dspanz. digital service providers australia new zealand

217 Flinders Street
Adelaide SA 5000
dspanz.org | hello@dspanz.org

15 April 2023

Department of Home Affairs
PO Box 25
Belconnen ACT 2616

Via online form.

Re: 2023-2030 Australian Cyber Security Strategy Discussion Paper

To Whom It May Concern:

The Association of Digital Service Providers Australia New Zealand (DSPANZ) welcomes the opportunity to provide this submission on behalf of our members and the 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 Sea.

DSPANZ broadly supports developing the 2023-2030 Australian Cyber Security Strategy. We look forward to working alongside the government on its release and associated outcomes.

In summary, this submission raises the following:

- Digital Service Providers (DSPs) view digital identity solutions and a contemporary set of business registers as vital pieces of technology to facilitate secure interactions and meet their cybersecurity requirements;
- Creating consistency between cybersecurity frameworks and obligations by recognising existing security standards and controls will assist in reducing the burden and streamline the process when meeting their security obligations;
- Payroll, superannuation, eInvoicing, and API sets provided by the ATO, ASIC and Fair Work Commission should be critical infrastructure;
- The government should consider rationalising the bodies and legislation involved in cyber security;
- The government should lead by example in demonstrating and delivering cybersecurity best practice;
- The government needs to be more high profile when communicating how they can assist businesses and individuals when dealing with cyber incidents;

- There are several successful examples of government and industry working together to uplift cyber resilience while ensuring that functioning and interoperable ecosystems still exist;
- There is an opportunity for government and industry to work together to improve the Essential Eight; and
- The government should continue to regularly consult with industry to ensure the Strategy meets the government's and industry's expectations.

DSPANZ welcomes the opportunity to provide further feedback on our submission. Please contact Maggie Leese for more information.

Yours faithfully,

Matthew Prouse,
President & Director
DSPANZ.

1. What ideas would you like to see included in the Strategy to make Australia the most cyber secure nation in the world by 2030?

With more business processes moving into natural business systems, specifically business software, DSPs will need to rely on secure and scalable digital solutions. The following two pieces of technology are vital to facilitating secure interactions and assisting DSPs with meeting their cybersecurity requirements:

1. Low or no-cost public digital identity solutions that DSPs can leverage to verify individuals and businesses; and
2. A contemporary set of business registers that will provide higher integrity data for DSPs and natural business processes to rely on.

2. What legislative or regulatory reforms should Government pursue to: enhance cyber resilience across the digital economy?

We want to move away from previous approaches to small business security focused on large businesses securing their supply chains. This approach misses many small businesses that do not interact with large organisations. In addition, it is burdensome for small businesses that must meet varying security requirements each time they provide services to large organisations.

a. **What is the appropriate mechanism for reforms to improve mandatory operational cyber security standards across the economy (e.g. legislation, regulation, or further regulatory guidance)?**

   DSPANZ believes that creating consistency across cyber security standards and aligning them with recognised international standards (such as ISO, SOC2, and NIST) would assist in improving cyber security standards across the economy. We have expanded on this in our answer to point "e" below.

b. **Is further reform to the *Security of Critical Infrastructure Act* required? Should this extend beyond the existing definitions of 'critical assets' so that customer data and 'systems' are included in this definition?**

   We would like to see the following recognised under the *Security of Critical Infrastructure Act* as they are critical infrastructure for DSPs and business processes:

   - Payroll and superannuation data and systems
   - eInvoicing
   - API sets provided by the ATO, ASIC and Fair Work Commission

   Taking payroll as an example, COVID-19 drove a quick shift to digital payment capabilities meaning the community is less resilient to payment and payroll disruptions. The recent collapse of Silicon Valley Bank and resulting impacts on payroll service providers demonstrated that payroll should be critical infrastructure.

   While we advocate these inclusions, we want to avoid placing another set of security requirements on DSPs. We recommend recognising existing security standards and frameworks such as ISO 27001, SOC2, NIST and the ATO's Operational Security Framework, including the associated Security Standard for Add-on Marketplaces (SSAM).

c. **Should the obligations of company directors specifically address cyber security risks and consequences?**
Existing director obligations cover risks such as cyber security. For smaller businesses, many of which are sole operators, this would require an individual to voluntarily take on a cyber security role on top of several other functions they are responsible for within the business.

d. **Should Australia consider a Cyber Security Act, and what should this include?**
The government should consider rationalising the bodies and legislation involved in cyber security. For example, several government bodies currently handle security or publish security information in Australia. This includes but is not limited to:
    - Australian Cyber Security Centre
    - Australian Prudential Regulation Authority
    - Australian Signals Directorate
    - Australian Taxation Office
    - Department of Defence
    - Department of Home Affairs
    - Office of the Australian Information Commissioner
    - Services Australia

    While each body is responsible for different aspects of security, there is often overlap in the organisations they cover and the information they provide. It is confusing for businesses, particularly small businesses, to understand their obligations and where they can obtain assistance.

    From this perspective, introducing a Cyber Security Act may create further confusion for businesses unless it involves rationalising the varying bodies, responsibilities and standards involved.

    Recent cyber incidents, like the ESXiArgs ransomware campaign, highlight that ensuring organisations have the cybersecurity basics right will yield the most significant benefit. While there is a tendency to focus on the "new", many exploits or cyber incidents still occur due to unpatched software or lax password management.

e. **How should Government seek to monitor the regulatory burden on businesses as a result of legal obligations to cyber security, and are there opportunities to streamline existing regulatory frameworks?**
One of the biggest challenges facing the business software industry is the proliferation of security standards and requirements across Australia (see above). Many DSPs are required to support multiple, often conflicting, standards to provide their software products and services. There is often little commonality between security standards and questionnaires that ultimately achieve the same security outcome. If a DSP operates internationally, this increases the number of standards they must comply with and the complexity they navigate.

    There is an opportunity to create consistency between cybersecurity frameworks and obligations by recognising or leveraging existing security standards and controls.

We want to avoid the creation of new standards and terminology for existing security controls or security outcomes. This consistency would help streamline the process and reduce the burden on DSPs and other organisations when meeting security obligations.

DSPANZ wants to be involved in consultation on simplifying and streamlining existing regulatory frameworks and reducing reporting obligations.

f. **Should the Government prohibit the payment of ransoms and extortion demands by cyber criminals by:**
(a) victims of cyber crime; and/or
(b) insurers? If so, under what circumstances?
    - **What impact would a strict prohibition of payment of ransoms and extortion demands by cyber criminals have on victims of cybercrime, companies and insurers?**

We anticipate that this would negatively impact many organisations that do not have a high level of cyber security expertise and would view paying a ransom or extortion demand as the quickest way to get their business up and running again.

We understand that many cyber insurance policies do not currently cover ransomware.

g. **Should Government clarify its position with respect to payment or non-payment of ransoms by companies, and the circumstances in which this may constitute a breach of Australian law?**
The government should clarify their position on paying ransoms and educate organisations about what to do during a ransomware attack.

3. How can Australia, working with our neighbours, build our regional cyber resilience and better respond to cyber incidents?
Following our response to "3. e" above, DSPs would appreciate a consistent approach to security frameworks across the APAC region.

6. How can Commonwealth Government departments and agencies better demonstrate and deliver cyber security best practice and serve as a model for other entities?
We believe the government needs to lead by example, which includes improving its cyber security maturity. The ACSC's Commonwealth Cyber Security Posture in 2022 report demonstrates that significant improvements are required to uplift the government's maturity.

The government should regulate the cyber insurance market and standardise what cyber insurance policies include. Cyber insurance should be treated similarly to major catastrophe insurance, where the risk is pooled and standard yet comprehensive terms are applied.

7. What can government do to improve information sharing with industry on cyber threats?

DSPANZ has long advocated for the government to improve their threat intelligence sharing with industry. In particular, DSPs would like the ATO to share common threats they are seeing to help identify and mitigate potential risks.

While the ACSC's Partnership Program is important in threat intelligence sharing, it is currently unavailable to non-Australian entities, even though they have an established presence in Australia. As an ACSC Partner, DSPANZ cannot share materials and events with some of our members, for example, our New Zealand members. We want to see changes to the eligibility of the Program to allow greater participation and enable Partners to share this valuable information with their communities.

8. During a cyber incident, would an explicit obligation of confidentiality upon the Australian Signals Directorate (ASD) Australian Cyber Security Centre (ACSC) improve engagement with organisations that experience a cyber incident so as to allow information to be shared between the organisation and ASD/ACSC without the concern that this will be shared with regulators?
We believe an obligation of confidentiality would assist in improving engagement with organisations reporting cyber incidents. For organisations, including DSPs, that must report to other bodies outside of the ASD and ACSC, we anticipate that this would not have the intended impact.

9. Would expanding the existing regime for notification of cyber security incidents (e.g. to require mandatory reporting of ransomware or extortion demands) improve the public understanding of the nature and scale of ransomware and extortion as a cybercrime type?
DSPANZ has previously provided feedback to Home Affairs about ransomware incident reporting. We supported the objective of the obligation but raised concerns about adding a new reporting obligation for Australian businesses without a clear corresponding benefit. While this would give the government better data on ransomware incidents, the government must commit to sharing detailed information back to the industry to provide a benefit.

12. What more can Government do to support Australia's cyber security workforce through education, immigration, and accreditation?
It is currently difficult for smaller DSPs to find ISO 27001 auditors catering to small businesses in Australia. We need to attract more small business-specific security auditors to help small businesses meaningfully uplift their security and assist in meeting relevant security standards.

13. How should the government respond to major cyber incidents (beyond existing law enforcement and operational responses) to protect Australians?
The role of the government and the actions they can take during an incident is not well-understood by individuals and the industry. The government needs to be more high profile when communicating how they can assist businesses and individuals when dealing with cyber threats and intrusions.

For DSPs, being able to provide clear information to their users on what actions the government can take to protect them during a security incident would be beneficial. This

information could improve confidence when users report incidents and allow them to understand how information may be shared or used.

a. **Should government consider a single reporting portal for all cyber incidents, harmonising existing requirements to report separately to multiple regulators?**
While a single reporting portal could help streamline the security incident reporting process, we anticipate several challenges with this approach - namely, the specific details different regulators require and the ability to share reports between regulators.

DSPs reporting to the ATO under the Operational Security Framework must report specific product, device and TFN information to assist the ATO with their response. We expect that this level of detail would not be required in a reporting portal and that DSPs would be required to report this information to the ATO using a separate reporting mechanism.

As mentioned, DSPANZ wants to participate in consultation on streamlining reporting obligations.

14. What would an effective post-incident review and consequence management model with industry involve?
The Gateway Network Governance Body (GNGB), which oversees the Superannuation Transaction Network (STN), conducts an incident response exercise each year simulating an attack on the network. The outcomes and recommendations from the exercise are shared with GNGB members to help build the resilience of the superannuation ecosystem. We recognise this exercise as a working model of government and industry collaborating on incident reviews and management.

15. How can government and industry work to improve cyber security best practice knowledge and behaviours, and support victims of cybercrime?
We would like to acknowledge the collaboration between the ATO and DSPs to uplift security across our ecosystem with the introduction of the Operational Security Framework and the SSAM. This collaboration is a successful example of government and industry working together to improve cybersecurity outcomes while ensuring that a functioning and interoperable ecosystem still exists. The Operational Security Framework and SSAM also introduced best practice controls such as Multi-Factor Authentication (MFA) for many Australian businesses.

DSPANZ is particularly interested in working with the ACSC and ASD to improve the Essential Eight standard to make it easier for small businesses to understand and implement. A further opportunity exists to develop a version of the Essential Eight that applies to non-Microsoft environments.

The government should educate certain industries and organisations on why they may be a target for cybercriminals. This education would involve giving organisations the tools to determine whether they collect commonly targeted datasets and how to protect such data.

a. **What assistance do small businesses need from government to manage their cyber security risks to keep their data and their customers' data safe?**
   We would like to see any data breach or security incident penalties applying to small businesses be proportional to their size. Any security incident will likely be an extinction-level event for a small business. It is doubtful that many Australian small businesses will have sufficient funds or resources to recover from the financial, brand or reputational damage caused by a security incident. We note that increasing penalties, such as under the Privacy Act, will only create further economic costs for small business owners as they exit their businesses.

16. What opportunities are available for government to enhance Australia's cyber security technologies ecosystem and support the uptake of cyber security services and technologies in Australia?
As mentioned, GNGB's annual security exercise is a notable example of continuously improving the ecosystem's security and establishing a baseline for cyber resilience that members must comply with.

18. Are there opportunities for government to better use procurement as a lever to support and encourage the Australian cyber security ecosystem and ensure that there is a viable path to market for Australian cyber security firms?
We should avoid creating bespoke cybersecurity requirements and questionnaires within procurement processes. Instead, the government should require organisations to meet internationally recognised cyber security standards, for example, and encourage other large businesses to do the same.

We recognise that few cyber security firms support smaller businesses in Australia.

19. How should the Strategy evolve to address the cyber security of emerging technologies and promote security by design in new technologies?
Building on our answer to question 15, the journey the ATO and DSPs have been on since the introduction of the Operational Security Framework and SSAM means that any new software or applications within this ecosystem will meet a high security standard. This approach has led to clear and consistent requirements and focuses on risk mitigation rather than control compliance.

The Strategy should recognise the importance of government and industry collaboration in developing workable security requirements and ensuring functioning ecosystems.

21. What evaluation measures would support ongoing public transparency and input regarding the implementation of the Strategy?
The government should continue to regularly consult with industry to ensure the Strategy meets the government's and industry's expectations. We welcome future consultation opportunities.