FINANCIAL ADVICE ASSOCIATION AUSTRALIA

28 August 2026

Committee Secretary
Select Committee on Cyber Security for Small to Medium Sized Businesses and Organisations
Parliament House
Canberra ACT 2600

Online submission

Dear Committee Secretary,

Inquiry into cyber security for small to medium sized businesses and organisations

The Financial Advice Association Australia[1] (FAAA) welcomes the opportunity to make a submission to the House Select Committee on Cyber Security for Small to Medium Sized Businesses and Organisations (the Committee), in response to its inquiry into the cyber security preparedness of small to medium sized businesses and organisations.

The financial advice profession is predominantly made up of small businesses. The large majority of FAAA members operate as small businesses, either with their own licence or authorised by a licensee. They hold a significant volume of highly sensitive client financial, identity and health information and engage daily with superannuation funds, insurers, platforms and government agencies on behalf of their clients. This combination of small business resourcing and high-value client data makes the financial advice profession a useful case study for the Committee in considering the cyber maturity of small to medium sized businesses more broadly.

In addition, many of our members advise small businesses on their financial advice needs including risk management and insurance, business succession, structuring and entities, cashflow management and wealth alignment.

Thus, we are both a small business sector, and a sector that advises small businesses.

This submission is informed by structured engagement the FAAA has undertaken with its members, including licensees and practitioners.

[1] The Financial Advice Association Australia (FAAA) is the largest association representing the financial advice profession in Australia, with over 10,000 members. It was formed in 2023 following the merger of the two leading financial planning/advice bodies in Australia - the Financial Planning Association (FPA) and the Association of Financial Advisers (AFA). With this merger, a united professional association that advocates for the interests of financial advisers and their clients across the country was created.

Of key importance to our members were measures to:

- strengthen the cyber resilience of small businesses by prioritising education, capability-building and informed decision-making over additional compliance obligations;
- improve the ability of small businesses to identify, assess and engage suitable cyber security providers and services;
- support ongoing, practical cyber security training that reflects changing technologies, emerging threats and the operational realities of small businesses;
- examine the growing cyber security expectations placed on small businesses by larger organisations and whether these are appropriate and proportionate; and
- address cyber security risks associated with current identity authentication practices used by government agencies and large institutions when engaging with small businesses.

We have responded below to each of the Committee's terms of reference and have also raised an additional matter that we believe warrants the Committee's specific attention.

FAAA feedback on the Committee's terms of reference

1. The cyber maturity of Australian small to medium sized businesses and organisations, including not-for-profit organisations

It is our observation that small advice businesses have sometimes not given cyber security the attention it warrants, not because they do not regard it as important, but because it is one of a very large number of competing regulatory and operational obligations that a small business owner must manage at any given time. In our view, several structural features of small financial advice businesses compound this problem.

A small AFS licensee is, by definition, required to meet the same breadth of obligations as a large licensee with a fraction of the staff and budget, and cyber security necessarily competes for that limited time and money against every other licensee obligation.

Cyber security guidance is also frequently written in highly technical language that assumes a level of expertise most small business owners do not have and cannot reasonably be expected to acquire.

We are advised that the majority of small licensees rely on their own internal IT arrangements, while a smaller proportion rely on external service providers ("Managed Service Providers" or MSPs). Those that rely on external providers sometimes have limited visibility over the adequacy of the provider's work and are, in effect, trusting that the provider is meeting appropriate standards. This presents a risk that outsourcing IT or cyber functions may create a false sense of security, such that a business relying on the guidance of an external provider may not be meeting a recognised minimum standard, such as the Essential Eight[2], and may only become aware of this after an incident has occurred.

[2] The Australian Signals Directorate's (ASD) Essential Eight is a set of eight baseline cyber security mitigation strategies designed to help organisations reduce the risk of cyber incidents and make it more difficult for adversaries to compromise systems. Further information is available from ASD's Essential Eight guidance.

Members also noted increasing uncertainty regarding the cyber implications of emerging AI tools. Small businesses are beginning to adopt AI-enabled products, often through software providers and third-party platforms. However, many businesses have limited visibility regarding the associated cyber, operational and data governance risks, particularly where AI capabilities are embedded within existing products and services. Recent observations from ASIC and APRA highlight that AI-related risks often arise through existing technology and third-party dependencies rather than standalone AI systems, reinforcing the need for practical guidance that enables small businesses to understand and manage these risks proportionately.

2. The adequacy, appropriateness and accessibility of guidance provided to small to medium sized businesses and organisations by Government in relation to cyber security

FAAA members were generally supportive of the existence of government cyber security guidance but raised concerns about its practical usability. The most consistent feedback was that cyber.gov.au, while comprehensive, is a resource-intensive site for a time-poor small business owner to navigate, and that members had spent disproportionate amounts of time attempting to determine which elements of the available guidance were applicable to a business of their size. It was also noted that guidance is dispersed across a number of government bodies with differing formats, and that some published resources, including small business checklists, are not updated with sufficient frequency to reflect a threat environment that is constantly evolving. Members expressed a preference for:

- plain-language, practical checklists over dense technical documentation;
- guidance illustrated with real case studies that make the consequences of inaction tangible; and
- a single, clearly signposted point of entry rather than guidance spread across multiple government bodies.

There was also support for a more proactive government role in alerting small businesses to emerging risks, on the basis that the threat environment changes too quickly for non-experts, including financial advice businesses, to monitor unaided.

3. Whether there are appropriate standards for small to medium sized businesses and organisations in relation to cyber security

FAAA members had a clear preference for continued investment in education and support ahead of furthering a compliance-driven approach to cyber security regulation. Members were concerned that a business could implement a recognised baseline, such as the Essential Eight, and reasonably consider its cyber risk to be addressed, when in practice a single gap, for example, reliance on an outsourced provider that has not fully implemented the framework, could still leave the business exposed. In our view, a checklist-based approach, without the practical capability required to give effect to it, risks creating a false sense of security.

There was greater support for standards applying to the cyber security service providers on which small businesses rely, rather than to small businesses themselves. Members raised the concept of an accreditation scheme for cyber security providers, comparable to other forms of professional accreditation, to assist small, non-expert businesses to identify a credible provider. This was regarded

as a potentially effective preventative measure, on the basis that it could make engaging a properly credentialled provider a more attractive and lower-risk option, without imposing an additional compliance burden on the small business itself. This support was qualified by concerns that accreditation could become a bottleneck that reduces the number of available providers and increases price and that a small pool of accredited providers would reduce a business's ability to select a provider suited to its needs.

In the absence of an accreditation scheme, it was suggested that small businesses would benefit from being equipped with a short, standard set of questions to put to a prospective provider, covering matters such as relevant certifications and minimum service requirements. We suggest this could be added to government's small business cyber tools. It was acknowledged, however, that a small business still requires some baseline understanding of cyber security to make use of the answers it receives, which underscores the need for improved, accessible education.

4. The ease for small to medium sized businesses and organisations to procure appropriate cyber security services in Australia

While members viewed cyber security as an essential investment that delivers tangible value to businesses and their clients, they noted that establishing and maintaining robust cyber security arrangements can involve substantial ongoing expenditure. Members indicated that the cyber security services market is generally accessible, with many small and medium-sized businesses engaging external providers to support their cyber resilience and regulatory obligations. However, cost remains a significant consideration in procuring and maintaining appropriately scaled cyber security services, alongside constraints relating to time, technical expertise, understanding regulatory expectations, and identifying providers with the requisite capability and experience. This is particularly relevant given the evolving nature of cyber threats, which requires organisations to review and update their controls over time.

Members also observed that smaller businesses can face challenges in independently assessing the effectiveness of specialist cyber security services. Many businesses rely on trusted MSPs to deliver and maintain cyber security controls, however have limited internal capability to benchmark performance or validate technical outcomes that providers deliver. Whilst ongoing MSPs can provide valuable expertise and support, their cost may be difficult to absorb for smaller organisations. As a result, businesses must balance the need for appropriate cyber security oversight and assurance with the practical realities of operating within finite financial and resourcing constraints.

5. The importance of training for employees on good cyber security practices to the overall cyber security of small to medium sized businesses and organisations

FAAA members were unanimous that ongoing staff training is important for the management of cyber risk in a small business, given that financial advisers and their support staff are not cyber security experts and cannot reasonably be expected to become so. They also do not have the resources or funds to develop tailored cyber security training themselves. Members therefore supported government developing and providing standardised baseline cyber security training to small businesses free of charge. This would help ensure a consistent minimum level of cyber security knowledge and capability across all small businesses, while reducing the cost and compliance burden of each business having to source or develop its own training.

Members considered that this training should:

- be genuinely ongoing and used as a regular reminder, rather than a one-off induction exercise;
- be delivered in plain, practical language that staff can act on, for example, not clicking suspicious links and reporting concerns immediately, supported by more technical material where relevant;
- extend to support staff and not only advisers, so that the whole practice shares an understanding of its cyber security environment; and
- be regularly updated to reflect emerging tools and risks, including artificial intelligence, AI-enabled cyber threats, the governance of AI tools used within businesses and the practical risks associated with increasingly autonomous systems and third-party AI services.

FAAA members also suggested that, to help ensure a consistent minimum level of cyber security capability across small businesses, consideration could be given to government-funded or government-provided baseline cyber security training for small businesses.

An additional consideration could be, for government to issue some form of digital certificate / recognition that a business has completed appropriate training and can be considered to be cyber-secure to a certain standard. This would be very useful information for clients, and a valuable incentive for small businesses to complete appropriate cyber security training and improvements in their businesses. Government may be able to charge a fee for the verification, which might need regular review and updating, which would create at least some revenue to help support ongoing activities.

6. The impact of cyber security maturity on the feasibility for small to medium businesses and organisations to participate in Government and large corporate supply chains

This term of reference was of particular concern to FAAA members, who described a significant and, in their assessment, growing imbalance of bargaining power between small advice businesses and the large superannuation funds, insurers and platforms whose systems they must use in order to service their clients. Product providers are increasingly imposing cyber security-related contractual terms on small advice businesses as a condition of continued access to their platforms. Members advised that such terms are commonly presented on a non-negotiable basis, incorporated into broader distribution or platform agreements. In practice, a small advice business has little genuine capacity to decline these terms, as doing so would mean losing the ability to recommend the platform or product to clients.

Members also raised concerns about clarity as to where liability sits when client information is held within, or accessed through, third-party systems. For example, where information is stored within systems such as Microsoft OneDrive or protected by a software provider's security infrastructure, members considered that responsibility for a breach originating within those systems should appropriately sit with the relevant provider. Conversely, where access is gained because an advice business has allowed an unauthorised party into its systems, or because a staff member has compromised or disclosed their login credentials, responsibility would more appropriately sit with the advice business. Members considered that clearer delineation of responsibility is needed to attribute the source of the security failure.

We note that discussions are currently underway between banks, telecom providers and social media platforms in relation to the Scams Prevention Framework. These deliberations may have relevance for the matters being considered by this Committee and it may be worthwhile for the Committee to engage with those discussions.

7. An additional matter for the Committee's consideration: authentication practices for unsolicited institutional contact

A key concern raised with the FAAA during our member engagement, and one we believe is not squarely addressed by the current terms of reference, relates to the authentication practices employed by institutions and government agencies when they initiate contact with small businesses.

Financial advice practices regularly receive such calls from Services Australia (Centrelink), superannuation funds and insurers. In many cases these organisations initiate the contact and then require the practice to answer authentication questions before they will explain the reason for the call. The difficulty is that such calls frequently originate from unknown, withheld or otherwise unverified telephone numbers, meaning the business is asked to disclose identifying information before it has had any opportunity to independently verify the identity of the caller. This is inconsistent with the cyber security messaging provided to businesses and consumers, which consistently encourages caution in relation to unsolicited calls and verification of a caller's identity before personal or identifying client information is shared. Larger organisations may have formal procedures in place to manage this risk. Many small advice practices, sole practitioners and older staff members may not, which in our view creates an avoidable exposure to social engineering and impersonation attacks. We do not consider this issue to be isolated to the financial advice profession; rather, it appears to be a systemic feature of how institutions and government agencies currently manage outbound authentication.

The recognised best practice response, to decline to provide any information during the unsolicited call and instead return the call using a publicly listed number, is straightforward to state, however difficult to apply in practice. We were advised that this approach commonly involves lengthy, costly wait times and operational inefficiencies that create pressure on staff to complete the authentication process while the original caller remains on the line, rather than following the safer but slower process. This creates a direct conflict between efficient client service and sound cyber security practice, compounded by an imbalance of power in which government agencies and large institutions are able to call a small business and require it to identify itself and/or its relevant client, while the institution or agency placing the call often cannot itself be readily identified or verified by the business receiving it.

The FAAA is not aware of clear, consistent guidance for how a small business should manage this scenario and would welcome the Committee's consideration of what constitutes best practice for a small businesses receiving this type of call, and whether this issue has previously been considered by government agencies or by the institutions that place such calls.

Recommendations

The FAAA recommends that:

1. the Government's cyber security guidance for small business be consolidated behind a single, plain-language entry point, be reviewed regularly to reflect the current threat environment, be

supported by practical case studies, and include a proactive mechanism for alerting small business to emerging risks;

2. any new standards regime for cyber security should prioritise education and support over compliance-based obligations on small businesses themselves, and that the Government give further consideration to an accreditation framework for cyber security service providers, designed to test genuine capability while preserving competition and business choice, in preference to imposing further direct obligations on small businesses;

3. the Government consider how it can assist small businesses to evaluate cyber security services prior to purchase, whether through provider accreditation, a standard set of vetting questions, or subsidised access to independent cyber health checks, to address the imbalance between what small businesses can afford and what they need to know to procure services effectively;

4. the Government develop practical guidance for small businesses on managing cyber and operational risks associated with emerging AI technologies, including governance arrangements, third-party dependencies, concentration risk, incident escalation and recovery planning, with a particular focus on translating these concepts into proportionate actions for small organisations;

5. Government-supported training resources for small businesses be modular and ongoing rather than one-off, distinguish between plain-language behavioural guidance and technical detail, be eligible for professional development recognition where appropriate, be updated to address emerging tools; and potentially be associated with a digital certificate or some other way a business can demonstrate to its clients that it has met a cybersecurity standard;

6. the Committee examine the terms that large product providers and platforms impose on small advice practices and other small businesses as a condition of market access, and consider whether small businesses require statutory or regulatory protection against unreasonable or non-negotiable cyber security terms imposed by materially larger counterparties on whom they depend for access to the market; and

7. the Committee examine the identity authentication practices used by government agencies, superannuation funds, insurers and other institutions when initiating unsolicited contact with small businesses, and work with those institutions to develop a consistent, workable standard that does not require a small business to disclose identifying information to a caller whom it cannot independently verify.

Conclusion

The FAAA welcomes the opportunity to provide feedback on the Committee's terms of reference, informed by consultation with our working group of financial advisers. Drawing on their practical experiences and insights, we have provided our analysis of the key issues affecting small financial advice businesses and recommendations for the Committee's consideration.

If you have any questions about our feedback, please do not hesitate to contact me on 0484 278 106 or sarah.abood@faaa.au.

Yours sincerely,

Sarah Abood
Chief Executive Officer
Financial Advice Association Australia (FAAA)