Stakeholder feedback form

Leveraging insights yielded from extensive industry consultation, the NSW Department of Industry has developed a Government-led and industry-driven Strategy to grow the NSW cyber security industry. The component parts of this Strategy, detailed below, collectively seek to harness the existing skills and capabilities within NSW to develop and position NSW as a globally competitive market for cyber security. The table below outlines the strategies underpinning the focus areas to enable the growth of the Cyber Security Industry in NSW. The Department of Industry welcomes your feedback.

Intro / Background

Overall the NSW Cyber Security Strategy is a positive step for the state. It outlines an array of useful information and is well articulated. The AIIA commend NSW Government in establishing a draft Cyber Security Strategy to ensure a market environment that allows the sector to flourish. The strategy is a comprehensive look at the landscape and our aim through providing this member feedback is to help NSW Government establish a strategy that takes into consideration the issues most pressing to industry and the sector in general.

We applaud NSW Government for addressing issues that AIIA members have raised previously, we are encouraged that these are highlighted and included in the Strategy: including the need to grow local start-ups and SMEs as well as building on cyber security education through higher education programs, TAFEs, primary and secondary schooling and the inherent problems with procurement and how accreditation should be approached. The AIIA believe over the long term, this Strategy and the initiatives outlined within compliment work at the federal level to grow Australia's cyber ecosystem.

We have reached out to our members regarding this draft and they have reverted with feedback which are outlined below.

Issues raised by members

1. Alignment with federal strategy and state initiatives.
2. Investment strategy and growth criteria.
3. Thresholds and accreditation
4. Education and SME accreditation
5. A) Procurement, time and cost constraints for SMEs
6. B) Lifting the profile of local SMEs
7. Risk conversation
8. Minimum standards
9. Secondments and exchanges

General Comments

If you would like to comment on specific draft initiatives, please use the table below.

Table 1: Strategies underpinning the NSW Cyber Security Industry Development Strategy

Focus Area	Strategy	Comment
1. Small and Medium Enterprise Supporting the growth of this market segment offers the largest potential opportunity for growth of the cyber security industry in NSW, as SMEs are currently underrepresented in the NSW cyber security industry compared to other countries. The objective of these strategies is to support the development and success of small and medium enterprises (SMEs), including start-ups.	**A. Review Government procurement policies for digital services**	A) Procurement has improved but requires further work, if the SME cyber security market is to prosper and local firms to compete against larger providers then procurement needs to progress. Members advise procurement takes too long and engagement is expensive, this is a barrier for local firms to develop access with Government. The AIIA is supportive of an open marketplace the Federal Government are developing and we are encouraged that NSW Government aims to work closely with Federal Government on this rather than 'reinventing the wheel'. We see the simplification of procurement as beneficial to the whole market. In the short term, we recognise there are persisting issues with panels, however we note that if local firms can access Government procurement through panels that are not overly burdensome the payoff would be twofold: firstly, it signals to the market that government is serious in supporting local industry, which may result in more entrants and start-ups willing to start a business. Secondly it allows those companies to start building their profiles with the backing by state government. The messaging to the market would be substantial. B) Australia is host to significant local talent in the SME space. Government can play a more active role in promoting this talent and lifting the profile of these local firms. The AIIA strongly supports the NSW Government coordinating the NSW Cyber Security Industry Showcase as it will aid in lifting the profile of local firms and will make it easier for SMEs to buy with government and will streamline purchasing.

Focus Area	Strategy	Comment
		Member consensus is that industry leads over government in growing the cyber security capability and attached services. If Government want to grow the local industry, they need to lead by example and invest in local companies that build products and provide services in the cyber security space.
	B. SME accreditation	The AIIA is generally supportive of Government requesting thresholds be met through accreditation. Feedback from members, note that where accreditation for SMEs is required, that it does not inadvertently create more barriers than the opportunities it provides. Close consultation with industry on these requirements is strongly recommended. The AIIA supports voluntary minimum standards, industry codes and guidelines supported by easily accessible toolkits.
	C. Provide access to mentoring support	The AIIA strongly advocate for and support secondments and exchanges, this will boost cyber security skills in the short term and help the skills shortage Australia is currently experiencing in the sector. The AIIA would be happy to work with government and coordinate industry members.
	D. Increased early-stage product development support for SMEs	Government should invest in growth capacity through university and TAFE faculties, with more faculty positions and hubs focusing on specific cyber initiatives. This has been done in the US and UK and has resulted in a number of technical universities spinning out companies through research hubs. As an example: Stanford, MIT and the University of Georgia have done this in the States. St Andrews in Scotland, Cambridge and Oxford in the UK. The Chinese are starting to follow suit with Tsinghua University and Shanghai Jiao Tong, this will only continue. UTS, RMIT, QUT as local examples, have the resources to do this in Australia. The AIIA recommend government incentivise partnerships between growth centres and industry. With more flexible IP requirements placed on the projects. In a number of instances, the partnering institution claimed ownership over the product developed with an industry member, serving as a disincentive for the growth centre in encouraging collaboration. Separately, a member advised that due to the rent requirements placed on the industry member, the project became unviable and was ultimately pursued outside the university. Separately,

Focus Area	Strategy	Comment
2. Invest Stakeholder engagement indicated that the current Australian (and NSW) investment environment presents a barrier to attracting inbound investment and in some instances, acts as a driver for local companies relocating to other jurisdictions (e.g. Silicon Valley in California, United States of America (USA). As such, the objective of these strategies is to support SMEs, particularly those at the start-up stage, and in the process of securing early stage venture capital for the development and commercialisation of technical products through an improved operating environment will reduce the incentive to relocate out of NSW. Additionally, investors may require support in developing digital literacy to make targeted investments in the industry.	**A. Increase cyber security research profile**	The AIIA supports the need for a mature conversation on the risks associated with the cyber security industry in general. Rick can never be fully eliminated and should be managed proportionately. AIIA recommends developing a risk framework as part of this strategy in close consultation with industry and other relevant stakeholders. Initiatives to legislative around cyber security including mandatory standards should be developed based on the agreed risk framework. This process should not be rushed as it underpins the entire economy.
	B. Build capacity of organisations to access available resources to support commercialisation efforts and become export 'ready'	Last year an industry supply chain tool for ICT SMEs was developed as part of the Commonwealth Government Entrepreneurs' Programme. The tool is essentially a survey that assesses and provides a score on a SME's readiness and capability to enter the global supply chain. Similar tools are also available for other sectors. The problem is that access to the tool is only available if SME's meet certain monetary thresholds and other requirements. The assessment process itself is also half a day long and facilitated by an expert industry advisor. To allow greater access to what is considered a valuable industry support tool, Government could investigate supporting a truncated online self – assessment version.
3. Innovate and Collaborate Australia and specifically, NSW, has a strong	**A. Leverage partnerships across government, industry, industry associations and academia to establish a**	The key issue here is alignment with federal strategy to ensure no duplication and to compliment the initiatives federal agencies are undertaking in the sector. As examples, the NSW Cyber Industry Advisory and Cyber Security Node need to ensure continuity with federal counterparts.

Focus Area	Strategy	Comment
foundation upon which it can further develop its cyber security research capabilities – with active participants from university, government and the private sectors. Government facilitating the creation of new partnerships to encourage collaboration across key industry participants. This focus area seeks to tap into the new partnerships and entities created through Australia's Cyber Security Strategy.	**network of industry participants**	
	B. Establish a NSW Cyber Security Node	
	C. Establish the NSW Cyber Security Industry Advisory Group	
	D. Coordinate the NSW Cyber Security Industry Showcase	
4. Skills and Workforce The objective of these strategies is to promote the development of the future talent pipeline of cyber security professionals to close the workforce gap and develop cyber security as a critical industry in NSW.	**A. Drive participation in STEM subjects and increase computer literacy in schools**	
	B. Invest in vocational education (e.g. TAFE) certifications for technical cyber security skills development	