dspanz. digital service providers australia new zealand

217 Flinders Street
Adelaide SA 5000

C/- Hudson Gavin Martin
Level 16 45 Queen Street
Auckland 1010

hello@dspanz.org
dspanz.org

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

Via email: cssmbo.reps@aph.gov.au.

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

Dear Committee Secretary,

The Association of Digital Service Providers Australia New Zealand (DSPANZ) welcomes the opportunity to make this submission to the House Select Committee on Cyber Security for Small to Medium Sized Businesses and Organisations' inquiry into the cyber security preparedness of small and medium-sized businesses and organisations.

DSPANZ members provide the software and digital services that underpin many of the day-to-day activities of Australian businesses, including accounting, payroll, superannuation, payments, invoicing, identity, reporting and other business administration processes. Through these products and services, Digital Service Providers (DSPs) support a significant number of Australia's small and medium-sized businesses and organisations.

This gives DSPANZ a distinct perspective for the inquiry. DSPs are responsible for protecting sensitive information held and processed through their software and services and, in doing so, can help expose their small business customers to good security practices as a normal part of using business software. More than half of DSPANZ are also themselves small or medium-sized businesses, including providers required to meet sophisticated security and assurance requirements to interact with government digital services.

DSPANZ supports strong cyber security expectations. Our submission focuses on ensuring those expectations are practical, proportionate and build on the security practices and assurance already operating across the digital economy.

In particular, DSPANZ recommends that the government:

1. **Recognise the role DSPs already play in supporting small business cyber security** and engage the business software sector when developing cyber security policies, standards or requirements that may affect DSPs or their customers.
2. **Prioritise the recognition and reuse of existing security standards and assurance**, including across government digital services, procurement and supply chains, with

additional requirements focused on identifiable additional risks rather than duplicating controls that have already been appropriately assured.

3. **Ensure government cyber security guidance is practical for small businesses**, including through the development of the new Essentials series, with clear pathways for organisations without dedicated cyber security capability to achieve appropriate security outcomes.

DSPANZ considers these measures can support stronger cyber security outcomes while reducing unnecessary complexity for businesses and technology providers. In particular, greater coordination and recognition of existing assurance can allow organisations to focus their resources on improving security rather than repeatedly demonstrating substantially equivalent controls.

DSPANZ welcomes the opportunity to provide further feedback on our submission. Please contact Maggie Leese at maggie@dspanz.org for more information.

About DSPANZ
Digital Service Providers Australia New Zealand is the gateway for the government into the dynamic, world-class business software sector in Australia and Aotearoa New Zealand. Our members range from large, well-established companies to new and nimble innovators working at the cutting edge of business software and app development on both sides of the Tasman.

Yours faithfully,

Chris Denney
Interim CEO & Executive Director
DSPANZ.

1. Introduction

DSPANZ supports the objective of improving the cyber security and resilience of Australia's small and medium-sized businesses and organisations.

DSPs provide software and services that businesses of all sizes use to manage day-to-day activities and compliance processes, including accounting, payroll, payments and regulatory reporting. These platforms can hold and process sensitive information relating to employees, customers, suppliers and financial transactions. Protecting this information requires DSPs to maintain appropriate security practices.

Many DSPANZ members provide products that connect with Australian Taxation Office (ATO) digital services and must meet the ATO's DSP Operational Security Framework (OSF). DSPs may also demonstrate their security posture through internationally recognised standards and assurance frameworks. The results in a more secure supply chain for the clients of DSPs and their customers.

DSPANZ's interest in this inquiry also extends beyond the role our members play in supporting small business customers. More than half of DSPANZ members are themselves small or medium-sized businesses. These members can face the same resource and capability constraints as many small businesses while also being expected to maintain a high security posture because of the services they provide and information they manage.

DSPANZ therefore brings two complementary perspectives to the inquiry:

- **DSPs as providers to small, medium and large businesses:** software providers that protect business information and support good security practices for their customers; and
- **DSps as small and medium-sized businesses:** technology businesses that must themselves navigate increasingly sophisticated cyber security, assurance and supply-chain requirements.

These perspectives inform DSPANZ's view that strong cyber security outcomes should be supported by requirements that are practical, proportionate and recognise existing security practices and assurance.

2. DSPs help support good security practices for small business customers

DSPs occupy an important position in the small business cyber security ecosystem. They have a responsibility to maintain appropriate security practices and protect the information they hold, while the controls associated with their products can also support better security outcomes for their customers.

This should not be interpreted as transferring responsibility for small business cyber security to DSPs. Businesses remain responsible for the risks and activities within their control. Rather, it recognises that the security of the technology services on which a business relies forms part of its broader cyber security environment.

The role of DSPs also provides an important implementation perspective when the government develops cyber security policies, standards and guidance. Requirements relating to authentication, access, information security or other aspects of business technology can have practical implications for software providers and their customers. Early engagement with DSPs can help government understand those implications and ensure requirements achieve their intended security outcomes in practice.

Recommendation 1:
The government should recognise the role DSPs already play in the Australia software supply chain and engage the business software sector when developing cyber security policies, standards or requirements that may affect DSPs or their customers.

3. Recognising and reusing existing cyber security frameworks

DSPANZ supports clear and appropriately high cyber security expectations where appropriate. However, improving cyber security does not necessarily require additional standards or assurance frameworks. The government should place greater emphasis on recognising and reusing existing standards and assurance where they provide confidence in equivalent security outcomes.

This issue is particularly relevant to DSPs. DSPs can operate across multiple government programs, regulated ecosystems and customer supply chains and may be required to demonstrate their security posture against internationally recognised standards, government frameworks, agency-specific requirements and customer assurance processes, such as:

- Australian Information Security Manual
- ISO 27001
- Security and Organization Controls 2 (SOC 2)
- National Institute of Standards and Technology Cybersecurity Framework (NIST CSF).

The ATO's DSP OSF provides an established example. It sets minimum security requirements for DSPs accessing ATO digital services, with requirements and assurance reflecting the risks associated with the services being provided.

DSPANZ supports appropriate security requirements for access to government systems. However, where a DSP has already demonstrated relevant controls through the OSF, an internationally recognised standard or another recognised government framework, that assurance should be reused wherever possible..

There is already a precedent for this approach. The Consumer Data Right (CDR) recognises the OSF within aspects of the Accredited Data Recipient accreditation process, demonstrating the potential for government frameworks to recognise assurance obtained elsewhere rather than treating each regulatory ecosystem as entirely separate.

Greater recognition of existing assurance could also support a more proportionate approach to assessing whether organisations have taken reasonable steps to manage cyber security risks. Where an organisation can demonstrate genuine and documented efforts to meet an appropriate recognised security framework, including relevant independent assurance, this should be capable of contributing to evidence that reasonable security steps have been taken.

DSPANZ recognises that the controls reasonably expected of an organisation will depend on the services it provides, the information it handles and the risks it controls, meaning that this concept should not operate as a blanket safe harbour. However, an organisation that has implemented, maintained and demonstrated appropriate controls should be distinguished from one that has not taken reasonable precautions.

The OSF is again a useful example. It does not establish a general reasonable steps or liability standard. Rather, it demonstrates that the government already has experience establishing a recognised baseline of security controls and accepting structured evidence

that DSPs have implemented them. DSPANZ considers there is merit in extending this principle across government rather than creating new certification schemes where appropriate frameworks and assurance already exist.

The same principle is relevant when DSPs supply services to government agencies and large businesses. Different security questionnaires, contractual requirements, certifications and evidence requests can require a DSP to repeatedly demonstrate substantially the same security posture. For smaller DSPs, the cumulative burden can be significant despite already maintaining sophisticated security controls.

Towards a more coordinated approach

These issues will become increasingly important as government digital services expand and Australia's cyber security and digital regulatory frameworks continue to develop.

The government should consider not only whether individual frameworks are reasonable, but their cumulative impact on organisations required to satisfy several of them. A series of individually reasonable but differently structured requirements can collectively create a significant compliance burden without necessarily improving security outcomes.

In the longer term, DSPANZ considers there is merit in a more coordinated approach to the standards businesses must meet to participate in Australia's digital economy. DSPANZ continues to advocate for a Digital Economy Regulator that could, among other functions, support common baseline security and data standards for interacting with government digital systems. Individual agencies could then apply additional requirements where justified by the specific risks associated with their services.

Recommendation 2:
The government should adopt a coordinated, risk-based approach to cyber security requirements that prioritises the reuse and recognition of existing government and internationally recognised security standards and assurance. Where appropriate, recognised assurance should contribute to demonstrating that an organisation has taken reasonable steps to manage relevant cyber security risks. Additional agency, procurement or supply chain requirements should address identifiable additional risks rather than duplicate controls that have already been appropriately assured.

4. Cyber security guidance must be practical for small and medium-sized businesses

The government has an important role in providing businesses with clear and trusted guidance on appropriate cyber security practices. However, there can be a gap between understanding the importance of cyber security and having the capability to implement recommended practices.

The Essential Eight illustrates this challenge. While it provides an important and widely recognised baseline of cyber security controls, some requirements can be difficult to translate to the operating environment of a sole trader or small business without dedicated information technology or cyber security capability.

The issue is therefore not simply one of awareness. Government guidance should help close the capability gap by providing practice and proportionate pathways for businesses with different levels of technical expertise and resources to achieve appropriate security outcomes.

This is particularly timely as the Australian Signals Directorate considers the evolution of the Essential Eight into a broader Essentials series. DSPANZ considers this transition as an opportunity to ensure Australia's next generation of baseline cyber security guidance reflects the diversity of organisational capability and technology environments across the economy.

Recommendation 3:
In developing government cyber security guidance, including the new Essentials series, the government should ensure that baseline security expectations are practical and accessible for organisations without dedicated cyber security capability and provide clear pathways for small businesses to achieve appropriate security outcomes.

5. Conclusion

DSPANZ supports the objective of strengthening the cyber security and resilience of Australia's small and medium-sized businesses and organisations.

Business software already plays an important role in this environment. DSPs are responsible for protecting their systems and the information they hold or process and, through the security practices associated with their services, can also support good security practices among their small business customers. The government should recognise this role and engage DSPs where cyber security policy, standards or requirements may affect business software or the customers that rely on it.

At the same time, DSPs may themselves be small and medium-sized businesses required to maintain and demonstrate a sophisticated security posture. Their experience highlights the importance of ensuring Australia's cyber security settings are coordinated and proportionate. Where an organisation has already demonstrated appropriate controls through a recognised government framework or international standard, that assurance should be reused wherever it provides confidence in equivalent security outcomes.

This approach can strengthen the incentives for businesses to invest in recognised security practices while directing resources towards substantive security improvements instead of duplicative assurance.

As government cyber security guidance and Australia's broader digital regulatory environment continue to evolve, DSPANZ encourages the government to build on what already works. Practical guidance for small businesses, recognised and reusable security frameworks, and early engagement with the technology providers that support businesses and the digital economy.