31 August 2026

Committee Secretary
Select Committee on Cyber Security for
Small to Medium Sized Businesses and Organisations
PO Box 6021
Parliament House
Canberra ACT 2600

Email: cssmbo.reps@aph.gov.au

Dear Secretary,

SMSF ASSOCIATION SUBMISSION – CYBER SECURITY FOR SMALL TO MEDIUM SIZED BUSINESSES

The SMSF Association welcomes the opportunity to provide this submission to the House of Representatives Select Committee on Cyber Security regarding its inquiry into cyber security for small to medium sized businesses and organisations.

Many of our members work in, own or advise small and medium-sized accounting, audit and financial advice practices. These businesses hold significant amounts of sensitive financial and personal information and are increasingly reliant on cloud-based software, third-party applications and external technology providers in delivering professional services.

Our submission highlights a number of practical challenges facing these businesses, including the cost and complexity of maintaining appropriate cyber security protections, dependence on third-party technology providers, limited bargaining power over contractual arrangements, access to affordable and appropriately skilled cyber security services, cyber insurance, legacy systems and data retention requirements.

We also encourage the development of practical, proportionate and accessible cyber security guidance and standards that recognise the particular circumstances and resources of small businesses, while avoiding unnecessary duplication of existing regulatory and professional obligations.

The SMSF Association would be pleased to discuss the matters raised in our submission further with the Committee.

Yours sincerely,

Tracey Scotchbrook

Tracey Scotchbrook
Head of Policy and Advocacy

Cyber security for small and medium businesses

Submission to the House Select Committee on Cyber Security for Small to Medium Sized Businesses and Organisations.

SMSF Association | August 2026

Table of Contents

Executive Summary

Cyber security is now a core business-resilience issue for small professional practices. For SMSF professionals, the policy problem is not simply a lack of awareness or "cyber hygiene". Modern accounting, audit and advice services depend on cloud software, digital identity, online lodgement channels, client portals, bank feeds, document systems and third-party applications. These tools are essential to deliver timely, compliant and affordable services, but they also create a distributed technology supply chain over which a small practice has limited control.

At the same time, regulated professionals can carry substantial legal and professional obligations in relation to information security, confidentiality, outsourcing, supervision and record keeping. ASIC, the Tax Practitioners Board (TPB), the Australian Taxation Office (ATO), AUSTRAC and professional

standards bodies each provide relevant requirements or guidance. Much of that guidance is sensible. The practical difficulty is translating overlapping obligations into a proportionate, affordable and auditable set of controls for a small firm.

The Association therefore supports a policy approach that makes good cyber security easier to adopt, easier to verify and easier to carry across regulatory and commercial relationships. The Government's recently announced CyberSmart program is a particularly important opportunity. It should become a nationally recognised SME baseline rather than an additional layer sitting beside multiple regulator, licensee, insurer and procurement requirements.

About the SMSF Association

The SMSF Association is the peak body representing the self-managed superannuation fund (SMSF) sector which is comprised of over 1.2 million SMSF members and a diverse range of financial professionals. The SMSF Association continues to build integrity through professional and education standards for practitioners who service the SMSF sector. The SMSF Association consists of professional members, principally accountants, auditors, lawyers, financial advisers, tax professionals and actuaries. Additionally, the SMSF Association represents SMSF trustee members and provides them with access to independent education materials to assist them in the running of their SMSF.

Summary of Recommendations

#	Recommendation	What it would do	Terms of reference
1	**Make CyberSmart the recognised SME baseline**	Co-design the standard with regulated professional-service SMEs; include proportionate tiers and map it to common regulatory expectations.	2, 3, 6
2	**Create a cross-regulator implementation pathway**	Publish one practical cyber obligations map for SMEs regulated across tax, financial services, privacy and AML/CTF settings, with common terminology and evidence requirements.	2, 3
3	**Lift transparency and accountability in the technology supply chain**	Develop a standard supplier disclosure covering data location, subprocessors, security responsibilities, incident notification, support/end-of-life, data export, retention/deletion and exit arrangements.	3, 4, 7
4	**Improve access to trusted, affordable cyber expertise**	Extend tailored government assistance beyond businesses with 19 or fewer employees and establish a trusted provider/assurance pathway suitable for SMEs.	4
5	**Simplify incident reporting and improve data**	Create a single government "front door" and notification navigator, reduce duplicate reporting where possible, and publish anonymised sector/size data to address under-reporting.	1, 2, 7

#	Recommendation	What it would do	Terms of reference
6	**Support practical, role-based training**	Build on Cyber Wardens; encourage recurring scenario-based training for principals, employees and contractors, and recognition through professional CPD/CPE frameworks.	5
7	**Improve cyber insurance transparency and proportionality**	Work with insurers, brokers and licensees on clearer SME policy comparisons, proportionate minimum requirements and recognition of CyberSmart controls.	4, 6, 7
8	**Avoid a certification barrier to SME supply chains**	Use CyberSmart to reduce—not multiply—procurement requirements; allow transition periods, remediation pathways and "single assessment, multiple use" recognition.	6

1. Why this inquiry matters to SMSF professionals

The SMSF Association is the independent professional body representing Australia's self-managed super fund sector. Its mission is to lead the professionalism, integrity and sustainability of the SMSF sector. Our professional community includes accountants, SMSF auditors, financial advisers, lawyers, administrators, actuaries and other specialists supporting SMSF trustees.[2]

Many SMSF professionals work in sole-practitioner, small partnership, small company or small-team environments, including practices that are themselves Australian financial services (AFS) licensees or authorised representatives.

As of July 2026, there were 1,654 financial advice practices with one to nine advisers per practice. This represents 88.1 per cent of licensees and 28.2 per cent (4,301 advisers) of the total financial adviser population.[1] Looking more broadly, 98.4% of financial advice business have less than 100 financial advisers, representing 9,438 of financial advisers, or 61.9% of the total financial advisor population.[2] The TPB separately reported 63,865 registered tax practitioners, of which 46,900 are registered tax agents[3]. A large portion of these practitioners operate in small to medium sized businesses, including sole practitioners. This size of business is similarly represented in the SMSF auditor population. These profession based datasets are not directly comparable and do not establish a single firm-size statistic for all accounting, audit and advice businesses, but they demonstrate the breadth and fragmentation of the professional market in which our members operate.

Professional services firms hold sensitive client information including tax file numbers, identity documents, bank and investment information, financial statements, trust and company records, superannuation information, advice records and client communications. A cyber incident can therefore create consequences for clients well beyond the immediate IT outage, including identity theft, tax or refund fraud, privacy harm, financial loss and regulatory exposure. The ATO expressly

[1] Padua, 'Australian Financial Adviser Market – A structural analysis of supply, demand and the productivity imperative', (Report, 28 July 2026) 23.
[2] Ibid.
[3] Tax Practitioners Board, 'Annual Report 2024-25', (Report, 31 October 2025) 6.

warns that tax professionals who hold large amounts of client, staff and business information are a growing target for identity thieves.[4]

2. Cyber maturity should be understood in the context of SME capability

The Association supports the Committee examining cyber maturity but cautions against treating maturity as a binary question of whether a business is "secure" or "not secure", or whether it holds an enterprise-level certification. The relevant question for an SME is whether it has controls proportionate to the sensitivity of its information, its technology dependencies and the realistic resources available to it.

We are concerned that visibility of cybersecurity incidents, and therefore access to reliable data, is limited in the broader SME market. This is largely due to significant underreporting of incidents. Underreporting can arise due to the limited resources available to business and a need to focus on the issue and business operations, a lack of understanding of reporting obligations, embarrassment, and fear for the harm it may cause them and their business.

A useful SME maturity model should therefore test practical outcomes. Focus areas should include strong authentication, assessing suitability of software and whether existing software remains supported, backup processes and testing, whether the firm knows which providers hold its data, whether an incident can be detected and escalated, and whether the business can continue serving clients when a key platform fails.

3. Government and regulator guidance: the problem is translation and fragmentation

The difficulty for a small professional practice is converting guidance from several sources into one workable compliance system. Depending on the services provided, a firm may need to consider obligations and guidance from ASIC, the TPB, the ATO, AUSTRAC, privacy law, an AFS licensee, professional standards and contractual requirements imposed by large clients or technology providers.

ASIC states that AFS licensees must adequately manage cyber security risks as part of their licence obligations and have adequate technological systems, policies and procedures, but also states that it does not prescribe technical standards or specific requirements for individual licence holders. ASIC expects measures to be proportionate to the nature, scale and complexity of the organisation and the sensitivity of its information.[5] Further, ASIC emphasised the need for the licensee to manage cyber risk across its authorised representative network.

[4] Australian Taxation Office, 'Data breach guidance for tax professionals', *QC54173* (Web Page, 23 March 2026) < https://www.ato.gov.au/online-services/scams-cyber-safety-and-identity-protection/help-with-data-breaches/data-breach-guidance-for-tax-professionals>

[5] Australian Securities and Investments Commission, *What a Federal Court ruling on cybersecurity means for AFS licensees,* (12 May 2022) < https://www.asic.gov.au/about-asic/news-centre/articles/what-a-federal-court-ruling-on-cybersecurity-means-for-afs-licensees >

Issues can also extend beyond internal networks where business outsource some of their business operations.[6] ASIC reiterated that outsourcing does not remove an AFS licensee's responsibility to comply with its obligations

Members report that some licensee arrangements accordingly prescribe cyber policies, technology platforms, gateways, security requirements or insurance. Such controls may be reasonable and can uplift security. However, they can also impose significant cost, constrain technology choice and create duplicative assessments where a small practice serves several regulatory or commercial relationships. The solution should not be to reduce responsibility. Rather, SMEs and licensees should be given a common, credible baseline that demonstrates a minimum standard.

Similar issues exist for tax professionals. TPB guidance recognises external IT providers and cloud storage as third parties and places the onus on the practitioner to undertake appropriate due diligence and protect client confidentiality. [7] The TPB also notes there is no one-size-fits-all approach. Those obligations are important, but a sole practitioner cannot realistically perform the same supplier-security assessment as a bank or Commonwealth agency.

The Association recommends a cross-regulator implementation map that is co-developed with ASIC, TPB, ATO, AUSTRAC and the OAIC, that translates common cyber expectations into one set of SME actions and evidence. Where requirements differ, the map should state why. This would not displace legal obligations, but would act to reduce the cost of finding, interpreting and repeatedly evidencing them. It would ensure consistency and aid engagement and understanding by SMEs.

4. CyberSmart is the right direction—provided it reduces "white tape"

The Association welcomes the Government's June 2026 announcement of CyberSmart under Horizon 2 of the Australian Cyber Security Strategy. The Government has expressly recognised that the Essential Eight is not necessarily a useful SME implementation tool and that SMEs need a simpler, adaptable and fit-for-purpose standard. CyberSmart is intended to include certification and a trust mark, with uptake supported through government procurement and regulatory levers.[8]

This creates an opportunity to solve several problems at once. We recommend that CyberSmart:

- be co-designed with small accounting, audit, financial advice, legal and other professional-service businesses that hold sensitive client data;
- use a baseline tier that a sole practitioner or small firm can implement without enterprise-level security staff, with optional higher-risk modules for businesses handling sensitive financial or identity information;

[6] Australian Securities and Investments Commission, *ASIC flags risks in offshore outsourcing after review identifies governance gaps,* (25-234MR, 10 October 2025) < https://www.asic.gov.au/about-asic/news-centre/find-a-media-release/2025-releases/25-234mr-asic-flags-risks-in-offshore-outsourcing-after-review-identifies-governance-gaps >

[7] Tax Practitioners Board, *Confidentiality of client information* (TPB(GS) 26/2014, 20 July 2026).

[8] Department of Home Affairs, *Horizon 2: Expanding our reach (2026–2028)* < https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/horizon-2 >

- map clearly to the Essential Eight and other established frameworks, while avoiding an assumption that SMEs should obtain ISO/IEC 27001 certification unless their risk profile or customers genuinely justify it;
- produce portable evidence—so the same certification or assessment can be recognised by government buyers, AFS licensees, insurers and large corporate customers rather than generating separate questionnaires and audits; and
- include a practical remediation pathway, reasonable transition periods and low-cost reassessment so certification is an uplift mechanism rather than a barrier to market entry.

The objective should be "single assessment, multiple use". If CyberSmart becomes simply another certificate added to existing licensing and registration obligations, insurer and procurement requirements, it will increase compliance cost without achieving the Government's stated goal of reducing white tape.

5. Cloud software and third-party applications are both essential and a source of structural risk

Modern professional practices cannot realistically retreat from digital services. Cloud accounting software, document management, electronic signatures, secure portals, practice-management systems, bank feeds, audit tools, digital identity and online lodgment systems all enable SME professional services businesses to provide services in a timely and cost-effective way. Removing those efficiencies would make small practices less competitive and, in many cases, make compliance harder rather than easier.

The concern is that a typical technology stack is no longer one supplier. A core platform may connect to multiple third-party applications, plug-ins and integrations. Each connection can introduce another vendor, credential, permission set, support team, subprocessor, jurisdiction and contractual relationship. The small firm may remain accountable to its client even where the point of failure sits elsewhere in the chain.

TPB guidance captures this dynamic well, noting that users of cloud storage and outsourced IT can be third-party arrangements, that practitioners should understand where information is stored and disclosed, and the practitioner retains responsibility for appropriate due diligence.

Small businesses also tend to acquire software and cloud services under standard-form terms rather than individually negotiated contracts. An SME the procurement team does not have the bargaining power of a large institution.

We recommend a standard SME cyber supplier disclosure—potentially linked to CyberSmart procurement—covering at least:

- where primary data is hosted and the material use of offshore support or subprocessors;
- the respective security responsibilities of customer and provider;
- minimum authentication, access-control, backup and recovery arrangements;
- timeframes and channels for notifying customers of security incidents;

- support and end-of-life dates, including notice before material deprecation;
- data portability and export formats, including access during termination or migration; and
- what customer data will be retained, archived or deleted after termination and for how long.

Australian Signals Directorate's 'Secure by Design' guidance supports this focus on secure deprecation. It states that software as a service and managed-service providers should clearly communicate how services will be deprecated, including what data will be deleted or retained.[9] That principle is highly relevant to SMEs that can lose system access after changing provider while still carrying record-keeping obligations.

6. Access to trusted cyber expertise is a market-access issue

Small practices often know they need specialist help but face two related problems, affordability and assurance. A quality cyber assessment, remediation project or managed service can be expensive relative to an SME's revenue. At the same time, it can be difficult for a non-technical business owner to distinguish a capable adviser from a provider selling a generic package or a proprietary solution.

Government support is therefore valuable. The Small Business Cyber Resilience Service provides free, tailored, person-to-person assistance, but eligibility is currently limited to sole traders and businesses with 19 or fewer full-time-equivalent employees. There is a policy gap for firms that are too large for the free service but remain far below enterprise scale.

The Association recommends:

- extending the tailored support model, or creating a parallel subsidised service, for businesses with 20–199 employees on a co-contribution basis;
- a trusted-provider pathway or directory linked to CyberSmart, with transparent minimum competencies, relevant insurance and disclosure of material commercial relationships;
- small grants or vouchers for an initial independent cyber assessment and remediation plan, with controls scaled to business risk rather than a fixed technology bundle; and
- support for regional and sole-practitioner firms that may have fewer local provider options.

We do not presently recommend a broad new occupational licensing regime for all cyber service providers. The first priority should be improving transparency, assurance and access without creating another layer of cost and complexity. Consideration should also be given to what level of additional assurance obligations would be required of service providers.

7. Cyber insurance can assist recovery, but it should not become a proxy for cyber maturity

Members have raised the increasing role of cyber insurance, including circumstances where an AFS licensee or other commercial counterparty expects a practice to hold cover. Insurance can provide

[9] Australian Signals Directorate, *Secure by Design Foundations* (July 2024): Foundation 6: Secure deprecation < https://www.cyber.gov.au/business-government/secure-design/secure-by-design/secure-by-design-foundations >

valuable incident-response expertise and financial protection, but it is not a substitute for prevention, resilience and clear allocation of technology risk.

Cyber insurance take-up among small businesses remains low. Policy coverage, conditions and exclusions vary between products. SMEs may find it difficult to assess whether a policy is fit for their risk and whether the security controls required as conditions of cover are proportionate and achievable. A mandated policy can add cost without necessarily solving the underlying supply-chain exposure.

Government should work with the insurance industry, intermediaries and relevant regulators to encourage a simple SME comparison disclosure for cyber policies, improve access to claims and incident data, and align underwriting questions with CyberSmart wherever appropriate. Where licensees or procurement contracts require insurance, requirements should be proportionate to the nature and value of the risk and should not require SMEs to insure risks that are practically uninsurable.

8. Training is essential, but systemic risk cannot be trained away

The Association strongly supports practical staff training. People remain an important part of cyber resilience, particularly in relation to phishing, business email compromise, password reuse, social engineering, false payment instructions and increasingly sophisticated AI-assisted impersonation. Training should include business principals and contractors as well as employees.

However, training should not be treated as the solution to failures in unsupported software, insecure supplier architecture, excessive privileged access, weak contractual incident notification or poor data portability. A trained employee cannot patch a third-party service or compel an offshore provider to disclose a breach.

The Government should build on the Cyber Wardens program with short, recurring, scenario-based modules relevant to professional services. Joint regulator tools, resources and guidelines and training resources would enhance sector specific obligations and ensure a centralised hub to assist practitioners.

9. Record keeping, legacy systems and data portability need to be treated as cyber issues

Professional firms cannot apply a simple data minimisation strategy. They must retain records for legal, professional and evidentiary reasons. For example, TPB requirements generally require proper client records to be retained for at least five years after the relevant tax agent service is provided. AUSTRAC's current AML/CTF guidance generally requires relevant records for seven years, with customer due diligence records retained for seven years after a business relationship ends.

Tax and superannuation law have various document retention obligations. While some of these may be a client responsibility, client expectations are that the professional service provider has retained those records. There are circumstances where the Commissioner of Taxation is not time limited and can review and audit aged transactions, returns or events.

These retention obligations can collide with technology lifecycle risk. A firm may need to keep historical records after moving to a new practice system, but a former provider may restrict access, charge for archive retrieval, retain copies under its own policies, or provide data only in a format

that is difficult to use. Running an unsupported legacy system solely to preserve historical records can itself create a cyber vulnerability.

The Association recommends that secure lifecycle and exit arrangements become part of SME cyber standards and supplier expectations. A professional practice should be able to export records in a usable format, understand exactly what the former provider retains, maintain secure read-only access where necessary, and obtain confirmation of deletion when retention is no longer required. Providers should give meaningful advance notice of end-of-support and material changes that require a migration.

Record-retention periods differ across tax, superannuation, financial-services, privacy, AML/CTF and professional obligations. The common policy point is that SMEs with regulated client records often need secure, reliable access to historical information for years after the service is performed. Data portability and secure archival arrangements are therefore core cyber-resilience requirements.

10. Supply-chain requirements should lift security without excluding SMEs

The Committee's focus on participation in government and large corporate supply chains is particularly important. Cyber security requirements can appropriately protect the larger organisation from third-party risk. But inconsistent or enterprise-level requirements can also operate as a barrier to SMEs even where the work being procured is low risk.

CyberSmart provides a mechanism to address this. Government should encourage procurement frameworks to accept a CyberSmart level that is proportionate to the data and system access involved, rather than defaulting to ISO certification or bespoke questionnaires. Higher assurance should be required where the risk genuinely warrants it. SMEs should be given reasonable transition periods and an opportunity to remediate gaps before exclusion from a supply chain. This would strengthen the weakest links in supply chains while preserving competition and diversity among smaller providers.

11. Incident reporting needs a simpler front door and better data

The extent of under-reporting by SMEs means government does not have a complete picture of cyber harm to SMEs. There are understandable reasons for this. Firms may be uncertain about whether an event is reportable, may face multiple potential notification channels, may fear reputational consequences, or may be occupied with restoring systems and protecting clients.

For a regulated professional practice, one incident may potentially engage ReportCyber, an AFS licensee or ASIC, the OAIC's Notifiable Data Breaches scheme, the TPB, the ATO, AUSTRAC, insurers and affected clients, depending on the facts. The Association supports a single government incident "front door" and notification navigator that tells an SME what notifications are likely to apply, captures core facts once where legally possible and allows secure referral between agencies.

Government should also publish more anonymised incident data by business size, sector, attack type, root cause, third-party involvement and financial/non-financial impact. Better data would improve policy, insurer pricing, software-provider accountability and SME understanding of real-world risks without requiring publication of identifiable victim information.

Conclusion

Small professional practices are not smaller versions of large corporations. They often hold highly sensitive data and operate under significant regulatory obligations, yet they do so with fewer people, less bargaining power, less internal cyber expertise and substantial dependence on external technology providers.

The Association's central recommendation is therefore that cyber policy for SMEs should focus on practical adoption and shared responsibility. Government should give SMEs a recognised baseline, make regulator expectations interoperable, improve supplier transparency, provide access to trusted expertise, simplify reporting and ensure that procurement and insurance settings reinforce rather than duplicate the same controls.

CyberSmart is a timely opportunity to achieve that outcome. If designed with the realities of regulated small businesses in mind, it can reduce complexity while lifting security. If it becomes another separate certification layered on top of existing regulator, licensee, insurer and customer requirements, the opportunity will be lost.