dspanz. digital service providers australia new zealand

217 Flinders Street
Adelaide SA 5000

hello@dspanz.org
dspanz.org

24 June 2022

Department of Home Affairs

Via online submission form.

Re: National Data Security Action Plan Discussion Paper

To Whom it May Concern:

Digital Service Providers Australia New Zealand (DSPANZ) welcomes the opportunity to make this submission on behalf of our members and the business software industry. As an association, DSPANZ is interested in helping to reduce the burden our members (commonly known as Digital Service Providers or DSPs) face when meeting their security obligations.

In this submission, we have raised the following issues:

- It can be difficult for organisations to navigate the plethora of different security standards and even more difficult if they have limited security expertise;
- The Government should reflect existing security standards, policies and controls rather than creating anything new;
- Organisations may be required to meet different security standards with conflicting controls which can considerably impact how they operate;
- Where applicable, security standards and guidance should follow a tiered approach to make them more accessible to smaller organisations while also providing a pathway for how they can uplift their security as they mature;
- The Government should focus on how they can directly support smaller organisations rather than relying on large organisations to perform this role as they manage their supply chains;
- The Government has a role to play in creating consistency across different reporting obligations as well as considering how they can share information about security incidents between agencies; and
- The Government should consult with a wide variety of stakeholders and work alongside industry when considering any new concepts or policy for data security.

DSPANZ would appreciate the opportunity to engage further on this submission. For further information, please contact Maggie Leese on maggie@dspanz.org or +61 487 641 702.

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 New Zealand. Our members range from large, well-established companies through to new and nimble innovators who are working at the cutting edge of business software and app development on both sides of the Tasman.

Yours faithfully,

Simon Foster,
President & Director,
DSPANZ

Maggie Leese,
Manager - Communications & Advocacy,
DSPANZ

1. What do you consider are some of the international barriers to data security uplift?
It can be difficult for organisations to navigate the plethora of different security standards and frameworks that exist internationally, and in Australia itself, and make a decision on which standard best suits their needs. While tools and resources are available to assist organisations in understanding the different standards and their controls, they are not necessarily accessible to organisations that have limited security expertise.

2. How can Australian Government guidance best align with international data protection and security frameworks?
The Australian Government's overall approach to data security should be to recognise existing standards and/or controls rather than creating anything new. This would better support the industries and organisations that already comply with international standards and help to create consistency between international standards and any Australian-based frameworks.

Common industry standards, for example the Digital Service Provider Operational Security Framework (DSP OSF) and APRA's CPS 234, should also be recognised across government agencies where it is appropriate. This would allow organisations to provide their existing certification details, or re-use the same evidence, rather than having to start from scratch.

Further, when creating any guidance or putting together a set of controls, the Government should look to reflect the wording used in existing standards rather than creating new definitions or explanations. While additional explanatory information may be added to help with the understanding of the control, keeping the high level details consistent across Australian-based standards will help to avoid any ambiguity around what particular security controls are aiming to achieve.

For example, if a security standard is looking to include certain ISO 27001 controls, the standard should use similar, if not the same, wording as the current ISO 27001 documentation.

Are there any existing frameworks that you think would be applicable to Australia's practices (e.g. the European Union's General Data Protection Regulation)?
From our perspective, the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA) are good examples of policy for the Australian Government to consider. If the Government is considering creating an Australian-based framework, we highly recommend aligning it with the GDPR to make it easier for the Australian organisations that are already meeting these requirements.

We also recommend consulting with a wide variety of stakeholders, including ourselves, and working alongside the industry to better understand potential impacts and to ensure that it is fit for purpose.

5. Does Australia need an explicit approach to data localisation?
While we are not suggesting that Australia needs an explicit approach, following a similar model to Canada may make meeting data localisation requirements easier for our members and other

organisations. The Canadian data localisation laws allow for processing in cloud (or other) environments to happen outside of Canada so long as a copy of the data (such as a backup) resides in Canada.

6. How can data security policy be better harmonised across all jurisdictions?
Following on from our answer to question 2, we believe that recognising existing standards and reflecting the wording used for existing controls will help to harmonise standards and policies.

8. What are the main challenges currently faced by industry as a result of inconsistent data security practices between all levels of Government, including municipal governments?

Conflicting security requirements
Our members are often required to meet different security standards that contain controls that conflict with one another. This means that DSPs have to spend time and money to change their business processes in order to meet the different requirements and continue running their software products and services.

For example, in order to participate in the Consumer Data Right (CDR) and receive CDR-derived data, our accounting software members are required to become accredited and meet the CDR security requirements. However, the security requirements were at a much higher level and therefore conflicted with the security standard they already complied with, the DSP OSF, meaning it would heavily impact how they operate.

While we had success in the CDR space with the ACCC recognising the DSP OSF as an alternative accreditation method, our members continue to face challenges due to conflicting security requirements in other areas. This is why we recommend recognising existing standards and consulting with wider groups of stakeholders before introducing any security standards.

One size fits all approach
Another common challenge, especially for smaller organisations, is that some standards take a "one size fits all" approach which does not consider the levels of risk involved when interacting with different types of datasets. Where applicable, we recommend taking a tiered approach to security standards to make them more accessible to organisations who are only accessing lower risk datasets. It can also provide a pathway for organisations to mature their security posture as they grow or look to interact with higher risk datasets.

11. Does your business appropriately consider data security risks in their supply chains?
A trend that we have noticed across many industries is the Government often relies on larger organisations to influence the security of businesses within their supply chains. While we agree that large organisations have a role to play here, the Government should shift their focus and consider how they can better support smaller organisations to improve their security posture.

For organisations who are interested in implementing a standard for their supply chains, we can recommend the Security Standard for Add-on Marketplaces (SSAM). The SSAM was

co-created between industry and government to set the minimum security requirements for the third party software providers who consume Application Programming Interfaces (APIs) provided by DSPs. It is a mandatory requirement in the DSP OSF for any DSPs that operate app marketplaces or allow API connections to third party software. DSPANZ can provide more details on how these two standards currently work together in the business management software space.

12. Should there be overarching guidance on securing data for businesses of all sizes, or is it important to provide guidance based on a company's size? For example, a ' size' threshold).
Following on from our response to question 8, we recommend taking a tiered approach to any guidance or security standards where it is practicable. Not only would this make the information more accessible to businesses of different sizes, it would help businesses to understand the path they can take to uplift their security as they grow.

Further, the Government should consider the UK's Cyber Essentials scheme and Canada's Baseline Cyber Security Controls for Small and Medium Organisations as good examples of small business guidance.

15. Should there be enhanced accountability mechanisms for government agencies and industry in the event of data breaches? How else could governments and industry improve public trust?
A pain point for many of our members is that they are required to report security incidents to a number of different regulators who can have different guidance on what and when to report. While many organisations will try to do the right thing, it can be confusing especially when also managing an incident. We believe that the Government has an important role to play in creating consistency across the different reporting obligations to help organisations better understand what information should be shared and the timeframe that it should be shared within. They should also consider how they can share information about security incidents between agencies to help reduce the number of regulators that organisations need to report to.