Secretariat: PO Box 463
Canberra ACT 2600

Our advocacy team is based in Canberra

Email: ceo@cosboa.org.au
www.cosboa.org.au

Cyber Security Strategy
Department of Home Affairs
By email: CSSH2@homeaffairs.gov.au

Dear Minister,

Developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy

Introduction

The Council of Small Business Organisations (**COSBOA**) thanks the Department of Home Affairs for its continued consultation on the 2023-2030 Australian Cyber Security Strategy and welcomes the proposal for Horizon 2. Small businesses constitute 97% of all Australian businesses, forming the backbone of our economy and communities. However, small businesses remain particularly vulnerable to cyber threats, and face fundamentally different challenges than large enterprises or government entities. They typically lack dedicated IT personnel, operate with limited budgets, and often don't have the capacity to navigate complex cyber security frameworks designed for larger organisations.

Executive Summary

Small businesses and not-for-profit organisations continue to face significant cyber security challenges despite their critical contribution to Australia's economy and society. While the government's proposed approach for Horizon 2 provides a valuable framework, its practical implementation must acknowledge the unique constraints faced by Australia's 2.7 million small businesses. Addressing the cyber resilience of this sector requires solutions that are accessible, affordable, achievable, and manageable for organisations with limited resources.

COSBOA strongly advocates for an approach that prioritises education and support over penalties and complex regulation. We call for:

- targeted cyber awareness messaging,
- scaling of successful programs like Cyber Wardens,
- improved accessibility of cyber insurance
- practical threat sharing mechanisms, and
- compliance support that acknowledges the reality of small business operations.

These measures must be designed with the understanding that most small businesses lack dedicated IT staff and operate with significant time and resource constraints.

COSBOA notes that the discussion paper presented a series of questions for review; instead of addressing each question directly, we have responded below to the broader themes from a small business perspective.

The challenge small businesses face

Disproportionate vulnerability and impact

Small businesses face an impossible equation: they are simultaneously more vulnerable to cyber-attacks due to limited resources yet suffer disproportionately severe consequences when breaches occur. Unlike larger enterprises that can absorb financial impacts, a significant cyber incident can be an existential threat for a small business. Despite this heightened risk profile, most cyber security guidance and solutions remain oriented toward larger organisations with dedicated IT departments and substantial budgets.

Regulatory Complexity and Implementation Barriers

Australia's regulatory system for cyber security is too complicated for most small businesses to comprehend, let alone implement effectively. Small business owners typically wear multiple hats—from operations to marketing to finance—and have precious little time to decipher complex cyber security requirements. The reality is that most small business owners are time-poor and lack the technical knowledge to translate regulatory requirements into practical actions.

Inaccessible Cyber Insurance

Cyber insurance represents an increasingly difficult issue for small businesses. As cyber-attacks increase in frequency and severity, insurers have responded by raising premiums, introducing more stringent eligibility requirements, or withdrawing from the market entirely. This creates a classic example of negative externality: a small business who most needs protection is the least able to access it. Many small businesses are priced out of the market or unable to meet technical requirements that presume enterprise-level capabilities.

Ineffective Communication of Threats and Solutions

Current cyber threat sharing mechanisms and security guidance often fail to resonate with small businesses. Technical jargon, complex frameworks, and enterprise-focused recommendations create an immediate disconnect for small business owners seeking practical solutions. When a small café owner, independent tradesperson, or community organisation leader seeks answers about cyber security, they typically encounter information that neither addresses their specific context nor provides actionable steps within their resource constraints.

Proposed Solutions

COSBOA considers the below solutions be considered as part of the roll out of Horizon 2.

Designed for small business

Government cyber awareness campaigns must be specifically designed for small businesses rather than adapted from enterprise-focused messaging. This means:

- using sector-specific examples and scenarios that small business owners can immediately relate to;
- focusing on practical, low-cost measures that can be implemented without technical expertise;
- developing messaging that acknowledges the time constraints of small business owners;
- creating resources in plain language that avoid technical jargon; and
- distributing information through channels that small businesses already engage with.

For example, rather than using generic messaging about implementing multi-factor authentication, campaigns could demonstrate a local retailer setting up basic security measures on their point-of-sale system in under five minutes.

Scale Up Successful Programs

The CyberWardens program, designed "by small business, for small business," has demonstrated early success in building cyber resilience in the small business sector. We recommend:

- increasing government investment to scale this program nationally;
- supporting continuous vulnerability monitoring that is affordable for small organisations;
- developing the "CyberWardens Champion" approach within organisations, similar to workplace safety officers; and
- ensuring the program remains accessible to businesses with limited resources and technical knowledge.

COSBOA endorses the submission made by CyberWardens that outlines opportunities for Horizon 2.

Address Cyber Insurance Accessibility

To improve access to cyber insurance for small businesses, we recommend:

- working with the insurance industry to develop standardised, simplified cyber insurance products specifically for small businesses;
- creating government-backed insurance schemes or subsidies for small businesses that implement basic cyber security measures;
- establishing clear, achievable security standards that, when met, guarantee insurance eligibility; and
- supporting industry-led initiatives that combine practical security improvements with insurance access.

Develop Practical Threat Sharing Mechanisms

Small businesses need cyber threat information that is immediately actionable. We recommend:

- creating a simplified, business-friendly threat alert system that avoids technical jargon;
- developing sector-specific threat updates relevant to different types of small businesses;
- establishing a "small business cyber hotline" for immediate, practical advice during incidents;
- supporting industry associations to become trusted intermediaries for cyber threat information; and
- ensuring all threat sharing mechanisms include specific, practical steps small businesses can take.

Support Compliance Without Excessive Burden

To help small businesses meet cyber security requirements without overwhelming them, we recommend:

- developing tiered compliance frameworks that recognise the different capabilities of organisations based on size and sector;
- creating simple self-assessment tools that guide small businesses through basic security measures;
- offering compliance assistance rather than focusing on penalties for non-compliance;

- ensuring any new regulations include implementation support specifically designed for small businesses; and
- providing templates and tools that simplify compliance documentation.

Next Steps and Conclusion

COSBOA recommends the following specific four actions as part of the Horizon 2 Cyber Security Strategy implementation:

1. Commit to significant expansion of the CyberWardens program with dedicated funding over the next three years.
2. Develop a Small Business Cyber Security Toolkit with sector-specific guidance, templates, and resources that can be immediately implemented.
3. Create a regulatory pathway that provides small businesses with clear, staged steps toward improved cyber security rather than overwhelming compliance requirements.
4. Establish formal feedback mechanisms to continuously improve the relevance and accessibility of government cyber security initiatives for small businesses.

Building the cyber resilience of Australia's small business sector requires recognition that these organisations face unique challenges that cannot be addressed through frameworks designed for larger enterprises. By focusing on education over enforcement, practical support over penalties, and accessible solutions over complex requirements, the government can significantly improve the cyber security posture of the small business sector.

COSBOA is committed to partner with government to ensure the successful implementation of the Horizon 2 Cyber Security Strategy in a way that genuinely meets the needs of small businesses across Australia.

We welcome any future consultation the Department wishes to undertake, and we look forward to continued involvement through the Executive Cyber Council Working Group.

Kind regards,

Matthew Addison
Chair, COSBOA