Department of Home Affairs
cybersecuritystrategy@homeaffairs.gov.au

31 October 2019

Consultation on Australia's Cyber Security Strategy

Thank you for the opportunity to provide this submission.

The Australian Digital Inclusion Alliance (ADIA) is a shared initiative with over 400 business, government, academic and community organisations working together to accelerate action on digital inclusion. Our member organisations conduct a variety of research and practical programs aimed at reducing the digital divide and enabling greater social and economic participation for everyone in Australia. ADIA is supported by Infoxchange and backed by Australia Post, Google and Telstra.

Digital inclusion is based on the premise that everyone in Australia should be able to make full and safe use of digital technologies – to manage their health and wellbeing, access education and services, organise their finances, connect with friends and family, and the world beyond. It goes beyond simply owning a computer, or having access to a smartphone. At its heart, digital inclusion is about social and economic participation: using online and mobile technologies to improve skills, enhance quality of life, educate and promote wellbeing across the whole of society. We believe everyone in Australia should be able to make full use of digital technologies.

Our submission will specifically address the ways in which improving digital inclusion in Australia will create more cyber aware communities and will equip more consumers with the skills that they need to stay safe online.

A Cyber Aware Community

The ADIA strongly supports the Department's position that "Australians need the right knowledge to make cyber-smart consumer choices".[1] The ADIA submits that in order to empower consumers to demand services and products that are designed with cyber security in mind, we must ensure that ***all consumers*** are equipped with the foundational skills that are necessary to stay safe online. This includes consumers who are particularly susceptible to being digital excluded, such as people with low levels of income, education and employment, along with older Australians, people with a disability, remote Indigenous communities and people in regional areas.

[1] Home Affairs, *Australia's 2020 Cyber Security Strategy*, page 16.

One way of ensuring that these communities are empowered to be more cyber-aware is through the implementation of ***a whole of government digital skills strategy*** that encompasses all the skills needed to thrive in today's connected world.

- **Essential digital skills** encompass the *ability* to do certain things online, and beyond that to do them *safely and effectively*. This enables Australians to manage their health and wellbeing, access education and services, organise their finances, connect with friends and family, and the world beyond. At its heart, having essential digital skills is about social and economic participation: using online and mobile technologies safely to improve skills, enhance quality of life, educate and promote wellbeing across the whole of society.

- Essential digital skills are important because digital technology plays a central and empowering role in our lives. With services, including Government services, increasingly being delivered online, it is more important than ever that no one gets left behind. The Australian Digital Inclusion Index shows that while online participation is increasing across Australia, gaps continue to exist between those who are digitally included and excluded – linked closely to social exclusion and disadvantage. Everyone in Australia should be able to make full and safe use of digital technologies.

- There is currently an array of quality work underway to better equip Australians with essential digital skills. This ranges from private and community sector efforts, such as Go Digi, Digital Springboard, Digital Garage and Tech Savvy Seniors; to Government efforts, such as the Be Connected program, the work of the Office of the eSafety Commissioner, the Australian Digital Health Agency's work to increase digital health literacy and the Department of Prime Minister and Cabinet's work to support Indigenous people and communities.

Whilst all of these efforts are worthwhile, they would be more impactful if they were measured against implementation of a Digital Skills Strategy. The development and existence of such a strategy would allow all private sector, community and government work to be directed towards desired outcomes, including increased awareness of cyber security risks; it would also facilitate an analysis of whether there are any gaps in activity, or indeed overinvestment in certain areas.

Question 22: To what extent do you agree that a lack of cyber awareness drives poor consumer choices and/or market offerings?

The ADIA submits that consumer choices are driven by a user's understanding of the technology that they are engaging with. As the Department's Discussion Paper points out, it is through education that the risks of cyber threats are appreciated and measures to mitigate these risks are learned. The need for better education around these threats is particularly urgent for groups that are more likely to be digitally excluded. These include people with low levels of income, education and employment,

along with older Australians, people with a disability, remote Indigenous communities and people in regional areas.

The 2019 Australian Digital Inclusion Index found that ***less than half*** of all Australians think that computers and technology give them more control over their lives, and ***less than 40%*** indicated that they feel like they can keep up with a changing technological landscape. This is an even greater issue for people aged 65 and over. ***Just over a quarter*** of this age group report feeling empowered by computers, and just ***one in eight*** feel they can keep up with technological changes.

A 2018 study published by RMIT examining cyber safety in remote Aboriginal communities found that cyber safety issues are limiting some of the benefits of internet use in these communities.[2] The study found that marginalised communities are less likely to have a foundational understanding of digital skills and are therefore more likely to be susceptible to cyber threats such as identity fraud or phishing scams.

However, with a growing number of government, education, information and community services moving online, these groups will increasingly be forced to engage with online technologies in order to get by. Because of this, it is now more important than ever that a framework is put in place to ensure that all Australians have the ability to engage with the internet safely and securely. For this reason, the ADIA strongly supports the introduction of a ***a whole of government digital skills strategy*** that encompasses all the skills needed to thrive in today's connected world.

Question 24: What are examples of best practice behaviour change campaigns or measures? How did they achieve scale and how were they evaluated?

One way to support increased cyber awareness in the community would be the development of a ***nationally accepted digital skills framework***. An important aspect of a digital skills framework would be the core competencies that allow users to stay safe online. These range from foundational skills, such as the need to maintain secure passwords, to more advanced skills such as the ability to recognise a phishing scam. A review of 63 international digital skills frameworks conducted by RMIT found that:

> *Safety, framed particularly in terms of cyber security, privacy and protection of personal data, is prominent and needs to be included in discussions of digital skills.*[3]

A digital skills framework would define the essential digital skills Australians need to safely and effectively engage online. This framework could perform two functions:

- inform the development of school curricula; and
- inform the provision of digital skills programs by private sector, community organisations and government.

[2] Rennie, E et al (2018) *Cyber Safety in Remote Aboriginal Communities*, Final Report, page 8.
[3] Gekara et al, 'Skilling the Australian workforce for the digital economy' (2018) page 9.

There is an appetite for a clearly articulated set of competencies we are working to equip all Australians with, so that providers can tailor and target their training programs. This would ensure all providers of training are pushing in the same direction, towards common goals. This would increase the effectiveness of the myriad of efforts underway and provide a meaningful way to track progress.

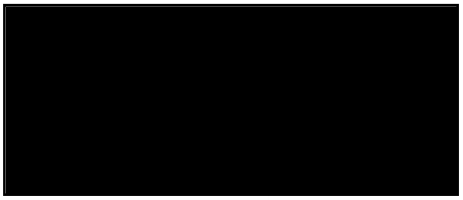
A digital skills framework could be a key component of a Digital Skills Strategy. It's worth noting that a comparable framework has been developed in the UK, with the aim of being used "by everyone in the UK engaged in supporting adults to enhance their essential digital skills." Other jurisdictions such as New Zealand and Canada are currently in the process of developing their own digital skills frameworks.

The ADIA would welcome Government leadership in these critical areas. We would appreciate the opportunity to discuss this with you further.

Please don't hesitate to be in touch with Ishtar Vij, convenor of the Australian Digital Inclusion Alliance.

Yours faithfully

David Spriggs
CEO, Infoxchange
Chair, Australian Digital Inclusion Alliance



Ishtar Vij
Director, Eloquium Group
Convenor, Australian Digital Inclusion Alliance