

SUBMISSION

CSCAU'S SUBMISSION IN RESPONSE TO SCAMS PREVENTION FRAMEWORK – EXPOSURE DRAFT LEGISLATION

02 October 2024



Cyber Security Certification Australia Pty Ltd
ACN 650 892 514

15 Moore Street
Canberra ACT 2601
Australia

COPYRIGHT PROTECTED DOCUMENT

© Cyber Security Certification Australia Pty Ltd

This document is safeguarded under copyright law. Any form of unauthorized reproduction, distribution, or utilization of the content contained herein is strictly prohibited and may entail legal consequences.

Email: support@cscau.com.au

Web: www.cscau.com.au

Published in Australia

Table of Contents

EXECUTIVE SUMMARY	IV
1. ABOUT CSCAU	5
2. OUR RESPONSES	6
3. REFERENCES	7

Executive Summary

Our submission to the Scams Prevention Framework – Exposure Draft Legislation from Cyber Security Certification Australia Pty Ltd (CSCAU) is based on our extensive experience in the small and medium-sized business environment considering their challenges and capabilities.

We support the proposed Scams Prevention Framework and suggest that additional guidance can be provided for smaller businesses from the perspective of an associated regulated entity under Section 58AD.

The document focuses on the **Proposed legislation** questions. A summary of our recommendations is provided below. In Section 2, we provide an overview of CSCAU. Section 3 presents our detailed analysis supporting our recommendation.

Key Recommendations

1. Consider providing small business-specific guidance on preventing and detecting scams, such as by endorsing existing small business guidance, such as SMB1001.

1. About CSCAU

Cyber Security Certification Australia Pty Ltd (CSCAU) (<https://csc.au.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). We updated SMB1001 in 2024 following our dynamic standard mission. 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. Our responses

Currently, small businesses are only explicitly recognised as SPF consumers. However, small businesses may be recognised as a regulated entity under Section 58AD.

According to Section 58AD, a corporation that acts in the course of or in relation to, the carrying on or provision of a business or service that is part of a regulated sector is also deemed as being a regulated entity for the sector. Hence, any entity that provides services to banking, insurance or communications may also fall within this legislation. This may include small businesses, which is likely considering that Australian small businesses comprise 97.4% of all businesses (Australian Small Business and Family Enterprise Ombudsman, 2020).

If small businesses have the potential of being recognised in the legislation following Section 58AD, guidance and recommendations needs to be made available for smaller businesses in relation to Section 58BI and 58BM.

Section 58BI and 58BM states that a regulated entity must take reasonable steps to prevent and detect scams. It is further clarified that the steps required is not limited to acting on scam information (Section 58BL and 58BP) with further clarification being expected to be provided in sector-specific details.

However, smaller businesses need guidance that is accessible and relevant to their business. Typically, smaller businesses have less resources available to prevent and detect negative events, such as scams, compared to larger businesses. Smaller businesses may not necessarily have the knowledge either to implement relevant measures to detect and prevent scams. Hence, smaller businesses need tailored advice and guidance. Otherwise, it will be challenging for businesses to implement appropriate measures to prevent and detect scams.

We suggest that, in addition, to the sector-specific guidance, the Treasury could provide smaller business guidance specific to scam prevention and detection. Furthermore, this provision of guidance could include endorsement of existing smaller business guidance, such as SMB1001:2024. Endorsing existing guidance not specific to scams may be appropriate in helping to support businesses, irrespective of size, develop their protective and detective measures to enable the safeguarding the digital economy. We note that cyber security guidance may be of relevance as an entity detecting and preventing scams originating from an entity is similar to the cyber security measures that the entity would implement.

SMB1001:2024 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 providing small business-specific guidance on preventing and detecting scams, such as by endorsing existing small business guidance, such as SMB1001.

3. References

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.

