THE LAW SOCIETY
OF NEW SOUTH WALES

Our ref: PDL:CBns310323

31 March 2023

Dr James Popple
Chief Executive Officer
Law Council of Australia
DX 5719 Canberra

By email: shounok.chatterjee@lawcouncil.asn.au

Dear Dr Popple,

2023-2030 Australian Cyber Security Strategy – Discussion Paper

Thank you for the opportunity to contribute to the Law Council's submission to the Department of Home Affairs on the Australian Cyber Security Strategy Expert Advisory Board's paper entitled *2023–2030 Australian Cyber Security Strategy* (the Discussion Paper). The Law Society's Privacy and Data Law Committee has contributed to this submission.

In this submission, we have focussed on the key issues identified by the Law Council in its Memorandum dated 3 March 2023 (the Memo), rather than the specific questions set out in Attachment A to the Discussion Paper.

More explicit specification of cyber security obligations

As noted in the Memo, the Discussion Paper suggests 'more explicit specification of obligations, including some form of best practice cyber security standards.'

In our view, the Australian Cyber Security Centre's 'Essential Eight Maturity Model' (Essential Eight), which sets out a baseline model for cyber protection for Microsoft based internet-connected networks, provides a useful and versatile framework for implementing more specific cyber security standards. In particular, we note the Essential Eight defines four 'maturity levels' (Levels Zero through Three) based on 'mitigating increasing levels of adversary tradecraft… and targeting.' [1]

Accordingly, in seeking to define more explicit cyber security obligations, we suggest consideration should be given to setting specific security standards based on the type of entity involved, and the quantity and degree of sensitive data it holds, in accordance with the approach adopted under the Essential Eight.

However, we also suggest that the Essential Eight should be reviewed on an ongoing basis to ensure that it remains fit for purpose, and if necessary, should be updated to broadly align with international standards.

[1] Australian Cyber Security Centre, Essential Eight Maturity Model https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model.

THE LAW SOCIETY OF NEW SOUTH WALES
170 Phillip Street, Sydney NSW 2000, DX 362 Sydney
ACN 000 000 699 ABN 98 696 304 966
lawsociety.com.au
T +61 2 9926 0333 F +61 2 9231 5809
E lawsociety@lawsociety.com.au
Law Council OF AUSTRALIA
CONSTITUENT BODY

A new Cyber Security Act

As noted in the Memo, the Discussion Paper 'contemplates implementation through a new Cyber Security Act, drawing together cyber-specific legislative obligations and standards across industry and government.'

As a broad observation, we note that the current cyber security standards and models are susceptible to technological change. As such, we support further consideration of developing specific cyber security legislation, that would enable government to impose contemporaneous cyber security obligations predominantly through regulations and directions.

However, the development of a new Cyber Security Act would of course involve a range of additional considerations that may require significant further consultation and discussion. At a minimum, we note that such legislation must be supported by an appropriate enforcement and compliance regime, and should include appropriate exemptions. We also support the harmonisation of Australia's privacy, data and cyber security regimes, and emphasise the need to mitigate the regulatory burden on affected entities caused by diffuse state and federal laws and regulations.

Careful consideration must also be given to the scope of any proposed legislation, and the potential impacts of such legislation on various entities operating at different levels of the supply chain. We caution against an approach that encourages regulated entities to simply shift their cyber security obligations onto third parties (such as technological infrastructure or cyber security providers), which may disincentivise providers to deliver certain important services, or markedly increase their prices to compensate for the additional regulatory risk. We suggest that any proposed legislation must be mindful of the commercial relationships between businesses operating at multiple levels of the supply chain, including cyber security service providers, as well as the potential increase in overall costs of compliance on Australian businesses.

In seeking to draw together cyber-specific legislative obligations and standards across industry and government, we suggest further clarification is required to clearly delineate the roles and remit of the Australian Signals Directorate and Australian Cyber Security Centre going forward.

Expanding the *Security of Critical Infrastructure Act 2018*

The Discussion Paper proposes consideration of whether a significant expansion of the *Security of Critical Infrastructure Act 2018* (SOCI Act) is warranted, which would, notably, include customer data and 'systems' in the definition of critical assets.

We support in principle expanding the definition of critical assets under the SOCI Act to include customer data, noting that this form of personal information is critical to the regular functioning of society, and is in our view deserving of protection commensurate with other critical assets.

However, we suggest that any expansion of the powers and safeguards under the SOCI Act should not undermine the ability of individuals to pursue their rights under the *Privacy Act 1988*, and note that information gathering and other powers designed to assist individuals should be preserved.

Payment of ransoms to cyber criminals

We support in principle a prohibition on the payment of ransoms and extortion demands by cyber criminals, which would, in our view, have the likely effect of disrupting the typical business model of the majority of cybercrime. However, such a prohibition would require very significant further consideration of strategies to protect victims and mitigate the harms

associated with cybercrime, including the possibility of implementing a comprehensive support scheme for victims of cybercrime.

Uplifting cyber skills in Australia

There is a manifest need for legal professionals to increase their cyber skills and expertise, to counteract the evolving and increasingly sophisticated cyber security threats aimed at the legal profession. In addition to the government's proposed STEM agenda, we support initiatives to encourage and incentivise lawyers to upskill in cyber proficiency through the higher education system.

More broadly, we support initiatives to develop and grow the cyber security workforce in Australia by supporting small businesses, and ensuring they are well placed to employ and, in turn, upskill the workforce. We suggest a review of the incentives available for Australian entrepreneurs, particularly in the cyber security industry, with a view to fostering innovation and technological development into the future.

We hope this input is of assistance. Please contact Nathan Saad, Policy Lawyer, on (02) 9926 0174 or nathan.saad@lawsociety.com.au in the first instance if you have any queries.

Yours sincerely,

Cassandra Banks
President