



Australian Government



Australian
**Small Business and
Family Enterprise**
Ombudsman

1 November 2019

Department of Home Affairs
Cyber Security Strategy & Governance Team
Australian Cyber Security Centre
14 Brindabella Cct
Canberra, ACT 2611

via email: cybersecuritystrategy@homeaffairs.gov.au

Dear Sir/Madam

Australia's 2020 Cyber Security Strategy

We welcome the development of Australia's 2020 Cyber Security Strategy (the strategy) as it creates a significant opportunity to increase small and family business (SFB) engagement while building cyber security capability amongst participants. However, caution is needed when transferring the responsibility for cyber security identification of risk to end-users like SFBs as they are generally not well placed to identify or thwart malicious cyber activity.

Our recommendations are as follows:

1. *Strategy should specifically consider small business*

The strategy should specifically address small and family business (SFB) support throughout, to assist in creating opportunity for SFBs to better engage with industry. One example is to create an annual report that transparently demonstrates initiatives to involve SFBs so they are not priced out of supply chains. The report should convert to a commitment to the development of a sovereign capability that is sustainable and contributes to growth in skilled workers and SFBs. Additionally, the report should provide a clarity over the cyber security landscape at the time and assist in better information sharing between government and industry.

2. *Procurement is a great lever*

Reviews of government procurement at each of Commonwealth, State and Territory and local levels could be conducted to identify greater opportunity to engage SFBs in the supply chain and raise awareness of cyber risks and safety. The goal being supporting an increase of overall levels of cyber security capabilities across sectors.

3. *Government to have a role in risk to assist small business that lacks resources*

Government should have a continuing role in cyber risk management to ensure that all business, regardless of size, have capability to build cyber security capability, and particularly at the small end. A one-size fits all method of transferring risk to industry has the potential for small and family businesses to be exposed to excessive risk and cost.

T 1300 650 460 E info@asbfeo.gov.au

www.asbfeo.gov.au

Office of the Australian Small Business and Family Enterprise Ombudsman
GPO Box 1791, Canberra City ACT 2601

Thank you for the opportunity to comment. If you would like to discuss this matter further, please contact [REDACTED]

Yours sincerely

[REDACTED]

Kate Carnell AO
Australian Small Business and Family Enterprise Ombudsman