Xero Submission

Strengthening Australia's cyber security regulations and incentives

September 2021

External(np)

3 September 2021

Technology Policy Branch
Department of Home Affairs
4 National Circuit
Barton ACT 2600

SUBMITTED VIA WEBFORM

To Whom It May Concern

STRENGTHENING AUSTRALIA'S CYBER SECURITY REGULATIONS AND INCENTIVES SUBMISSION

In a world lived increasingly online, we all have a role to play to ensure people can participate fully, and with confidence. An important component to enable participation is ensuring appropriate protection in every online interaction. Achieving appropriate protection will be an evolving and ongoing task, ideally in a manner that is not disruptive to either providers or consumers of online services.

As the accounting software choice for over 1.1 million small businesses in Australia, cyber security is an issue that permeates every facet of Xero's business. Xero is a Digital Service Provider (**DSP**) that integrates with the Australian Taxation Office via API, communicating sensitive information on behalf of our customers to simplify compliance. Xero is required to meet strict security criteria to gain and maintain DSP status as outlined in the DSP Operational Framework. Our small business customers can interact with Xero and our ecosystem with the confidence they are secure. However, small business cyber security is not so uniform, creating a range of risks internal and external to the business, including supply chain risk.

Xero welcomes the opportunity to provide this initial feedback on the 'Strengthening Australia's Cyber Security Regulations and Incentives consultation paper (**paper)**. We have made three suggestions which we believe will build increased cyber resilience among Australia's small business sector, with a specific focus on supply chain risk. Xero will be in contact with you to offer any additional assistance to the process going forward.

Your sincerely

[redacted]

Angus Capel
Head of GX (Government Experience), Australia

[redacted]

Charlotte Wylie
GM Security Engineering

1. Introduction

1.1. Xero supports the paper's consideration to support small businesses to minimise supply chain risk - we have a very strongly aligned set of shared values with the government and the small business community in this important area. Xero's short submission focuses entirely on the cyber health check for small business proposal, making three suggestions to increase the utility of this initiative including partnering with experts to assess qualification for trust mark (proposal 1), a supporting education and awareness campaign (proposal 2) and requirement to register on the e-invoicing network as part of the qualification process (proposal 3).

1.2. We would also like to acknowledge the broader security boosting initiatives proposed in the current paper and how they support Australia's Cyber Security Strategy 2020. We specifically note with interest the ideas raised around greater use of cyber security standards to set new clear minimum expectations around corporate governance such as through a principles-based voluntary standard for larger businesses.

2. Question 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?

2.1. Xero supports the paper's consideration to support small businesses to minimise supply chain risk. We also acknowledge broader security boosting initiatives and support outlined in Australia's Cyber Security Strategy 2020. As part of a suite of cyber initiatives, Xero supports the 'cyber health checks for small businesses' proposal.

2.2. In principle, helping businesses to understand adequate cyber hygiene via a trusted source (the Government), to display publicly is a positive initiative. Xero supports the ability to display the trust mark, to demonstrate to other businesses (and consumers) the business adheres to a reasonable standard of cyber hygiene. However, the voluntary nature of the health check may warrant further consideration.

2.3. If a small business can gain the trust mark via a tick-box exercise, before displaying it prominently on its business communications, the weight of the initiative may be undermined. This could be deliberately disregarding requirements to gain access to the trust mark or honestly believing measures are in place to meet trust mark requirements when they are not. Either way, it is reasonable to expect businesses and consumers will consider themselves protected when dealing with a business displaying the trust mark, when in reality there is limited assurance.

2.4. While not eliminating the chance of this occurrence, Xero suggests the trust mark be still a voluntary exercise, but one that should be completed in partnership with an appropriate expert (**Proposal 1**). We note the significant SME investment in Australia's Cyber Security Strategy 2020, and suggest consideration of whether the ACSC and Connect and Partner program would be appropriate channels to partner with small businesses to assess practices

against the trust mark criteria, along with providing other services and advice. Additional accountability would increase the likelihood businesses earn the trust mark appropriately, in turn increasing confidence in the symbol.

2.5. Xero suggests the initiative be complemented with an education and awareness campaign (**Proposal 2**). The Cyber Security Strategy 2020 measures to support small businesses should be assessed for success, in particular the $4.9 million public awareness campaign for consumers and small businesses. In Xero's experience, small business understanding of cyber threats and mitigating actions is inconsistent. Xero suggests increasing the cyber hygiene baseline by educating the most at risk will increase the overall security of the business ecosystem. This can be as simple as good password and login practice, and understanding where vulnerabilities lie, most likely email. Catering to those with the lowest knowledge - the source of the highest risk - should be the focus of such campaigns.

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

3.1. Xero suggests registration on the e-invoicing network should be a criteria item to attain the trust mark (**Proposal 3**).

3.2. According to the ACCC's latest Targeting Scams Report, businesses lost over $128m to business email compromise scams. False billing scams were the most commonly reported scam and accounted for over 75 percent of losses to business. E-invoicing has the potential to vastly minimise business losses by reducing business email compromise scams.

3.3. E-invoicing is the transfer of invoice information directly from the invoice sender's software to the invoice receiver's software, regardless of provider, via the Peppol network. The system includes a validation of the invoice sender, and ensuring bank account details match records on file before information is transmitted.

3.4. E-invoicing will replace businesses emailing invoices, removing the prospects of scammers sending false invoices via email. Singapore has been successful in driving e-invoice network registration and use by making registration a requirement of receiving government support. This model is one that Xero supports the Australian Government emulating and Xero stands ready to share its experiences and learnings in this area if such would be of any assistance to the current review team or more widely.

4. Conclusion

4.1. Xero would like to thank the Government for the opportunity to provide input on the paper. We agree with the direction of thinking from the Government that small businesses require a specific approach to manage the risks of low cyber awareness. We would welcome the chance to discuss our submission further, should this be of interest.

Xero Submission

Strengthening Australia's cyber security regulations and incentives

September 2021