Submission in response to:
Strengthening Australia’s cyber security regulations and incentives

This submission is made in response to the call for views detailed in the document “Strengthening Australia’s cyber security regulations and incentives”, published by the Department of Home Affairs.

About Ignite Systems

Ignite Systems is a Victorian based Managed Security Services Provider (MSSP) providing managed cyber security services exclusively to small businesses. Since 2004 (initially trading as TechOnline) we have provided cyber security services to many hundreds of small businesses across Victoria and interstate.

As a result of our extensive experience in servicing small businesses with managed cyber security services designed specifically for this market, we have unique insight into the challenges associated with improving the cyber security posture of this cohort.

I have personally been involved in providing Cyber Security Awareness Training to 1,000’s of people, almost entirely people involved in small business. For many years I have provided advice, including producing cyber security guidelines, to both the Law Institute of Victoria and the Australian Institute of Conveyancers (Victorian Branch). I have also authored a number of articles on cyber security, including several published by the Australian Strategic Policy Institute.

Ian Bloomfield
Managing Director
Ignite Systems Pty Ltd
[redacted]

Note that the headings in this document reference the sections in the discussion paper.

2. Why should government take action?

Seeking your views

1 What are the factors preventing the adoption of cyber security best practice in Australia?

Based on our experience, these are some of the factors preventing Australian small businesses (1 to 20 employees) from adopting cyber security best practice.

- **Make cyber security an imperative** - Lack of a coherent program of information/education specifically targeting small businesses that makes it clear that a business with anything less than a 'recommended' minimum standard of cyber security is putting its clients at risk, and that not acting to address the situation could potentially be considered negligent.
- **Set a clear minimum standard** - There has not been a set of cyber measures very clearly stated as the 'recommended minimum' all small businesses should adopt.
- **Cyber security is not DIY** - To date, almost all of the cyber security information emanating from the Australian government targeting small business, either implicitly or explicitly assumes a do-it-yourself approach. There is no clear message about the important role of outsourced cyber security services and that using these services should be considered the preferred approach.
- **Allow informed decisions about risk** - There is a need to inform and educate the general public that doing business with a small business that does not satisfy a 'recommended' minimum standard of cyber security is putting them at risk.
- **Focus on high-risk small businesses** - Small businesses comprise a very wide variety of business types ranging from a sole trader plumber to a medical clinic comprising several general practitioners and staff. The cyber risks differ significantly depending on the type and amount of information a business processes and retains. The various types of small business should be categorised according to their 'information risk profile' they represent i.e. the type and quantity of information they process and retain. Actions to improve the cyber security posture of small businesses should be targeted at the business categories with a high-risk profile. Engagement with these prioritised small business categories should leverage the various peak bodies, such as the Council of Small Business Organisations Australia, Small Business Association of Australia, Royal Australian College of General Practitioners, Law Council of Australia, the Australian Institute of Conveyancers, and the Institute of Public Accountants.

Seeking your views

2 Do negative externalities and information asymmetries create a need for Government action on cyber security? Why or why not?

NO FEEDBACK PROVIDED

3. The current regulatory framework

Seeking your views

3 What are the strengths and limitations of Australia’s current regulatory framework for cyber security?

NO FEEDBACK PROVIDED

Seeking your views

4 How could Australia’s current regulatory environment evolve to improve clarity, coverage and enforcement of cyber security requirements?

The current regulatory framework in relation to cyber security requirements, does not adequately address the unique attributes of small businesses:

- **Make small business a priority** - As a group, the single biggest employer, employing over 40% of the business workforce, contributes over 32% of Australia’s total GDP, and over 20% of total tax revenue from companies[1].
- **Prioritise high-risk small business categories** - The various types of small businesses are extremely diverse, and the cyber security risk profile is equally extremely wide ranging. The cyber security regulatory framework needs to take account of this by segmenting small businesses based on their information risk profile. This risk profile should be based on the type and quantity of information a business processes and retains as a priority e.g. businesses involved in home renovations have a low risk profile compared to legal service providers. The cyber security regulatory regime should then be prioritised to address those categories with a higher risk profile.
- **Link privacy to cyber security** - There needs to be a more coherent connection between the privacy regulatory regime and the cyber security regulatory regime for small businesses. These two regulatory environments are currently completely disconnected, making it confusing for small businesses to understand their obligations regarding privacy versus cyber security.

4. Governance standards for large businesses

NO FEEDBACK PROVIDED

[1] Small Business Counts report (2020): www.asbfeo.gov.au/resources/small-business-counts

5. Minimum standards for personal information

Seeking your views

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?

A better approach is to make use of existing cyber security standards, such as the ACSC Essential Eight[2], and the Top 4 of the ACSC Strategies to Mitigate Cyber Security Incidents[3] (referenced as ‘Core Requirements’ in the Protective Security Policy Framework, Policy 10: Safeguarding information from cyber threats[4]). These existing cyber security standards sit outside of the Privacy Act and they should be referenced by the Privacy Act as either recommended minimum standards or as mandated requirements. This addresses these significant issues that currently exist with the Privacy Act:

- The Office of the Australian Information Commissioner is not an appropriate body to determine cyber security standards.
- There is no clear link between cyber security as referenced in the Privacy Act, and the cyber security standards referenced by other areas of the Australian Government e.g. ACSC Essential Eight.
- Cyber security standards need to be regularly reviewed and revised (as with the latest revision of the ACSC Essential Eight Maturity Model), and the Office of the Australian Information Commissioner is not appropriately structured or resourced to carry out this function.

Seeking your views

9 What cost effective and achievable technical controls could be included as part of a code under the Privacy Act (including any specific standards)?

As recommended in response to Seeking your views 8 above, the Privacy Act should reference existing cyber security standards that sit outside of the Privacy Act, and be consistent with what is referenced by other areas of the Australian Government. The ACSC Essential Eight is extensively referenced across many areas of the Australian Government are a proven set of strategies to mitigate against cyber intrusion. As has been the case with the Australian Government Protective Security Policy Framework (PSPF), the Top 4 of the ACSC Strategies to Mitigate Cyber Security Incidents should be a mandated minimum requirement.

Seeking your views

10 What technologies, sectors or types of data should be covered by a code under the Privacy Act to achieve the best cyber security outcomes?

As recommended in response to Seeking your views 4 above, the cyber security regulatory framework should take account of the differing levels of cyber security risk associated with different categories of small business. Currently there are only two small business categories (with revenues less than $3 million) considered as APP entities under the Privacy Act - health service providers, and contracted service providers for a Commonwealth contract.

[2] Essential Eight Explained: www.cyber.gov.au/sites/default/files/2019-03/Essential_Eight_Explained.pdf

[3] Strategies to Mitigate Cyber Security Incidents: www.cyber.gov.au/acsc/view-all-content/publications/strategies-mitigate-cyber-security-incidents

[4] Policy 10: Safeguarding information from cyber threats: www.protectivesecurity.gov.au/system/files/2021-06/pspf-policy-10-safeguarding-information-from-cyber-threats.pdf

The scope of APP entities should take account of the volume of Personal Information and Sensitive Information that the various categories of small businesses process and retain. The scope should be expanded to include the high-risk small business categories, such as legal practitioners, conveyancers, accountants, and insurance brokers. From our experience with these small business categories, they all process and retain large volumes of Personal Information and Sensitive Information. In our assessment, the cyber security posture with these small business categories is universally poor.

In our view, expanding the scope of APP entities to include all high-risk small business categories, in conjunction with a requirement to comply with a minimum cyber security code, would substantially reduce the overall risk these businesses currently represent to the Australian public.

6. Standards for smart devices

NO FEEDBACK PROVIDED

7. Labelling for smart devices

NO FEEDBACK PROVIDED

8. Responsible disclosure policies

NO FEEDBACK PROVIDED

9. Health checks for small businesses

Seeking your views

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 have no doubt that a cyber security health check program would improve the cyber security of Australia's small businesses, but to be effective it needs to include the following elements:

- In addition to a self-assessment, there needs to be higher level external assessment by a certified assessor - similar to the UK Cyber Essentials and Cyber Essentials Plus Certification.
- A comprehensive program of information/education specifically targeting small businesses, that clearly articulates the following:
  - The 'check measures' are a 'recommended' minimum standard of cyber security.
  - Businesses not acting to achieve this 'recommended' minimum standard are putting their clients at risk.
  - Implementing business cyber security is not DIY, and outsourced cyber security services play an important role. Using outsourced cyber security services should be considered the preferred approach to achieve the 'recommended' minimum standard.
- As a follow-on from the introduction of the health check program, conduct a comprehensive public media program. This should target those areas of the general public likely to receive products or services from small businesses operating in the segments that the health check program has been promoted to. The key message should be, that doing business with a small business that does not declare their status regarding the 'check measures' is potentially putting them at risk.

Seeking your views

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?

It is not a practical objective for all small businesses to benefit commercially from a health check program. As recommended in response to Seeking your views 4 above, small businesses should be segmented based on their information risk profile. The program should be focussed on those small businesses that have a high information risk profile e.g. health service providers, legal practitioners, conveyancers, accountants, and insurance brokers.

The following arrangements have the potential to ensure a commercial benefit for those organisations that participate in the health check program:

- A comprehensive public media campaign with a clear message that considering the 'check measures' status of a small business should be part of the selection process before doing business with them. The takeaway should be that engaging a small business that does not satisfy the 'check measures', or has not declared their status regarding the 'check measures' could put peoples Personal Information at risk. An effective campaign will drive business to those small businesses that are able to promote their achievement in satisfying the 'check measures'.
- Some form of tax incentive for those organisations that use the services of a certified third party to confirm they have satisfied all of the 'check measures'.

Seeking your views

25 Is there anything else we should consider in the design of a health check program?

The following are important considerations in designing a health check program:

- The check program needs to be based on the existing ACSC "Strategies to Mitigate Cyber Security Incidents"[5]. This is important for several reasons:
    - For some time now these ACSC strategies have been promoted by the Australian Government as the referenceable standard for business when considering the mitigation of cyber security risk. For small businesses in particular, it is important for the health check program to leverage the existing messaging, and any move away from this will only muddy the water.
    - As the paramount cyber security body, the ACSC must be seen as the primary sponsor of the check program, in much the same way as the NCSC is the primary sponsor of the Cyber Essentials program in the UK. To be consistent with this, the cyber security mitigation strategies that have been developed and promoted by the ACSC for many years must form part of any health check program.
- A progressive roll-out of the check program is essential to ensure that the necessary effort can be appropriately focussed, and to allow scope to fine tune the program. Consideration should be given to starting the program with those small businesses involved in the federal and state government supply chains. One of the main benefits of this approach is that these supply chains are already well structured, allowing for easier incorporation of the health check program, and importantly making it possible to get better and more timely feedback so the program can be tweaked as necessary. REFER ADDITIONAL NOTE BELOW
- As highlighted in the ACSC 2020 Health Sector Snapshot[6], "The health sector remains a valuable and vulnerable target for malicious cyber activity". The majority of NDIA health services providers are small businesses with representation across all states and territories, so this would be an ideal supply chain area to focus on for the initial rollout of the health check program.

NOTE: On page 50 under the heading "Implementation issues and risks" there is the following statement.

> ***"The Australian Government's procurement rules already encourage strong cyber security, and we think there would be challenges to implementing additional requirements that only apply to small businesses."***

This statement does not stand up to scrutiny. The Commonwealth Procurement Rules (14 December 2020)[7] clause 8.3 only states the following:

> "Relevant entities ***should consider*** and manage their procurement security risk, including in relation to cyber security risk, in accordance with the Australian Government's Protective Security Policy Framework."

Supply chains have been identified as significantly vulnerable, so there is clear justification for all businesses involved in Commonwealth procurement to have stronger cyber security.

[5] Strategies to Mitigate Cyber Security Incidents: www.cyber.gov.au/acsc/view-all-content/publications/strategies-mitigate-cyber-security-incidents

[6] 2020 Health Sector Snapshot: www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/2020-health-sector-snapshot

[7] Commonwealth Procurement Rules: www.finance.gov.au/government/procurement/commonwealth-procurement-rules