CPA Australia Ltd
Level 20, 28 Freshwater Place
Southbank VIC 3006
Australia

GPO Box 2820
Melbourne VIC 3001
Australia

Phone 1300 737 373
Outside Aust +613 9606 9677

Website cpaaustralia.com.au

29 July 2020

NSW Government Cyber Security Strategy Project Team
By email: cyberstrategynsw@customerservice.nsw.gov.au

Dear Sir or Madam

Submission on NSW Cyber Security Strategy

CPA Australia represents the diverse interests of more than 166,000 members working in over a 100 countries and regions around the world. We make this submission on behalf of our members and in the broader public interest.

CPA Australia considers the NSW Cyber Security Strategy an important initiative to raise awareness across industries of the increasingly significant role cyber security plays in the economy and society more broadly and to support the development of robust and consistent cyber security strategies.

While we consider all issues and questions raised by the NSW Government Cyber Security Strategy Project Team as relevant and timely, we identified the issues raised in **questions 6, 11, 13 and 20** as being most significant for our members and the accounting profession in general. Each of those questions is supplemented by three key issue areas, to which we provide corresponding recommendations.

Below is a list of our policy recommendations. How those recommendations address the identified key issue areas, is explained in more detail in the attachment.

Question 6: How can inter-government relationships be improved to bolster NSW's cyber security posture and resilience?

> **Recommendation 1:** Seek alignment with the Australian Cyber Security Strategy 2020 by reviewing industry panel report for learnings
>
> **Recommendation 2:** Seek panel assistance on cyber security strategy from organisations of different sizes representing different sectors
>
> **Recommendation 3:** Implementation of a state-wide collaboration platform that encourages sharing of information and expertise between state government agencies and other stakeholder groups

Question 11: In which areas do you currently lack the skills you need? What are the future skills needs in cyber security sector? What are expected skills gaps based on trends?

> **Recommendation 4:** Invest in soft skills and interpersonal skills training for cyber security staff by making it mandatory in professional development plans

Recommendation 5: Encourage the creation of more job descriptions for cyber security roles where cross-sector skills and experience are desirable and sought

Recommendation 6: Encourage secondments into security operation centres that are available at any level of government and place more security analyst roles across government, with focus on incident response and investigative responsibilities

Question 13: How can the NSW Government, educational institutes and industry build a market of high-quality cyber security professionals in Australia?

Recommendation 7: Improve re-training and re-purposing opportunities for agency staff through industry certifications in cyber security

Recommendation 8: Provide grants to education providers to support them in the development of cyber security education courses or certifications to encourage cyber security skills development across industries in NSW

Recommendation 9: Give preference in procurement to cyber security suppliers who invest in local talent hiring

Question 20: What are the obstacles to research, development and commercialisation in cyber security?

Recommendation 10: Encourage industry participation in research initiatives by making research skills more obtainable and accessible

Recommendation 11: Provide a tax or other incentive for the private sector to invest in local cyber security suppliers. Require NSW government agencies to give preference to local cyber security providers

Recommendation 12: Create an incubation hub that supports ongoing development of cybersecurity skills that can be accessed by local cyber security providers

If you require further information on the views expressed in this submission, please contact Nigel Hedges, Head of Information Security at nigel.hedges@cpaaustralia.com.au, or Dr Jana Schmitz, Policy Research Analyst at jana.schmitz@cpaaustralia.com.au.

Your sincerely

Dr. Gary Pflugrath
Executive General Manager, Policy and Advocacy

Inter-government relationships

How can inter-government relationships be improved to bolster NSW's cyber security posture and resilience?

Key issue areas:

1. Seek core alignment with the forming of Australia Cyber Security Strategy 2020
2. Inclusion of diverse communities and industries in panels or policy working groups
3. Electronic Forums for all tiers of the NSW Government to which non-NSW Governments are also granted access

The Australian Cyber Security Strategy 2020 Industry Panel Report (the Panel Report) and the NSW Government Cyber Security Strategy both note that there is little cross-referencing to, or indication of, intentional or clear alignment with other significant national cyber security strategies. The Panel Report calls for greater collaboration between all tiers of government. The NSW Government Cyber Security Strategy could proactively reciprocate this by acknowledging and finding commonalities with the Australian Cyber Security Strategy.

It was further noted in the Panel Report that only large telecommunication and defence organisations participated in the panel. However, cyber security posture and resilience affects all sectors. Federal and state governments should seek participation from a variety of organisations of different sizes representing different sectors. This includes specifically targeting organisation that participate in the cyber security buying-selling ecosystem. The buying-selling ecosystem refers to the cyber security suppliers, vendors, partners, integrators and consultancies that provide many of the products, services and solutions for the execution of the strategy.

The NSW Government should play a key facilitation role in providing a community collaboration platform that both government and industry could use to exchange information and experiences regarding common issues, and to consult each other on matters such as risk mitigation and best practice approaches. Moreover, other stakeholder groups such as state government departments (other than NSW), not-for-profit organisations, regulators, standard-setters, third-party cyber security vendors, and private sector companies (across sectors) should be encouraged to engage with the NSW Government on the collaboration platform.

Recommendations:

- Seek alignment with the Australian Cyber Security Strategy 2020 by reviewing industry panel report for learnings
- Seek panel assistance on cyber security strategy from organisations of different sizes representing different sectors
- Implementation of a state-wide collaboration platform that encourages sharing of information and expertise between state government agencies and other stakeholder groups

Cyber security skills

In which areas do you currently lack the skills you need? What are the future skills needs in cyber security sector? What are expected skills gaps based on trends?

Key issue areas:

1. Lack of interpersonal and business skills among cyber security professionals

2. Cross sector skills transfer and break down the barriers of contribution related to clearance
3. Security analysis and operational roles in short demand

Cyber security professionals across sectors, including the public sector, typically lack important business and interpersonal skills. This hampers their ability to influence, motivate and persuade stakeholders on cyber security issues, especially where cyber security knowledge is lacking at Board and executive level.

Private sector cyber security knowledge and experience can provide important perspectives that can sometimes be lacking in long-term public sector career workers. For public sector roles requiring clearance, in some cases the lack of ability to obtain clearance is precluding a portion of the workforce from applying for those roles. More roles should be structured to allow entry from outside the traditional pool of public sector workers.

In recent years, universities and other education institutions have focused education services on penetration testing and hacking. While we note that the variety in coursework modules has increased, the focus on security analysis and security operations is limited. To compensate for this gap, government should enable staff across management levels to gain professional experience in security analysis and operations by encouraging staff rotations within government cyber security areas and staff secondments in private sector security operation centres (SOCs). Such measures will help to enhance cyber security expertise among government staff, overcome the technical language barrier and improve the communication between non-cyber security personnel and management and cyber security experts. Moreover, we encourage the government to invest in local security operations managing detection and response teams, and to resist the temptation of short-term benefits by outsourcing such operations to suppliers that source SOC workforce internationally.

Recommendations:

- Invest in soft skills and interpersonal skills training for cyber security staff by making it mandatory in professional development plans
- Encourage the creation of more job descriptions for cyber security roles where cross-sector skills and experience are desirable and sought
- Encourage secondments into security operation centres that are available at any level of government and place more security analyst roles across government with a focus on incident response and investigative responsibilities

Building a local, high quality workforce

How can the NSW Government, educational institutes and industry build a market of high-quality cyber security professionals in Australia?

Key issue areas:

1. Need to build and allow for multiple pathways for entry into the cyber security profession
2. Incentivise universities and other education providers to develop relevant cyber security education
3. Align with cyber security suppliers who support local cyber security workforce

In response to the perceived cyber skills shortage across states emphasised in Australia's Cyber Security Sector Competitiveness Plan 2019, we recommend the development of more educational pathways for entry into cyber security jobs. The NSW Government should work with the Federal Government and other state governments to establish an accreditation panel or listing of industry certifications that are recognised for prior learning at education institutions (such as CISSP, CISM, CRISC, CGEIT, CISA) and other microcredentials or other online courses.

When upskilling an agency's workforce, the NSW Government should encourage industry certifications as a pathway for public servants who express an interest in cyber security work.

Education providers should be supported and encouraged to produce cyber security professional development and education relevant to a range of sectors.

To encourage students and jobseekers looking to upskill and/or reskill by electing and completing cyber security modules, we recommend the provision of special grants or relief programs for such people. Cyber security competes with other important endeavours such as STEM. However, financial support to education providers would encourage cross-sector workforce entry opportunities for cyber security professions and at the very least improve security awareness across industries. Ultimately, such measures may effectively reduce the cost of cyber security incidents.

The NSW Government should consider including a desirable requirement for local workforce hiring, when detailing non-functional requirements in their tender requests related to cyber security projects.

Recommendations:

- Improve re-training and re-purposing opportunities for agency staff through industry certifications in cyber security
- Provide grants to education providers to support them in the development of cyber security education courses or certifications to encourage cyber security skills development across industries in NSW
- Give preference in procurement to cyber security suppliers who invest in local talent hiring

Impediments to progress in research, development and commercialisation

What are the obstacles to research, development and commercialisation in cyber security?

Key issue areas:

1. Research opportunities are inaccessible by industry
2. Neither the Government nor private sector support, encourages or incentivises investment in local cyber security start-ups
3. Limited resource pool for local cyber security start-ups to develop products or services

Universities often discourage industry-specific research by establishing entry barriers for non-academic professionals. More precisely, the entry barrier to conducting research is tethered to demonstrating the capability to employ academic research methods, collect and analyse empirical data and publish in academic journals. Thus, most research is conducted by those with an extensive academic background. Furthermore, research opportunities often require significant technical skills such as coding and quantitative analysis skills.

While we are supportive of academic research, we encourage more research that is supported by industry-collaboration between universities and professional experts. For example, we encourage research into cyber security program or cyber security maturity performance of information security management systems (government or non-government). To expand the scope of local research on cyber security, the NSW Government should provide opportunities to support industry experts seeking to participate in research studies. Such support measures could take the form of research grants that industry experts could use to develop their research skills.

The public and private sectors do not sufficiently invest in cyber security start-ups. Local businesses often consider financial and regulatory uncertainty as a key barrier to investing in a local technology start-up. However, in recent

years various organisations have conducted cost-intensive in-house 'hack-a-thons' (or innovation workshops) and supported the funding of various prototype innovations that are similarly uncertain in their longevity. This same appetite for experimentation should be extended to start-up adoption by encouraging and incentivising local business to engage and invest in local cyber security start-ups and businesses. NSW Government agencies should be encouraged to invest in local cyber security start-up suppliers provided they meet regulatory requirements and standards.

Cyber security start-ups are often unable to find or retain staff to assist them in the development, maintenance or sales of products and services. The NSW Government should provide an incubation workforce hub (similar to Stone & Chalk, YBF) that allows start-ups to engage with and recruit talent from a resource pool of cyber skilled (or re-skilled) professionals. To leverage expertise and knowledge and to encourage further technological advancement, we recommend that this hub become part of a multi-sector hub such as the Victorian Innovation Hub, which brings together start-ups across a range of sectors including medtech (medical technology), agtech (agriculture technology), fintech (financial technology) and cyber security.

Recommendations:

- Encourage industry participation in research initiatives by making research skills more obtainable and accessible
- Provide tax or other incentives to encourage the private sector to invest in local cyber security suppliers. Require NSW government agencies to give preference to local cyber security providers
- Create an incubation hub that supports ongoing development of cybersecurity skills that can be accessed by local cyber security providers.