dspanz. digital service providers australia new zealand

217 Flinders Street
Adelaide SA 5000

info@dspanz.asn.au
dspanz.asn.au

27 August 2021

Cyber, Digital and Technology Policy Division
Department of Home Affairs

Via online form.

Re: Strengthening Australia's cyber security regulations and incentives consultation

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. We would like to thank the Department of Home Affairs (Home Affairs) for the opportunity to participate in discussions leading up to this submission.

Overall, we support the intent of this work to lift cyber security across the digital economy. However, we would like to remind Home Affairs that this work should focus on the rationalisation and harmonisation, not proliferation, of existing standards both here and internationally. In summary, our submission covers the following:

- A mandatory approach to large corporate governance should be taken;
- We support the creation of a code, but do not agree with it being created under the Privacy Act;
- Requirements included in the ATO's Digital Service Provider (DSP) Operational Security Framework (OSF) are a great place to start for cost effective and achievable controls;
- We are also supportive of a mandatory approach for responsible disclosure as we do not believe that a voluntary approach will achieve the desired outcomes;
- We believe that a small business health check would help improve the cyber security of small businesses and the UK's Cyber Essentials program is a good model to consider; and
- The role DSPs play in increasing the cyber security of small businesses should be recognised.

DSPANZ would appreciate the opportunity to engage further on this submission. For further information, please contact Maggie Leese on [redacted]

About DSPANZ
Digital Service Providers Australia New Zealand is the gateway for 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,

[redacted]

Simon Foster,
President & Director,
DSPANZ

Formerly ABSIA

5. What is the best approach to strengthening corporate governance of cyber security risk? Why?
We believe that the Australian Prudential Regulatory Authority's (APRA) CPS 234 has been a step in the right direction towards increasing the understanding of cyber security risk amongst directors.

We do not believe that a voluntary standard will be the best way to strengthen corporate governance of cyber security risk. Instead we believe that a mandatory approach for large businesses, similar to the introduction of CPS 234, should be taken. We agree that a mandatory standard should not cover entities already covered by existing regulation.

To better support businesses with costs and the timeframe to implement, we would suggest starting with large businesses who are considered a higher risk. Alternatively, it may only be these higher risk businesses that are required to comply with the governance standard.

6. What cyber security support, if any, should be provided to directors of small and medium companies?
Directors of small and medium companies are likely going to need more support than larger businesses who will often have more resources and larger budgets for cyber security. For smaller companies, Home Affairs could consider developing resources that provide examples of low or no cost tools and materials that could assist them in uplifting their cyber security.

Thought should also be given to how large businesses can influence smaller businesses in their supply chain. We believe that having a standard approach to this may help small and medium companies improve their cyber security and therefore reduce difficulties in procurement processes with larger businesses who will often have conflicting requirements.

8. Would a cyber security code under the Privacy Act be an effective way to promote the uptake of cyber security standards in Australia? If not, what other approach could be taken?

We do not agree with creating a code under the Privacy Act
To achieve an uptake of cyber security standards, this code should be as accessible as possible for all business types across all sectors which is why we believe that a code within the Privacy Act is not the best option. As it currently stands, the three million dollar turnover threshold means that it does not apply to many small businesses. Even though this threshold may change through the review of the Privacy Act, we expect that it will still not be far reaching enough to apply broadly and achieve an adequate uptake.

Instead of the Privacy Act, we would suggest investigating whether a code under the Corporations Act is a suitable option. The Corporations Act can encompass director obligations and also capture the target organisations. If the code were to be under the Corporations Act, then ASIC could assist with regulation.

The code should take a tiered or risk-based approach

Home Affairs should consider a tiered or risk based approach to allow businesses to adopt controls based on their risk profile. This should also be done on a sector by sector basis as risks will differ across different industries. We agree that Home Affairs should consult and work with the different industries to co-develop the codes. This would also allow the different versions to provide sufficient information and resources that are relevant to each industry.

Together with a tiered approach, Home Affairs could consider a longer transition period to give businesses adequate time to comply.

The code should be future focused
It is important that the code is future focused and considers what security standards are needed for the many businesses that will look to digitise their operations in the coming year. There should also be a commitment to regularly review the code in light of changing threat environments.

Providing information to help justify costs
Home Affairs should be cognisant of any costs involved, especially for software providers, as they will need to decide between absorbing these costs or passing them onto their users. In the case where costs are passed on, users may not understand why prices have increased because, more often than not, they will be unable to understand the benefit to them. From our experience with other regulatory changes, information from the regulator is extremely useful for software providers to utilise in educating their users about why changes have been made to their software.

9. What cost effective and achievable technical controls could be included as part of a code under the Privacy Act (including any specific standards)?
We believe that the requirements included in both the ATO's Digital Service Provider (DSP) Operational Security Framework (OSF) and the Security Standard for Add-on Marketplaces (SSAM) are a great place to start. The former is a particularly good example of a tiered approach to a cyber security standard. In the three years that the OSF has been in place, two for the SSAM, we have seen a significant uplift in the whole ecosystem's cyber security and a significant decrease in the amount of compromised tax data.

It is also important to note the indirect effect that the OSF has had on improving SME cyber security as it targets the software suppliers (DSPs) that sell to small businesses such as Xero, MYOB and QuickBooks Online. The implementation of the OSF has meant that controls such as multi-factor authentication (MFA) have been rolled out to millions of users across Australia. The role DSPs play here is quite important and should be recognised by Home Affairs. However, we do not wish to place this compliance burden solely on DSPs.

At the very least, we would like to see the OSF and the SSAM recognised as ways to meet the code. DSPANZ would be pleased to provide insights on the OSF and SSAM should Home Affairs be interested.

While the Essential 8 is important and should be recognised in the code given some software providers will be required to meet it, it needs to be made clear that it is not suited to cloud environments.

10. What technologies, sectors or types of data should be covered by a code under the Privacy to achieve the best cyber security outcomes?
We believe this code should primarily cover digital technologies, especially those consuming and transmitting sensitive data. Home Affairs could look to implement a threshold, like the SSAM, of 1,000 connections.

22. Would voluntary guidance encourage Australian businesses to implement responsible disclosure policies? If not, what alternative approaches should be considered?
Again, we believe that a voluntary approach will not achieve the desired outcomes. We are supportive of a regulatory approach that targets large businesses and that this guidance should be co-designed with industry.

Here, we also encourage Home Affairs to think about ways to increase threat intelligence sharing amongst businesses.

23. Would a cyber security health check program improve Australia's cyber security? If not, what other approach could be taken to improve supply chain management for small businesses?
We believe that a health check program would be an appropriate way to improve the cyber security of small businesses so long as it is about helping these businesses.

On top of a health check program, Home Affairs should identify opportunities to indirectly improve the cyber security of small businesses, a great example being the OSF's effect on small businesses. One option could be to encourage the uptake of cloud software as it is much easier to secure for small businesses when compared to desktop and in-house software. Here, we encourage Home Affairs to consider providing assistance for DSPs to migrate to cloud offerings and uplift their cyber security capability. The end result would be small businesses benefiting from their software being in a more secure environment.

24. Would small businesses benefit commercially from a health check program? How else could we encourage small businesses to participate in a health check program?
For some businesses, we believe they will benefit commercially from such a program. An example being that if a small business lifts their cyber security, it may put them in a better position to meet cyber security requirements for both government and large business procurement processes that they may not have met otherwise.

25. Is there anything else we should consider in the design of a health check program?
We believe that the UK's Cyber Essentials program mentioned in the discussion paper is a good model to consider.