BCA
Business Council of Australia

Horizon 2 of the 2023–2030 Australian Cyber Security Strategy

BCA Submission

August 2025

Contents

Figures

1. Executive summary

The Business Council of Australia (BCA) welcomes the opportunity to provide a submission to Horizon 2 of the 2023–2030 Australian Cyber Security Strategy. We support government's ambitious goal of making Australia the world's most cyber-secure nation by 2030.

Achieving this will require continued cooperation between government, businesses, and the community. The collaborative approach established in Horizon 1, particularly through the Executive Cyber Council, has been a positive step.

As we move into Horizon 2, the focus should be on scaling cyber maturity across the entire economy. This includes providing further support for small to medium-sized businesses and growing a diverse cyber workforce. While many of the proposed legislative changes in Horizon 1 were welcome and well-intentioned, the full impact of measures must be carefully assessed to ensure continued progress.

Australia's cyber security landscape from 2026 to 2028 will face evolving challenges driven by rapid advancements in AI, quantum computing, IoT-OT convergence, supply chain vulnerabilities, and intensified state-sponsored and cybercrime threats. To better address these, government should adopt a strategic framework centred on *economic security*, treating cyber resilience as a part of the blending economic growth, national security, resilience and sovereignty. This approach helps embeds cyber security within Australia's productivity agenda to shift focus from only harm mitigation to enabling economic benefits.

Key recommendations include implementing the low-cost Dynamic Standards International SMB1001 standard for small and medium businesses, expanding access to the ASD's National Cyber Intel Partnership, and large businesses including cyber awareness in their interactions with smaller partners.

To reduce regulatory burdens, government should clarify 'limited use' obligations under the SOCI Act. Promoting security-by-design through national standards, incentives, and increased security literacy among non-security staff is also critical. A National Digital & AI Skills Partnership, involving government, industry, and education providers, would help address the cyber skills shortage by scaling microcredentials and aligning training with employer needs.

Government should provide legal clarity on permissible Active Cyber Defence, fund additional pilots to integrate the logistics and tertiary education sectors into the Critical Infrastructure - Information Sharing and Analysis Centre (CI-ISAC) and establish a vulnerability disclosure program to encourage safe reporting. Mutual recognition of cyber accreditations across AUKUS countries would reduce compliance costs and foster greater collaboration across industrial and innovation bases.

2. Key recommendations

1. Horizon 2 should be framed in the concept of economic security.
2. Align the proposed Cyber Security Policy Evaluation Model with existing policy evaluation guidance from Treasury.
3. Implement a low or no-cost cyber standard for SMBs, mapped to international standards. This already exists off-the-shelf in the Dynamic Standards International (DSI) SMB1001 standard.
4. Leverage large–small business relationships to drive security uplift. Encourage large enterprises to embed cyber awareness, guidance, and baseline security expectations into their routine interactions with smaller suppliers and partners.
5. Improve cyber insurance accessibility. Encourage pooled or simplified SMB cyber insurance tied to an SMB standard.
6. Government should ensure any further privacy regulation reforms are carefully balanced with proportionate, risk-based cyber security requirements and support.
7. Government should clarify detail and application of 'limited use' obligation.
8. Government should establish a secure-by-design pledge based on the US CISA's.
9. Government should prioritise modernisation of public sector legacy IT systems and remove barriers to cloud migration to strengthen cyber resilience, improve productivity and address growth in the public sector IT budget.
10. Government should provide clarity on permissible and non-permissible Active Cyber Defence in Australia.
11. Government should fund additional ISAC pilots in logistics and tertiary education sectors.
12. Broaden access to ASD's National Cyber Intel Partnership (NCIP). Create an option for large firms to sponsor SMB seats in NCIP.
13. Government should establish a vulnerability disclosure program to provide security researchers with a mechanism for safe reporting.
14. Government should stress-test policy frameworks in crisis scenarios via joint red team exercises with industry, as seen in the EU's 'Cyber Europe' simulations.
15. Business would benefit from more timely reporting on ransomware alerts, trends and guides from government.
16. Establish a dedicated forum for cyber regulators to strengthen knowledge-sharing, identify regulatory gaps and overlaps, and coordinate expertise and capabilities.
17. Government, education providers and industry should work together to establish a National Digital & AI Skills Partnership to deliver cyber skills uplift across Australia.
18. Create a National Cyber Skills Framework to align qualifications with job roles, ensuring graduates have relevant skills.
19. Government should reform the Research and Development Tax Incentive to encourage more business investment in cyber security innovation.
20. Government should seek international alignment and mutual recognition of cyber security regulations, focusing first on divergent requirements on cyber incident reporting.
21. Government should work with the US and UK governments to develop a mutual recognition framework for cyber accreditations in defence supply chains, especially focused on AUKUS Pillar II.

3. Detailed response

3.1 Outlook for Horizon 2

Over the 2026 to 2028, Australia's cyber security technology landscape will be shaped by:

- AI and automation – Rapid advances in generative AI will enable both defensive automation (threat detection, incident triage) and offensive capabilities (phishing at scale, automated vulnerability discovery).
- Quantum technologies – Progress in quantum computing heightens the urgency for migration to post-quantum cryptography.
- IoT and OT convergence – Increasing interconnection of industrial control systems with enterprise IT expands the attack surface, particularly in energy, transport, health, and manufacturing.
- Supply chain risk – Software and hardware dependencies, particularly from complex global suppliers, remain a critical vulnerability, requiring deeper assurance mechanisms and provenance tracking.
- Critical infrastructure resilience – Natural disasters and cyber–physical convergence demand joint resilience planning across sectors.

Strategic factors include:

- Global threat actor evolution – State-sponsored campaigns are intensifying against Australia and allies, with resources and capabilities to target even the most secure critical infrastructure, while cybercrime-as-a-service lowers the skill barrier for high-impact ransomware and fraud.
- Workforce capability – Addressing a shortfall of cyber professionals through national skills pipelines, cross-sector secondments, and vocational pathways.
- Regulatory harmonisation – Simplifying overlapping compliance regimes and aligning with international frameworks (e.g. ISO 27001, NIST CSF) would reduce costs for business while maintaining assurance.
- Geopolitical alignment – Strengthening cyber diplomacy with regional partners to counter hostile influence and secure supply chains in critical technologies.

Cyber incidents cost Australia tens of billions of dollars annually. Investments in resilience should be treated as economic productivity measures, not just security costs. To propagate and progress this idea, government would benefit from framing Horizon 2 in the concept of *economic security*.

Economic security refers to a nation's ability to safeguard the resources, industries, and infrastructure that underpin its prosperity and sovereignty from external shocks, coercion, or disruption. It is increasingly seen as inseparable from national security, particularly in an era of global supply chain fragility, technological competition, and geopolitical tension.

For example, Japan has created the role of Minister for Economic Security in 2021 and embedded economic security into law through its 2022 Economic Security Promotion Act, which strengthens protection of critical technologies, secures supply chains for strategic goods such as semiconductors, and tightens oversight of sensitive infrastructure.

Australia's *Report of the 2024 Independent Intelligence Review*[1] released in March 2025 is the first major government document to promote adoption of the concept of economic security in Australia. It recommends that 'a distinct economic security function be established in the Treasury, including secondees from relevant NIC agencies.'[2]

Taking an economic security framing would also embed cyber security within government's productivity agenda. Economic security is closely tied to productivity because a stable and resilient economic environment enables consistent output, innovation, and efficient resource allocation, which are critical drivers of productivity.

When a nation ensures economic security through secure supply chains, protected critical industries, and reduced vulnerabilities to external shocks, businesses can operate without disruptions, invest confidently in research and development, and optimise labour and capital. This would also help shift the narrative from merely mitigating harms to enabling benefits, giving cyber security a more positive and enabling character for business.

[1] https://www.pmc.gov.au/resources/2024-independent-intelligence-review
[2] https://www.pmc.gov.au/resources/2024-independent-intelligence-review p.61, 62

Recommendation

1. Horizon 2 should be framed in the concept of economic security.

3.1.1 A conceptual framework for evaluating cyber security outcomes

The proposed high-level model for Horizon 2 has room for simplification. The proposed model is more complex than the conventional policy evaluation process, which is simpler and more thorough. The Australian Centre for Evaluation, within Treasury, provides a Commonwealth Evaluation Toolkit that outlines this model.[3]

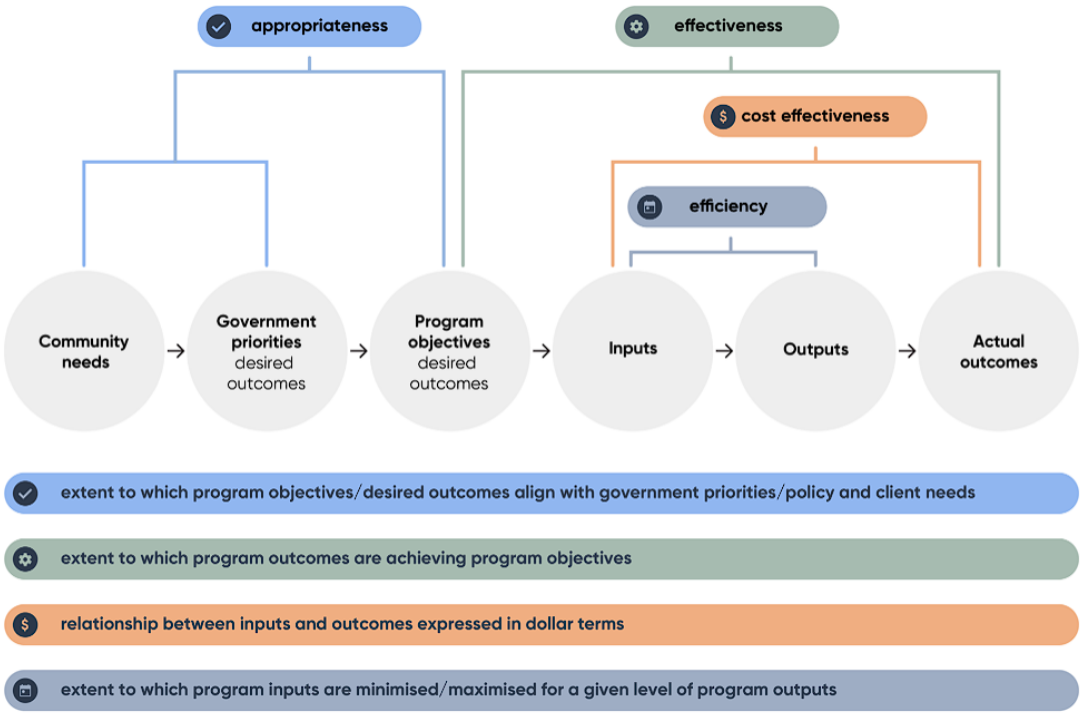

Figure 1: Key dimensions of policy evaluation (Australian Treasury)

The proposed Cyber Security Policy Evaluation Model would be better if it more closely followed the model shown in Figure 1. The Cyber Security Policy Evaluation Model already includes many of the elements that can be readily adapted into the Treasury model for policy evaluation.

Recommendation

2. Align the proposed Cyber Security Policy Evaluation Model with existing policy evaluation guidance from Treasury.

3.2 Shield 1: Strong businesses and citizens

3.2.1 Cyber security in SMBs and the NFP sector

Small and medium businesses (SMBs) underpin Australia's economy, yet they are disproportionately exposed to cyber threats. Strengthening their resilience requires practical measures that are affordable, easy to adopt, and connected to broader national efforts.

A good starting point is a baseline cyber standard with a simple certification pathway. This should be offered at low or no cost, aligned with international frameworks, and anchored in proven local solutions. The Dynamic Standards International (DSI) SMB1001 standard, developed with input from Australian Signals Directorate (ASD), Council of Small Business Organisations Australia, Telstra and others, is ready to be scaled. Recognising and promoting such off-the-shelf solutions would accelerate adoption and give SMBs clarity on what good practice looks like.

[3] https://evaluation.treasury.gov.au/toolkit/commonwealth-evaluation-toolkit

Finally, government should encourage large businesses to actively guide their smaller partners. By embedding clear expectations and basic cyber practices into everyday dealings, big firms can help lift the cyber hygiene and maturity of the broader ecosystem. Coupled with simplified or pooled cyber insurance tied to an SMB standard, these steps would create a virtuous cycle of uplift, assurance, and accountability.

Recommendations

3. Implement a low or no-cost cyber standard for SMBs, mapped to international standards. This already exists off-the-shelf in the Dynamic Standards International (DSI) SMB1001 standard.
4. Leverage large–small business relationships to drive security uplift. Encourage large enterprises to embed cyber awareness, guidance, and baseline security expectations into their routine interactions with smaller suppliers and partners.
5. Improve cyber insurance accessibility. Encourage pooled or simplified SMB cyber insurance tied to an SMB standard.

3.2.2 Privacy reform

A balanced approach to privacy reform must also take into account the intersection with cyber security risk management, particularly for SMBs that often have lower levels of maturity in both privacy compliance and cyber resilience. While outcomes-based regulation provides welcome flexibility, it may unintentionally place additional burdens on companies that lack the resources to design compliance programs while simultaneously defending against escalating cyber threats. For large or small organisations, any reform pathway should therefore be carefully calibrated to avoid creating parallel compliance obligations that divert resources away from risk management.

For SMBs, the priority must remain on building strong cyber security foundations such as patching, access controls, and incident response planning which reduce the risk of personal information compromise. Privacy obligations that are misaligned with cyber risk management could inadvertently increase vulnerability by forcing businesses into compliance exercises that do not meaningfully enhance security. To ensure reforms are effective, privacy regulation should be integrated with proportionate, risk-based cyber security requirements, accompanied by a low or no-cost cyber certification, practical guidance, templates, and capacity-building initiatives. This alignment would both lift the baseline of protection for individuals' personal information and ensure regulatory reform does not undermine resilience where it is most fragile.

Recommendation

6. Government should ensure any further privacy regulation reforms are carefully balanced with proportionate, risk-based cyber security requirements and support.

3.2.3 Regulatory and compliance burden

Large businesses are often navigating complex, multi-jurisdictional environments. Overlapping or unclear obligations frequently create compliance fatigue, particularly in heavily regulated sectors like finance, healthcare, or critical infrastructure. For large businesses, this manifests as significant resource allocation to repetitive reporting. Unlike smaller organisations, which struggle with limited budgets, large enterprises face inefficiencies at scale, with dedicated compliance teams grappling with bureaucratic demands that dilute their focus on addressing actual threats.

- To address these challenges, large businesses are adopting sophisticated strategies to integrate regulatory compliance with operational resilience, ensuring they meet obligations while enhancing cyber security. Many are embracing a shift-left approach, embedding cyber security into procurement, system design, and governance processes from the outset. This proactive integration minimises duplication and aligns compliance with practical security outcomes.
- There's also a growing shift towards outcome-based frameworks, where organisations prioritise measurable improvements in cyber maturity and resilience over rigid adherence to prescriptive checklists. Furthermore, large businesses are employing risk-based triage, directing compliance efforts towards areas of material risk rather than spreading resources uniformly across all regulatory domains.
- Business welcomes Australia's inclusion of a 'limited use' exception in its cyber legislation, recognising it as an important step toward encouraging disclosure without automatically exposing organisations to greater liability. However, many companies see room for refinement. International companies in particular may not

respond to this incentive, given that their compliance focus is on broader global standards rather than Australian-specific carve-outs. The legislation is on the books but understanding of how it works could be better. Businesses argue it will only achieve its intended effect if lawyers, regulators, and industry bodies actively explain how it works in practice. More targeted outreach and engagement would help to build confidence that reporting won't create unnecessary legal or commercial risks, ensuring organisations feel safe enough to use the regime as intended.

Recommendation

7. Government should clarify detail and application of 'limited use' obligation.

3.3 Shield 2: Safe technology

Safety and security-by-design are important to building trust, resilience, and innovation in Australia's digital economy. In an era where cyber threats evolve rapidly, embedding security-by-design safeguards can ensure organisations remain at the forefront of technological change (such as AI and quantum) help prevent cascading failures, such as those seen in global supply chain attacks like the 2020 SolarWinds incident.

Large businesses face significant barriers to adopting security-by-design. The pressure for rapid market delivery often leads to de-prioritising security processes, accumulating technical debt with unaddressed vulnerabilities. Legacy systems, widespread in the public sector and common in Australia's corporate and critical infrastructure, are difficult and costly to secure due to their outdated and poorly documented nature. Additionally, a cultural misconception that security is merely a compliance issue, rather than a core engineering discipline, hinders the integration of security as a shared responsibility across teams.

Another challenge is the difficulty in quantifying the ROI of security-by-design, as its benefits lie in preventing incidents, which is hard to measure. A shortage of skilled cybersecurity professionals in Australia exacerbates the issue, with few engineers combining development and security expertise, leading to friction between teams. Moreover, managing third-party risks in complex digital ecosystems, with diverse vendors and cloud providers, poses governance challenges, as each external component expands the organisation's attack surface.

Australia's national cyber security posture would be strengthened by the adoption of a government-supported secure-by-design pledge akin to that launched by the US Cybersecurity and Infrastructure Security Agency (CISA). The CISA pledge, rolled out in May 2024, encourages software developers to commit to seven foundational and measurable security goals, including eliminating default passwords, enhancing vulnerability disclosure, promoting memory-safe coding, and enabling multi-factor authentication, aiming to shift cyber security responsibility toward vendors and embed stronger protections upfront in development. A similar Australian pledge would amplify existing efforts like the ASD's Secure-by-Design Foundations[4] by introducing publicly trackable commitments and fostering greater accountability across the tech sector.

Government must also take direct action to modernise legacy IT systems, which remain in widespread use across the Australian Public Service, exposing both the Australian Government and citizens to significant cyber risk. Over 70 per cent of agencies remain reliant on these legacy systems, which are particularly prevalent in larger and more complex agencies.[5] Transitioning to cloud-based platforms will not only strengthen security, but can also reduce costs, unlock significant productivity gains by enabling AI systems, reduce emissions, and enhance operational resilience.

Recommendations

8. Government should establish a secure-by-design pledge based on the US CISA's.
9. Government should prioritise modernisation of public sector legacy IT systems and remove barriers to cloud migration to strengthen cyber resilience, improve productivity and address growth in the public sector IT budget.

3.4 Shield 3: World-class threat sharing and blocking

A strong, proactive cyber posture means government enables industry to defend against malicious actors. Current efforts such as ASD's Cyber Threat Intelligence Sharing platform (CTIS) platform are a foundation, but government must move to remove barriers, incentivise action, and reduce duplication.

[4] https://www.cyber.gov.au/resources-business-and-government/governance-and-user-education/secure-by-design/secure-design-foundations
[5] https://www.finance.gov.au/sites/default/files/2025-03/2024_Data-Maturity-Report.pdf

First, clarity on permissible active defence is essential. At present, legal uncertainty prevents businesses from using proportionate defensive measures such as automated IP blocking or deception technologies. The UK's National Cyber Security Centre explicitly recognises such activities as part of responsible defence[6], and Australia should issue similar guidance, ensuring SMBs and large enterprises alike can act without fear of liability.

Second, industry-led threat intelligence sharing ecosystems should be expanded. The Health Cyber Sharing Network (HCSN) pilot funded under Horizon 1 is showing how more sectors can be brought into a cross-sectoral ISAC model in Australia.[7] Following on from this, government should fund additional pilots – the logistics and higher education sectors should be next, given their roles in systemic resilience.

Third, information sharing must extend beyond large enterprises. Broader access to the National Cyber Intelligence Partnership (NCIP) would allow real-time threat blocking to reach smaller suppliers, with large organisations potentially sponsoring SMB participation. A major challenge for SMBs is lack of context around threat information, which limits prioritisation and actionability. The Critical Infrastructure – Information Sharing and Analysis Centre (CI-ISAC), a member-driven non-government organisation, addresses this by providing technical indicators, detection data, and contextual advisories through an accessible member portal. This enables organisations of any maturity level to gain actionable insights via a user-friendly interface. As a formal CTIS partner, CI-ISAC also acts as a trusted intermediary, bridging gaps between members.

Fourth, on vulnerability disclosure, Australia should adopt a centralised 'safe harbour' program. This could be modelled on examples such as the US Department of Defense's Vulnerability Disclosure Program[8], or the Dutch Coordinated Vulnerability Disclosure program (CVD).[9] A national scheme would provide legal certainty for researchers and low-cost assurance for businesses.

Finally, government should stress-test policy frameworks in crisis scenarios via joint red team exercises with industry, as seen in the EU's 'Cyber Europe' simulations[10], drawing lessons from Exercise Convergence 2025.[11] As highlighted in the discussion paper, the Cyber Operational Resilience Intelligence-led Exercises program (CORIE) would be a suitable way to do this. These exercises reveal legislative gaps before a real crisis occurs, building confidence in the shared responsibilities of government and business. However, these are costly and resource intensive, so government should carefully co-develop exercises with industry participants.

Recommendations

10. Government should provide clarity on permissible and non-permissible Active Cyber Defence in Australia.
11. Government should fund additional ISAC pilots in logistics and tertiary education sectors.
12. Broaden access to ASD's National Cyber Intel Partnership (NCIP). Create an option for large firms to sponsor SMB seats in NCIP.
13. Government should establish a vulnerability disclosure program to provide security researchers with a mechanism for safe reporting.
14. Government should stress-test policy frameworks in crisis scenarios via joint red team exercises with industry, as seen in the EU's 'Cyber Europe' simulations.
15. Business would benefit from more timely reporting on ransomware alerts, trends and guides from government.

3.5 Shield 4: Protected critical infrastructure

The Security of Critical Infrastructure (SOCI) Act has undergone multiple rounds of amendments, each layering new obligations, ranging from expanded sector coverage to data-storage definitions and risk-management refinements. Originally targeted at utilities, the Act has since increased to encompass 11 sectors and 22 asset classes, ranging from food and groceries and education to data processing and transport. Uniform obligations across diverse sectors does not accommodate the significant variations in risk profiles and maturity levels.

The SOCI Act now includes the 'data storage or data processing' industry, covering cloud computing and SaaS providers. This adds to existing regulations like the Privacy Act 1988, Telecommunications Act 1997, and various

[6] https://www.ncsc.gov.uk/blog-post/introducing-active-cyber-defence-2
[7] https://ci-isac.org.au/hcsn/
[8] https://www.dc3.mil/Missions/Vulnerability-Disclosure/Vulnerability-Disclosure-Program-VDP/
[9] https://www.government.nl/topics/cybercrime/fighting-cybercrime-in-the-netherlands/responsible-disclosure
[10] https://www.enisa.europa.eu/topics/skills-and-competences-for-companies/cyber-europe
[11] https://www.nema.gov.au/about-us/media-centre/collaborative-crisis-management-exercise-convergence-2025-action

government and international cyber security standards. These overlapping frameworks create compliance challenges for cloud and SaaS providers, particularly in incident response and reporting, where inconsistent requirements across sectors and jurisdictions complicate processes. The complexity of managing multiple clients and supply chains, combined with recent high-profile data breaches, highlights the difficulty of balancing compliance with effective security management.

Case Study: Cisco and critical infrastructure

Cisco has observed a wide spectrum of approaches adopted by critical infrastructure asset owners when engaging on supply chain assurance and cyber security risk. At one end are customers who undertake highly detailed and comprehensive security risk assessments of Cisco and its associated cloud services. These reviews frequently mirror, and in many instances directly overlap with, the types of questions that form part of recognised international audit standards, such as ISO/IEC 27001 and SOC 2. Cisco also places at the same end of the spectrum those customers who request formal ISO or SOC documentation as evidence of compliance.

At the opposite end of the spectrum, Cisco occasionally encounters customers whose inquiries are far less granular, with some limiting their engagement to broad questions such as whether Cisco is "SOCI compliant" or using similar terminology. This divergence indicates that the SOCI Act remains relatively new in its application and interpretation. Consequently, sectors and organisations with comparatively lower levels of maturity in cyber risk assessment practices are still in the process of developing the necessary capabilities and frameworks to engage with suppliers and service providers at the same level of detail as their more mature counterparts.

Cisco considers that, as regulatory and industry understanding of the SOCI framework continues to evolve, greater consistency and depth of engagement across sectors will emerge. It would be advantageous for the proposed Cyber Security Policy Evaluation Model to be applied to the requirements of the SOCI Act. This would provide an evidence-based mechanism to assess the effectiveness of existing obligations, while also informing any potential refinements to the legislative or regulatory settings. This would support both industry and government in ensuring that compliance expectations are clear, practicable, and aligned with best practice in cyber security risk management.

Cloud and SaaS providers also face challenges in risk management, as mandated by the SOCI Act's Critical Infrastructure Risk Management Program (CIRMP) Rules, which require identifying and mitigating cyber risks. Multiple risk management frameworks, including Australian and international standards like ISO 31000, create inconsistencies in definitions and expectations. Supply chain complexity further complicates compliance, as cloud services often integrate components from various suppliers across industries. The lack of a unified standard for supply chain resilience, coupled with sector-specific requirements and a shortage of skilled professionals, increases costs and challenges.

To assist with these challenges, government could establish a dedicated forum for cyber regulators. It would bring together regulators across critical infrastructure sectors and sector-specific frameworks, enabling stronger knowledge-sharing, identification of regulatory gaps and overlaps, and more effective coordination of expertise and capabilities. Similar models already exist, such as Digital Platform Regulators Forum[12] and the Council of Australian Financial Regulators.[13]

Recommendation

16. Establish a dedicated forum for cyber regulators to strengthen knowledge-sharing, identify regulatory gaps and overlaps, and coordinate expertise and capabilities.

3.6 Shield 5: Sovereign capabilities

3.6.1 Skills

The traditional, long-form education pathways alone cannot meet the urgent demand for cyber professionals. While we must strengthen the national curriculum to start teaching cyber education from an early age, we must also formally recognise and accredit high-quality, industry-relevant microcredentials and specialised bootcamps. This allows individuals to quickly gain targeted skills and enter the workforce, offering a more agile response to evolving cyber threats.

[12] http://dp-reg.gov.au/
[13] https://www.cfr.gov.au/

Government support for, and collaboration with, industry bodies to establish clear accreditation standards would provide confidence in these qualifications, enabling businesses to swiftly identify and onboard skilled talent. This also opens up pathways for mid-career transitions, allowing individuals from other sectors with transferable skills to rapidly re-skill and contribute.

Major technology companies, both domestic and international, possess invaluable expertise, training infrastructure, and a deep understanding of the skills required in the modern cyber landscape. Government should leverage and nationalise existing mechanisms for digital, AI and cyber skilling such as the NSW Digital and Workforce Compact[14] and the Institute of Applied Technology – Digital.[15] A national approach would amplify these successes, ensure every state benefits, and open high-value career pathways to all Australians.

This could be achieved through a National Digital & AI Skills Partnership (including cyber security skills) and would be a coordinated national system that:

- Directly links training to employer demand, ensuring skills investment translates into jobs.
- Expands and accelerates talent pipelines in every state and territory, with consistent quality and reach and a coherent strategy across education, higher education and VET systems.
- Opens high-value digital and AI careers to Australians from all regions and backgrounds.
- Creates a workforce with the agility to adapt as technology evolves – lifting productivity and competitiveness.

It would focus on three priority cohorts:

- The existing workforce – creating fast, flexible upskilling and reskilling pathways for those already in work, particularly in sectors undergoing transformation and capability-constrained SMBs.
- The next generation – ensuring students leave school with foundational AI and digital fluency, and access to practical, work-aligned post-school training.
- Tertiary learners – reshaping degrees and qualifications to better match emerging technologies, employer needs and improve employment outcomes.

The Partnership would embed continuous collaboration between government, education providers, and industry with defined roles, equal voice, and shared accountability.

- Government (as a whole-of-government effort) would:
  - Fund demand-led training models and scale proven pilots.
  - Convene and coordinate national activity, setting clear, measurable goals.
  - Incentivise inclusive upskilling, especially for SMBs and under-represented groups.
  - Partner with industry to lift AI capability in the non-market sector (e.g. education, health, public service).
  - Align funding and policy to support non-traditional, applied pathways such as microcredentials, digital apprenticeships, and industry-based qualifications.
- Education providers would:
  - Co-design courses and microcredentials with industry.
  - Fast-track curriculum updates to meet emerging skill needs.
  - Deliver applied, modular training for students and workers.
- Industry would:
  - Co-design and directly invest in skilling programs for the workforce and community.
  - Signal future demand and provide real-world content.
  - Recognise high-quality, industry-backed credentials in hiring and promotion.

The Partnership would work alongside existing coordination bodies including Jobs and Skills Councils and the Australian Tertiary Education Commission to ensure training systems are responsive, complementary, and aligned to national workforce priorities.

[14] https://www.nsw.gov.au/education-and-training/nsw-digital-compact
[15] https://www.iat.tafensw.edu.au/iat-digital

Recommendation

17. Government, education providers and industry should work together to establish a National Digital & AI Skills Partnership to deliver cyber skills uplift across Australia.
18. Create a National Cyber Skills Framework to align qualifications with job roles, ensuring graduates have relevant skills.

3.6.2 Innovation and R&D

To nurture the growth of robust sovereign capabilities, government should improve existing incentives for businesses to invest in R&D, which would enable more and better cyber security innovation. Just 5 per cent of Australian businesses account for 48 per cent of the country's business R&D expenditure through the Research and Development Tax Incentive (RDTI). Reforms should include:

- Simplify RDTI rates to a consistent offset of 18.5 per cent above the company tax rate.
- Remove the $150 million RDTI cap.
- Introduce an RDTI collaboration premium for partnerships between businesses and higher education or government research institutions.

For more details explanation and supporting recommendations, see the BCA's *Submission to the Strategic Examination of R&D*[16] and report *Unlocking Australia's R&D potential*.[17]

Recommendation

19. Government should reform the Research and Development Tax Incentive to encourage more business investment in cyber security innovation.

3.7 Shield 6: Strong region and global leadership

Business has a crucial role to play in amplifying Australia's commitment to deterring malicious cyber actors, strengthening regional cyber resilience, and shaping international norms.

3.7.1 International regulatory alignment

Divergent cyber regulations across international jurisdictions are a significant strain on multinational businesses, including Australian businesses seeking to expand globally. They not only create additional complexity and cost that impacts productivity, they also impact operational efficacy and responsiveness. Cyber incident reporting requirements are a key example where we see divergent global requirements on thresholds for reporting, timeframes and information requirements.

By contributing their practical experience and expertise to discussions on global cyber norms and standards, businesses can help shape frameworks that both improve cyber resilience and reduce unnecessary compliance costs. Participation in national efforts to uphold international cyber norms and defend against malicious actors enhances the reputation of Australia as a responsible and secure place to do business. In an increasingly trust-sensitive digital economy, this reputation can be a powerful differentiator, attracting customers, investors, and top talent.

3.7.2 Mutual recognition of AUKUS cyber security accreditations

A significant challenge facing companies operating within the AUKUS alliance is the duplicative and costly burden of meeting separate national cyber security regulations. While the US, UK, and Australia are close allies with well-developed domestic standards, the lack of alignment means commercial organisations must undergo similar accreditation and compliance processes three times. This creates significant friction, increases costs, and delays the delivery of critical capabilities, particularly for advanced technologies being jointly developed under Pillar II.

To address this, industry stakeholders across the three countries including the BCA are proposing the development of a mutual recognition framework for cyber accreditations. This is easier than attempting a complete harmonisation of regulations. The core principle is to 'accredit once, use thrice,' allowing a certification

[16] https://www.bca.com.au/submission_to_the_strategic_examination_of_r_d
[17] https://www.bca.com.au/unlocking_australia_s_r_d_potential

from one AUKUS nation to be accepted by the others. By agreeing on a set of mutually acceptable standards for both organisations and technologies, the alliance can foster greater collaboration, enhance innovation, and uplift the overall cyber security maturity of its shared defence industrial base.

Recommendation

20. Government should seek international alignment and mutual recognition of cyber security regulations, focusing first on divergent requirements on cyber incident reporting.
21. Government should work with the US and UK governments to develop a mutual recognition framework for cyber accreditations in defence supply chains, especially focused on AUKUS Pillar II.

BCA

Business Council of Australia

BUSINESS COUNCIL OF AUSTRALIA
[redacted]
www.bca.com.au

© Copyright August 2025 Business Council of Australia ABN 75 008 483 216

All rights reserved. No part of this publication may be reproduced or used in any way without acknowledgement to the Business Council of Australia.

The Business Council of Australia has taken reasonable care in publishing the information contained in this publication but does not guarantee that the information is complete, accurate or current. In particular, the BCA is not responsible for the accuracy of information that has been provided by other parties. The information in this publication is not intended to be used as the basis for making any investment decision and must not be relied upon as investment advice. To the maximum extent permitted by law, the BCA disclaims all liability (including liability in negligence) to any person arising out of use or reliance on the information contained in this publication including for loss or damage which you or anyone else might suffer as a result of that use or reliance.