1 March 2024

Department of Home Affairs
Via Online Form

To whom it may concern

Consultation on proposed cyber security legislative reforms

Thank you for the opportunity to make a submission to the *2023-2030 Australian Cyber Security Strategy Legislative Reforms Consultation Paper (Consultation Paper*).

IIS Partners (IIS) is an Australian based consultancy that provides expert advice to entities on meeting their privacy and data security obligations, managing privacy and security risk, and implementing a privacy by design (PbD) and security by design (SbD) approach to product and service development. We have worked extensively with public and private sector clients in Australia and globally, and we bring a practical perspective to law reform – particularly how privacy and security law is implemented 'on the ground' and the challenges entities tend to encounter.

IIS fully supports the Australian Government's commitment to shepherding a new era of public-private co-leadership to enhance Australia's cyber security and resilience. We have longstanding interest and engagement in cyber security law reform and adjacent programs of work including privacy law reform (see, for example, our submission to the Attorney General) and digital identity (see our submissions to the Department of Finance and to the Senate Economics Legislation Committee on the Digital ID Bill).

We understand that changes to legislation can have significant impacts on how businesses make decisions, but more importantly how this impacts all Australians. Putting the individual first when considering the risks and impacts is not just the right thing to do, it is IIS Partners' 20-years belief that it is "just good business" and will add the most value for Australian businesses and citizens.

Our comments, outlined below, are concerned with Measures 3, 5 and 6, as set out in the Consultation Paper.

IIS Partners
INFORMATION INTEGRITY SOLUTIONS

Limited use obligation (Measure 3)

We understand that the proposed introduction of a limited use obligation on the Australian Signals Directorate (ASD) and the Cyber Coordinator is aimed at encouraging entities to share cyber security incident information and thereby enable a quick response to security threats. Information disclosed would not be able to be used for regulatory purposes.

IIS supports the overall objective of Measure 3, as long as the powers of regulators to investigate and take enforcement action remain intact and are not diminished or curtailed through the operation of a limited use mechanism. The Consultation Paper makes clear on pp 19-20 that such a mechanism would not operate as a form of 'safe harbour' and 'will not exempt an organisation from regulatory obligations, nor reduce an organisation's legal liability on the basis of voluntary reporting to ASD or the Cyber Coordinator.'

Therefore, we **support** the Consultation Paper's explicit statement that the limited use obligation will not remove regulatory obligations or legal liability. We would **not support** a scenario in which voluntary reporting to ASD or the Cyber Coordinator diminished the ability of a regulator, such as the Australian Information Commissioner, to take appropriate regulatory action. Further, we **suggest** that it be made clear that voluntary reporting does not satisfy or replace mandatory data breach notification obligations under the *Privacy Act 1988*.

Protecting Critical Infrastructure data storage systems (Measure 5)

IIS supports proposed amendments to the *Security of Critical Infrastructure Act 2018* (SOCI Act) that would expand the definition of 'asset' to include data storage systems holding 'business critical data.' This will mean that such data storage systems are brought under the coverage of the SOCI Act and are subject to its security, reporting and risk management arrangements.

As the Consultation Paper points out, there will be overlap with the operation of the Privacy Act where such data storage systems contain personal information.

The Consultation Paper states that 'the Department of Home Affairs will work closely with the Attorney-General's Department to ensure amendments to the SOCI Act are complementary to existing and proposed obligations under the Privacy Act' (p 38). The Consultation Paper also states that 'the relationship between the SOCI Act and the Privacy Act will […] be supported by appropriate guidance material' (p 38).

While we **support** the proposed amendment to the SOCI Act under Measure 5, we **recommend** appropriate supplementary funding to relevant agencies, including the Office of the Australian Information Commissioner, to support

development of guidance material which will be critical to minimising regulatory burden and explaining the interaction of SOCI and privacy legislation.

Consequence management powers (Measure 6)

IIS supports the proposal for a last resort directions power to enhance the Government's ability to help entities manage the consequences of security incidents. We also support the scope of the directions power, as set out on p 43 of the Consultation Paper – particularly its use to direct an entity to replace documents at the entity's own expense of individuals or businesses impacted by the incident (where this is not duplicative with other legislative levers). In our view, this would enhance the ability of individuals to recover from a security incident and reduce overall harm.

According to the Paper, the directions power would be able to be used if there is no existing power available to support a fast and effective response (p 42). IIS would caution against making the bar too high for the use of such a power. It is conceivable that the existence of powers in other legislation succeeds in quashing use of the directions power at every opportunity, including in cases where the directions power is the most effective and efficient regulatory mechanism for responding to an incident. IIS therefore recommends incorporating appropriate caveats to enable use of the directions power, even where another regulatory power exists but may be less appropriate, targeted, or fast acting.

The Consultation Paper lists a number of safeguards and oversight mechanisms for use of the directions power (pp 44-5). In relation to the requirement that the Minister consider the public interest when determining whether to use the power, IIS suggests that any public interest test specify irrelevant factors. Irrelevant factors should include cases where the direction may impose a financial cost on the entity. Our concern is that, in weighing the public interest, the interests of the community may be outweighed by the financial interests of the entity.

IIS **supports** the proposal for a last resort directions power, particularly its use to direct an entity to replace documents *at the entity's own expense* of individuals or businesses impacted by the incident. We **recommend** incorporating appropriate caveats to enable use of the directions power, even where another regulatory power exists but may be less appropriate, targeted, or fast acting. And we **recommend** that any associated public interest test is appropriately weighted towards community and national interests.

This submission was authored by Natasha Roberts, Malcolm Crompton AM, and me. We thank you for considering our comments.

IIS Partners would be pleased to discuss any aspect of our submission or the related Consultation Paper.

Our submission may be made public and published online.

Yours sincerely

Michael S. Trovato

Managing Partner
CDSPE, CISM, CISA, MAISA, GAICD

Information Integrity Solutions Pty Ltd
PO Box 978, Strawberry Hills NSW 2012, Australia
www.iispartners.com, mtrovato@iispartners.com
61 2 8303 2438