COUNCIL OF SMALL BUSINESS ORGANISATIONS AUSTRALIA

Secretariat: [redacted]
Our advocacy team is based in Canberra
Email: info@cosboa.org.au
www.cosboa.org.au

27 August 2021

Melissa Nguyen
Policy Officer — Digital Economy Resilience and Market Reform
Technology Policy Branch | Cyber, Digital and Technology Policy Division
Department of Home Affairs
techpolicy@homeaffairs.gov.au.
Via online portal.

Dear Melissa,

Thank you for the opportunity to comment on the *Australian Government discussion paper, Strengthening Australia's cyber security regulations and incentives* (The Paper) and the time your team has spent discussing the ideas within the paper with COSBOA.

COSBOA's role promoting and representing the interests of small business means that our response to your wide-ranging paper will address its impacts on our member's interests. Many of the issues raised, address structural matters for which we do not claim expertise. What we are acutely aware of, are the impacts on small business, when the market is left to decide. We welcome the Government's inquiry, the ideas around regulation and the opportunity to contribute from the perspective of small business.

Yours sincerely,

Castaly Haddon

COSBOA Policy

On behalf of

Alexi Boyd
Interim Chief Executive Officer

Council of Small Business Organisations Australia (COSBOA)

ABOUT COSBOA The Council of Small Business Organisations Australia (COSBOA) is the national peak body representing the interests of small business. Collectively, COSBOA's members represent an estimated 1.3 million of the 2.5 million small and family businesses that operate in Australia.

COSBOA is the big voice for small businesses people since 1977. As a collaboration of peak organisations, we promote small business with independent, tenacious advocacy to powerful decision-makers to get a better deal for millions of small businesses people and a better economy for all Australian people.

Small and medium sized enterprises (SMEs) are major contributors to the Australian economy. SMEs employ 68% of Australia's workforce. In GDP terms SMEs together contribute 56% of value added. For this reason, small and medium businesses will be the key partners with Government in re-building the Australian economy.

Discussion Questions

Chapter 2: Why should government take action?

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

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

For small business, time, resources, money, and knowledge contribute to slow cyber security adoption. There's also a matter of who to trust and poorly established pathways and processes for adoption. There's also a critical fight for survival, against a backdrop of natural disasters and pandemics, cybersecurity is a long way down the to do list. There's also misplaced trust, small business people assume the products they use will have built in protections. There's poor availability and little clarity around standards for cybersecurity on almost every IT device used by small businesses.

Many small businesses are unaware of the size of the problem, and don't think it will happen to them. Until it does. Small business needs to be able to report cybersecurity crimes that encourages reporting, anonymity may be required to remove stigma and shame as small business people, understandably, are reluctant to report incidents. Having accurate data about the impacts specifically on small business would help motivate businesses to act.

Insurance for cybersecurity is an increasingly difficult issue, for small businesses, not mentioned in the paper. This is a classic example of negative externality. Even if a business wants to purchase protection, business decisions by others removes this option.

COSBOA would agree that negative externalities and information asymmetries create a need for Government action and regulation on cyber security. The market does not always deliver the best outcome. Such regulation though, must be well considered. In section 10 we discuss some of the complexities and unintended consequences for small business in current regulatory reforms.

COSBOA agrees that small business requires assurances that the devices they buy have cybersecurity by design and there's clear ways to ascertain the level of protection and that such protections are well communicated and understood. There's considerable work required in this space.

Chapter 3: The current regulatory framework

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

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

Many small businesses are very similar to individual consumers in their vulnerabilities. They might be sole traders, partnerships, micro businesses, tradies, contractors or single consultants. Yet they must comply with the same laws that govern big businesses, (except for businesses with revenue under $3M, where the Privacy Act does not apply.) Australia's regulatory system for cyber security is too complicated for most small businesses to comprehend. A plethora of Government Departments and legislative instruments are involved. For small business, we need the four C's that good regulation delivers, certainty, consistency, clarity and the ability to compete. Regulation for small business must be

practical and realistic and achievable. For many small business, their experience is the end result of a long line of regulatory impacts, for which they had no control or input.

The regulatory framework should consider small business needs and provide practical rules that assist them adopt cybersecurity protections.

Chapter 4: Governance standards for large businesses

5 What is the best approach to strengthening corporate governance of cyber security risk? Why?

6 What cyber security support, if any, should be provided to directors of small and medium companies?

7 Are additional education and awareness raising initiatives for senior business leaders required? What should this look like?

While this section deals with the Corporations Act and large businesses, small Pty Ltd business are also governed by the same Act. The other problem with this section is the definition of a small business. At present there's at least 13 different small business definitions used within the Federal Government.

The problem of defining a small/medium and large business is complicated. We deal with support for small businesses adopting cybersecurity in section 9.

Chapter 5: Minimum standards for personal information

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?

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

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?

NA

Chapter 6: Standards for smart devices

11 What is the best approach to strengthening the cyber security of smart devices in Australia? Why?

12 Would ESTI EN 303 645 be an appropriate international standard for Australia to adopt for as a standard for smart devices?

a. If yes, should only the top 3 requirements be mandated, or is a higher standard of security appropriate?

b. If not, what standard should be considered?

13 [For online marketplaces] Would you be willing to voluntarily remove smart products from your marketplace that do not comply with a security standard?

14 What would the costs of a mandatory standard for smart devices be for consumers, manufacturers, retailers, wholesalers and online marketplaces? Are they different from the international data presented in this paper?

15 Is a standard for smart devices likely to have unintended consequences on the Australian market? Are they different from the international data presented in this paper?

Many small businesses have similar vulnerabilities to consumers. Standards that created a built in level of security would be welcomed.

Chapter 7: Labelling for smart devices

16 What is the best approach to encouraging consumers to purchase secure smart devices? Why?

17 Would a combination of labelling and standards for smart devices be a practical and effective approach? Why or why not?

18 Is there likely to be sufficient industry uptake of a voluntary label for smart devices? Why or why not? a. If so, which existing labelling scheme should Australia seek to follow?

19 Would a security expiry date label be most appropriate for a mandatory labelling scheme for smart devices? Why or why not?

20 Should a mandatory labelling scheme cover mobile phones, as well as other smart devices? Why or why not?

21 Would it be beneficial for manufacturers to label smart devices both digitally and physically? Why or why not?

COSBOA is unable to comment on the perspective of device manufacturers, however from a small business perspective of using the devices, as customers buying IOT devices and being impacted by lax cybersecurity functions, COSBOA agrees with implementing a voluntary star or ranking labelling scheme along the lines of Option1 with higher rankings requiring independent verification and based on already agreed international standards with local co-design for the implementation.

Small business people are often very similar in profile as consumers, especially sole traders and micro businesses. Such a labelling scheme would make it easier for these consumers to understand the risks and mitigate them, at the point of purchase.

COSBOA's view is that this would be a first step in a transition to mandating a star or ranking labelling scheme. This would encourage the industry to engage in the co-design of the voluntary scheme, as it is setting the framework for the mandatory scheme. This sets a clear policy direction, while giving industry the time to transition and engage. Such a scheme should cover all devices, including mobile phones, on the IOT and across all advertising spaces, both on physical packaging and digital marketplaces, amongst the normal list of specifications given for such products.

Chapter 8: Responsible disclosure policies

22 Would voluntary guidance encourage Australian businesses to implement responsible disclosure policies? If not, what alternative approaches should be considered?

COSBOA's view is that Option 1 would be a sensible first step, being voluntary approach to increasing Responsible disclosure. In addition, a transition to making hardware, firmware, and software manufacturers liable for damages from incidents that exploit known and unpatched vulnerabilities would protect small business people.

Chapter 9: Health checks for small 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?

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?

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

The concept of small businesses being more aware and proactive of their cybersecurity is obviously beneficial. The practicality of HOW to get time, resource and knowledge poor small business people to add another task, expense, and expertise to their long to do list requires understanding of the small business world.

As everyone benefits from small business being cyber secure, then it's a shared responsibility1 and should not be moved down the line to the business with the least capacity to enact. This is moving cost to small business to protect supply chain for larger businesses. Consideration of how it could work is required.

While we agree doing a health check is low cost, what happens next is not. Ticking boxes does not guarantee any real action. The UK program makes expert assistance available post health check and we agree this is required for such a program to have any impact.

For small business and for the Government, being aware of the cybersecurity deficiencies isn't the aim, It's getting businesses to take action.

The marketing and financial benefits of having a cybersecurity health check trust mark are unknown and so would not be an incentive for small business people.

Not only does the health check create more to do, but it raises the issue of who to turn to, who to trust, what is good value for money, what's essential and what's not? Small business people have so many problems navigating this, they avoid it. The Health Check on it's own, has a high probability of failing to achieve the stated outcomes.

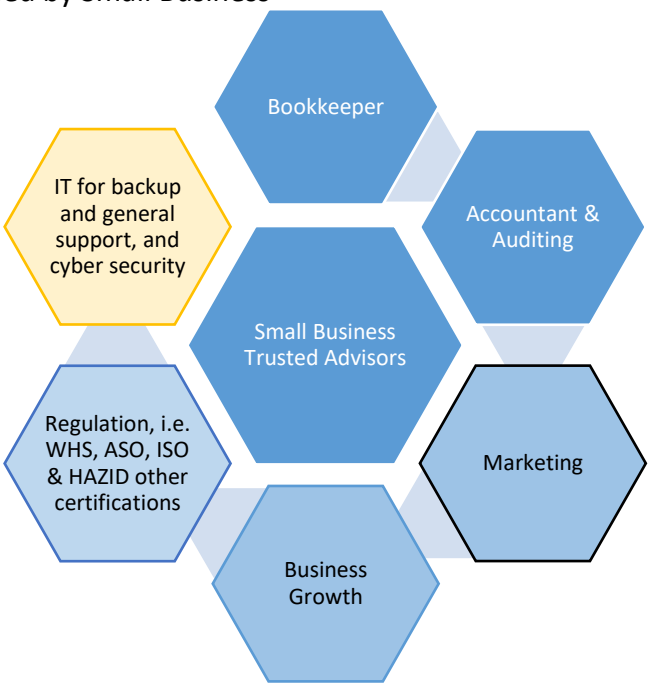
Initially, we need to provide support to small business to navigate the pathway from being aware to acting. This is missing from the proposal. COSBOA sees a program that included the following elements would address the Government and small business concerns;

1. A Health Check for small businesses, that has basic standards agreed by industry participants, is common and consistent and available everywhere…and updated by some central authority annually.
2. A Trust Mark for IT Suppliers, who provide expertise to convert the health check into a regular program of activities to ensure cyber security. In effect, a light touch certification for IT suppliers built around desired codes and standards, that allows small business to engage with experts with some assurances and certainty.
3. In the beginning, to establish the program, incentives, like a cash discount for business under a certain threshold. And Cybersecure verification to small business who use certified trust marked IT suppliers, therefore delivering consistency of standards, and increasing small business uptake. The Trust Mark is moved from the small business to the supplier. Once the program is established, incentives could be reduced or removed.
4. Awareness and communication of the program and it's benefits through industry associations, who are on the ground working with small businesses would be ideal.

Creating a pathway to trusted advisers is well known pathway for small business…

[1] Pg 3 Executive Summary *Strengthening Australia's cyber security regulations and incentives (The Paper)*

Trusted Advisors used by Small Business



Standards for IT advisors are not governed with the same rigour as an established profession like accounting and book keeping. Such standards would assist small businesses take up cybersecurity in the same way they use trusted advisors for book keeping and accounting, both are similar, highly technical and specialised skilled professionals.

It would be incumbent on the IT Suppliers to update their skills, and certification annually, and do annual reviews for their clients, therefore ensuring the up-to-date application of standards in a rapidly evolving threat environment.

Chapter 10: Clear legal remedies for consumers

26 What issues have arisen to demonstrate any gaps in the Australian Consumer Law in terms of its application to digital products and cyber security risk?

27 Are the reforms already being considered to protect consumers online through the Privacy Act 1988 and the Australian Consumer Law sufficient for cyber security? What other action should the Government consider, if any?

The review of the Privacy Act 1988 and its intersection with Consumer Data Law legislation currently being enacted, is creating issues for small business. We have attached our submission to that consultation process. In summary, there appears to COSBOA a tension between the right of consumers to protect their data, and the need of small businesses to share their data. This tension must be resolved in a practical way. What can be lost in the conversation is the consideration that small businesses are also consumers of data and should be considered as having the same rights to utilise and share their data to improve aspects of their business such as business efficiency. Business people are not captured by the privacy rules in the same ways as individuals. This allows businesses to function and fulfil a plethora of obligations, most of which are driven by Government regulatory requirements. They rely on agile software solutions to do this. There are over 1000 individual software companies in Australia providing numerous bespoke business software solutions. Their efficiency is dependent on the smooth transfer of critical business data. Careful consideration

is needed where the CDR and Privacy Act rules intersect with these relationships. There's layers of relationships that have been established over many years that make the transfer of Consumer protections to small business fraught with difficulties.

Most of these software providers are small businesses themselves that will not be able to comply with the complexity of the rules. We have worked with our members, including the Digital Solution Providers Australia and New Zealand (DSPANZ).

We note the Government is also considering whether the small business exception from the Privacy Act should be retained, and how any changes would interact with a direct right of action. COSBOA would welcome further involvement in these deliberations.

Chapter 11: Other issues

28 What other policies should we consider to set clear minimum cyber security expectations, increase transparency and disclosure, and protect the rights consumers

Attachment Consumer Data Submission

Secretariat: PO Box 576
Crows Nest NSW 1585
(02) 9431 8646

Our advocacy team is based in Canberra

Email: info@cosboa.org.au
www.cosboa.org.au

6 August 2021

Australian Government Treasury
Via emails, [redacted]

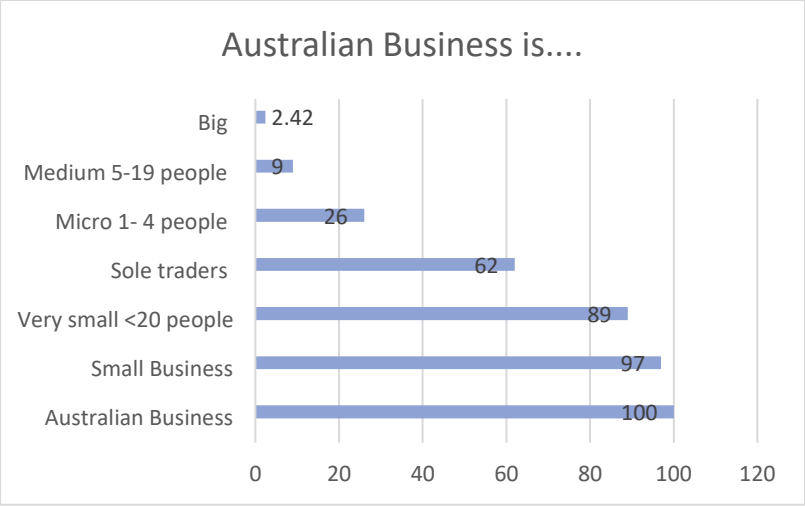
Consumer Data Rights Rules amendments (version3)

Dear CDR Team,

Thank you for the opportunity to comment on the Consumer Data Rights Rules amendments (version3) and your consideration of our thoughts past the deadlines set. Our members brought this consultation to our attention only days before the deadline. With COVID-19 lockdowns consuming much of COSBOA's time, energy and attention, our ability to resource an in-depth analysis of comprehensive legislation is limited. We acknowledge the significant body of work that has been conducted since 2017 and the most recent work to create changes that recognise some of the difficulties this legislation creates for small businesses.

Given the circumstances, we request further time and consultation with your team to offer the small business perspective. In an effort to progress we would make the following initial points;

Small businesses can be very small, one to four people in a business account for a very large proportion of all small businesses.



Statistics from the Australian Small Business and Family Enterprise Ombudsman 2021.

Many of these small businesses are very similar to individual consumers in their vulnerabilities. Yet they must comply with the same laws that govern big businesses. They rely on agile software solutions to do this, and we've included examples attached to this letter. There are over 1000 individual software companies in Australia providing numerous bespoke business software solutions. Their efficiency is dependent on the smooth transfer of critical business data. Careful consideration is needed where the CDR rules intersect with these relationships.

Most of these software providers are small businesses themselves that will not be able to comply with the complexity of the CDR rules. We have worked with our members, including the Digital Solution Providers Australia and New Zealand (DSPANZ), to understand the CDR rules. We understand they have also made submissions raising the details of the difficulties being created.

There appears to COSBOA a tension between the right of consumers to protect their data, and the need of small businesses to share their data. This tension must be resolved in a practical way. What can be lost in the conversation is the consideration that small businesses are also consumers of data and should be considered as having the same rights to utilise and share their data to improve aspects of their business such as business efficiency. Business people are not captured by the privacy rules in the same ways as individuals. This allows businesses to function and fulfil a plethora of obligations, most of which are driven by Government regulatory requirements.

The removal, limitation, or regulation of the data sharing, that has been utilised for many years now in the small business sector will have consequences that we don't believe are well understood by the Department, at this point of the policy development. Our reading of the proposed rules is they are complex and far reaching. Advice from our members is that although the intentions of the legislation is sound, overly complex implementation and the impacts on both the small business software companies and their clients, needs further consideration.

The place of trusted advisors, the regulation and definition of who they are and what they do in these amendments (version 3), do not reflect the current, real life small business experience. Through software small business people have for years successfully shared their own financial data with advisors which they trust because they choose to do so to improve their business. This has occurred through a robust system of compliance checks for advisors as professionals; engagement letters, software protections and relationships built over time. They need to retain that capability of sharing data for efficiencies and to meet government regulations and on occasion those tey reach out to can change. For example, the recent JobKeeper payments relied on the use of single touch payroll and businesses submitting tax information according on time. Those that had failed were excluded from the subsidies. Many small businesses use software to meet their record keeping obligations. In cases of urgency, it is not only financial advisors, but others who assist the small business owner and it must be up to them to determine who they can trust with this information.

Small Business people have for many years managed who accesses their data, what level of access is granted and for how long, in partnership with DSP's. We're curious to know what problem the CDR rules are solving for small business people?

We would welcome further consultation in detail, as time allows and as required to meet your deadlines as this important work is developed.

Yours sincerely,

Alexi Boyd
Interim Chief Executive Officer

Council of Small Business Organisations Australia (COSBOA)

ABOUT COSBOA The Council of Small Business Organisations Australia (COSBOA) is the national peak body representing the interests of small business. Collectively, COSBOA's members represent an estimated 1.3 million of the 2.5 million small and family businesses that operate in Australia.

COSBOA is the big voice for small businesses people since 1977. As a collaboration of peak organisations, we promote small business with independent, tenacious advocacy to powerful decision-makers to get a better deal for millions of small businesses people and a better economy for all Australian people.

Small and medium sized enterprises (SMEs) are major contributors to the Australian economy. SMEs employ 68% of Australia's workforce. In GDP terms SMEs together contribute 56% of value added. For this reason, small and medium businesses will be the key partners with Government in re-building the Australian economy.

Examples of Small Business sharing their own data.

There are numerous examples of sectors of the small business economy who rely heavily on the visibility of bank feed data in their financial software not only for reconciling in real time but also for secondary software which is crucial to running their business.

For example, a naturopath owns a small business clinic that employs 10 people and sees dozens of clients each day. They utilise Cliniko for their practice management software; for customer relationships & queries, marketing, booking appointments, sending invoices, closing invoices etc. The business owner relies heavily on the software and literally could not function if the system suddenly became unavailable. Cliniko has a proportion of its functionality linked to the bank feed data in the small business owner's primary financial software – Xero. Xero collects the bank feed and Cliniko has open API visibility over this bank feed data for closing invoices as well as other utilities. A proportion of the software which the small business owner utilises to run their business is rendered useless and would mean, for a start, double handling of invoices.

There are numerous examples where switching off bank feeds in the primary accounting platform would mean limiting the functionality of the secondary software. In the case of Dext (formally known as ReceiptBank) which has over 55,000 small business users in APAC (the vast majority in Australia) where it relies on visibility of the bank feed data for its core functionality of closing receipts. NextMinute, an emerging project management software platform designed for tradies has 150 clients for whom the platform on which they run their business would be useless.

These are just three examples; there are hundreds of software platforms which small businesses use for client account management, project management and running many facets of their business. Restricting the access of secondary software in any way to this data would mean a huge backwards step in terms of digitisation and efficiency for these businesses.