Australian Institute of Company Directors

Level 5
No.1 Martin Place
Sydney NSW 2000

1300 739 119
contact@aicd.com.au
aicd.com.au

ABN 11 008 484 197

28 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

Dear Committee Secretary

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

Thank you for the opportunity to provide a submission on the inquiry into cyber security for small to medium sized businesses (**SMBs**) and organisations (**Inquiry**).

The Australian Institute of Company Directors Limited (**AICD**)'s mission is to be the independent and trusted voice of governance, building the capability of a community of leaders for the benefit of society. The AICD's membership of more than 54,000 includes directors and governance leaders of not-for-profits (**NFPs**), large and small businesses and the public sector. Many of our members are closely involved in the management and governance of SMBs and NFPs, and are grappling with the challenges of building cyber and data resilience on a daily basis.

In recent years, the AICD has engaged extensively on Government consultations and proposed reforms in cyber security, critical infrastructure and data management policy areas, including submissions on the *Cyber Security Act 2024* (**CS Act**), the development of the 2023–2030 Australian Cyber Security Strategy (**Cyber Strategy**), amendments to the *Security of Critical Infrastructure Act 2018* (**SOCI Act**) and reform of the *Privacy Act 1988* (**Privacy Act**).

We have also supported directors in improving their knowledge of digital governance best practice through extensive guidance materials, including the Cyber Security Governance Principles, Guidance with the Australian Signals Directorate (**ASD**) on Frontier AI cyber threats, A Director's Guide to AI Governance and the Data Governance Foundations for Boards publications.

Our submission has been informed by engagement with senior directors and cyber security experts.

1. Executive Summary

SMBs and NFPs play a critical role in the Australian economy and community, however they face structural barriers to improving cyber and data resilience, including limited financial and people resources and competing operational priorities.

Large Australian organisations, supported by effective board oversight, have made important strides in recent years in building cyber resilience, underpinned by significant investments in controls, new infrastructure and heightened regulatory focus. The Inquiry is a valuable opportunity to identify how improvements in cyber security maturity can be extended to the significant populations of SMBs and NFPs to uplift their cyber and data resilience and develop practical, risk-based policy responses that reflect the realities of governing and operating a small organisation.

Australia's response to cyber security challenges requires a partnership-based 'Team Australia' approach. Cyber security and data risks cut across organisational and sectoral boundaries, and cannot be effectively addressed by Government, business or individuals acting alone. The AICD acknowledges the significant work undertaken by the Government already to deliver the Cyber Strategy, including the commitments under the Horizon 2 Action Plan. Achieving meaningful change will require an ongoing, coordinated and vigilant effort from Government, large organisations, SMBs, NFPs and technology providers.

The key points in our submission are:

- **Accessible and consolidated guidance:** We strongly support the CyberSmart Hub proposed in the Cyber Strategy Horizon 2 Action Plan. It should provide SMBs and NFPs with a clear entry point to Government guidance, and distinguish between legal obligations, recommended baseline practices and measures for organisations with higher risk exposure. New guidance should also explain how malicious actors may use artificial intelligence (**AI**) to increase the speed, scale and sophistication of cyber attacks.

- **A standard for IT infrastructure and other cyber security providers:** The Inquiry should consider the role of managed service providers (**MSP**), managed security service providers (**MSSP**) and Software as a Service (**SaaS**) vendors who design, operate and secure the systems on which SMBs and NFPs rely. We recommend consideration by the Inquiry of how these critical providers can be incentivised not only to improve their own resilience, but also to offer stronger controls in baseline offerings to SMBs and NFPs.

- **Training and awareness:** We support the Government's planned cyber awareness and workforce training initiatives in the Horizon 2 Action Plan. Training should be practical, freely available and differentiated by role and sector, including tailored programs for directors and managers in particular sectors and industries. These resources should be linked to CyberSmart and promoted through a well-resourced awareness campaign.

- **Supply-chain participation:** Many Government agencies and large organisations now expect suppliers to demonstrate a baseline level of cyber security maturity, which SMBs and NFPs can struggle to meet. The AICD recognises the potential value of CyberSmart certification in giving procuring organisations, including the Government, greater confidence in smaller suppliers. Our strong view is that these mechanisms should be implemented proportionately, and paired with adequate support for SMBs and NFPs to uplift their cyber maturity.

- **Cyber insurance:** Cyber insurance can form a useful part of a broader cyber risk management framework, and may encourage organisations to adopt stronger controls. However, affordability, exclusions and minimum eligibility requirements can make suitable cover difficult for smaller organisations to obtain. Insurance should complement, rather than substitute for, investment in prevention, preparedness and resilience.

- **No further broad-based regulation:** We do not support imposing additional general cyber security or data governance regulation on SMBs and NFPs. In particular, we do not support removing the Privacy Act small business exemption and placing the full weight of these obligations on SMBs and NFPs. A concentrated and well-resourced program of education, practical guidance, standards and capability-building is more likely to produce meaningful improvements than additional layers of compliance.

Overall, the AICD considers that the Government should prioritise the timely and effective delivery of its Horizon 2 Action Plan. The objective should be to make effective cyber security and data governance easier and more affordable for SMBs and NFPs to achieve, while placing appropriate responsibility on the

technology providers, institutions and supply-chain participants that are better positioned to address cyber security and data risks at scale.

2. Cyber Strategy – Horizon 2

The AICD welcomes the Government's substantial program of work to strengthen the cyber resilience of SMBs and NFPs under the Cyber Strategy. In particular, the Horizon 2 Action Plan contains various actions and initiatives intended to scale cyber security maturity across the Australian economy. The Cyber Strategy recognises that smaller organisations often lack the financial resources, specialist expertise and internal capability needed to navigate an increasingly complex cyber threat environment.

We support the development of the CyberSmart program, including a tailored cyber security standard and certification regime for small organisations. A clear, proportionate and practical standard has the potential to help smaller organisations identify priority actions, assess their cyber maturity and make informed investments. Further, a certification mark that has market traction and awareness should promote adoption of the standard as SMBs seek to differentiate themselves, including in tender and procurement processes.

The Government's commitment to continued investment in cyber awareness programs is also welcome. Clear and accessible education, supported by practical tools such as the enhanced Cyber Health Check Tool, can help business owners, directors, employees and volunteers understand their respective responsibilities and adopt stronger cyber security practices.

The AICD also supports the Government's focus on secure-by-design standards for commonly used connected technologies. Improving the security of products and services relied upon by smaller organisations can reduce the burden placed on individual businesses and provide greater protection to entities with limited capacity to defend themselves. Collectively, these initiatives represent a constructive shift towards practical support, shared responsibility and reducing cyber risk in an effective way without new punitive regulation for SMBs and NFPs.

We note that effective implementation of all the actions identified in the Horizon 2 Action Plan will be critical. Initiatives should be adequately resourced, easy for SMBs and NFPs to navigate and designed with their operational and financial constraints in mind.

3. Terms of Reference

This section responds to each of the questions set out in the Inquiry's terms of reference.

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

There is a maturity gap in the cyber and data resilience of SMBs and NFPs as compared to larger, well-resourced organisations. Informed by stakeholder feedback, our view is that the resilience of SMBs and NFPs has improved in recent years. However, the cyber threat landscape is rapidly evolving, particularly in the context of the capability of frontier AI models to identify systemic and individual organisation vulnerabilities.

The directors and owners of SMBs and NFPs often face resourcing constraints and competing priorities that can result in cyber security controls not receiving appropriate attention or funding. These constraints mean SMBs and NFPs often take a leaner approach to cyber security matters than larger organisations, such as choosing not to have a dedicated IT team or selecting entry-level packages from their MSP, MSSP or SaaS provider(s) that do not include more costly cyber security controls.

We welcome the Government's focus on improving the cyber maturity of smaller organisations under the Horizon 2 Action Plan. In particular, the proposed CyberSmart program and enhanced Cyber Health Check

Tool have the potential to help SMBs and NFPs identify priority actions and make informed, risk-based decisions within the constraints of their comparatively limited resources.

Heightened challenges for NFPs

We highlight that NFPs face particular challenges in building cyber and data resilience that can be distinct from SMBs. In particular, they can often face uncertainty about future funding, whether from private funders or Government programs. Uncertainty about the medium to long term financial stability of an NFP can mean boards and management are hesitant to make significant capital investments into new digital and data technology, including greater cyber protections.[1]

An additional challenge for NFPs is that they often rely on volunteers to undertake key operations and provide services to clients. This means that it can be difficult to promote features of a cyber resilient culture like email hygiene, mandatory training and strong password/key practices. A predominantly volunteer workforce may be more likely to take shortcuts in data entry practices or systems access, for example, to expedite offering services to clients.

We highlight the work by the Australian Charities and Not-for-profits Commission (**ACNC**), in particular its focus on raising awareness of cyber resilience practice improvements for NFPs and charities. However, we remain of the view that more can be done to support the resilience of this critical component of the Australian economy and society. We note that this has been recognised in the Horizon 2 Action Plan, which identifies driving cyber uplift and maturity in the NFP sector as one of its six key actions.

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

The AICD has consistently heard in this, and previous consultations, that SMB and NFP directors, owners and managers face significant challenges navigating guidance on cyber and data resilience, and understanding 'what good looks like'.

A key issue for SMBs and NFPs is that there is no single 'source of truth' that they can turn to in order to understand better cyber security practices. The websites containing cyber security guidance that may be relevant to SMBs and NFPs include Cyber.gov.au, Business.gov.au, the Office of the Australian Information Commissioner, the National Office of Cyber Security, the Australian Signals Directorate, AUSTRAC, APRA, ASIC, Australian Taxation Office and the Australian Digital Health Agency. Most of these websites have multiple webpages with different information, resources and links to additional guidance. This is in addition to trusted sources in industry, including the Council of Small Business Organisations Australia (**COSBOA**) and the AICD.

Given the resourcing constraints many SMBs and NFPs face, combing through and reconciling these various resources is in itself a challenge.

Raising awareness and targeted guidance

The AICD strongly supports the Government's commitment to establish a centralised CyberSmart Hub for smaller organisations under Horizon 2. The proposed consolidation of Government guidance, together with information to help organisations identify suitable cyber security products and services, responds directly to concerns raised by AICD members. To be most effective, the CyberSmart Hub should provide a clear and practical entry point to Government guidance, and clearly distinguish between legal obligations, recommended baseline practices and additional measures relevant to organisations with higher risk

[1] The latest Australian Charities Report states that while Australian NFPs are experiencing positive growth, this is outpaced by their expenses. See page 19.

exposure. It should also cover where an SMB can go to for help, including in the event of a significant incident.

In the AICD's view, the key is that SMBs and NFPs are clearly able to understand what 'good' cyber security looks like for their business. We see great opportunity for guidance that is tailored to specific industries and sectors. For example, covering what strong cyber and data practices look like for care providers.

There should be clear and consistent pathways between the CyberSmart Hub, Business.gov.au, cyber.gov.au and regulator-specific guidance. The CyberSmart Hub should also be actively maintained and promoted. Consolidating information will have limited impact if directors, owners, managers and volunteers are not aware that the resource exists, or cannot readily determine which guidance applies to their organisation.

Guidance on AI driven cyber risks

AI is rapidly disrupting the cyber security landscape.[2] SMBs and NFPs are particularly exposed to AI-enabled cyber threats due to their lower level of cyber maturity. This is partly because many SMBs and NFPs rely heavily on MSPs and MSSPs, which are themselves directly exposed to frontier AI-enabled threats and have varying levels of capability to respond to this rapidly evolving threat landscape. Any weaknesses in the systems of these providers put those they provide services to at risk. As such, how malicious actors may use AI to increase the speed, scale and sophistication of cyber attacks is a clear area where the Government could work to supplement the adequacy of guidance, support and standards relevant to SMBs, NFPs, MSPs and MSSPs.

The AICD notes the Government's commitment in Horizon 2 to improve understanding of AI-related security threats, and increase information sharing concerning AI incidents. We consider it appropriate that SMBs and NFPs be considered as a key group that should benefit from this uplift.

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

A standard for SMBs and NFPs

The AICD welcomes the Government's commitment to develop the CyberSmart program, including a tailored cyber security standard, certification regime and trust mark for small organisations. A clear and proportionate standard has the potential to provide SMBs and NFPs with a more accessible pathway for identifying priority controls and assessing their cyber maturity. It may also give customers and larger organisations greater confidence when engaging smaller suppliers.

The AICD recommends that the CyberSmart standard is designed around the operating environments and constraints of smaller organisations. This includes recognising their reliance on cloud environments, external providers and entry-level digital products, as well as their limited internal IT and cyber security capability. The standard should focus on practical, risk-based outcomes, and avoid unnecessary prescription.

It will also be important to ensure that certification is affordable and proportionate. If the standard is not straightforward and cost-effective, we expect that its uptake within the SMB and NFP environment will be limited given the resource constraints these organisations face. Where CyberSmart certification is promoted through Government procurement or critical infrastructure supply chains, smaller organisations should be provided with appropriate guidance, implementation support and transition periods. Otherwise, the introduction of certification risks creating an additional barrier to participation and widespread uptake by SMBs and NFPs.

[2] See Opportunities for AI in cyber defence | Cyber.gov.au.

Essential Eight

We note that the ASD is currently consulting on updating and modernising the Essential Eight to establish a set of baseline 'Essentials'. The update of this critical resource is vitally important given the evolving threat landscape, including the new and developing threats posed by AI. The update and modernisation of the Essentials should recognise this change, as well as the shift of entities to cloud-based systems over physical networks and storage.

Currently, the Essential Eight is more applicable to entities that have control over their network and services, and have sufficient resourcing to implement the recommended controls. Our understanding from stakeholder feedback is that it has limited relevance as a baseline for cyber maturity for most SMBs and NFPs given their resourcing challenges, and high reliance on external providers.

We encourage the Inquiry to consider how the important work on the Essential Eight update can be aligned and harmonised with CyberSmart, and the development of any SMB standard. It would be counterproductive for a new 'Essentials' framework to exist alongside a separate SMB standard. This outcome would only perpetuate uncertainty, confusion and complexity regarding how SMBs and NFPs can practically implement cyber controls to build resilience.

At a minimum, clear guidance explaining how the Essential Eight/Essentials interacts with CyberSmart, and which framework is appropriate for organisations of different sizes, capabilities and risk profiles will be necessary.

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

Reliance on MSPs, MSSPs and SaaS vendors

As mentioned above, many SMBs and NFPs rely on MSPs, MSSPs and SaaS vendors to supply key digital systems, software and infrastructure. These providers are key to the overall cyber and data resilience of smaller organisations, and in many cases the SMB or NFP has no or highly limited ability to influence the cyber and data settings of these suppliers. Further, access to enhanced cyber settings through these providers that are common at large organisations (e.g. multi-factor authentication (**MFA**) support) can be restricted or not viable as they require paying significant sums for additional features, or more employee licences.

We have received feedback that SMBs and NFPs will often obtain cyber security software and controls (e.g. threat blocking, email hygiene, phishing testing) from an MSP/MSSP as a component of an overall bundled service offering. Stakeholders have noted that in some cases the additional security settings offered by the MSP are not appropriate to the organisation or not effective, and certainly don't respond to the evolving threat landscape. Since SMBs and NFPs are unlikely to have an internal role with responsibility for maintaining cyber controls and keeping pace with evolving requirements, this may not become apparent until there is a cyber security event, or external assurance reveals shortcomings in the security and data protection offering.

Due to the ubiquity of outsourcing digital systems and infrastructure by SMBs and NFPs, we recommend the Inquiry consider whether a focus on standards and certification for those key providers would be more effective than a strategy that solely targets small organisations themselves.

This standard and certification could be designed in a manner that promotes the offering of more comprehensive and effective cyber controls as a part of standard/entry offerings by MSP/MSSPs and SaaS vendors for SMBs and NFPs. Further, it would signal to SMBs and NFPs which providers are meeting baseline security settings, and as such provide a competitive advantage to providers that hold the certification.

This work could be coordinated with the CyberSmart program, the proposed SMB standard and the proposed product-specific and service-specific guidance in the CyberSmart Hub. The objective should be to ensure that expectations placed on smaller organisations are matched by appropriate expectations on the providers that design, operate and secure the systems on which they rely. The Government could promote uptake of the standard through making certification a condition of tendering for certain Government digital contracts.

Separately, in light of the challenges facing SMBs and NFPs in finding and dealing with service providers, the AICD strongly supports the Government's commitment to include product-specific and service-specific guidance in the CyberSmart Hub. If appropriately designed, this guidance should help smaller organisations compare available products and make more informed procurement decisions.

Tiered product offerings

Separately, stakeholders have noted that large SaaS providers tier product offerings such that entry licences or subscriptions typically used by SMBs and small NFPs may only have baseline security offerings. For example, some offerings may not have MFA as a standard component. To access enhanced cyber and data protection settings the organisation needs to purchase a higher priced licence or subscription. With limited staff and financial resources, it is often not feasible for SMBs and NFPs to pay significantly more for SaaS offerings.

We recommend that the Inquiry consider how the Government can prompt SaaS providers to improve the baseline security offerings that are included in entry level licences/subscriptions to SMBs and NFPs. Our recommendation above that a standard and supporting certification directed at MSP/MSSPs and SaaS be considered may also assist in addressing these issues.

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

The AICD's view is that targeted training for the leaders of SMBs and NFPs is a key part of improving the cyber security practices of SMBs and NFPs. We note the current intention in the Horizon 2 Action Plan for the ASD to develop standards that require and guide the training of an organisation's people through the proposed ASD Essential Series for Enterprise IT.

We consider that it would also be appropriate for the ASD to assess the potential for tailored training programs for directors and managers of SMBs and NFPs on cyber and data protection controls and governance. This would extend beyond the existing CyberWardens program or ASD Essential Series for Enterprise IT, and be specifically tailored for managers and directors in particular sectors or industries, such as care or education.

Tailored, industry-specific programs where there is active outreach may get greater traction with key individuals at these organisations than broader education offerings that are general in nature (i.e. CyberWardens).

If the CyberSmart standard is introduced, the training should also be linked to that standard to allow organisations to understand how workforce practices contribute to their overall cyber maturity. This support for SMBs and NFPs in adopting the voluntary CyberSmart standard will be critical to its uptake, given the resource and expertise limitations they face.

We understand that it can be difficult for Government to reach those working at SMBs and NFPs. We recommend that the Inquiry assess the best delivery method for training, and whether this should be provided by bodies with stronger linkages in particular sectors or professions.

We also consider that any training, standards development and new sources of guidance must be supported by a well-resourced awareness raising campaign targeted at SMBs and NFPs that covers key cyber security controls, and where to obtain further information. New sources of training and guidance will have limited uptake and impact if managers, directors and owners of SMBs and NFPs are not aware that they exist.

f) 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

The challenges faced by SMBs and NFPs

Verifiable cyber security maturity has become a prerequisite for participation in Government and large corporate supply chains. Many Government agencies and large organisations now expect suppliers to demonstrate a baseline level of cyber security capability. When these heightened cyber resilience and data-related regulatory requirements and expectations are placed on large companies at the head of a particular supply chain, they can cascade down to subsequent entities.

The AICD has engaged with directors of APRA regulated entities reflecting on the implementation of prudential standards CPS 230 (Operational Risk Management) and CPS 234 (Information Security). Based on this engagement, we understand that the requirements of Government and large organisations to participate in their supply chains include completion of security questionnaires, rigorous MFA settings, incident response plans, staff training, cyber insurance, compliance with recognised frameworks, or implementation of controls aligned with the Essential Eight and international standards (e.g. NIST and ISO 27001).

The cost of implementing these controls can be significant relative to the size of many SMBs and NFPs, so it can be very challenging for them to participate in both the digital supply chains of larger, more highly regulated companies, and Government procurement processes. We appreciate the importance of strong cyber and data requirements through critical supply chains, but it is important that this does not result in highly concentrated markets where only the very largest vendors can provide digital services and infrastructure.

Potential solution – CyberSmart certification

The AICD recognises the potential value of CyberSmart certification in giving procuring organisations, including the Government, greater confidence in smaller suppliers. The Government has indicated that procurement and SOCI Act levers may be used to promote uptake of the CyberSmart standard within government and critical infrastructure supply chains.

Our view is that these mechanisms should be implemented proportionately. Certification costs and technical requirements could create barriers for smaller organisations if they are not accompanied by practical support, reasonable transition periods and recognition of different levels of risk. CyberSmart should assist SMBs and NFPs to compete for contracts, rather than become an additional compliance threshold that excludes otherwise capable suppliers. As identified in our comments above, the standard should be as straightforward as possible, and not require specialist cyber security knowledge to meet. If the standard involves a significant investment of time and resources, we expect its feasibility and uptake may be limited.

Given the potential trade-offs, we encourage the Inquiry to assess how SMBs can be supported in continuing to provide competition, innovation and agile products and services in Government and private sector supply chains.

4. Access to cyber insurance

Cyber insurance is a vital aspect of cyber resilience, not only because it provides financial cover for an incident, but also because the process of obtaining insurance itself can support stronger cyber resilience. It is

common for insurers to require an organisation to demonstrate that specified cyber security controls are in place before offering cover. This can provide business owners, directors and managers with a framework by which to identify weaknesses and improve their organisation's cyber security practices.

However, from engagement with our stakeholders, we understand that the affordability and accessibility of cyber insurance remains a challenge for many SMBs and NFPs. This is supported by research from the Actuaries Institute that only 10 – 25% of SMBs hold a standalone cyber insurance policy.[3]

While it is common that SMB cyber insurance is offered as a bundle with other forms of business insurance, we understand that high premiums, exclusions, coverage limits and minimum control requirements can make suitable cover difficult for smaller organisations to obtain. Cyber insurance should therefore be viewed as one element of a broader risk management approach, rather than as a substitute for investing in cyber resilience. There is also a question as to whether cyber insurance offerings have evolved sufficiently to reflect the emerging risks associated with AI-enabled cyber threats.

On this basis, the principal focus of Government and industry initiatives should remain on helping SMBs and NFPs prevent, prepare for and respond effectively to cyber incidents. While insurance may help mitigate some losses after an incident occurs, it cannot prevent the operational disruption, reputational damage or harm to clients and other stakeholders that may result from an attack.

5. Further regulation

We do not support imposing new regulation on SMBs and NFPs to address cyber security risks across the Australian economy. Given Australia's current productivity challenges, and how regulatory complexity contributes to this problem, our view is that contemplating further cyber-focused legislative change would be counterproductive. Further regulation should only be considered where there is a clear evidence base that the benefits will outweigh the costs, and that the same outcomes cannot be achieved through more targeted and proportionate measures.

There is no silver bullet for building resilience amongst smaller organisations. Rather, a concentrated and well-resourced campaign focused on awareness, education and support may over time make a material difference. Many of the actions and initiatives identified in Horizon 2 will form an important part of this effort. The additional layering of regulation is not the answer.

Removal of the Privacy Act small business exemption

We expect that the Inquiry may receive submissions calling for the removal of the small business exemption as regulatory reform to improve data protection practices. We note that the Privacy Act Review recommended removing the small business exemption, which the Government has agreed to in-principle following further consultation and consideration of the impact of doing so.

Consistent with previous submissions, the AICD does not support the removal of the exemption.[4] While smaller organisations should be supported to strengthen their privacy, data governance and cyber security practices, it has not been demonstrated that the potential benefits of applying the full Privacy Act framework to all small organisations would outweigh the associated costs and regulatory burden. Applying the Privacy Act to all entities regardless of size would ignore the reality of the very limited resources and staffing of SMBs and NFPs, and the often lower privacy risk profile of these organisations.

Many SMBs and NFPs may also be unaware of the Privacy Act obligations or lack the capability to interpret and implement them, creating a significant risk of inadvertent non-compliance. The necessary expenditure on

[3] See Cyber Protection Gap Widens for SMEs page 5.

[4] See our previous submission on the Review of the Privacy Act here AICD-Submission-PAR-Final-Report-March-2023-FINAL.pdf.

legal advice, policies and administrative processes may also divert limited resources away from practical security controls that would more directly reduce the risk of data loss or misuse.

Our strong view is that if the Government considers the exemption is out of date, then it should explore extending Privacy Act obligations to particular industries, activities or business models involving higher privacy risks or the collection of substantial amounts of sensitive personal information. Alternatively, obligations could be applied in a proportionate and graduated manner, with smaller entities exempt from the more prescriptive requirements of the Privacy Act.

The immediate policy priority should be to help SMBs and NFPs improve their privacy and data protection practices through practical guidance, education and capability-building support. This is consistent with the broader approach under the Horizon 2 Action Plan, which recognises that constructive support and accessible tools are critical to improving the cyber resilience of smaller organisations.

6. Next Steps

We hope our submission will be of assistance. If you would like to discuss any aspects further, please contact Elise Plunket, Policy Adviser at eplunket@aicd.com.au or Simon Mitchell, Acting Head of Policy at smitchell@aicd.com.au.

Yours sincerely,

Louise Petschler GAICD
GM, Education & Policy Leadership