

29 July 2020

Cyber Security NSW, Department of Customer Service
Level 23, McKell Building, 2-24 Rawson Place
Sydney NSW 2000

To whom it may concern

ABSIA's Response to 2020 NSW Cyber Security Strategy

The Australian Business Software Industry Association (ABSIA) welcomes the opportunity to make this submission on behalf of the business software industry.

ABSIA is a not-for-profit association representing the Australian business software industry. It strives to be at the forefront of decision making in the industry and to influence policies to create the best outcomes for the business community. ABSIA's Directors and members participate on more than 15 government and international working groups and committees.

While ABSIA is nationally focused, almost 50% of our members operate in NSW and four of our eight Board Directors are located in NSW.

The business software industry advocates that the NSW Cyber Security Strategy should:

- Provide software SMEs with both practical and tangible assistance targeted to improve their cyber resilience, for example, the GoSecure scheme in Singapore;
- Improve threat intelligence sharing especially among SMEs;
- Increase consultation with associations, such as ABSIA, to better understand any potential impacts within their specific industries and to increase the adoption of cyber secure practices. Industry partnerships should also be improved and SME participation increased; and
- Leverage existing security frameworks such as ABSIA's Security Standard for Add-on Marketplaces (SSAM) that is mandated for the ATO's digital supply chain.

ABSIA would appreciate the opportunity to engage directly on these suggestions. For further information, please contact Ian Gibson, ABSIA Director, on ian.gibson@absia.asn.au. Additional information is also provided as **Attachment A - Introductory Table**.

Yours faithfully,

Chris Howard
President & Director, Australian Business Software Industry Association

ABSIA's Response to 2020 NSW Cyber Security Strategy

Provide software SMEs with both practical and tangible assistance

Singapore has a grant program to increase the cyber capability of ICT SMEs called [GoSecure](#). We recommend that the NSW Government examines this as an example to follow. Increasing the capability of ICT SMEs will improve the cyber resilience of the broader SME marketplace.

One point to note is that these programs often exclude international businesses that are Australian-based. There are several ABSIA members, not to mention other businesses, that would be interested in such grants but have the potential to be excluded as they are not wholly Australian owned and/or operated.

We also encourage the NSW Government to support existing small software businesses, and not just start-ups and scale-ups.

Improve threat intelligence sharing

The NSW Government could improve and grow threat intelligence sharing. Whether this is internally within the government itself or within the industry, more threat intelligence sharing would be beneficial to understand common threats, weaknesses and other vulnerabilities that should be addressed by the government and industry.

Improve industry partnerships and increase consultation and SME participation

The NSW Government has a critical role in increasing overall cyber security resilience in NSW. As the NSW Government is currently focusing on digitalising, it should be a role model for the industry and public. Cyber security resilience however will not automatically happen when the NSW Government sets policy, procedures and standards, it will require the cooperation of the industry and public.

To ensure this cooperation, there needs to be collaborative partnerships between the government and industry. At the moment, ABSIA has found there is a perception that there are no successful government-industry partnership models. The ATO's Digital Partnership Office (DPO) is an example of such a partnership and one the NSW Government should consider. The DPO is one reason the ATO has such strong industry engagement with the tax, payroll, superannuation, e-invoicing and related software providers. This collaborative partnership has resulted in two important pieces of security work, the Digital Service Provider (DSP) Operational Framework¹ and the Security Standard for Add-on Marketplaces (SSAM)².

Our recommendation is that the NSW Government creates their own version of a "digital partnership office", to foster collaborative partnerships and share information between the NSW Government and industry.

¹ DSP Operational Framework outlines the minimum security standards that DSPs need to adhere to when connecting to the ATO via API. More information [can be found here](#).

² The SSAM provides a minimum security standard for add-on software applications that connect to DSPs via API. This is a recommended standard and implemented in part or full by DSPs. More information [can be found here](#).

ABSIA's Response to 2020 NSW Cyber Security Strategy

We also recommend the NSW Government seeks engagement with specialist ICT industry associations like ABSIA and the [Medical Software Industry Association \(MSIA\)](#).

The NSW Government's approach should promote SME participation. More recently, the Australian Small Business and Family Enterprise Ombudsman, Kate Carnell, called for at least 30% SME participation in government procurement and the establishment of a small business procurement panel to manage government contracts worth less than \$10 million³. SMEs are often overlooked in procurement as well as in the conversations surrounding cyber security. SMEs should be encouraged to participate in further consultations to ensure their voices and needs are heard. The NSW Government has the opportunity to be a leader here.

3

<https://www.canberratimes.com.au/story/6855541/act-should-have-lowest-payroll-tax-to-boost-small-business-kate-carnell/?cs=14225>

ABSIA's Response to 2020 NSW Cyber Security Strategy

Attachment A - Introduction Table

ABSIA is an industry association, so we have answered these questions to reflect our members.

Information	Respondent details - Please provide range if exact number not available
Name of Organisation	Australian Business Software Industry Association (ABSIA)
Contact for further queries	Ian Gibson ian.gibson@absia.asn.au
Number of association members (total)	84
Number of employees in cyber security roles	100+ (employed by ABSIA member organisations in cyber security roles)
Annual turnover of organisation (\$, total)	\$500,000+ (estimate of our members annual turnover)
Annual turnover of organisation (\$, cyber security activities)	-
Do you export cyber security services/products?	Yes - some members do
If so, what proportion of cyber security turnover is attributable to exports?	-
Specific area of cyber security expertise	Please select those which apply: <ul style="list-style-type: none"> ● Identification, authentication and access controls ● Implementing secure systems

ABSIA's Response to 2020 NSW Cyber Security Strategy

Which industry sectors are your main customers?

The majority of ABSIA members are payroll and accounting software developers. However, overall our members provide services to the selected sectors.

Please select those which apply:

- **Financial Services**
- **Health and social care**
- **Education**
- **Energy**
- **Telecommunications**
- **Transport and logistics**
- **Retail**
- **Resources**
- **Advanced Manufacturing**
- **Agriculture**