Submission in Response to the Consultation on Horizon 2 of the 2023-2030 Australian Cyber Security Strategy.

Submitted by: CyberCert
Date: 29 August 2025

Please download the full submission from:
https://cybercert.ai/submissions/horizon2/CyberCert-DHA-Submission-29Aug.pdf

Level 38 / 71 Eagle Street,
Brisbane QLD 4000

https://cybercert.ai **CyberCert Pty Ltd**

Table of contents

Executive Summary

At CyberCert, we see Australia's 900,000 active Small and Medium-sized Businesses (SMBs) as the beating heart of its economy, an economy envied across the world. Their continued success, and in turn the economic and strategic prosperity of Australia, relies on their cyber resilience. Our experience has demonstrated that the SMB sector is both Australia's most significant and under- addressed cyber security vulnerability.

We share in the Australian Government's ambition in building an Australia that is a world leader in cyber security. We believe that this will only be achievable by securing Australia's SMB foundation. We recognise that there are clear and present threats to Australia's SMBs, as evidenced in the Australian Cyber Security Centre's own publications. If anything, we believe the ACSC's known cybercrime events - one cybercrime every six minutes, with the average cost of a breach for a small business rising to $49,600 - likely understates the true scope of the challenge faced by the sector.

Our submission below describes a proven, market-ready, and scalable ecosystem to address this critical national challenge: the CyberCert certification program, built upon the SMB1001 standard. CyberCert is not a proposal for a new initiative; it is an existing, operational solution with demonstrated market traction, including over 300 activated partners and more than 3,000 SMB certifications in progress.[2] Its core design principles - partner-powered delivery, deep insurer integration, and alignment with government and enterprise requirements - make it the ideal mechanism to translate the strategic goals of Horizon 2 into measurable, whole-of-economy outcomes.

Horizon 2 of the 2023-2030 Australian Cyber Security Strategy is an opportunity to target investment (both financial and effort) to improve the cyber resilience of Australia's SMBs. In our submission below, we describe how certification supports cyber security in several areas, including in promoting cyber security awareness, understanding of cyber risk and implementation of cyber controls, and stimulation of the cyber security industry. Ultimately, we see an opportunity in Horizon 2 to leverage an existing cyber framework designed for SMBs, SMB1001 and CyberCert, to support and inform guidance for cyber security control implementation specific to SMBs.

In an industry with many frameworks and interpretations on what makes an organisation "cyber resilient", we believe that SMB1001, created by Dynamic Standards International, cuts through for SMBs. As the certification body for SMB1001, we have seen firsthand how this standard is both graspable for SMBs and contributes to real improvements in their cyber hygiene and resilience.

The value proposition for our nation is compelling. A scaled rollout of CyberCert to 100,000 SMBs by 2028 presents a tangible return on investment for Australia, including over $5 billion in potential breach loss avoidance, more than $1 billion in economic uplift from secure technology adoption, and the creation of over 9 million hours of annual sovereign cyber service work.[2] This directly stimulates the local IT industry and builds the national cyber workforce from the ground up.

Our submission demonstrates how SMB1001 and CyberCert aligns with and could enhance the Strategy's Four North Stars and Six Shields, turning your objectives into certifiable, auditable action, summarised below:

The value of certification against SMB1001, as aligned with the 2023-2030 Australian Cyber Security Strategy.

As noted in the Strategy, we are at a critical juncture. Continuing with awareness campaigns and passive resources has improved Australia's cyber resilience, but more is needed to combat the escalating threat to our SMBs. We must collectively build on these resources and connect cyber security directly to procurement and economic incentives.

This is a national 'seatbelt moment'.[2] Australia led the world in seatbelt safety, driving uptake in the use of this critical safety component from 5% to over 90% in seven years through mandates, not just awareness. We can achieve the same for cyber safety. To this end, we

propose a collaborative "co- pilot" program with the government to endorse and amplify a proven system that will not only structurally improve the safety of our digital economy, but enable it to thrive. This is a strategic investment in national resilience and prosperity.

1. Introduction: Addressing Australia's Most Significant Cyber Vulnerability

The 2023-2030 Australian Cyber Security Strategy sets a bold vision for Australia to be a world leader in cyber security by 2030.[3] Critical to achieving this vision is addressing the profound and growing vulnerability of our nation's economic engine: its 900,000 active Small and Medium-sized Businesses (SMBs).[2] These businesses are not a peripheral concern; they are the frontline of Australia's cyber resilience, and are the connective tissue of Australia's economic supply chain.

The threat is quantified and escalating. According to the ASD's ACSC, a cybercrime is reported every six minutes in Australia. While large enterprises often dominate headlines, small businesses are disproportionately targeted and harmed, with 43% of all cybercrimes aimed at this sector.[5] The financial impact is severe and worsening, with the average cost per incident for an SMB rising 8% in the last financial year to $49,600. The Horizon 2 Discussion Paper also highlights that SMBs are "increasingly vulnerable" and often "lack the capability and resources" to navigate this hostile environment.[4]

This situation points to a significant gap between the sophistication of the threat and the cyber resilience of SMBs. Horizon 1 of the Strategy successfully delivered a range of valuable resources, including the Small Business Cyber Security Resilience Service, the Ransomware Playbook, and awareness campaigns.[7] However, we believe there is more to be done. The availability of guidance has not easily translated into the desired reduction of financial impact. We assess that the reason for this gap is not only limitations in resources, but also limitations in energy and motivation. SMBs often don't have the bandwidth or specialist expertise to dedicate to cyber security, and they can find themselves overwhelmed by the complexity of existing standards.[5] They are laser-focused on revenue-driving activities like customer acquisition (62%) and client relationships (60%), with cyber security (22%) ranking as their lowest priority.[14]

We believe that the solution is not more information, but a new mechanism for implementation - an ecosystem that energises SMBs by tying cyber security directly to their potential revenue. CyberCert, powered by the SMB1001 standard, can be that mechanism. It is a proven, de-risked solution already delivering results in the market, with over 300 partners - the trusted IT providers and Managed Service Providers (MSPs) that SMBs already rely on - and over 3,000 certifications in progress.[2] By leveraging this existing commercial relationship, CyberCert turns abstract advice into tangible, verified, and commercially valuable outcomes, bridging the gap between government strategy and main-street reality.

2. Delivering the Core Objectives of Horizon 2: Embed, Empower, Enhance

The Horizon 2 Discussion Paper describes three objectives: to Embed cyber security into daily life, to Empower businesses and citizens, and to Enhance the national cyber ecosystem.[3] The CyberCert model is uniquely designed to deliver against all three of these strategic pillars.

2.1. Embed

CyberCert embeds cyber security into the fabric of everyday commerce by integrating it into existing, natural business workflows.

- Commercial Integration: The partner-powered delivery model means that for thousands of SMBs, achieving and maintaining a certified level of cyber hygiene becomes a standard component of their IT service agreement with their MSP. It ceases to be a separate, complex project and becomes an embedded, operational norm.[2]
- Insurance Integration: By working directly with leading insurers and brokers, CyberCert embeds robust cyber risk management into the process of obtaining essential business insurance. Certification becomes a clear pathway to coverage, transforming cyber security from a technical issue into a fundamental aspect of commercial risk management and governance.[2]

2.2. Empower

CyberCert empowers SMBs and Not-for-Profit organisations (NFPs) by making cyber security accessible, achievable, and commercially advantageous.

- Accessible Uplift Pathway: The tiered SMB1001 standard provides a clear, jargon-free roadmap for improvement. It treats cyber security as a journey, not a binary pass/fail outcome. A small business can start at a Bronze or Silver level and mature its posture over time, providing an achievable pathway that avoids the often overwhelming complexity of enterprise-grade frameworks.[8] This directly addresses the government's goal to "reduce the barrier for applying protective frameworks".4 It empowers business owners to "Know & show they're secure" without needing to become technical experts themselves.[2]
- Commercial Empowerment: Certification is a powerful business enabler. It provides SMBs with an independent, trusted, verifiable credential they can use to win contracts with large enterprises and government agencies that have stringent supply chain security requirements. This transforms cyber security from a perceived cost centre into a tangible source of competitive advantage and revenue growth, providing the motivation that is currently lacking.

2.3. Enhance

Adoption of the CyberCert ecosystem at scale has the potential to enhance the capability, resilience, and sovereign capacity of Australia's entire cyber landscape.

- Regulatory Enhancement: CyberCert enhances the effectiveness of the regulatory framework by providing a practical mechanism for validating cyber resilience. For SMBs struggling to interpret their obligations under schemes like the Privacy Act's Australian Privacy Principle 11 (APP11), achieving a CyberCert certification provides clear, auditable evidence that they have taken "reasonable steps" to secure data. This simplifies the complexity noted in the discussion paper and reduces the compliance burden on business.[2]
- Workforce Enhancement: The model directly enhances Australia's sovereign cyber workforce. By creating a sustainable, market-driven demand for certification services, it generates a pipeline of over 9 million hours of work annually for local MSPs and cyber professionals.[2] This stimulates hiring, training, and upskilling, providing a structural, long-term solution to the national skills shortage identified in the Horizon 2 paper and by industry bodies.

3. A Comprehensive Response to the Horizon 2 Consultation

This section provides a direct response to the specific questions posed in the Horizon 2 Policy Discussion Paper 4, structured within the framework of the Strategy's Six Cyber Shields.

3.1. Shield 1: Strong Businesses and Citizens

This shield focuses on uplifting the resilience of the broadest part of the economy. We acknowledge the focus and investment applied to this area and have valued the Federal Government raising the profile of cyber security, including through a range of public media. On a personal note, we have enjoyed seeing ACSC guidance appear across multiple information feeds and see this as a positive step in supporting Australian citizens take control of their personal cyber resilience.

While the guidance and awareness material released is an important component of the Strategy, the material we have observed appears to be heavily focused on the individual. Described below are our considerations for improving cyber resilience for SMBs.

Responses to Q7 & QB: Encouraging Uptake of Cyber Resources by SMBs and NFPs

The government's existing resources - such as the Small Business Cyber Resilience Service, Cyber Wardens, and cyber.gov.au guidance - are valuable, but uptake remains limited because SMBs lack the motivation to engage. The most powerful lever to drive meaningful participation is procurement.

The UK's Cyber Essentials program proved the power of procurement mandates. Since its launch in 2014, adoption has grown steadily- surpassing 100,000 certified businesses by 2022, with tens of thousands more each year. When certification became a requirement for certain government contracts, uptake accelerated sharply, showing that making certification a commercial necessity is the most effective way to drive rapid, widespread engagement.[13]

By endorsing CyberCert and introducing it through a stepped procurement approach, the government can make certification the obvious, low-friction alternative: SMBs can continue filling out complex, inconsistent questionnaires, or they can "get it once, show it to many" with a CyberCert certificate. Importantly, the framework provides SMBs with a simplified and obvious pathway to also meet broader compliance obligations - turning guidance and resources into certifiable outcomes.

With time and support to achieve certification, suppliers can transition smoothly before mandates take effect. This energises the entire SMB sector: motivated by contracts, SMBs proactively use government resources, private-sector MSPs deliver the uplift, and the result is a systemic increase in national cyber resilience and economic stimulation.

Response to Q9: Existing or Developing Cyber Security Standards for SMBs and NFPs

The SMB1001 standard is a strong example of an "existing or developing cyber security standard" the Policy Discussion Paper describes.[2] It has been designed from the ground up to address the specific needs and constraints of smaller entities, a gap acknowledged by industry and government alike. Its key features directly align with the desired outcomes:

- **Tiered and Accessible:** With five levels of certification (Bronze to Diamond), it treats cyber security as a journey, not a binary outcome. It is designed for growth, and its tiers are achievable for every SMB, from a local florist implementing foundational controls to a $50m technology scale-up implementing robust and highly resilient controls. This avoids the one-size-fits-all problem of enterprise frameworks.[8]
- **Market-Validated:** SMB1001 is not a theoretical construct. It is actively used within a growing ecosystem of SMBs, MSPs, insurers, and enterprises who recognise its practicality and value.9
- **Dynamic:** The standard is updated annually by industry experts to remain aligned with the evolving threat landscape, and improvements in technology, ensuring its continued relevance.

SMB1001 is an opportunity for the federal government to integrate this industry-led, market-proven solution as a certification option in procurement processes. This would provide a clear signal to SMBs and the delivery ecosystem, accelerating adoption and maximising national benefit.[10]

Response to Q11: Affordability and Accessibility of Cyber Insurance

The consultation paper rightly questions the affordability and accessibility of cyber insurance for SMBs.[4] We have observed that insurers face significant challenges in accurately assessing and pricing the risk of an individual SMB. Application forms and lengthy questionnaires are unreliable, and manual audits are prohibitively expensive. This uncertainty leads to higher premiums, extensive exclusions, or outright denial of coverage.

A certification option such as CyberCert directly solves this market challenge. The certification provides insurers with independent and auditable proof of an SMB's security posture. It transforms an SMB's cyber resilience from an unquantifiable risk into a known and verifiable quantity. This de- risks the underwriting process, enabling insurers to offer coverage with greater confidence and more competitive pricing. The active integration of CyberCert within major insurance partners is concrete evidence of this model's effectiveness in making insurance more accessible.[2]

Responses to Q12 & Q13: Understanding and Protecting Against Ransomware

Ransomware remains a primary threat to Australian businesses. While awareness is necessary and important, prevention depends entirely on the consistent implementation of fundamental security controls. Aligning with a certification framework such as SMB1001 builds resilience against ransomware by requiring foundational controls. SMB1001 defines

tiered requirements for cyber controls and enables independent validation of the very controls that the government's own Ransomware Playbook recommends, such as multi-factor authentication (MFA), regular and tested data backups, and timely software patching.

An SMB with a CyberCert certification has not just unlocked the playbook; they have verifiably implemented its core strategies, significantly reducing their vulnerability to attack.

Responses to Q16 & Q17: Harmonising and Simplifying Cyber Regulation

Australian businesses find the current regulatory landscape complex and burdensome.[4] At CyberCert, we have tackled this challenge by using SMB1001 as a practical "bridge standard" that harmonises and simplifies control implementation for SMBs. It translates the high-level principles of multiple regulatory frameworks - such as the "reasonable steps" requirement of APP11 under the Privacy Act 1988, and supply chain expectations under the Security of Critical Infrastructure Act 2018 (SOCI Act) - into a single, achievable set of controls.[2] An SMB that achieves a Gold level of certification can confidently demonstrate to regulators, customers, and insurers that it has a robust and compliant security program in place, reducing its compliance overhead and allowing it to focus on its core business.

The Most Powerful Lever: Procurement Efficiencies and Mandates

We have demonstrated that a clear, achievable, and affordable path to SMB cyber resilience already exists. Evidence from the UK and our own market shows that procurement mandates are the single most effective lever for driving rapid, widespread adoption.

Importantly, a tiered approach ensures this cuts down on complexity - Suppliers are given a viable alternative to answering complex, inconsistent questionnaires. Over time, as certification uptake grows, procurement can move from optional to mandated, with suppliers having had the time and support to achieve their certification. Ultimately, significantly reducing red tape as the SMB need only achieve certification once during the validity period.

By taking this approach, Australia can lead the world in SMB cyber resilience by 2030 - streamlining procurement, cutting compliance burden, and expanding contract access.

A true win-win-win.

3.2. Shield 2: Safe Technology

Responses to Q18 & Q19: Standards for Devices and Supporting Consumers

The government's work on standards for smart devices and other technologies, as enacted through the Cyber Security Act 2024, is a vital step forward.[7] However, threat actors do not confine themselves to a single device, rather they attack weaknesses across a network. A secure-by-design product deployed in an insecure SMB environment remains a significant source of risk.

CyberCert assessments look at an organisation holistically. The controls described by the SMB1001 tiers - such as secure configuration of hardware and software, firewall

implementation, and robust user access control - creates a foundational security posture necessary for the safe adoption of new technologies.[8] It ensures that the digital "house" an SMB operates is secure, allowing them to bring "safe appliances" into it with confidence. Therefore, CyberCert is the necessary counterpart to product-specific standards, ensuring a holistic approach to safe technology adoption across the economy.

3.3. Shield 3: World-Class Threat Sharing and Blocking

Response to Q28: Supporting a Thriving Threat Sharing Ecosystem

The government's current threat-sharing initiatives, such as funding for Information Sharing and Analysis Centres (ISACs), are valuable, however we observe that they are focused on mature, critical infrastructure sectors.[7] This approach may leave information sharing gaps within the SMB landscape and the supply chain of critical infrastructure.

A certified ecosystem is uniquely positioned to fill this critical intelligence gap. A national database of CyberCert certifications would create an unprecedented, real-time source of whole-of-economy cyber posture intelligence. For the first time, government and industry would have visibility, in aggregated and anonymised form, into the true state of resilience across the economy. It would answer strategic questions such as:

- What percentage of SMBs in the national logistics supply chain have implemented MFA?
- Which geographic regions or industry sectors have the lowest adoption of data backup controls?
- Is the national baseline of security improving month-on-month in response to policy interventions?

This data provides a powerful leading indicator of national resilience, shifting the focus from lagging indicators of failure (incident reports) to proactive measures of preparedness. Partnering with CyberCert would give the government a national dashboard to monitor risk, target investment, and measure the real-world impact of the Australian Cyber Security Strategy.

3.4. Shield 4: Protected Critical Infrastructure

Responses to Q34 & Q36: Risks Not Addressed by the SOCI Act and Support for Operators

The most significant cyber risks to Australia's critical infrastructure (CI) is not within the CI operators themselves, but deep within their vast and complex supply chains. The SOCI Act places obligations on CI operators, but they are often unable to then enforce these security standards on their many third- and fourth-party SMB suppliers.[4] This vulnerability is a vector for attack, as traditional third- party risk management often fails to extend across the entire supply chain. Most large organisations have less than 10% of partners with mature security.

CyberCert provides a scalable verification mechanism that CI operators desperately need. Instead of attempting to conduct thousands of individual, costly audits, a CI operator can simply require a specific CyberCert level (e.g., Gold) as a prerequisite for its suppliers. This outsources the complexity and cost of verification to an efficient, market-based system, allowing for certification of even the smallest suppliers. It also makes the principles of the SOCI Act practically enforceable at scale, hardening the entire supply chain and dramatically reducing the systemic risk to Australia's most essential services.

3.5. Shield 5: Sovereign Capabilities

Responses to Q39 & 041: Growing the Cyber Workforce and Identifying Transferable Skills

The persistent shortage of skilled cyber professionals in Australia - estimated at 28,000 - is a critical constraint on national security and economic growth. While grants create a market incentive, it is also important to stimulate the demand side of the market to create durable career pathways.

CyberCert is a strong example of how certification can be a vehicle for sovereign workforce development. A rollout to 100,000 SMBs will create over 9 million hours of high-value, recurring cyber security service work annually.[2] This provides the commercial incentive for Australia's nationwide network of local MSPs to hire more technicians, invest in training, and upskill their existing staff in areas with highly transferable skills (e.g., network administration, systems engineering). This is a clear secondary benefit of integrating cyber certification into procurement.

Response to Q44: Identifying and Prioritising Sovereign Capabilities

A critical, yet often overlooked, sovereign capability is a robust, geographically distributed network of local IT service providers who act as the trusted technology partners for the SMB economy. This network of MSPs is an essential national asset. The CyberCert program is designed to activate, upskill, and sustain this network, transforming it into a frontline cyber defence force for the Australian economy.

3.6. Shield 6: Resilient Region and Global Leadership

By endorsing and scaling the CyberCert model, Australia has the opportunity to establish a world- leading, exportable blueprint for national SMB cyber uplift. The concept of a government-backed, tiered certification for smaller entities is recognised as international best practice. However, the CyberCert model represents a next-generation approach through its unique combination of partner- powered delivery, deep insurer integration, and a scalable Saas platform for verification and audit. It is already active in Australia, New Zealand, the US, Canada, and the UK, demonstrating its global relevance.[2]

The following table provides a comparative analysis of leading international frameworks, highlighting the innovative advantages of the Australian model.

Attribute	Australia (CyberCert)	United Kingdom (Cyber Essentials)	Singapore (SG Cyber Safe Mark)	Canada (CyberSecure Canada)
Governance Model	Industry-led, dynamic standard (SMB1001) [8]	Government-backed, NCSC-defined [10]	Government-led (CSA)	Government-led, now SCC -managed [3]
Delivery Model	**Partner-powered (MSP-led) [2]**	Assessor-led self-assessment & audit [11]	Assessor-led certification	Third-party certification bodies [12]
Tiers/Levels	5 Levels (Bronze to Diamond) [8]	2 Levels (Essentials, Essentials Plus) [11]	2 Marks (Essentials, Trust)	3 Levels (Self-assessed to external) [12]
Insurer Integration	**Deeply integrated pathway to coverage [2]**	Encouraged, but separate process [11]	Not a primary feature	Not a primary feature [12]
Supply Chain Focus	**Primary use case for CI & Enterprise [2]**	Key driver for government contracts [10]	Encouraged	Key driver for defence contracts [12]
Scalability	**SaaS-based platform for audit & mgmt [2]**	Portal-based self-assessment [11]	Traditional certification process	Traditional certification process [12]

Table 3: Comparative analysis of leading international frameworks

This analysis demonstrates that while the goal is similar across jurisdictions, the CyberCert model's emphasis on leveraging the existing MSP and partner ecosystem, and integrating with the insurance market provides a more scalable and commercially sustainable path to mass adoption. By formally backing this model, the Australian Government can champion a globally significant innovation, exporting this capability and knowledge throughout the Inda-Pacific region and fulfilling the leadership ambition of Shield 6.

4. Conclusion: Seizing a National 'Seatbelt Moment' for the Digital Economy

The evidence is unequivocal: Australia's SMB sector represents a systemic economic and national security risk. The current approach of providing advice and resources, while forming a helpful knowledge base, has proven insufficient to counter the escalating financial and operational damage being inflicted on this vital part of our economy. A structural intervention is now required.

The CyberCert ecosystem, built on the SMB1001 standard, is that intervention. It is not another tool or standard; it is the catalyst required to activate the entire national ecosystem - SMBs, their trusted MSPs, the insurance industry, and enterprise supply chains - towards the common goal of measurable, certifiable cyber resilience. It provides the clear, affordable, and practical solution needed to drive mass adoption of baseline cyber hygiene.

This is Australia's 'seatbelt moment' for the digital economy.[2] Australia became a world leader in road safety not through awareness campaigns alone, but through decisive action. Before mandates were introduced in the 1970s, seatbelt usage was estimated at a mere 5%. By 1977, just seven years after Victoria became the first jurisdiction in the world to make wearing them compulsory, that figure had soared to 90%. This dramatic shift, which saved countless lives, was driven by a simple, effective standard combined with a public-private partnership that leveraged mandates to make safety a non-negotiable part of daily life.

The same logic applies to cyber safety today. We have the standard. We have the delivery mechanism. What is required now is the political will to make baseline cyber certification a condition of doing business with the government. This single act will energise the market, secure the supply chain, and build a resilient digital economy from the ground up.

Of course, this doesn't happen overnight, and a staged approach is required. We formally request the opportunity to present this Co-Pilot Program in detail to the Department of Home Affairs and work together to secure Australia's future.

References

- Australian Government Department of Home Affairs. (2025). Charting New Horizons: Developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy - Policy Discussion Paper. [4]
- Australian Government Department of Home Affairs. (2025). Appendix B - Status of Horizon 1 Initiatives (as at 30 June 2025). [7]
- Australian Signals Directorate's Australian Cyber Security Centre. (2024). ACSC Annual Cyber Threat Report, 2023-2024.
- Council of Small Business Organisations Australia (COSBOA). (2024). Submission to the Department of Home Affairs on Cyber Security Legislative Reforms. [5]
- CyberCert. (2025). Response to Consultation on developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy. [2]
- Defence Security & Industry (OSI). (n.d.). SMB1001. Retrieved from https://dsi.org/smb1001 [8]

Works cited

1. Small business cybercrime fight expands to construction industry - Media Statements, accessed on August 24, 2025, https://statements.qld.gov.au/statements/103359

2. Response to Consultation on developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy - Proposed Solution.pdf (See Annexe A)

3. Council of Small Business Organisations Australia (COSBOA) - submission - Department of Home Affairs, accessed on August 24, 2025, https://www.homeaffairs.gov.au/reports-and-pubs/files/cyber-security-legislative- reforms/Council-of-Small-Business-Organisations-Australia-COSBOA-submission.PDF

4. Annual Cyber Threat Report highlights evolving threat - Defence Ministers, accessed on August 24, 2025, https:// www.minister.defence.gov.au/media-releases/2024-11-20/annual-cyber-threat-report-highlights-evolving-threat

5. SMB1001:2025 - Dynamic Standards International (OSI), accessed on August 24, 2025, https://dsi.org/smb1001

6. Top 10 Insights from the Annual Cyber Threat Report 2023-2024: A Business Perspective, accessed on August 24, 2025, https://jamcyber.com/blog/cyber-insights/top-10-insights-from-the-annual-cyber-threat-report-2023-2024/

7. Annual Cyber Threat Report 2023-2024[1] Cyber.gov.au, accessed on August 24, 2025, https://www.cyber.gov.au/ about-us/view-all-contenUreports-and-statistics/annual-cyber-threat-report-2023-2024

8. Cyber Essentials scheme: overview - GOV.UK, accessed on August 24, 2025, https://www.gov.uk/governmenU publications/cyber-essentials-scheme-overview

9. Dynamic Standards International (OSI), accessed on August 24, 2025, https://dsi.org/

10. Cyber security Certification for Organisations - Cyber Security Agency of Singapore, accessed on August 24, 2025, https://www.csa.gov.sg/our-programmes/support-for-enterprises/sg-cyber-safe-programme/cybersecurity- certification-for-organisations/

11. Small business cyber security I Cyber.gov.au, accessed on August 24, 2025, https://www.cyber.gov.au/resources-business-and-governmenUessential-cyber-security/small-business-cybersecurity

12. SG Cyber Safe Programme I Cyber Security Agency of Singapore, accessed on August 24, 2025, https:// www.csa.gov.sg/our-programmes/support-for-enterprises/sg-cyber-safe-programme

13. The Seatbelt Moment for Australia's Digital Economy: Securing the Supply Chain by Streamlining SMB Cyber Resilience [White paper] (See Annexe B)

14. New data reveals up to 309,000 Australian small businesses say they've been targeted by cyberattacks, yet many are forced to cut cybersecurity costs , accessed on August 24, 2025, https://www.mastercard.com/news/ap/en/ newsroom/press-releases/en/2023/new-data-reveals-up-to-309-000-australian-small-businesses-say-they-ve- been-targeted-by-cyberattacks-yet-many-are-forced-to-cut-cybersecurity-costs/

ANNEXE A - Submission in Response to the Consultation on Horizon 2 of the 2023-2030 Australian Cyber Security Strategy. - [White paper]

Executive Summary

Australia's 2.4 million Small and Medium-sized Businesses (SMBs) are the engine of our national economy, yet they are critically vulnerable to the persistent and growing threat of cyberattacks. The data paints a stark picture: a cybercrime is reported every six minutes, costing the average small business $49,600 per incident.[1] This pervasive vulnerability is not the result of a lack of information but a fundamental lack of motivation and energy, creating a systemic risk that permeates the entire national supply chain and exposes government entities to significant threats.

Current government efforts, which are well-intentioned, primarily focus on providing resources and advice, and have proven insufficient because they fail to address the core issue.[4] SMBs are overwhelmed by the demands of daily operations and view cybersecurity as a complex, low-priority cost centre rather than an essential business function. Compounding this problem, the existing security frameworks for government procurement - the Protective Security Policy Framework (PSPF) and the Information Security Manual (ISM) - represent an increase in red tape. These complex and often opaque requirements effectively exclude the very SMBs the government aims to support and engage.[6]

This paper presents a proven, market-driven solution that directly addresses these challenges. By mandating a simple, affordable, and achievable foundational cybersecurity certification -"CyberCert"- as a prerequisite for government contracts, Australia can energise the entire SMB ecosystem to uplift its cyber hygiene. This approach is not theoretical; it is backed by compelling international

precedent.

This proposed policy shift mirrors Australia's world-leading seatbelt legislation of the 1970s. That decisive mandate transformed voluntary seatbelt adoption rates from a mere 5% to over 90% in just seven years, demonstrating how clear government action can rapidly shift behaviour to secure a vital public good. We stand at a similar inflection point for our digital economy.

The recommendation of this report is clear: the Australian Government must mandate CyberCert for its SMB suppliers. This single policy change will not add to the regulatory burden; on the contrary, it will dramatically reduce red tape. It will replace a complex, ambiguous system with a clear, simple, and accessible standard, creating an explicit pathway for SMBs to participate in government procurement. This action will stimulate a sovereign cyber services industry, secure our national supply chain, and position Australia as the world's most cyber-resilient nation for SMBs by 2030 - all with minimal direct government expenditure.

1. The Unbuckled Digital Economy: Australia's Systemic SMB Security Risk

The cybersecurity posture of Australia's small and medium-sized business sector represents a critical and unaddressed threat to the nation's economic security. This vulnerability is not an isolated issue affecting individual businesses but a systemic weakness that exposes the entire national supply chain, including government operations, to significant and escalating risk. The current state of inaction is akin to driving in a high-speed digital economy without the fundamental protection of a seatbelt.

1.1 The Engine Room at Risk: SMBs as the Backbone of the Economy

Small and medium-sized businesses are the lifeblood of the Australian economy, constituting 98% of all businesses and playing an indispensable role in innovation, employment, and economic growth.[9] Their operational landscape has been irrevocably transformed in recent years. Accelerated by the global pandemic, SMBs have increasingly adopted digital tools and cloud services to remain competitive, transitioning to remote work and digitising core processes.[9] While this digital transformation has unlocked new efficiencies, it has also dramatically expanded their digital footprint and, consequently, their vulnerability to cyber threats.

The hyper-connected nature of the modern business ecosystem means that the traditional view of SMBs as "low-risk" targets is dangerously outdated. Through integrations with larger partners and the use of cloud platforms, even the smallest sole trader can now hold or access significant volumes of sensitive data.[9] This interconnectedness creates a cascading risk profile; the compromise of a single SMB is no longer a contained event. It can serve as a vector for attackers to infiltrate the supply chains of their larger corporate and government partners. The aggregate vulnerability of millions of SMBs thus constitutes a systemic national security risk, where the weakest link threatens the integrity of the entire chain.

1.2 A Barrage of Unmitigated Threats

The threat landscape facing Australian SMBs is not abstract; it is a daily, high-volume barrage of malicious activity with tangible and severe financial consequences. The statistics compiled by the Australian Signals Directorate (ASD) and other bodies reveal a crisis that is both widespread and intensifying.

A cybercrime is reported, on average, every six minutes in Australia.[1] A significant portion of these attacks are aimed directly at small businesses, which are often perceived by malicious actors as softer targets due to their limited security resources. Studies indicate that 43% of all cyberattacks are aimed at small businesses.[10] The financial impact of a successful attack is substantial. The average self-reported cost of a cybercrime for a small business has risen to $49,600, an increase of 8% year- on-year.[2] However, this figure often represents only the

immediate financial loss. The true cost of a significant data breach, when factoring in remediation, legal fees, regulatory fines, and long-term reputational damage, can be far higher. The average cost of a data breach across all Australian businesses is estimated at $3.35 million.[12] For an SMB, such a cost is often insurmountable and can lead to business failure.

The attack vectors are persistent and well-understood. Business Email Compromise (BEC), where criminals impersonate executives or suppliers to authorise fraudulent payments, remains a highly damaging threat, with average losses of $64,000 per report.[9] Phishing attacks, used to steal credentials, and ransomware, which can cripple operations entirely, are also among the most common and destructive threats faced by the sector.[10]

Metric	Statistic	Source(s)
Frequency of Cybercrime Reports	1 every 6 minutes	[1]
Average Cost per Report (Small Business)	$49,600 (up 8% YoY)	[2]
SMBs Targeted in Attacks	43% of all attacks	[10]
Annual Cybersecurity Spend	Almost half spend <$500	[16]
Stated Business Priority	Lowest priority (22%) vs. Customer Acquisition (62%)	[5]
Cybersecurity Plan in Place	Only 36%	[17]

Table 1: The Australian SMB Cybersecurity Deficit

1.3 The Anatomy of Inaction: The Motivation Paradox

Despite the clear and present danger, SMB engagement with cybersecurity remains critically low. This is not due to a lack of available information. Government bodies like the Australian Cyber Security Centre (ACSC) provide extensive guides, checklists, and resources for small businesses.[4] The failure of these initiatives to drive meaningful change reveals a fundamental misdiagnosis of the problem. The core issue is not a lack of resources, but a profound lack of energy and motivation.

SMB owners are consumed by the daily pressures of running their business - managing cash flow, acquiring customers, and handling operations. In this context, cybersecurity is consistently relegated to the lowest priority. A Mastercard study found that small business leaders are laser-focused on revenue-driving activities like customer acquisition (62%) and client relationships (60%), with cybersecurity ranking last at just 22%. This creates a "Motivation Paradox": while 80% of SMBs rate cybersecurity as important, their actions do not reflect this belief.[16] Almost half rate their own understanding as 'average' or 'below average', and a similar proportion spend less than $500 per year on cybersecurity measures.[9] They cite cost, time, and a lack of knowledge as primary barriers to investment.

This paradox demonstrates that awareness campaigns and resource libraries are necessary but not sufficient. They are designed to solve an information deficit, but the real problem is a motivation deficit. SMBs are rational economic actors who respond to clear and immediate economic signals, not abstract warnings of potential future risk. To energise this sector, cybersecurity must be reframed from a discretionary cost into a mandatory prerequisite for revenue generation. A simple thought experiment illustrates this point: a government-sponsored webinar titled "How to Secure Your Small Business" would likely see low attendance. In contrast, a webinar on "Preparing for Cybersecurity Certification for Federal Government Suppliers" would be oversubscribed. The latter directly connects cybersecurity action to the tangible reward of winning a contract, transforming it from a burdensome cost into a strategic investment. Any effective policy must harness this powerful motivational lever.

1.4 The Supply Chain's Weakest Link

The collective vulnerability of Australia's millions of SMBs creates a dangerously porous national supply chain. The UK's National Cyber Security Centre (NCSC) has observed that an increasing number of cyber attacks are perpetrated through vulnerabilities in the supply chain, where smaller, less secure suppliers are used as a gateway to target larger organisations.[18] A single compromised IT provider, accounting firm, or logistics partner can provide a threat actor with a backdoor into the networks of dozens of their corporate and government clients.

This dynamic means that the security of large enterprises and government departments is inextricably linked to the security of their smallest suppliers. Without a baseline of cyber hygiene across the entire ecosystem, any investments made by larger organisations in their own security can be undermined by a single weak link. Therefore, uplifting the cyber resilience of the SMB sector is not merely an act of protecting small businesses; it is a critical act of national economic defence, essential for securing the integrity of the entire Australian economy.

2. A Proven Blueprint for National Adoption: Lessons from the UK's Cyber Essentials Mandate

The proposition of using government procurement as a lever to drive nationwide cybersecurity adoption is not a theoretical exercise. The United Kingdom's Cyber Essentials (CE) scheme provides a comprehensive and highly successful case study, offering a proven blueprint for how a simple, procurement-led mandate can transform a nation's cyber resilience.

2.1 From Initiative to Imperative: The Cyber Essentials Framework

Launched in 2014, Cyber Essentials is a UK government-backed framework designed to provide a clear, simple, and low-cost pathway for organisations of all sizes to protect themselves against the most common cyber threats.[19] The scheme's effectiveness is rooted in its focus on five basic technical controls that, when implemented correctly, can protect an organisation against approximately 80% of common, internet-based cyber attacks.[19] These foundational controls are:

1. **Firewalls:** Creating a secure barrier between an organisation's internal network and the internet.[18]
2. **Secure Configuration:** Ensuring that devices and software are set up to minimise vulnerabilities and provide only the services required.[18]
3. **User Access Control:** Managing user accounts to ensure access to data and services is restricted to those who need it, applying the principle of least privilege.[18]
4. **Malware Protection:** Using anti-malware software and other measures to prevent, detect, and remove malicious software.[18]
5. **Security Update Management:** Applying patches and updates in a timely manner to ensure software is protected against known vulnerabilities.[18]

The scheme operates on a two-tiered system. The baseline Cyber Essentials certification is achieved through a verified self-assessment questionnaire, providing a foundational level of assurance.[19]

Cyber Essentials Plus offers a higher level of assurance by including a hands-on technical audit and vulnerability assessment conducted by an independent third party.[19]

2.2 The Power of Procurement: A Catalyst for Exponential Growth

The transformative power of the Cyber Essentials scheme was fully unleashed when it was integrated into government procurement policy. In 2014, the UK government began requiring suppliers to hold at least the basic Cyber Essentials certification for certain types of public

contracts.[22] This mandate was applied proportionately, focusing on contracts that involved the handling of sensitive or personal data, or the provision of ICT products and services.[22]

The impact of this procurement lever was clear and measurable. While the scheme saw modest uptake in its early years, the introduction of a procurement mandate served as a powerful catalyst. Certification numbers grew steadily to more than 100,000 by 2022, with tens of thousands more added each year since. In 2023-24 alone, nearly 45,000 certificates were issued, bringing the total to over 140,000 to date. This growth provides strong empirical evidence that tying certification to revenue is the single most effective driver of engagement. A decade after its launch, Cyber Essentials continues to demonstrate sustained momentum, with mandates proving to be a durable, high-impact policy lever.[23] This exponential growth provides unequivocal empirical proof that tying certification to revenue is the single most effective driver of engagement. This momentum has been sustained over time; a decade after its launch, over 215,000 certificates have been awarded in total, with nearly 50,000 issued in the last 12 months alone, demonstrating the policy's enduring impact.[20]

2.3 Beyond Compliance: The Economic and Security Ecosystem Effect

The success of the Cyber Essentials mandate extends far beyond simple compliance numbers. It has generated a series of powerful, positive externalities that have strengthened the UK's entire economic and security landscape.

First, it has demonstrably reduced cyber risk. Independent analysis shows that organisations with Cyber Essentials controls in place make 92% fewer cyber insurance claims.[18] This risk reduction is so significant that many UK insurers now offer free cyber liability insurance (up to £25,000) to SMBs that achieve certification, creating a powerful financial incentive.[21]

First, it has demonstrably reduced cyber risk. Independent analysis shows that organisations with Cyber Essentials controls in place make 92% fewer cyber insurance claims.[18] This risk reduction is so significant that many UK insurers now offer free cyber liability insurance (up to £25,000) to SMBs that achieve certification, creating a powerful financial incentive.[21]

Second, it has enhanced market competitiveness and created a virtuous cycle of supply chain security. A survey of certified organisations found that 69% believe the certification has increased their market competitiveness, and 61% state they are now more likely to choose suppliers who are also certified.[18] This creates a powerful market-driven incentive for businesses to adopt the standard, as it becomes a recognised badge of trust and good practice.

Third, and perhaps most significantly, the mandate has acted as a powerful economic stimulus, creating a thriving domestic cybersecurity ecosystem. The demand for certification services is met by a private sector network of over 350 accredited Certification Bodies and more than 900 qualified Assessors located across the UK.[23] Critically, 85% of these service providers are themselves micro or small businesses. This demonstrates that a government mandate does not need to be delivered by government; instead, it can create a self-sustaining market that builds sovereign capability, creates skilled jobs, and distributes economic opportunity across the country.[23]

2.4 Learning and Adapting: Building a Better Model for Australia

A nuanced assessment of the UK's experience also requires acknowledging its limitations, which provide a clear roadmap for designing a superior Australian model. Over its decade of operation, the Cyber Essentials scheme has faced some valid criticisms. Some argue that the self-assessment model can be reduced to a "box-ticking" exercise if not taken seriously by the organisation.[26] Others have pointed to its rigidity, noting that its prescriptive requirements can be challenging to apply to modern, cloud-native architectures or organisations that have adopted more advanced security models, such as passwordless single sign-on, which may not align perfectly with the standard's specific controls.[27] Furthermore, the strict 14-day window for patching high-severity vulnerabilities can be a significant operational challenge for some businesses, particularly those with complex legacy infrastructure.[26]

These criticisms are not a reason to dismiss the model's success but are invaluable lessons for Australia. They present a clear opportunity to develop a "Cyber Essentials 2.0" for the Australian context. The proposed SMB1001 framework, described as a "journey, not a binary outcome," is perfectly positioned to be this next-generation standard. By learning from the UK's experience, SMB1001 can be designed with greater flexibility. It can incorporate pathways for organisations to demonstrate equivalent controls, accommodating modern security practices and diverse technological environments. By explicitly addressing these known challenges from the outset, the Australian proposal becomes more robust, defensible, and forward-looking, pre-empting potential objections and ensuring its relevance for the decade to come.

3. CyberCert: A Streamlined and Scalable Pathway for Australian Businesses

The proposed CyberCert framework is the ideal instrument to implement this proven, procurement- led strategy in the Australian context. It is designed specifically to overcome the barriers that prevent SMBs from engaging with cybersecurity and to replace the current, burdensome compliance regime with a clear, simple, and accessible pathway. Its core value proposition is not the addition of another layer of regulation, but the radical simplification and streamlining of existing requirements - a fundamental reduction of red tape.

3.1 Designed for Purpose: Affordable, Achievable, and Actionable

CyberCert has been developed from the ground up with the unique realities of Australian SMBs in mind. Its design philosophy is centred on three key attributes:

1. **Affordable:** With a starting price point of just $95, the certification is financially accessible to any business, from a sole trader to a medium-sized enterprise. This directly counters the primary objection from SMBs that cybersecurity is too costly to invest in.
2. **Achievable:** The standard is designed to be a practical and attainable baseline of cyber hygiene. It avoids the immense complexity and cost associated with mature frameworks like ISO 27001 or SOC 2, which are well beyond the reach of the vast majority of SMBs.
3. **Actionable:** CyberCert provides a clear, prescriptive set of actions that any business can understand and implement, often with the help of their existing IT provider. It demystifies cybersecurity, turning an abstract problem into a manageable project.

Crucially, CyberCert is conceptualised as a "journey, not a binary outcome". It establishes an essential entry point into cybersecurity maturity that every business participating in the digital economy should achieve. It is not the end of the security journey but the vital first step, creating a foundation upon which more mature practices can be built as a business grows.

3.2 Cutting the Gordian Knot of Compliance: From Red Tape to a Clear Pathway

The most powerful argument for CyberCert is its role in slashing the red tape that currently chokes SMB participation in government procurement. The current Australian government procurement landscape presents a formidable barrier to entry. Suppliers are required to navigate and comply with the Commonwealth Procurement Rules (CPRs), the principle-based Protective Security Policy Framework (PSPF), and the highly technical, 1,000+ page Information Security Manual (ISM).[6]

This compliance burden is disproportionately heavy for SMBs, which lack dedicated legal and security departments. The ambiguity of these frameworks requires deep interpretation and often necessitates engaging expensive consultants or Infosec Registered Assessor

Program (IRAP) assessors to demonstrate compliance, even for low-risk contracts.[6] The Australian National Audit Office (ANAO) has found that even government entities themselves struggle with the effective implementation of these rules.[8] If government agencies find the system complex, the expectation that a small business owner can navigate it is both unrealistic and prohibitive.

This complexity creates a system of "accidental exclusion," where procurement opportunities are effectively limited to large incumbents with the resources to manage the compliance overhead.

CyberCert cuts this Gordian knot. For a vast range of low-to-medium risk government contracts, it replaces the vague, high-effort requirement to "manage security risks" with a single, clear, low-effort standard. It transforms the procurement security process from a subjective, resource-intensive risk assessment into a simple, objective compliance check.

This does not add a new rule; it substitutes a complex, unworkable set of rules with one that is simple and effective, thereby opening the market to thousands of Australian SMBs.

Factor	Current Framework (PSPF/ISM)	Proposed CyberCert Framework
Accessibility	Opaque; requires interpretation of dense policy documents.[6]	Clear; based on a simple, published standard.
Cost to Demonstrate Compliance	High; may require expensive consultants or IRAP assessors.[6]	Low; fixed certification cost starting at $95.
Verification for Govt.	Complex; requires individual risk assessment of each supplier.[8]	Simple; instant verification via an online certificate registry.[5]
Expertise Required (for SMB)	Specialist cybersecurity and compliance knowledge.	Generalist IT provider or savvy business owner.
Outcome for SMB	High barrier to entry; discourages participation.	Clear pathway; encourages participation.

Table 2: From Red Tape to Clear Pathway: CyberCert vs. Current Procurement Security

3.3 A Common Language for the Entire Supply Chain

The adoption of CyberCert through a procurement mandate would create a scalable assurance model and a common language of security that benefits the entire economy. It establishes a baseline of cyber hygiene that is applicable to the smallest micro-business while also serving as a valuable stepping stone for larger businesses on their path towards more mature frameworks like the Essential Eight or ISO 27001.

This creates a clear and understandable language of security assurance that can flow through the entire supply chain. A prime contractor can easily require its subcontractors to hold CyberCert, creating a simple and verifiable way to manage third-party risk without imposing onerous or complex audit requirements. This has a tremendous flow-on effect,

uplifting cyber hygiene not just among direct government suppliers but across the broader digital economy.

The market is already signalling its readiness for such a standard. The fact that SMBs are now proactively asking their IT providers about achieving CyberCert certification represents a 180-degree turn from the traditional dynamic, where providers struggle to engage clients on security issues. This demonstrates a latent demand for a clear, simple, and recognised standard that can guide their investment and demonstrate their commitment to good practice.

4. The Procurement Lever: Activating the Market to Secure the Nation

A government procurement mandate is the most powerful, efficient, and economically sound policy tool available to address the systemic risk of SMB cyber vulnerability. It is a high-leverage intervention that activates market forces to achieve a critical national security objective, all while minimising direct government expenditure and administrative burden.

4.1 Energising Engagement Through Revenue

The central thesis of this proposal is that SMBs are fundamentally motivated by revenue. While the abstract threat of a future cyberattack is not a sufficient motivator to overcome the immediate pressures of cost, time, and complexity, the concrete opportunity to win a government contract is. By tying a foundational cybersecurity standard directly to an SMB's ability to generate revenue, the government can instantly align its national security objectives with the core business drivers of the SMB sector.

The thought experiment presented earlier - contrasting the likely attendance of a generic security webinar with one focused on certification for government suppliers - makes this principle tangible. The mandate transforms cybersecurity from a discretionary "cost of protection" into a non-negotiable "cost of doing business" for any company wishing to supply to the government. This reframing energises the market, prompting immediate action and investment in a way awareness campaigns alone are unable to achieve. The government wants a secure supply chain, and SMBs want government contracts; the mandate makes these two goals mutually reinforcing and interdependent.

4.2 A Self-Funding Mechanism for National Resilience

A key advantage of this policy is that it requires minimal, if any, direct government expenditure to implement. It is a self-funding mechanism for uplifting national resilience. The cost of achieving and maintaining CyberCert certification is borne by the supplier as a standard operational expense, analogous to professional indemnity insurance, accounting services, or workplace health and safety compliance.

The government's role is not to fund the uplift but to create the market conditions that make the uplift an economic necessity for suppliers. As demonstrated by the UK's experience, the private sector will quickly adapt to meet the new demand. A vibrant ecosystem of certification bodies, IT service providers, and cybersecurity consultants will emerge to help businesses achieve the standard, funded entirely by the businesses themselves.[23]

The return on this policy "investment" - which consists primarily of the political will to enact the mandate - is immense. The government achieves a dramatic, nationwide improvement in cyber resilience, a significant reduction in the multi-billion-dollar economic damage caused by cybercrime, and a marked decrease in its own supply chain risk. Simultaneously, it stimulates the growth of a sovereign cybersecurity services industry. This represents an

exceptionally high-leverage policy intervention, where a single regulatory change can trigger a cascade of positive, market-driven outcomes.

4.3 Streamlining for Government: Reducing the Burden on Procurement Officers

The "reducing red tape" benefit of CyberCert extends directly to government operations. Currently, the Commonwealth Procurement Rules require procurement officers to "consider and manage security risks" for every contract.[6] This is a complex, subjective, and time-consuming task, particularly for officers who are not cybersecurity experts. It forces them to conduct bespoke risk assessments for each supplier, leading to inconsistency and inefficiency.

CyberCert provides these officers with a simple, uniform, and verifiable standard. For the vast majority of low-to-medium risk contracts, the presence of a valid CyberCert certificate provides an immediate and reliable baseline of security assurance. This dramatically simplifies their due diligence and risk assessment process. Instead of a complex investigation, the process becomes a straightforward check against a public registry of certified businesses, similar to the UK's model.[5] This frees up the valuable time and expertise of government security and procurement teams, allowing them to focus their in-depth risk analysis efforts on the small number of high-risk, high-value contracts where it is most needed. This makes the entire government procurement system more efficient, effective, and secure.

5. A Call to Action: Fastening the Seatbelt on Australia's Economy

Australia stands at a critical juncture. We can continue with the current approach of incremental awareness campaigns and regulations, which have proven insufficient on their own to protect our economic engine, or we can take a decisive, proven, and transformative step to secure our digital future. This moment calls for the same foresight and leadership Australia demonstrated half a century ago when it led the world in road safety.

5.1 Australia's Historic Leadership: A Parallel Act of Foresight

In 1970, the state of Victoria became the first jurisdiction in the world to make the wearing of seatbelts compulsory. At the time, voluntary adoption was negligible. This was a bold, forward- thinking act of public policy that faced resistance but was driven by the undeniable evidence of its life-saving potential. Within seven years of the nationwide mandate, seatbelt usage rates soared from around 5% to over 90%, leading to a dramatic and sustained decline in road deaths and serious injuries. Australia's leadership set a global standard that has since saved countless lives.

The proposal to mandate CyberCert for government suppliers is a parallel act of foresight for the digital age. It is an opportunity for Australia to once again lead the world, this time in securing the economic and digital safety of its citizens and businesses. The parallels are striking: a systemic risk with devastating consequences, low voluntary adoption of a simple protective measure, and a clear, effective solution through a government-led mandate.

Factor	Road Safety (1970s)	Digital Economy (2020s)
Systemic Risk	Unacceptably high road trauma and fatalities.	Pervasive economic damage from cybercrime; compromised national supply chain.
Pre-Mandate State	~5% voluntary seatbelt use.	Low voluntary adoption of basic cyber hygiene.
The Mandate	Compulsory Seatbelt Wearing Laws (1970-1972).	Proposed CyberCert Procurement Requirement.
Post-Mandate Adoption	90%+ adoption by 1977.	Projected widespread adoption across government supply chain.
National Outcome	Dramatic reduction in road deaths and injuries; global safety leadership.	Drastically reduced economic loss; secure supply chain; global cyber resilience leadership.

Table 3: From Public Safety to Digital Security: A Mandate's Impact

5.2 Addressing the Obstacles to Action

The evidence is clear, the precedent is set, and the need is urgent. The path forward requires a collaborative effort between industry and government to overcome any remaining obstacles. To that end, we pose the following questions directly to the government as a call to action and an offer of partnership:

- Evidence from the United Kingdom shows strong outcomes from procurement-based certification. How is the Australian Government viewing the opportunity to apply a similar approach here to uplift SMB resilience?
- What considerations - political, administrative, or legislative - would need to be addressed to enable a foundational cyber certification to be embedded into procurement processes?
- This approach has been shown to work with minimal direct government expenditure, as the market adapts to the requirement. How can we work together to explore a practical pathway for implementation in Australia?

We urge a transparent disclosure of these concerns so that we, as a committed part of the Australian cybersecurity community, can work collaboratively with the government to identify and help remove these blocks.

5.3 Recommendations for a Phased Implementation

To ensure a smooth and successful transition, a pragmatic, phased implementation of the CyberCert mandate is recommended. This approach will allow the market of certification providers to scale effectively and give SMBs ample time to prepare, choose, then comply.

- **Phase O (First 12 Months):** Certification is introduced as a voluntary alternative to procurement questionnaires. Suppliers can choose: fill out complex, inconsistent questionnaires, or simply show a CyberCert certificate ("get it once, show it to many"). This positions certification as the frictionless option from the outset.
- **Phase 1 (Within 24 Months)** - Earlier at Per-Agency Discretion: The government should formally announce the policy and a clear effective date. The mandate should initially apply to all new !CT-related contracts and any contracts that involve the handling of personal or sensitive information, mirroring the successful initial scope of the UK's approach.[22]
- **Phase 2 (Within 36 Months):** The mandate should be expanded to cover all new government contracts above a specified value threshold (e.g., $80,000), capturing a broader range of suppliers.
- **Phase 3 (After 36 Months):** The mandate should apply to all government suppliers, both new and existing, upon the renewal of their contracts. This ensures that within a typical contract cycle, the entire government supply chain is covered by this foundational security standard.

5.4 The 2030 Vision: A Secure and Prosperous Digital Future

The implementation of this single policy change has the potential to fundamentally transform Australia's economic resilience. It will empower hundreds of thousands of small businesses, secure our national supply chain against common threats, reduce the economic drain of cybercrime, and stimulate a vibrant sovereign industry. By taking this decisive action, Australia can position itself as the best and most secure country in the world for SMBs to operate in by 2030. The blueprint is clear, the benefits are immense, and the precedent is undeniable. The only remaining question is the one we must ask ourselves as a nation: What is truly stopping us from achieving this critical national goal?

Works cited

1. Annual Cyber Threat Report 2023-2024 | Cyber.gov.au, accessed on August 24, 2025, https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2023-2024
2. Annual Cyber Threat Report highlights evolving threat - Defence Ministers, accessed on August 24, 2025, https://www.minister.defence.gov.au/media-releases/2024-11-20/annual-cyber-threat-report-highlights-evolving-threat
3. Cyber security for small and midsize business - CyberCX, accessed on August 24, 2025, https://cybercx.com.au/cyber-security-small-business/
4. Small business cyber security | Cyber.gov.au, accessed on August 24, 2025, https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/small-business-cybersecurity
5. NCSC Certificate Search - Cyber Essentials - IASME, accessed on August 24, 2025, https://iasme.co.uk/cyber-essentials/ncsc-certificate-search/
6. Security requirements | Selling to Government - Department of Finance, accessed on August 24, 2025, https://sellingtogov.finance.gov.au/faq/security-requirements
7. Guidelines for procurement and outsourcing | Cyber.gov.au, accessed on August 24, 2025, https://www.cyber.gov.au/resources-business-and-government/essential-cybersecurity/ism/cybersecurity-guidelines/guidelines-procurement-and-outsourcing
8. Management of Cyber Security Supply Chain Risks - Australian National Audit Office, accessed on August 24, 2025, https://www.anao.gov.au/work/performance-audit/management-cyber-security-supply-chain-risks
9. Apollo Secure submission - Department of Home Affairs, accessed on August 24, 2025, https://www.homeaffairs.gov.au/reports-and-pubs/PDFs/2023-2030-aus-cyber-security-strategy-discussion-paper/Apollo-Secure-submission.PDF
10. What you need to know about cyber attacks on small-to-medium businesses?, accessed on August 24, 2025, https://www.au.marsh.com/products-services/cyber-insurance/insights/increasing-cyber-attacks-australian-small-medium-enterprises.html
11. Australia—Small businesses vulnerable to rising cybercrime - Export Finance Australia, accessed on August 24, 2025, https://www.exportfinance.gov.au/resources/world-risk-developments/2023/march/australia-small-businesses-vulnerable-to-rising-cybercrime/
12. 13 Critical Data Breach Stats for Australian Businesses | UpGuard, accessed on August 24, 2025, https://www.upguard.com/blog/australian-data-breach-stats
13. Cyberattacks on small business, accessed on August 24, 2025, https://qsbc.qld.gov.au/cyberattacks-on-small-business/
14. Australia's cyber threats: ACSC report insights 2023-2024 - BDO Australia, accessed on August 24, 2025, https://www.bdo.com.au/en-au/insights/cyber-security/australia-s-cyber-threats-key-insights-from-the-acsc-report-2023-2024

15. Increasing cyber-attacks on Australian small and medium enterprises | Marsh Australia, accessed on August 24, 2025, https://www.nz.marsh.com/products-services/cyber-insurance/insights/increasing-cyber-attacks-australian-small-medium-enterprises.html
16. ACSC Small Business Survey Report - Australian Cyber Security Centre, accessed on August 24, 2025, https://www.cyber.gov.au/sites/default/files/2023-03/2023_ACSC_Cyber%20Security%20and%20Australian%20Small%20Businesses%20Survey%20Results_D1.pdf
17. 2023 Cyber Security Summary Report Results - Small Business Association of Australia, accessed on August 24, 2025, https://smallbusinessassociation.com.au/2023-cyber-security-summary-report-results/
18. Cyber Essentials - NCSC.GOV.UK, accessed on August 24, 2025, https://www.ncsc.gov.uk/cyberessentials/overview
19. Achieve Cyber Essentials Certification Now - IT Governance, accessed on August 24, 2025, https://www.itgovernance.co.uk/cyber-essentials-scheme
20. Cyber Essentials scheme: overview - GOV.UK, accessed on August 24, 2025, https://www.gov.uk/government/publications/cyber-essentials-scheme-overview
21. What is Cyber Essentials? | North West Cyber Resilience Centre, accessed on August 24, 2025, https://www.nwcrc.co.uk/what-is-cyber-essentials
22. Cyber Essentials Scheme - GOV.UK, accessed on August 24, 2025, https://assets.publishing.service.gov.uk/media/67af78c8a75f02dffca29bd8/PPN_014_Cyber_essentials_scheme.pdf
23. Cyber Essentials - story so far - National Cyber Security Centre, accessed on August 24, 2025, https://www.ncsc.gov.uk/files/Cyber-Essentials-brochure.pdf
24. Resources - NCSC.GOV.UK, accessed on August 24, 2025, https://www.ncsc.gov.uk/cyberessentials/resources
25. The benefits of Cyber Essentials certification - IASME, accessed on August 24, 2025, https://iasme.co.uk/cyber-essentials/
26. Exploring Cyber Essentials Challenges in 2023 - Aspire Technology Solutions, accessed on August 24, 2025, https://www.aspirets.com/blog/cyber-essentials-challenges-2023/
27. Cyber Essentials is BS : r/cybersecurity - Reddit, accessed on August 24, 2025, https://www.reddit.com/r/cybersecurity/comments/1h4s3yy/cyber_essentials_is_bs/
28. Digital Sourcing Consider First Policy guidance - BuyICT, accessed on August 24, 2025, https://www.buyict.gov.au/sp?id=resources_and_policies&kb=KB0010625
29. Cyber security procurement - Victorian Government, accessed on August 24, 2025, https://www.vic.gov.au/cybersecurity-procurement

ANNEXE B - Response to Consultation on developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy - Proposed Solution

This Annex was too large to include in the submission.

Please download from: https://cybercert.ai/submissions/horizon2/CyberCert-DHA-Submission-Proposed-Solution-29Aug.pdf