to prioritise the following recommendations as it enters Horizon 2. These recommendations aim to maximise security outcomes while simultaneously contributing to broader Government objectives on productivity and budget sustainability:

- **Recommendation 3: Make advanced technology adoption a national cyber security priority** – Horizon 2 of the Cyber Security Strategy should reflect the necessity for Australia to position itself at the forefront of advanced technology adoption. This includes promoting AI-enabled cyber defences, preparing for post-quantum cryptography and embracing other strategic and emerging technologies as opportunities for building cyber security and resilience. Policy frameworks must balance risk management with enabling innovation to stay ahead of malicious actors.

- **Recommendation 4: Advance security-by-design across the tech sector** – Align Australia's security-by-design efforts with international best practice – such as the voluntary CISA Secure by Design pledge model and relevant international standards and codes of practice – to encourage developers to make meaningful commitments to embed security and safety into technology development.

- **Recommendation 9: Take immediate action to modernise legacy IT in the public sector** – Accelerate the replacement and modernisation of outdated IT systems across the Australian Public Service, including by removing structural, cultural and capability barriers to cloud migration. This would strengthen cyber resilience, improve productivity and support budget sustainability.

- **Recommendation 11: Strengthen workforce capability through a National Digital and AI Skills Partnership** – Enable cyber, AI and broader digital skills development across the economy by creating a coordinated national partnership model. The partnership should involve government, industry, education providers, unions and other key stakeholders. It should advance reforms to our skills and training systems, support training of the existing workforce and ensure the next generation are equipped with digital skills for the future.

- **Recommendation 12: Prioritise international cyber security regulatory alignment** – Reduce the growing complexity caused by fragmented and duplicative cyber security regulations by better aligning with international standards and promoting reciprocity or mutual recognition agreements – starting with harmonising divergent requirements for cyber incident reporting.

- **Recommendation 13: Strengthen Australia's cyber deterrence posture through attributions, advisories, and sanctions in coordination with international partners.** This should include expanding the use of multidimensional deterrence measures – such as economic, diplomatic and military instruments – to impose meaningful costs that hold malicious actors (including state-based actors) to account. This is essential to help better protect critical infrastructure and Australian citizens.

We also offer the following feedback in response to other key questions in the consultation paper:

- **Recommendation 1: Continue to deliver cyber security awareness initiatives in partnership with the private and non-profit sectors that recognise the shared responsibilities for cyber security** and combine 1) simple, actionable guidance for all users, particularly individuals and small businesses; 2) targeted campaigns for higher-risk groups, and 3) cyber security education integrated in schools that build on (and potentially integrate with) existing successful initiatives for online safety.

- **Recommendation 2: Partner with an experienced cyber security organisation, such as the non-profit Cyber Readiness Institute**, to provide small businesses with practical, globally recognised cyber security resources and training.

- **Recommendation 5: Adopt a government-led approach to active cyber defence** – This should include explicit guidance for private sector organisations with clear boundaries on appropriate measures for adopting a more proactive cyber security posture. We recommend this include a clear prohibition on private-sector "hack-back" activities.

- **Recommendation 6: Continue to prioritise public-private partnership models for threat sharing and blocking,** including continuing to expand and evolve the Microsoft-ASD Cyber Shield.

- **Recommendation 7: Formalise public–private partnerships for cyber resilience and invest in joint operational preparedness,** so Australia is better prepared to prevent, withstand, and rapidly recover from large-scale digital disruptions, no matter the cause.

- **Recommendation 8: Adopt a voluntary, confidential coordinated vulnerability disclosure (CVD) framework** – Align with international standards and avoid imposing prescriptive, mandatory requirements that could create perverse outcomes for security.

- **Recommendation 10: Proceed with targeted SOCI Act reforms** including:
    a. A more tailored, risk-based approach to supporting cyber maturity on a sector-by-sector basis, which should be accompanied by formal and meaningful engagement mechanisms between the Department and relevant sectors.
    b. Increase collaboration among critical infrastructure regulators, which could be achieved through the establishment of a Cyber Regulators Forum.
    c. Maintain CIRMP exemptions under the legislation for organisations with Strategic Hosting Certification to avoid regulatory duplication.
    d. Further to our recommendation on international regulatory alignment, align the 12-hour and 72-hour incident reporting window under the SOCI Act into a single 72-hour requirement and clarify the scope of notifiable incidents.
    e. Introduce separate forms for Part 2A (CIRMP) and Part 2AA (Annual Report) obligations to improve clarity and guidance for SOCI Act reporting.
    f. In keeping with the ambition for sector-by-sector approaches, consider extending the 30-day update requirement for the Asset Registry for the data sector.

- **Recommendation 14: Continue to prioritise engagement on cyber rules, norms and standards in United Nations forums**, focusing on strengthening multistakeholder participation. This approach will help ensure legitimacy, resilience, and the protection of democratic values in global cyber governance.

Microsoft looks forward continuing to work closely with the Australian Government by bringing our global expertise, local investment and deep technical capabilities to support the ambition to make Australia one of the world's most cyber-secure and digitally resilient nations.

Shield 1 – Strong Businesses and Citizens

Cyber literacy and awareness

We were pleased to see Horizon 1 launch with the "Act Now, Stay Secure" education campaign, supplemented by efforts to work in concert with the private sector through the Executive Cyber Council to raise cyber awareness for small businesses. Horizon 2 needs to build on these initiatives, given basic cyber hygiene remains insufficient at a whole-of-economy and society level.

As the Government has already recognised, cyber security messaging should be grounded in real-world behaviours and practical decision-making. Simple, actionable advice such as "enable multi factor authentication" and "update your software" can be powerful, particularly for individuals and small businesses, although simple checklists alone are not sufficient.

A good framework for awareness on cyber security could be road safety: Australians are familiar with a layered approach that acknowledges that risk is ever-present, everyone has a role to play, and that safe outcomes depend on a combination of personal and industry responsibility, good infrastructure, appropriate rules/laws and responsive systems. As with road safety, targeted communications campaigns are also required for higher-risk groups to maximise impact.

We also support the concept of embedding education early through the school system to help embed cyber security as a cultural norm. One area where the Government is already investing heavily in school-based education is online safety, through initiatives such as eSafety's toolkits for schools, the work of the Alannah and Madeline Foundation, and the rollout of digital licence programs. We encourage the Government to consider how to leverage and coordinate any school-based education programs with this existing program of online safety work.

Recommendation 1: Continue to deliver cyber security awareness initiatives in partnership with the private and non-profit sectors that recognise the shared responsibilities for cyber security and combine 1) simple, actionable guidance for all users, particularly individuals and small businesses; 2) targeted campaigns for higher-risk groups, and 3) cyber security education integrated in schools that build on and potentially integrate with existing successful initiatives for online safety.

Uplift security in small businesses

Small businesses remain disproportionately vulnerable to cyber threats. While there is now a dedicated Cyber Security Standard for Small Businesses, many SMEs will continue to face barriers to adoption, ranging from limited resources and competing priorities to a lack of tailored support. As digital risks such as ransomware escalate in frequency and impact, it is essential that small businesses are equipped not only with clear standards, but also with the practical tools, incentives, and support needed to put cyber security into practice.

Government has a role to play here, but reaching small businesses at scale is challenging without partnerships with trusted organisations. Microsoft's experience shows that collaborative models are essential to delivering practical support. That's why we partner with the Cyber Readiness Institute (CRI), a global non-profit dedicated to improving the cyber

resilience of small and medium-sized enterprises[3]. CRI provides free, easy-to-use tools and training that help SMEs embed cyber hygiene into everyday operations, covering essentials like password management, phishing prevention, software updates and USB security. Its Cyber Readiness Program is designed for non-technical audiences and has reached thousands of businesses across more than 100 countries. Independent evaluations show measurable improvements in preparedness and behaviour change, demonstrating that tailored, scalable interventions can make a real difference. Similar strategic partnerships could be explored in Australia.

We also recognise that tech companies have a direct role to play to help small businesses strengthen their defences. That is why Microsoft has recently introduced a new Microsoft 365 security package tailored for SMEs[4]. This offering brings advanced security features, such as endpoint protection, identity management, threat detection, and automated response, within reach of smaller organisations, making enterprise-grade protection more accessible and affordable than ever before.

Recommendation 2: Partner with an experienced cyber security organisation, such as the non-profit Cyber Readiness Institute, to provide small businesses with practical, globally recognised cyber security resources and training.

Shield 2 – Safe Technology

Promoting safe use of emerging technologies

Strategic technologies such as artificial intelligence (AI) are rapidly reshaping the cybersecurity landscape. While these technologies introduce new risks and complexities, they also offer transformative opportunities to strengthen national resilience and stay ahead of increasingly sophisticated malicious actors. Governments must adopt a forward-leaning posture, one that embraces security innovation as a strategic asset, rather than treating emerging technologies solely as sources of risk.

The latest Microsoft Digital Defence Report highlights the accelerating pace and scale of cyber threats, including the use of AI by threat actors to automate reconnaissance, generate malicious code, and evade detection. In this environment, the cost of inaction is high: countries that fail to modernise and adopt secure technologies risk being outpaced by adversaries who are already leveraging these tools to gain strategic advantage.

To mitigate this risk, Horizon 2 should set clear national goals for advanced technology adoption. This includes promoting AI-enabled cyber defences that can detect and respond to threats in real time. It also includes preparing for the transition to post-quantum cryptography (PQC) to safeguard sensitive data against future quantum-enabled attacks. These goals should be underpinned by policy frameworks that balance innovation with risk management and do not impose unnecessary barriers to the safe and responsible adoption of these technologies.

There are a range of actions the Government could take to support this direction. For example:

- Consider using levers such as the Trusted Information Sharing Network and Protective Security Policy Framework to ensure entities not only consider how to address the risks

[3] Cyber Readiness Institute

[4] Microsoft 365 E5 Security is now available as an add-on to Microsoft 365 Business Premium | Microsoft Community Hub

of AI systems, but also consider the opportunities and capability-building pathways for AI-enabled cyber defence.

- Facilitate cross-sector collaboration on threat modelling, testing, and deployment of advanced defences, including AI-driven detection and response capabilities.
- Adopt a proportionate, risk-based and internationally interoperable approach to AI regulation, that takes account of existing laws.
- Promote quantum safety with efforts to support adoption of international standards, align quantum-safe strategies across jurisdictions, set early and progressive timelines for PQC, raise awareness, and lead by example with transparent transition plans.

Recommendation 3: Make advanced technology adoption a national cyber security priority – Horizon 2 of the Cyber Security Strategy should reflect the necessity for Australia to position itself at the forefront of advanced technology adoption. This includes promoting AI-enabled cyber defences, preparing for post-quantum cryptography and embracing other strategic and emerging technologies as opportunities for building cyber security and resilience. Policy frameworks must balance risk management with enabling innovation to stay ahead of malicious actors.

Security-by-design and default

Safe technology is foundational to a secure digital environment, as the Government has rightly recognised through the Cyber Security Strategy. Microsoft is prioritising safe technology above all else through our Secure Future Initiative – a multi-year engineering transformation launched in response to the evolving threat landscape and increasing sophistication of cyber attacks[5].

The Secure Future Initiative is Microsoft's largest cybersecurity engineering investment to date and reimagines how we design, build, test and operate technology to protect identities, networks, data and critical systems in Australia and across the world. Key elements include:

- Secure by Design: Embedding threat modelling, AI safety reviews, and vulnerability prioritisation into product engineering.
- Secure by Default: Enforcing protections like phishing-resistant MFA and confidential computing.
- Secure operations: Enhancing monitoring, detection, and response capabilities across our global infrastructure.

To support greater adoption and awareness of these practices within the wider tech industry, Australia should align its security-by-design efforts with international best practice, including voluntary commitments, international standards and codes of practice. One best practice model is the US CISA initiative of a voluntary security-by-design pledge[6]. The pledge has encouraged broad uplift in secure development practices across the tech industry that are tailored to individual companies and products, rather than a one-size fits all approach. Over 300 companies signed CISA's pledge in its first year, including Microsoft.

[5] Secure Future Initiative – Secure by Design | Microsoft
[6] Secure by Design Pledge | CISA

If the Government is inclined to explore further measures to support consumer awareness and choice of secure products, such as labelling schemes, we recommend any such schemes be voluntary and incentive-driven, aligned with international standards (including mutual recognition with equivalent international schemes) and have a practical implementation pathway to encourage broad participation (e.g. self-attestation supported by targeted compliance mechanisms, rather than third party certification).

Recommendation 4: Advance security-by-design across the tech sector – Align Australia's security-by-design efforts with international best practice – such as the voluntary CISA Secure by Design pledge model and relevant international standards and codes of practice – to encourage developers to make meaningful commitments to embed security and safety into technology development.

Shield 3 – World-Class Threat Sharing and Blocking

Advancing a proactive security posture and Active Cyber Defence

Microsoft supports a rules-based international order in cyberspace where governments, not private actors, are ultimately responsible for enforcing laws and responding to cyber threats. We therefore support the Government providing clarity to private sector organisations on how they can adopt a more proactive security posture, including by clarifying roles and responsibilities between the public and private sectors on Active Cyber Defence.

For example, there are often discussions about empowering victims to "hack back" against malicious cyber actors with the goal recovering stolen data, disrupting attacker operations, deterring threat activity or compensating for slow government responses. However, the reality is hack back is unlikely to meaningfully achieve these well-intentioned goals, and it simultaneously increases risks to the victim, innocent third parties, and society. Instead of hack back, Microsoft advocates for innovative legal and collaborative approaches with relevant government authorities to better disrupt attacker's operations. These include:

- Creating a private right of action: Governments should create private causes of action and seizure authorities in criminal statutes to enable the private sector to more easily pursue legal remedies and consequences against perpetrators.
- Strengthening law enforcement capabilities: Governments should invest in cybercrime units, improve cross border cooperation, and streamline digital evidence collection to hold attackers accountable.
- Changing law enforcement success metrics: Historically, law enforcement success has been measured largely by physical arrests. However, in the cyber domain, apprehending perpetrators is often far more difficult. To reflect this reality, governments should place equal value on measuring and rewarding operations that disrupt malicious infrastructure to incentivize more disruption operations.
- Supporting active defence within legal bounds: Encourage use of honeypots, sinkholes, and digital beacons that operate within the defender's own systems or with customer consent.
- Fostering public-private collaboration: Encourage joint operations, such as botnet takedowns, where private sector expertise complements government authority. Reduce

the barriers, risks, and obstacles to collaboration and evidence-sharing, particularly in criminal investigations and prosecutions.

- Enabling innovation in cyber defence: Allow room for evolving security practices that enhance resilience without crossing into retaliatory or unlawful territory.

By focusing on these areas, Australia can strengthen its cyber resilience, deter sophisticated adversaries and uphold international norms.

Recommendation 5: Adopt a government-led approach to active cyber defence – This should include explicit guidance for private sector organisations with clear boundaries on appropriate measures for adopting a more proactive cyber security posture. We recommend this include a clear prohibition on private-sector "hack-back" activities.

Amplifying existing models for threat sharing and blocking

Public–private partnerships are at the heart of effective cyber strategy. Nowhere is this more evident than in threat sharing and blocking.

The power of partnership is already clear: the Microsoft–ASD Cyber Shield initiative has shown how real-time threat intelligence sharing between the public and private sector can disrupt adversaries and bolster national defences[7]. This collaboration has enabled the identification and sanctioning of cyber criminals targeting Australian organisations, highlighting how joint efforts make Australians safer.

Microsoft stands ready to collaborate closely with the Australian Government to further expand and evolve the Cyber Shield model, working in partnership with broader industry. By leveraging this partnership, we can help facilitate real-time two-way threat intelligence sharing, enhance coordination during major cyber incidents, and support the development of innovative solutions for protecting critical national infrastructure.

Recommendation 6: Continue to prioritise public-private partnership models for threat sharing and blocking, including continuing to expand and evolve the Microsoft-ASD Cyber Shield.

Strengthening resilience

The increasing frequency and sophistication of cyber attacks, combined with other threats and risks that may cause large-scale digital disruptions, underscore the need for a robust, coordinated approach to national digital resilience that addresses prevention, preparation and response. This is a key lesson learned from the 2024 CrowdStrike incident.

Microsoft's experience supporting governments and critical infrastructure operators globally demonstrates that effective resilience requires both proactive planning and deep partnership between government and trusted technology providers.

In the Australian context, we recommend a focus on two core pillars:

[7] Microsoft and ASD Join Forces: Uniting Sentinel and CTIS for Enhanced Cyber Resilience - Microsoft Australia News Centre

1. Strategic public–private partnerships: Establish formal mechanisms for ongoing collaboration and dialogue between government and key technology partners for the nation, including arrangements for trusted information sharing to help identify actions to prevent or minimise the risk of a wide-scale disruption event.

2. Strengthening operational preparedness and rapid response: Prioritise the development of escalation protocols and real-time coordination between government and industry to respond during crisis scenarios. This should be supported by joint scenario planning and regular crisis simulation exercises to ensure all stakeholders are ready to act decisively and cohesively if faced with widespread disruption.

Microsoft stands ready to work with the Australian Government to enhance digital resilience, especially in an environment of heightened geopolitical volatility.

Recommendation 7: Formalise public–private partnerships for cyber resilience and invest in joint operational preparedness, so Australia is better prepared to prevent, withstand, and rapidly recover from large-scale digital disruptions, no matter the cause.

Managing vulnerability disclosure

A modern approach to coordinated vulnerability disclosure (CVD) is essential for strengthening Australia's cyber resilience and protecting critical systems. Microsoft's experience globally demonstrates that a voluntary, partnership-based CVD framework – rather than a prescriptive mandatory or punitive regime – delivers the best security outcomes. Alignment with international standards (such as ISO/IEC 29147 and 30111) and interoperability with global disclosure practices will ensure that Australia's approach is consistent with leading jurisdictions and supports cross-border collaboration[8].

Microsoft is a proponent of sharing information regarding significant security incidents, and we believe vulnerability reporting should occur after a manufacturer releases patches or effective mitigation. Alerting malicious actors about the existence of a vulnerability in a specific product or component significantly increases the likelihood they will research, discover, and exploit the vulnerability. Notifying entities of product security vulnerabilities once mitigation measures are in place allows these entities to take immediate action to defend against attacks prior to public disclosure. As products are required to authenticate the updates prior to installation, the notification should come directly from the vendor rather than a third party such as a government or another company.

We note that existing CVD practices already allow companies to issue security advisories to customers in significant situations by carefully balancing stakeholder interests. CVD practices should prioritise responses to actively exploited vulnerabilities and recognise that effective mitigations take time. Rushing unverified, unsafe, or unstable mitigations will cause customers to delay patching, resulting in lower overall levels of cybersecurity.

Recommendation 8: Adopt a voluntary, confidential coordinated vulnerability disclosure (CVD) framework – align with international standards and avoid imposing prescriptive, mandatory requirements that could create perverse outcomes for security.

[8] Interface 2024, *Vulnerability disclosure: guiding governments from norm to action*

Microsoft

Shield 4 – Protected Critical Infrastructure

Legacy IT and Commonwealth cyber security uplift

There is no silver bullet for cyber security uplift within the Australian Government, but one area requiring greater attention is the widespread use of legacy IT systems and the slow pace of modernisation.

Recent analysis by the Department of Finance shows over 70% of Commonwealth entities continue to rely on outdated infrastructure[9]. These systems are often end-of-life, unsupported by vendors, and increasingly incompatible with modern security standards. They can accumulate thousands of known vulnerabilities over time, many of which are severe and unpatched. This technical debt exposes government agencies to escalating risks of cyber breaches, data loss, and operational outages, undermining both service delivery and public trust[10]. The urgency to address these vulnerabilities has never been greater.

Modernising legacy on-premises IT systems must be recognised as a foundational priority for horizon 2 of the cyber security strategy. Research shows faster cloud adoption across the APS could prevent $178 million in potential cyber breach costs and avoid 2.9 million hours of IT downtime, while unlocking approximately $1.4 billion per year on average in savings and enabling greater use of productivity-enhancing AI technologies.[11] Modernising legacy systems is also critical for a secure transition to the quantum era.

Structural, cultural and capability barriers are preventing modernisation across the public sector. The following reforms are needed to address this challenge:

- Modernise financial and procurement frameworks: Adopt multi-year OpEx budgets rather than traditional short-term CapEx that encourage reinvestment in legacy IT; expand procurement evaluation to include innovation, security, sustainability and business outcomes; and consider incentives for transformation.
- Strengthen governance and align incentives: Amplify the mandate of the Digital Transformation Agency with clear whole-of-government goals for modernisation of public sector systems and adoption of AI technologies. Also establish coordinated mechanisms between the digital and security arms of government (e.g. NSC and ERC) to provide consistent modernisation signals and incentives to public sector agencies.
- Establish strategic partnerships to build cloud, AI and cyber capabilities: Develop public/private co-investment models to share transformation risks, build digital capabilities, and invest in digital skills across the Australian Public Service, including a whole-of-government Digital Productivity Co-Investment Fund.

Recommendation 9: Take immediate action to modernise legacy IT in the public sector – Accelerate the replacement and modernisation of outdated IT systems across the Australian Public Service, including by removing structural, cultural and capability barriers to cloud migration. This would strengthen cyber resilience, improve productivity and support budget sustainability.

[9] Department of Finance, Australian Public Service Data Maturity Report 2024
[10] ASD, Managing the risks of legacy IT: practitioner guidance
[11] Mandala 2025, Unlocking the Productivity Dividend of Digital Government

Maturing the regulatory framework for critical infrastructure

Australia's Security of Critical Infrastructure Act 2018 (SOCI Act) is widely regarded as a globally leading framework for critical infrastructure cyber regulation. Microsoft commends the Government's ambition to continue improving this regime in Horizon 2.

We support the proposal for a more tailored, risk-based approach to supporting cyber maturity on a sector-by-sector basis. A "one-size-fits-all" model can be inefficient. Utilities, banks, universities, and cloud providers face different threat profiles and have reached different security maturity levels. Evaluating each sector's cyber maturity and developing sector-specific uplift plans is a sensible step. However, it will be critical for the Department to use formal engagement structures at a sectoral level to underpin this work to ensure any sector-specific measures are fit-for-purpose and practical.

We strongly endorse increased collaboration among critical infrastructure regulators. A coordinated approach could help reduce duplication, harmonise definitions, and streamline compliance. Establishing a Cyber Regulators Forum could formalise this effort and improve regulatory clarity.

With respect to the proposal to introduce independent audit requirements for CIRMPs, we encourage the Government to maintain existing exemptions under the legislation for the CIRMP requirement for organisations holding a Strategic Hosting Certification. This existing exemption regime is critical to avoid regulatory duplication and reflect different risk profiles.

We have also identified the following additional reform opportunities to improve regulatory efficiency while maintaining high cyber security standards:

- The SOCI Act currently mandates different reporting windows for critical incidents (12-hours) and other incidents (72-hours). We recommend aligning and streamlining the requirement into a single 72-hour window, consistent with international best practice. This would allow organisations time to gather meaningful information to support investigation and response, deploy defensive measures, and ensure reporting is based on verified facts rather than speculation.
- The scope of notifiable incidents under the legislation is unclear with respect to different types of incidents (e.g. cyber security incidents versus other incidents such as technical failures and outages). Further clarification and guidance would be welcomed.
- Currently, there is no form available to submit an Annual Report under Part 2AA of the Act, only the CIRMP form under Part 2A. We suggest separate forms for Part 2A and Part 2AA reports to improve clarity and enhance SOCI Act reporting requirements.
- There is a 30-day update requirement for the Asset Registry, but material changes in the data sector typically occur less than once per year. In line with the proposal to adopt tailored approaches to different sectors, an extended timeframe for the data sector would maintain relevance while reducing administrative burden.

Recommendation 10: Proceed with targeted SOCI Act reforms including:

a. A more tailored, risk-based approach to supporting cyber maturity on a sector-by-sector basis, which should be accompanied by formal and meaningful engagement mechanisms between the Department and relevant sectors.

b. Increase collaboration among critical infrastructure regulators, which could be achieved through the establishment of a Cyber Regulators Forum.
c. Maintain CIRMP exemptions under the legislation for organisations with Strategic Hosting Certification to avoid regulatory duplication.
d. Further to our recommendation on international regulatory alignment, align the 12-hour and 72-hour incident reporting window under the SOCI Act into a single 72-hour requirement and clarify the scope of notifiable incidents.
e. Introduce separate forms for Part 2A (CIRMP) and Part 2AA (Annual Report) obligations to improve clarity and guidance for SOCI Act reporting.
f. In keeping with the ambition for sector-by-sector approaches, consider extending the 30-day update requirement for the Asset Registry for the data sector.

Shield 5 – Sovereign Capabilities

Building the workforce through a National Digital and AI Skills Partnership

Developing Australia's capabilities in cyber security requires a long-term, coordinated investment in digital workforce development – focusing not just solely on cyber security, but also on AI, cloud, data centres and broader digital skills.

Australia's current education and training systems (with a few exceptions) are struggling to keep pace with the breakneck speed of technological change. Curricula can take years to update while industry skill needs evolve in real time. Meanwhile, employers across sectors report challenges in finding the right digital talent, and workers lack accessible upskilling routes.

Microsoft has advocated for the creation of a National AI Skills Partnership – based on models such as the NSW Digital Skills and Workforce Compact or the UK "tech first" program – which would bring together government, industry, education providers, and other key stakeholders to build a pipeline of AI skilled workers across the digital economy. This proposal could be extended beyond AI to encompass digital skilling more broadly, including cyber security.

The partnership would focus on improving upskilling and reskilling pathways for the existing workforce, training the next generation of Australians in the foundational digital and AI skills they need for the modern workplace, and reforming our skills and training systems to deepen specialist capability and improve pathways into the workforce. Adopting such an approach would reflect the scale and urgency of the challenge across all aspects of Australia's digital workforce, and the need for shared responsibility in addressing it.

Microsoft's experience shows partnership-based models, such as the NSW Institute of Applied Technology – Digital (IAT-D), can deliver scalable, inclusive outcomes that blend vocational and university learning in collaboration with industry and align training with real-world job requirements.

Spotlight on the NSW IAT-D Model for Digital Skills Development
The Institute of Applied Technology – Digital (IAT-D) in NSW is a leading example of an agile, industry-aligned skilling model designed to support rapid upskilling and reskilling across Australia's digital workforce. It is a collaboration between TAFE NSW, Microsoft, Macquarie University and the University of Technology Sydney. Focused on short-course delivery, the IAT-D offers flexible, stackable training options that meet learners where they are – whether they're entering the workforce, transitioning careers, or deepening existing expertise. With over 300,000 enrolments to date, the IAT-D has demonstrated strong demand for practical, job-ready skills.

Its cybersecurity offerings include courses such as Introduction to Cyber Security, Application of AI for Cyber Security, Cyber Incident Threat Detection and Prevention, Cloud Security, and Digital Forensics, each designed in partnership with industry to reflect real-world needs and emerging threat landscapes.[12]

The focus of any partnership model must be on delivering real on-ground results. We propose an approach centred on three key elements: 1) a clear national vision, with concrete objectives to measure success; 2) a strong and accountable central coordinating mechanism or governing body, that brings everyone to the table, delivers coordinated action and ensures delivery; and 3) practical on-ground programs/initiatives that equip people with the skills needed for today and tomorrow, including by scaling what works already and addressing gaps for further action.

Recommendation 11: Strengthen workforce capability through a National Digital and AI Skills Partnership – Enable cyber, AI and broader digital skills development across the economy by creating a coordinated national partnership model. The partnership should involve government, industry, education providers, unions and other key stakeholders. It should advance reforms to our skills and training systems, support training of the existing workforce and ensure the next generation are equipped with digital skills for the future.

Shield 6 – Strong Region and Global Leadership

International regulatory alignment

Microsoft welcomes the Government's acknowledgment of the importance of international cyber security regulatory alignment. Globally, businesses face a patchwork of divergent cyber security regulations across jurisdictions, from incident reporting rules to cloud security certifications. Inconsistent rules are driving up compliance costs, creating operational complexity, and diverting resources away from actual security improvements impacting overall resilience. For companies operating across multiple markets, navigating a patchwork of definitions, timelines, and reporting thresholds is not only inefficient but also risks undermining the effectiveness of incident response and coordination.

From a security standpoint, regulatory fragmentation can inadvertently hinder collective defence. For example, when incident reporting requirements vary widely between jurisdictions, it becomes harder to share timely, actionable intelligence across borders. This slows down the detection of systemic threats and weakens the global response to malicious cyber activity. The Australian Strategic Policy Institute (ASPI) has recognised this challenge across the Indo-Pacific region and argued for a greater focus on regulatory alignment to reduce red tape and strengthen regional resilience.[13]

Microsoft recommends that Australia work through relevant international fora – including the OECD and the Quad – to prioritise international alignment on cyber incident reporting as a first step. This includes working with key partners to harmonise definitions of reportable incidents, establish consistent reporting timelines (such as the widely accepted 72-hour window), and promote reciprocal recognition of reporting obligations. By focusing on this foundational area, Australia can reduce regulatory friction, improve cross-border coordination, and help ensure that cybersecurity regulations support, not hinder, security outcomes.

[12] iat.tafensw.edu.au/iat-digital

[13] ASPI 2025, Indo-Pacific needs alignment, not uniformity, to remove cyber red tape

Recommendation 12: Prioritise international cyber security regulatory alignment – Reduce the growing complexity caused by fragmented and duplicative cybersecurity regulations by better aligning with international standards and promoting reciprocity or mutual recognition agreements– starting with harmonising divergent requirements for cyber incident reporting.

Strengthening cyber deterrence

The Australian Government's leadership in advancing cyber deterrence and accountability is commendable and sets a strong example for the region and beyond. The coordinated use of attributions, advisories, and sanctions—particularly in partnership with international allies—has demonstrably imposed costs and reputational damage on malicious actors, disrupting their operations and signalling that such behaviour will not be tolerated. These measures not only hold perpetrators to account but also raise awareness across government, industry, and the broader community, strengthening collective resilience against evolving threats.

These tools are essential components of a robust deterrence framework. Public attributions clarify the boundaries of acceptable behaviour in cyberspace and help defenders counter adversary tactics. Sanctions and other consequences, applied consistently and transparently, reinforce international norms and demonstrate resolve. However, these responses have been insufficient to deter adversaries from targeting critical infrastructure with cyber operations. Cyber deterrence must be multidimensional, leveraging not only cyber but also economic, diplomatic, and even military instruments to impose costs and signal consequences across domains.

Looking ahead to Horizon 2, Australia should consider expanding its toolkit for cyber diplomacy and deterrence. This could include targeted declassification of intelligence to expose adversary operations, strengthening bilateral and multilateral agreements – including at the United Nations – to uphold clear expectations for responsible state behaviour, and pursuing coalition-based responses to major incidents. Enhanced intelligence sharing, joint technical countermeasures, and coordinated public messaging can further amplify the impact of deterrence efforts.

Ultimately, cyber deterrence is a political challenge that requires political solutions. Australia's proactive stance -clarifying red lines, signalling consequences, and building broad coalitions - will be critical to shaping a safer and more stable digital environment. Continued leadership in setting norms, imposing meaningful costs, and fostering international collaboration will help ensure that cyberspace remains secure and resilient in the face of growing threats.

Recommendation 13: Strengthen Australia's cyber deterrence posture through coordinated attributions, advisories, and sanctions in coordination with international partners. This should include expanding the use of multidimensional deterrence measures—such as economic, diplomatic and military instruments—to impose meaningful costs that hold malicious actors (including state-based actors) to account.

Shaping international cyber rules, norms and standards

Australia should continue to prioritise engagement in United Nations forums, particularly the newly established permanent mechanism following the conclusion of the Open-Ended Working Group (OEWG) on ICT security. While the OEWG demonstrated that consensus is, to a certain extent, still possible even in a polarised geopolitical climate, the stakeholder provisions in the

permanent mechanism remain particularly weak. These provisions must be significantly strengthened to enable meaningful stakeholder inclusion - without which the mechanism risks losing legitimacy and effectiveness.

Australia has long championed the inclusion of non-governmental stakeholders in multilateral processes, and we commend its leadership in this space. However, Horizon 2 presents both an opportunity - and, frankly, a necessity - for Australia to push further: advocating for robust, systematic and meaningful multistakeholder participation that includes industry, civil society, and academia as essential contributors to norm development and implementation.

Microsoft has consistently emphasised that threats in cyberspace are too complex for any one stakeholder group to tackle alone. This is why "multistakeholder diplomacy" - i.e. diplomacy that brings together governments, industry and civil society - is so critical. Multistakeholder diplomacy is not about diluting state sovereignty - it is about enriching decision-making with diverse expertise and lived experience. Australia's efforts would be most impactful if directed toward strengthening stakeholder inclusion in UN processes, supporting transparency and capacity-building for underrepresented actors, and promoting norms that protect critical infrastructure - including cloud infrastructure - and uphold human rights online. This could include drawing on modalities from the Ad Hoc Committee on Cybercrime, as a baseline upon which to build.

All of the above will be particularly important to counter authoritarian visions for cyberspace that have been gaining momentum at the United Nations in recent years. These visions often seek to centralise control, restrict multistakeholder participation, and promote frameworks that could be used to undermine openness and human rights. Australia's leadership - both regionally and globally - will be essential to push back against these trends. This means not only continuing its support for stakeholder inclusion but also actively shaping the architecture and the substance of the permanent mechanism to ensure it reflects democratic values and inclusive governance. Australia's track record, including its role in initiatives like e.g. Let's Talk Cyber, positions it well to lead this charge. But more is needed: sustained advocacy, coalition-building, and a clear commitment to embedding stakeholder voices in every phase of the UN's cybersecurity deliberations while pushing back against authoritarian visions for cyberspace.

Microsoft also supports Australia's leadership role in uplifting cyber security and accelerating the digital transformation of governments in our region, particularly our Pacific Island and South East Asian neighbours. Microsoft welcomes a strategic, whole-of-government and multistakeholder approach to enhance regional security and resilience.

Recommendation 14: Continue to prioritise engagement on cyber rules, norms and standards in United Nations forums, focusing on strengthening stakeholder inclusion and multistakeholder participation. This approach will help ensure legitimacy, resilience, and the protection of democratic values in global cyber governance.