28 February 2024

Attn: The Hon Hamish Hansford
PO Box 25
Belconnen ACT 2616

Dear Hamish,

RE: CYBER SECURITY LEGISLATIVE REFORMS CONSULTATION PAPER

I am writing to you on behalf of Cyber Security Certification Australia (CSCAU) in relation to the Australian Cyber Security Strategy: Cyber Security Legislative Reforms Consultation Paper.

We are writing to express our strong support for the Australian Government's initiatives to strengthen Australia's cyber resilience. We believe that your work, particularly the introduction of Shield 1 and its related measures for small and medium-sized businesses (SMBs), is crucial for achieving this goal.

As you know, SMBs represent 95% of Australia's economy and are critical actors in every supply chain. Therefore, we believe that improving and uplifting their cyber resilience is essential for achieving the ambitious goal of making Australia the most cyber resilient nation by 2030.

CSCAU is an industry-led consortium focused on developing dynamic cyber security standards tailored to the needs of SMBs.

Our recently released standard, SMB1001:2023, is a multi-tiered cyber security certification program specifically designed to assist SMBs in enhancing their cyber resilience and demonstrating their cyber maturity.

This certification serves as their cyber trust mark.

We believe that the SMB1001 standard and certifications can significantly contribute to building a more cyber resilient Australia by:

- **Facilitating easier supply chain cyber risk management for critical infrastructure providers.**

- **Providing a clear and achievable framework for SMBs to improve their cyber security posture.**
- **Offering a valuable incentive for SMBs to take action by demonstrating their commitment to cyber security.**

Therefore, our primary recommendation in the Consultation Paper is the adoption of the SMB1001:2023 standard as part of the Security of Critical Infrastructure Act.

We welcome any feedback or questions you may have regarding CSCAU and our submission.

We can also provide you with electronic copies of the SMB1001:2023 standard, its datasheet, vision document and supplier cyber assurance program document.

Please contact [redacted] if you wish to receive any of these materials.

Thank you for your time and consideration.

Sincerely,

[redacted]

Mr Jason Murrell
Independent Chair, SC1001

CSCAU

Cyber Security Certification Australia

SUBMISSION

Legislative Reforms Consultation Paper

CSCAU's submission in response to 2023-2030 Australian Cyber Security Strategy

26 February 2024

Cyber Security Certification Australia Pty Ltd
15 Moore Street, Canberra ACT 2601, Australia
ACN 650 892 514

SUBMISSION

CSCAU'S SUBMISSION IN RESPONSE TO 2023-2030 AUSTRALIAN CYBER SECURITY STRATEGY: LEGISLATIVE REFORMS CONSULTATION PAPER

26 February 2024

Email: support@cscau.org
Web: www.cscau.com.au

Published in Australia

Cyber Security Certification Australia Pty Ltd
ACN 650 892 514

15 Moore Street
Canberra ACT 2601
Australia

Table of Contents

EXECUTIVE SUMMARY IV

1. ABOUT CSCAU 5

2. SMBS – THE BEDROCK OF THE AUSTRALIAN ECONOMY 6

3. OUR RESPONSE 7

3.1 MEASURE 1: HELPING PREVENT CYBER INCIDENTS - SECURE-BY-DESIGN STANDARDS FOR INTERNET OF THINGS DEVICES 7

3.2 MEASURE 8: ENFORCING CRITICAL INFRASTRUCTURE RISK MANAGEMENT OBLIGATIONS – REVIEW AND REMEDY POWERS 7

3.3 MEASURE 9: CONSOLIDATING TELECOMMUNICATION SECURITY REQUIREMENTS – TELECOMMUNICATIONS SECTOR SECURITY UNDER THE SOCI ACT 9

4. REFERENCES 12

5. ACKNOWLEDGEMENTS 13

APPENDIX A - AN OVERVIEW OF THE SMB1001 STANDARD'S LEVELS AND CONTROLS 14

Executive Summary

This submission to the 2023-2030 Australian Cyber Security Strategy: Legislative Reforms Consultation Paper compiles feedback from an expert working group from Cyber Security Certification Australia Pty Ltd (CSCAU) comprising SMB1001 *Multi-tiered cyber security certification standard for small and medium-sized businesses* Steering Committee members and staff.

The document focuses on Measures 1, 8 and 9 in the Consultation Paper and aims to consider the consultation from the small and medium business viewpoint to deepen the coverage of the proposed legislative reforms.

A summary of our recommendations is provided below. Our recommendations relate to Part 1 and 2 of the Consultation Paper: New cyber security legislation, and amendments to the Security of Critical Infrastructure Act 2018.

Section 2 provides an overview and analysis of our recommendation.

Additional analysis and discussion for our recommendations linked to the specific questions in the consultation paper is provided in Section 3.

An overview of the SMB1001 standard and its levels and controls are provided in Appendix A.

Key Recommendations

1. Consider not limiting Secure by Design standards to just the Internet of Things device supply chain, but to extend Secure by Design standards to multiple supply chains.

2. Consider the addition of additional guidance and frameworks such as SMB1001 to s10 of the Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023.

3. Consider adopting practical, SMB-appropriate prescriptive standards for supply chain cyber maturity uplift over time.

4. Encourage large organisations and governments to leverage SMB-achievable standards such as SMB1001 as procurement contractual requirements to encourage SMBs to uplift their cyber security at scale.

1. About CSCAU

Cyber Security Certification Australia Pty Ltd (CSCAU) (https://cscau.com.au) is a standards development industry council focused on uplifting the cyber security of small and medium-sized businesses (SMBs).

In 2023, CSCAU released a dynamic and tailored cyber security standard for SMBs: SMB1001 - Multi-tiered cyber security certification standard for small and medium-sized businesses (see Appendix A). SMB1001 comprises five levels with each level building on the previous level. The standard also has controls spanning technology management, access control, backup and recovery, policies, and education and training.

SMB1001 incorporates the adoption of and compliance against multiple prominent internationally renowned standards and frameworks such as Australia's Essential 8, UK's Cyber Essentials and USA's CMMC. A business certified against SMB1001 consequently complies with these standards - hence reducing the cost and governance load on small and medium sized businesses.

The dynamic nature of SMB1001 means that it is annually updated and reviewed to ensure its continued relevance for SMBs. An annual update and review shortens the typical standard lifecycle improving its responsiveness to developments in the threat environment, and incorporates improvements in controls and accessibility.

This annual review is conducted by CSCAU's Steering Committee composed of 20+ government, industry and SMB experts. In addition, a Standardisation and Certification Oversight Board oversees the governance of the updates made to the standard by the Steering Committee, aligning to international auditing and certification expectations.

2. SMBs – The Bedrock of the Australian Economy

CSCAU agrees with Shield 1 of the Australian Cyber Security Strategy as several sector-wide studies and government reports have shown that small and medium-sized businesses (SMBs) are vulnerable targets in supply chains from the perspective of cyber security.

In 2020, the Australian Small Business and Family Enterprise Ombudsman (2020) stated that "small business accounts for between 97.4% and 98.4% of all businesses, depending on whether you define a small business based on number of employees or turnover.". Evidently, a nation of cyber resilient SMBs would equate to a cyber resilient Australia.

As such, our submission is primarily concerned with the uplifting of SMB cyber maturity resulting in improvements of the supply chain security of Critical Infrastructure entities (CIs), and improvements in Australia's domestic cyber security posture across all business types – from sole proprietors to enterprises.

A staggering amount of businesses require protection from ransomware, business email compromise, invoice fraud, and insider threats. Unlike large-scale Critical Infrastructure providers that can navigate breach events through market resilience and/or dominance, small businesses can be devastated by a single cyber event (Australian Cyber Security Centre, n.d.). We agree that there is an opportunity for the Australian Government to address this, especially in the face of threats that our constituent-appointed decision makers are aware of.

3. Our Response

Our responses to the specific questions in the consultation paper are listed below.

3.1 Measure 1: Helping prevent cyber incidents - Secure-by-design standards for Internet of Things devices

Question 1 - Who in the smart device supply chain should be responsible for complying with a proposed mandatory cyber security standard?

Managing supply chain risk irrespective of sector requires the commitment of all members of the supply chain. Our recommendation is to consider not limiting to just the IoT device supply chain, but to consider multiple types of supply chains.

We acknowledge that smaller organisations have, typically, lesser resources to direct towards cyber security. Therefore, there should be a variation in expectations for smaller and larger organisations. Namely, smaller organisations should be expected to comply with a standard tailored for their capacity and capability, such as CSCAU's SMB1001:2023 (See Appendix A).

SMB1001:2023 is an Australian certification standard tailor made for small and medium-sized businesses. It is a multi-tiered cyber security standard aligning with ASD's Essential Eight in order to encourage its adoption, while recognising the capacity of SMBs for cyber security.

Recommendation: Consider not limiting Secure by Design standards to just the Internet of Things device supply chain, but to extend Secure by Design standards such as SMB1001 to multiple supply chains.

3.2 Measure 8: Enforcing critical infrastructure risk management obligations – Review and remedy powers

Question 42 - How would the proposed review and remedy power impact your approach to preventative risk?

We concur with the consultation paper that there is relevance in the proposed review and remedy power for the Secretary of Home Affairs or relevant Commonwealth regulator to direct a responsible entity to rectify seriously deficient elements of a Critical Infrastructure Risk Management Program (CIRMP).

We believe that this power may have the potential impact of encouraging responsible entities to mature their CIRMP over time.

Based on the consultation paper, it is currently unclear whether the threshold that must be met for the power to be executed. Conversely, what is the threshold of good maturity for a

CIRMP - noting that the Department of Home Affairs continues to mature its supporting literature.

In the consultation paper, reference is provided to two scenarios:

(1) A responsible entity does not meet, or is not taking reasonable steps to meet the required maturity level of the prescribed cyber security framework;
(2) The entity has failed to consider and minimise risks in the threat landscape that pose a potential risk to their asset.

Clarity about threshold determination required

To the best of our knowledge, in these scenarios, it is currently unclear how these thresholds will be determined. Namely, at what point will it be determined that an entity is not taking reasonable steps to meet a prescribed framework or failing to consider and minimise relevant risks. For responsible entities, this is a critical question to be addressed. Otherwise, the responsible entity will be unable to define what their goal is for their CIRMP. This may potentially hamper their respective CIRMP implementations. It could then be unreasonable to place the onus on the responsible entity if there is a lack of clarity in how thresholds are determined. Hence, we suggest that further clarity is then needed on what is considered sufficient maturity for a CIRMP through additional guidance, e.g. templates, scenarios and other materials.

The provision of this additional guidance may also be relevant in clarifying the complexity of specific areas of LIN 23/006, such as personnel security and supply chain security. In the latter area, guidance should not be solely focused on supply chain cyber risks but also recognise that there are different types of relevant supply chain risks that may arise, e.g. tariffs, sanctions and counterfeits.

Recommendations for LIN 23/006 s10

There may also be a need for additional guidance demonstrating how supply chain cyber hazards/risks could be managed. We suggest specifying relevant standards that can be used to manage supply chain cyber security that are fit-for-purpose, i.e. updating LIN 23/006 s10. A standard for supply chain cyber security considering the granularities and types of business size/scale would provide responsible entities with a clear maturity threshold for their supply chain to meet.

For LIN 23/006 s10 and supply chain hazards, we also recommend that additional frameworks or standards should be included. As a result, our recommendation is that in LIN 23/006 s10, it should be updated to include a list of relevant standards and frameworks, similar to LIN 23/006 s8(4)(b), to clarify the supply chain requirements for cyber security.

There is an opportunity for these standards and frameworks to be inclusive in nature to recognise the varying capacity of businesses of varying sizes in Australia that comprise a supply chain, i.e. including additional frameworks specifically relevant to small and medium-sized businesses, such as SMB1001:2023.

We believe that the current frameworks specified in LIN 23/006 s8(4)(b) are not able to cover the diversity of businesses in a responsible entity's supply chain. Currently, small and medium-sized businesses represent over 97.4% of Australian businesses and are contributors to all Australian supply chains. It is generally accepted that small and medium-sized businesses may not necessarily have the same access to resources as larger organisations. Implementing the listed frameworks may then not be feasible for smaller organisations due to the financial and administrative burden. For example, compliance or certification against ISO/IEC 27001 typically requires a cost of tens of thousands of dollars over a number of years. In comparison, a certification against SMB1001 would only cost $95 at Level 1 of the standard.

Including standards such as CSCAU's SMB1001 that are fit-for-purpose for small and medium sized organisations is signalling the holistic importance of cyber security and supply chain risk for all businesses. This provides implicit encouragement for businesses to implement cyber security regardless of their resource levels or constraints - thereby encouraging a nation-wide uplift of cyber resilience.

Recommendation: Consider the addition of additional guidance and frameworks such as SMB1001 to s10 of the Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023.

3.3 Measure 9: Consolidating telecommunication security requirements – Telecommunications sector security under the SOCI Act

We agree with the members of the Australian Telecommunications Security Reference Group's call for reduced complexity, minimised duplication and scalable obligations, and applaud the proposed co-design of the Telecommunications Security Risk Management Program (TSRMP) by the sector and the reference group.

Question 43 - What security standards are most relevant for the development of an RMP?

There is opportunity for the scope to be revisited more broadly beyond the telecommunications sector, and into the telecommunications ecosystem (which includes third-party service providers). Small and medium sized businesses constitute a significant proportion of the third-party service providers to the telecommunications sector. As such, there is an opportunity for Australia to consider security standards improving supply chain resilience via appropriate management of cyber risks introduced by third-party service providers.

Principles-based vs. prescriptive standards

Currently, the principles-based approach is prevalent in standards guiding general security improvement. However, we believe that prescriptive standards may be of value in enhancing security maturity across physical security and supply chain security – both of which are currently unaddressed.

While the explicit list of standards and practices found in LIN23/006 s8(4)(b) may impose a regulatory burden on CI entities, the optional approach taken in LIN23/006 s9(2) (to assess the suitability of critical workers) is more in favour of enhanced capabilities while acknowledging that entities still have discretion to adopt their own approach.

For instance, physical security risks may benefit from the application of Australian Security Intelligence Organisation's T4 and its libraries, the Australian Government's Protective Security Policy Framework, and/or the ASIS International Physical Security Asset Protection Standard. Acknowledging that industry specific standards and practices exist – such as the TAPA Facility Security Requirements (FSR) – the former standards and practices provide industry/sector-agnostic options for adoption, many of which are also principles-based.

From our collective experience, supply chain risks may benefit from standards and systems that specifically target the more vulnerable members of the supply chain i.e. small and medium-sized businesses (SMBs). Providing standards tailor-made for SMBs can provide SMBs with relevant and feasible guidance on implementing cyber security e.g. CSCAU's SMB1001. This standard could help SMBs manage their cyber security risks. In turn, those in their supply chain can use these standards to manage cyber risks that exist within their supply chains. A buyer organisation can now require its SMB suppliers to certify against the achievable and appropriate level of SMB1001 (e.g. a sole proprietor to be certified at Level 1 of SMB1001). At scale, and over time, a buyer organisation could prescribe for its suppliers to mature from Level 1 to Level 2 and so on over the years - effecting a cyber maturity uplift of its entire supply chain. The value of this approach to adoption within the supply chain rules is the overall positive impact that would take effect across Australia's sectors and industries. In being the world's "most cyber secure country" (Crozier, 2023), the adoption of this approach would enable such an objective to be achieved by the planned 2030 date.

Other standards and practices could also reduce supply chain risks, such as imposing vector requirements on CI third parties, or outlining other requirements such as police checks and/or audits of third party practices (i.e. ISO9001 for quality/integrity management, and/or ISO31000 for risk management). However, it has to be noted that the typical certification costs of ISO standards are usually out of reach for SMBs' budgets.

Recommendation: Consider adopting practical, SMB-appropriate prescriptive standards for supply chain cyber maturity uplift over time.

Question 47 - How do your procurement and network change management processes align with the existing and proposed notification arrangements? Can you suggest improvements to accommodate industry practice?

Beyond the telecommunications sector, procurement processes can be leveraged as a tool to encourage supply chain maturity and ease the process of notification arrangements.

Encouraging cyber security uplift across supply chains can be difficult as it requires the active participation of all members of the supply chain. However, it can be difficult to

encourage members of the supply chain to improve their cyber security maturity especially for smaller businesses, which is inclusive of highly experienced advisors/consultants and defence industry bodies. To address these issues, organisations need to be incentivised to adopt cyber security, such as an economic incentive or a 'ticket to trade' approach.

The 'ticket to trade' approach with embedded economic incentive is procurement-based uplift where contracts require potential or actual suppliers to implement a specific level of cyber security requirements. There is then an incentive for businesses to implement cyber security requirements given the commercial gain achieved by meeting the requirement. This currently occurs in some sectors, with a disruptive yet successful example being the Department of Employment and Workplace Relations' Right Fit For Risk (RFFR) Accreditation requirements, which impose ISO/IEC 27001 certification requirements on certain entities. Such requirements do however impose financial and administrative burdens that are not applicable to all business types and sizes. An ISO/IEC 27001 certification costs at least $30,000 per organisation. Alternative requirements should then be used for smaller businesses, such as the SMB1001 which is easier to achieve and relatively cheaper to certify against (e.g. Level 1 certification costs $95 excluding GST per SMB).

With SMB1001, suppliers may be required to implement a specific level of SMB1001 to be able to contract with the organisation. For example a supermarket chain could mandate its food suppliers to be at Level 1, franchisees at Level 2, and its accountants and lawyers handling private sensitive information to be at Level 3. The standard has a certification aspect providing the organisation with verifiable evidence that the supplier has implemented the requirements. The sliding scale of maturity allows for a journey to be established, with maturity increasing in alignment with supplier risk exposure. Conversely, if a supplier does not wish to certify against a baseline cyber hygiene requirement found in SMB1001 Level 1, then it may be a red flag for the buyer organisation.

By initiating these conversations with suppliers, it can also ease the process of notification in the event of a cyber incident as the discussion of cyber security with suppliers is then not unusual. For instance, SMB1001 has a specific control relating to incident response plans where an SMB needs to consider who they would need to contact if an incident occurs. This could readily be accommodated in contract requirements, allowing for notifications throughout supply chains. It is acknowledged however that such contract cycles could take years or decades, and subsequently the Commonwealth needs to act should the country's interests be prioritised. However, from a national perspective, using procurement as a lever reduces the need to 'over-legislate' to effect supply chain resilience.

Recommendation: Encourage large organisations and governments to leverage SMB-achievable standards such as SMB1001 as procurement contractual requirements to encourage SMBs to uplift their cyber security at scale.

4. References

Australian Cyber Security Centre. (n.d.). *Small Business Cyber Security*. Retrieved from https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/smallbusiness#:~:text=For%20a%20small%20business%2C%20even,over%20%2439%2C000%20for%20small%20businesses. Accessed 17 Feb 2024.

Australian Government Department of Employment and Workplace Relations. (2023). *Right fit for Risk Cyber Security Accreditation*. Retrieved from https://www.dewr.gov.au/right-fit-risk-cyber-security-accreditation. Accessed 14 Feb 2024.

Australian Small Business and Family Enterprise Ombudsman. (2020). *ASBFEO Small Business Counts*. Retrieved from https://asbfeo.gov.au/sites/default/files/2021-11/ASBFEO%20Small%20Business%20Counts%20Dec%202020%20v2_0.pdf. Accessed 14 Feb 2024.

Crozier, R. (December 8 2022). Gov sets target to make Australia the "most cyber secure country" by 2030. *itNews.* Retrieved from https://www.itnews.com.au/news/gov-sets-target-to-make-australia-most-cyber-secure-country-by-2030-588895. Accessed 14 Feb 2024.

5. Acknowledgements

We acknowledge the contributions from the working group members in their individual capacities, listed in last name alphabetical order:

- Mr Daniel Cox
- The Hon Meegan Fitzharris
- Mr Darren Hopkins
- Professor Ryan Ko
- Mr Peter Maynard
- Mr Jason Murrell
- Ms Danielle Pentony
- Dr Elinor Tsen
- Adjunct Professor Beau Tydd

Appendix A - An overview of the SMB1001 standard's levels and controls

Table 1: Overview of SMB1001's five levels and costs of certification

Certification Requirements	Level 1	Level 2	Level 3	Level 4	Level 5
Typical certification cost per organisation	$95	$195	$395	$3,595	$5,995
NUMBER OF REQUIREMENTS	6	14	22	28	35
Engage a technical support specialist for your organization	✓	✓	✓	✓	✓
Install and configure a firewall	✓	✓	✓	✓	✓
Install anti-virus software on all organizational devices	✓	✓	✓	✓	✓
Automatically install tested and approved software updates and patches on all organizational devices	✓	✓	✓	✓	✓
Change passwords routinely	✓	✓	✓	✓	✓
Implement a backup and recovery strategy for important digital assets	✓	✓	✓	✓	✓
Install TLS certificates on all public internet facing websites		✓	✓	✓	✓
Ensure employee accounts do not have administrative privileges		✓	✓	✓	✓
Ensure employees have individual user accounts		✓	✓	✓	✓
Implement a password manager system		✓	✓	✓	✓
Multi-factor authentication (MFA) on all employee email accounts		✓	✓	✓	✓

Confidentiality agreement for all employees		✓	✓	✓	✓
Implement a policy with procedures to prevent Invoice Fraud		✓	✓	✓	✓
Implement a visitor register		✓	✓	✓	✓
Ensure all servers are updated and patched			✓	✓	✓
MFA on all business applications and social media accounts			✓	✓	✓
Implement a cyber security policy			✓	✓	✓
Implement a response plan for cyber related incidents			✓	✓	✓
Utilize secure methods of physical document destruction			✓	✓	✓
Ensure all computer devices that store sensitive, private, and/or confidential Information are disposed of securely			✓	✓	✓
Implement and maintain a digital asset register			✓	✓	✓
Conduct cyber security awareness training for all employees			✓	✓	✓
Ensure all public internet facing resources are regularly scanned for vulnerabilities				✓	✓
Management of remote access cloud credentials				✓	✓
MFA where important digital data is stored				✓	✓
MFA on VPN connections				✓	✓
MFA on RDP connections				✓	✓
Purchase and maintain business insurance				✓	✓
Ensure important digital data is encrypted at rest					✓

Implement application control					✓
Disable untrusted Microsoft Office macros					✓
Conduct penetration, vulnerability and social engineering testing					✓
Implement a digital trust program with your suppliers					✓
Conduct police vetting on employees with administrative privileges or controlled access					✓
Conduct training to test the incident response plan					✓

Certification Conditions and Prerequisites

- *Level 1, 2 and 3 certifications require director (or equivalent) attestation and are valid for 12 months.*
- *Level 4 and 5 Certifications require director (or equivalent) attestation and an external audit by an Independent Verification Organisation (IVO) and are valid for 12 months.*

6 February 2024

Attn: The Hon Hamish Hansford
PO Box 25
Belconnen ACT 2616

07/03/2024
07:51