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

11 July 2025

Department of Home Affairs
PO Box 25
Belconnen ACT 2616

Via online form.

Re: Voluntary Code of Practice for App Store Operators and App Developers Discussion Paper

To Whom It May Concern:

The Association of Digital Service Providers Australia New Zealand (DSPANZ) welcomes the opportunity to submit this on behalf of our members and the broader business software industry.

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.

DSPANZ broadly supports the introduction of an Australian voluntary Code of Practice for App Store Operators and App Developers.

We recognise that there is an opportunity for the government to leverage existing standards, such as the Security Standard for Add-on Marketplaces (SSAM) developed by DSPANZ, which currently supports industry best practice security between app store operators and app developers in the tax ecosystem.

In our submission, DSPANZ provides the following feedback:

- There is a need to clearly define "business-to-business API developers" within the Code to clarify its intended scope.
- The government should recognise the SSAM under the Code of Practice, given that it provides clear, actionable controls that meet the majority of the UK Government's Code of Practice.
- Following international examples for introducing best practice cybersecurity principles between app store operators and app developers, such as the UK's Code

of Practice, supports interoperability for those operating in multiple jurisdictions and reduces the complexity in meeting differing standards. If the government follows international best practice, it could then consider providing additional guidance, tailored to an Australian audience.

- There is currently a gap between the UK and Australia's data protection and privacy requirements, which will create a challenge for Australia in aligning with the UK's Code of Practice.
- There is a need for Australia to consider establishing a "Digital Economy Regulator" who would have the authority to oversee the development and enforcement of security, certification, data standards and other requirements that organisations must typically meet to leverage digital services provided by the government and participate in the digital economy.

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

Yours faithfully,

Chris Denney,
President & Director
DSPANZ.

About the Security Standard for Add-on Marketplaces

DSPANZ is the custodian of the Security Standard for Add-on Marketplaces (SSAM), which outlines security requirements for Digital Service Providers (DSPs) operating marketplaces or app stores. These add-on marketplaces enable DSP customers to find and integrate add-on apps with their existing software platforms. For example, a business may integrate a point-of-sale system with its accounting software.

DSPs utilise the SSAM to put security requirements in place for the add-on apps that connect with their software and therefore can be listed in their add-on marketplace.

The SSAM was co-created with DSPs, app developers and the Australian Taxation Office (ATO). DSPs that connect to ATO digital services are required to demonstrate that they have the SSAM (or other appropriate security controls) in place if they operate a marketplace under the ATO's DSP Operational Security Framework.

One of the benefits of the SSAM was that it helped streamline the onboarding process for app developers, as it created alignment between the different marketplaces' security requirements, meaning that those who integrated with multiple marketplaces could reuse their evidence.

Discussion Paper Questions

1. Do you think a voluntary Code of Practice will sufficiently uplift security processes in the Australian context for app store operators and developers, and provide clear guidance on actions that can be taken to protect consumers and businesses from cyber attacks?

Introducing an Australian Code of Practice may prove beneficial in standardising the security controls required across different app store operators, thereby reducing the burden on app developers in demonstrating their compliance with relevant requirements.

A Code of Conduct may help uplift security processes for app store operators and developers. However, our experience suggests that a voluntary Code of Practice alone will not achieve the overarching whole-of-economy security outcomes sought by the government. DSPANZ recognises that a supporting legislative framework or ties to existing requirements would create more substantial uplifts.

For example, when introducing the Security Standard for Add-on Marketplaces (SSAM) to establish baseline security requirements across the broader ecosystem, it became a requirement within the ATO's DSP Operational Security Framework. Under this framework, DSPs operating add-on marketplaces must demonstrate that they have requirements in place for the app developers that can ultimately connect to the tax and super ecosystem, with the SSAM recognised as an appropriate baseline standard to follow. While the SSAM itself is not mandatory, DSPs that connect to ATO API's must follow the Operational Security Framework and meet the third party add-on marketplaces requirement.

Given that the SSAM is already in place within the tax and super ecosystem, DSPANZ recommends that it be recognised under the Code of Practice. The SSAM provides clear, actionable controls that meet the majority of the UK Code's principles. Any additional requirements or controls could then be viewed as an addition to the SSAM.

DSPANZ welcomes the opportunity to discuss further the alignment between the SSAM and an Australian Code of Practice.

- **If no, what other approaches would you consider to be more effective?**

2. Is the UK Government's Code of Practice for app store operators and app developers a useful model to consider adopting for enhancing cyber security for apps in the Australian market?
DSPANZ believes that the UK Government's Code of Practice is a valuable model to consider as an Australian Code should follow international best practice security standards and guidance. If an Australian Code deviates from international approaches, there is a risk of creating complexity for app store operators or app developers operating in multiple jurisdictions.

- **What else would you like to see included in the Code of Practice that isn't in the UK Government's Code to make applications more secure?**
  It should be recognised that many app store operators and app developers have a global footprint and operate across multiple jurisdictions. As such, it would be beneficial to provide supplementary information or guidance on how existing security controls from internationally recognised standards, such as ISO 27001, can be used to demonstrate compliance with the Code's principles.

- **How important is it to have exact alignment to the UK Code?**
  Following the same set of overarching principles as the UK will support interoperability. As DSPANZ has suggested above, deviating from the UK's Code or other international approaches can create complexity for providers operating in multiple jurisdictions.

  The government can utilise supplementary guidance to tailor the information for an Australian audience, referencing relevant legislation and privacy requirements as required.

3. Are there challenges for Australian industry in adopting a Code of Practice like the UK Government's?
The UK has a more modern interpretation of data protection and privacy requirements, which has been embedded within its Code of Practice and accompanying guidance.

Australia's data protection and security requirements, in comparison, are falling behind, presenting a significant gap for an Australian Code. While the proposed Tranche 2 changes to the Privacy Act are expected to establish more robust data protection requirements, legislation is yet to be introduced.

DSPANZ has previously provided feedback to Treasury's consultation on the *Proposed New Digital Competition Regime* about the importance of having security requirements in place between app store operators and app developers, and ensuring they are not misinterpreted as barriers to interoperability or anti-competitive conduct.

The introduction of an Australian Code of Practice and adopting it should not be viewed as a barrier to interoperability or anti-competitive.

- **What additional guidance would industry need in the Australian context to meet a Code of Practice?**
  DSPANZ recommends clearly defining "business-to-business API developers" within the Code to clarify its intended scope.

  Based on our understanding of the Code, its purpose and the exclusion of business-to-business API developers, we anticipate that it would not apply to DSPs with add-on marketplaces.

5. What other initiatives should the Australian Government pursue to secure apps for Australian consumers?
DSPANZ recognises there is a proliferation of security requirements, standards and guidance across the Australian economy that organisations must follow (including, ATO DSP Operational Security Framework, SuperStream, Consumer Data Right, and Digital ID).

We encourage the government to consider establishing a "Digital Economy Regulator" as a central source for organisations that leverage Commonwealth Government APIs and participate in digital economy initiatives. A regulator could play a crucial role in overseeing initiatives such as Digital ID and the Consumer Data Right, and provide guidance on security, certification, data standards and other requirements that organisations must typically meet.