

FOR IMMEDIATE RELEASE

6 August 2020

**\$1.66B CYBER SECURITY PACKAGE MUST HELP AUSTRALIAN BUSINESSES
BECOME MORE DIGITALLY AWARE SAYS AUSTRALIA'S TECH HEAVYWEIGHT**

Australia's peak industry body for innovation technology, The Australian Information Industry Association (AIIA), today supports the Prime Minister's new four-year cyber security strategy, designed to combat online fraudsters and empower businesses to be more cyber vigilant.

Entitled, '[Australia's Cyber Security Strategy 2020](#)', part of the package allows small and medium-sized businesses to upgrade their cyber security and resilience - including an \$8.3 million Cyber Security Connect and Protect Program, designed to offer tailored advice and assistance from trusted sources. The government also stated that they will work with large companies and service providers to provide small businesses with better information and resources such as threat blocking and antivirus training.

The strategy includes giving \$66 million in funding to operators of critical infrastructure to assess their networks for vulnerabilities. These include power plants, communications and ports so they can better fend off serious cyber attacks.

The AIIA CEO, Ron Gauci, said: "We support any measures, both strategically and investment-wise, that will help Australian businesses to become more cyber aware.

"We know that critical infrastructure is increasingly becoming a target for cyber crime. Operational technology used in critical infrastructure, manufacturing, sensors or building controllers traditionally operate on separate networks with different protocols. In recent years we have seen the line blurred with these devices becoming IP-enabled or connected to IoT-type devices.

"We appreciate that the Prime Minister has listened and understands the need to continue investment and support with cyber security - as evident by [The Cyber Security Review](#), which was led by The Department of the Prime Minister and Cabinet, which highlighted that cybercrime is costing the Australian economy in excess of \$1 billion annually in direct costs alone.

"Whilst the cyber security industry has long suffered a shortage of skills, there is an even larger gap of experts who understand the traditionally engineering focused domain of operational technology and cyber security.

"Australia is currently short of [2,300 workers in cyber security](#), with an expected demand of at least 17,600 additional professionals required in the sector by 2026 - we hope this investment and focus goes some way to addressing the gap," Mr Gauci said.

As detailed in a recent set of recommendations put to Australian Government as part of the AIIA White Paper titled '[Building Australia's Digital Future in a Post-COVID World](#)', the AIIA put forward the following suggestions relating to cyber security:

1. Secure remote working, access to secure infrastructure and robust business continuity solutions are key to supporting Australian businesses but investment in these areas will also stimulate employment, particularly across technology innovators and incubation hubs.
2. Extend Australia's 2020 Cyber Security strategy to include Cyber Resiliency and enhance and promote support to Australian SMEs through Cyber awareness and support programmes and continue to invest in Cyber Security skills, in particular the area of Operational Technology security.
3. Improved Governance and operational initiatives to strengthen the collaborative learning structure created through the national Joint Cyber Security Centres network to encourage knowledge transfer between government and industry around both cyber resiliency and cyber incidents and further extend this support to SMEs.
4. That the Australian Signals Directorate (ACSC) continues to take a leadership role in advising and providing support on cyber security issues.
5. Provide incentives to support small businesses to invest in cyber security upskilling and better promote available initiatives.

Mr Gauci continued: "Similar to the AIIA's white paper recommendations, we are pleased that the paper goes beyond just cyber security and looks at the cyber resilience of industries which we support and think are vital. Cyber security and cyber resilience of businesses are distinct concerns.

"The 2020 cyber strategy supports our recommendations that SMEs need greater awareness and understanding on cyber threats and there is an important role for government in this area which we will be pleased to support as a leading tech association.

"We're actively engaged and working with both tertiary and Vet providers to offer cyber courses, particularly cyber security micro-credentials, such as: *Greater collaboration to build Australia's cyber skills pipeline*," Mr Gauci concluded.

ENDS

Notes to Editor

- The Australian Information Industry Association (AIIA) is Australia's peak industry representative body for innovation technology
- The AIIA is a not-for-profit organisation aimed at fuelling Australia's future social and economic prosperity through technology innovation.
- The AIIA recently released a Whitepaper titled '[Building Australia's Digital Future in a Post-COVID World](#)', which emphasised the need to look beyond traditional infrastructure investment by government with more focus on technology infrastructure.

For media enquiries: Thrive PR and Communications



Jacinta Chapman - Group Account Director
M: 0409 850 413
E: jacinta.chapman@thrivepr.com.au

Nathan McGregor - Account Director
M: 0490 494 048
E: nathan.mcgregor@thrivepr.com.au

About AIIA

The Australian Information Industry Association (AIIA) is Australia's peak representative body and advocacy group for those in the digital ecosystem. Since 1978 AIIA has pursued activities to stimulate and grow the digital ecosystem, to create a favourable business environment for members and to contribute to Australia's economic prosperity. We do this by delivering outstanding member value by providing a strong voice of influence; building a sense of community through events and education; enabling a network for collaboration and inspiration; and developing compelling content and relevant and interesting information.