Level 36, Tower Two
Collins Square
727 Collins Street
Melbourne Vic 3008

GPO Box 2291U
Melbourne Vic 3000
Australia

ABN: 51 194 660 183
Telephone: +61 3 9288 5555
Facsimile: +61 3 9288 6666
DX: 30824 Melbourne
www.kpmg.com.au

Department of Home Affairs
Email: AusCyberStrategy@homeaffairs.gov.au

1 March 2024

Re: Australian Cyber Security Strategy: Legislative Reforms Consultation Paper

As a leading professional services firm, KPMG Australia (KPMG) is committed to meeting the requirements of all our stakeholders – not only the organisations we audit and advise, but also employees, governments, regulators – and the wider community. We strive to contribute in a positive way to the debate that is shaping the Australian economy and we welcome the opportunity to provide a submission to the *Cyber Security Legislative Reforms Consultation Paper* (the consultation paper) building on our February 2022 submission, *Cyber Security Considerations 2022*[1] and our May 2023 submission in response to the *2023-2030 Australian Cyber Security Strategy Discussion Paper*[2].

KPMG welcomes the Government's consultation paper and subsequent action plan as a national imperative to work towards Australia being the most cyber secure nation in the world by 2030. We are also supportive of greater security standards and transparency on the security features of technology products. KPMG was pleased to see our recommendation to establish a major incident review board included in our last response featured in this consultation paper. The establishment of a major incident review board, co-led by government and industry, will provide a more independent and consistent approach to understanding the root causes for major incidents.

In this response, we have included relevant sections of our *2023-2030 Australian Cyber Security Strategy Discussion Paper* submission in response to the consultation questions and built on these where appropriate at the Appendix of this submission.

[1] Cyber security considerations 2022 (kpmg.com)
[2] 2023-2030 Australian Cyber Security Strategy Discussion Paper – KPMG Submission - KPMG Australia

We understand the evolving cyber risk environment and the emergence of new technologies such as generative artificial intelligence. We have noted in our paper *Safe and responsible AI in Australia*[3] that the successful adoption of responsible AI needs to be assisted by addressing the public's current lack of trust in AI by ensuring the right mix of policy setting regulations and laws to ensure AI use is safe. We also encourage the Government to consider an appropriate enforcement regime so that industry is better incentivised to meet the requirements set out in the *Security of Critical Infrastructure Act 2018* (SOCI Act).

We stand ready to help our clients and the community be prepared for the unique cyber security challenges identified in the discussion paper and look forward to working with the Government in strengthening Australia's cyber security capability.

Should you wish to discuss these issues or proposals further, please do not hesitate to reach out.

Yours sincerely,

Greg Miller
Lead Partner, Government Cyber and Critical Infrastructure
KPMG Australia

Martijn Verbree
Lead Partner, Cyber Security
KPMG Australia

[3] Safe and responsible AI in Australia – KPMG Submission - KPMG Australia

Appendix: Consultation paper themes

Measure 1: Helping prevent cyber incidents – Secure-by-design standards for Internet of Things devices

1. Who in the smart device supply chain should be responsible for complying with a proposed mandatory cyber security standard?
2. Are the first three principles of the ETSI EN 303 645 standard an appropriate minimum baseline for consumer-grade IoT devices sold in Australia?
3. What alternative standard, if any, should the Government consider?
4. Should a broad definition, subject to exceptions, be used to define the smart devices that are subject to an Australian mandatory standard? Should this be the same as the definition in the PTSI Act in the UK?
5. What types of smart devices should not be covered by a mandatory cyber security standard?
6. What is an appropriate timeframe for industry to adjust to new cyber security requirements for smart devices?
7. Does the Regulatory Powers Act provide a suitable framework for monitoring compliance and enforcement of a mandatory cyber security standard for IoT devices?

KPMG Response Q1-7

KPMG welcomes greater security standards and transparency on the security features of technology products.

KPMG supports a minimum baseline requirement for almost all IoT and ICS devices used in smart homes and smart cities, that balances security and consumer experience. Immediate and significant investment should be made in the development of standards, appropriate use guidelines for the use of emerging technologies such as Quantum computing, Artificial Intelligence and web 3 (block chain, Metaverse) to manage potential harm to the society.

The UK model is a good starting point. KPMG would support a market mechanism and greater use of the private sector to make quicker progress in standards development and implementation (noting other jurisdictions, such as Germany, have been ambitious in filling the technology security void). Voluntary codes should transition to mandatory codes and standards, with relevant regulators suitably resourced to enforce any new regime.

KPMG considers the current cyber security-related regulations are a good baseline and expect that the Review of Australia's Privacy Act and other reform underway will ensure the currency of the regulations. We note that despite the ongoing gaps, there are already a large number of applicable regulations and growing number of regulators. Navigating the complexities of the environment is difficult. To improve the understanding of the applicability of legislation and regulation we suggest that clear

definition of roles and responsibilities of regulators and legislation associated with mandatory reporting requirements be established.

Measure 2: Further understanding cyber incidents – Ransomware reporting for businesses

8. What mandatory information, if any, should be reported if an entity has been subject to a ransomware or cyber extortion incident?
9. What additional mandatory information should be reported if a payment is made?
10. What is the appropriate scope of a ransomware reporting obligation to increase visibility of ransomware and cyber extortion threats, whilst minimising the regulatory burden on entities with less capacity to fulfil these obligations?
11. Should the scope of the ransomware reporting obligation be limited to larger businesses, such as those with an annual turnover of more than $10 million per year?
12. What is an appropriate time period to require reports to be provided after an entity experiences a ransomware or cyber extortion attack, or after an entity makes a payment?
13. To what extent would the no-fault and no-liability principles provide more confidence for entities reporting a ransomware or cyber extortion incident?
14. How can the Government ensure that no-fault and no-liability principles balance public expectations that businesses should take accountability for their cyber security?
15. What is an appropriate enforcement mechanism for a ransomware reporting obligation?
16. What types of anonymised information about ransomware incidents would be most helpful for industry to receive? How frequently should reporting information be shared, and with whom?

KPMG response Q8-16

KPMG recommends that the government carefully consider the risks associated with an express legislative ban on ransomware or extortion payments. Any legislative ban on ransomware payments should consider appropriate education and support schemes and whether a ban should be progressed in partnership with like countries (e.g., across the Five Eyes partnership). A legislative ban would need to incorporate exemptions to provide for the payment of a ransom in exceptional circumstances, such as immediate risks to health and safety.

We would support other mechanisms such as an anonymised reporting scheme to better inform government on ransomware payment prevalence. Such an approach would better inform industry about risks and the threat environment.

Please also refer to our response to Questions 17-19 that relate to the confidentiality needs of impacted organisations.

Measure 3: Encouraging engagement during cyber incidents – Limited use obligation on the Australian Signals Directorate and the National Cyber Security Coordinator

17. What should be included in the 'prescribed cyber security purposes' for a limited use obligation on cyber incident information shared with ASD and the Cyber Coordinator?
18. What restrictions, if any, should apply to the use or sharing of cyber incident information provided to ASD or the Cyber Coordinator?
19. What else can Government do to promote and incentivise entities to share information and collaborate with ASD and the Cyber Coordinator in the aftermath of a cyber incident?

KPMG response Q17-19

KPMG considers that it is important to take into account the confidentiality needs of impacted organisations to be protected from reputational damage as well as exposure to the further risk of targeted attacks. Confidentiality will encourage greater voluntary incident reporting. The potential for organisations to be identified or for their confidential information to be disclosed as part of a cyber incident report, is likely to inhibit voluntary reporting. We know from our clients there is still a general reticence to report incidents, with organisations making a risk calculation on whether and when to report. KPMG considers that there can be a better balance struck between transparency and data anonymisation that seeks to achieve the public policy objective of intelligence gathering and remediating harm caused by breaches, while also limiting the cost through reputational damage.

This information could help government and businesses make informed decisions about their digital and cyber security investments as well as the development of targeted policy approaches. It would also demonstrate if regulatory reforms and business practices are having any impact on reducing the number of cyber incidents. KPMG supports incentives for organisations that do voluntarily report incidents, given the additional investment organisations are making to do so.

Mandatory incident reporting as required under the SOCI Act has different considerations in relation to privacy and confidentiality. Where an incident is reported to Australian Cyber Security Centre (ACSC), it would be expected that this information would be passed onto the regulator (Home Affairs) in line with the respective legislation, except when it falls under the definition of protected information within the Act.

Measure 4: Learning lessons after cyber incidents – A Cyber Incident Review Board

20. What should be the purpose and scope of the proposed Cyber Incident Review Board (CIRB)?
21. What limitations should be imposed on a CIRB to ensure that it does not interfere with law enforcement, national security, intelligence, and regulatory activities?
22. How should a CIRB ensure that it adopts a 'no-fault' approach when reviewing cyber incidents?
23. What factors would make a cyber incident worth reviewing by a CIRB?
24. Who should be a member of a CIRB? How should these members be appointed?
25. What level of proven independent expertise should CIRB members bring to reviews? What domains of expertise would need to be represented on the board?
26. How should the Government manage issues of personnel security and conflicts of interest?
27. Who should chair a CIRB?
28. Who should be responsible for initiating reviews to be undertaken by a CIRB?
29. What powers should a CIRB be given to effectively perform its functions?
30. To what extent should the CIRB be covered by a 'limited use obligation', similar to that proposed for ASD and the Cyber Coordinator?
31. What enforcement mechanism(s) should apply for failure to comply with the information gathering powers of the CIRB?
32. What design features are required to ensure that a CIRB remains impartial and maintains credibility when conducting reviews of cyber incidents?
33. What design features are required to ensure a CIRB can maintain the integrity of and protection over sensitive information?

KPMG response Q20-33

KPMG was pleased to see our recommendation to establish a major incident review board included in our last response featured in this consultation paper.

The establishment of a major incident review board, co-led by government and industry, will provide a more independent and consistent approach to understanding the root causes for major incidents.

This board will provide a more independent and consistent approach to understanding the root causes of major incidents – be they affecting public or private

sector organisations – and build a catalogue over time of outstanding vulnerabilities affecting the Australian economy. Such a board could afford both governments and victim organisations an off-ramp for media interest in the 'why' and 'who is to blame' in the immediate aftermath of a cyber incident.

The CIRB could have an extended membership, consisting of industry associations, where relevant associations can be notified depending on the nature of the incident. The use of industry associations rather than just vendors or major telcos could also limit potential conflicts of interests. Alternatively, the CIRB could have a large membership similar to the Takeovers Panel[4] to better manage potential conflicts.

The CIRB could have the capacity for 'own motion', as well as government-initiated reviews. There would need to be a clear terms of reference, on which industry and state and territory governments are consulted. It would be important that the public sector is not exempt from the CIRB's purview. Government could consider establishing the CIRB with an initial voluntary mandate to be reviewed after 18 months of operation. This review time would provide more of an evidentiary basis for the scope and authority of the CIRB. The need for a CIRB is unlikely to dissipate in the foreseeable future. Establishing the CIRB as a credible and sustainable body will be vital to engender long-term support – continuity will be important in this field to achieve the Government's 2030 objective.

Measure 5: Protecting critical infrastructure – Data storage systems and business critical data

34. How are you currently managing risks to your corporate networks and systems holding business critical data?
35. How can the proposed amendments to the SOCI Act address the risk to data storage systems held by critical infrastructure while balancing regulatory burden?
36. What would be the financial and non-financial impacts of the proposed amendments? To what extent would the proposed obligations impact the ability to effectively use data for business purposes?

KPMG response Q34-36

Whilst SOCI is primarily focused on minimising risks from operational disruptions, personal information is caught by the regime under the category of the Data Storage and Processing asset class. This places obligations on those data storage and processing providers, where the service is for another critical infrastructure entity and relates to business-critical data, for which the definition includes, among other things, personal information of at least 20,000 individuals (as defined by the Privacy Act).

[4] Panel members | Takeovers Panel

Further, the Act does require consideration of impacts where personal information is compromised, however, it is not an explicit focus.

We believe it may be necessary to include customer data more explicitly in the ongoing reform of Critical Infrastructure through the SOCI Act to reinforce protection from cyber threats and strengthen Australia's cyber security nationally. This will provide a legal and regulatory framework to ensure that organisations responsible for collecting and managing customer data take appropriate measures to safeguard it against potential threats. It would also allow for incident management in the case of a significant data breach.

We also support the Government's proposal to establish playbooks for large-scale data breaches, as part of its response to the Privacy Act Review, as it will improve breach response governance.

Measure 6: Improving our national response to the consequences of significant incidents – Consequence management powers

37. How would the proposed directions power assist you in taking action to address the consequences of an incident, such as a major cyber attack on your critical infrastructure asset?
38. What other legislation or policy frameworks (e.g., at a state and territory level) would interact with the proposed consequence management power and should be considered prior to its use?
39. What principles, safeguards and oversight mechanisms should Government establish to manage the use of a consequence management power?

KPMG response Q37-39

Consequence management and directions powers may warrant deeper and more targeted consultation with the Australian economy. To better support consequence management, the Government could consider working with key industry sectors on appropriate risk appetite statement.

KPMG considers that there are already a large number of applicable regulations and growing number of regulators in the cyber domain. Navigating the complexities of the environment is difficult. To improve the understanding of the applicability of legislation and regulation we suggest that clear definition of roles and responsibilities of regulators and legislation across state and territories and the Commonwealth be established and communicated through appropriate industry guidance material. We are also mindful of capacity limitations of relevant government agencies to be suitably familiar with the domains of the 11 sectors. Further government-led confidence building measures (e.g. more and ongoing exercises, staff exchanges and joint initiatives) may help better understand the need and industry support for consequence management powers.

Measure 7: Simplifying how government and industry shares information in crisis situations – Protected information provisions

40. How can the current information sharing regime under the SOCI Act be improved?
41. How would a move towards a 'harm-based' threshold for information disclosure impact your decision-making? Would this change make it easier or more difficult to determine if information held by your asset should be disclosed?

KPMG response Q40-41

Information sharing between government, academia, and industry on the cyber threat landscape and emerging trends and threats is essential to maintain a resilient and robust cyber defence posture, and ensure that organisations within Australia at risk from cyber threat actors have a thorough understanding of the threats that they face by being able to collectively understand, analyse, predict, and ultimately counter these threats. Protecting sensitive information – i.e., Protected Information in SOCI entities – is an equally important dimension of our layered cyber defence.

The Protected Information provisions of the SOCI Act continue to cause angst among a number of regulated entities. There is a genuine nervousness about the penalties associated with Protected Information. The existing regime creates ambiguity and a lack of confidence on how and to whom organisations can share genuinely Protected Information or general sensitive information. Our experience is this ambiguity and nervousness is hindering appropriate sharing of information, even outside of an incident (e.g. to service providers or in transferring responsibility of an asset to another organisation).

The move to establish a protected information regime for the private sector is a net positive for our maturing security across the economy. However, we are yet to achieve the desire effect. Government could usefully invest in revising and simplifying definitions and developing use cases in collaboration with industry. Further, government could consider moving towards a 'harms-based' approach to managing protected information, which would be more in line with the objective of SOCI, namely encouraging critical infrastructure providers to better manage risks associated with their assets.

On the topic of information sharing, KPMG recommends that an independent non-profit body, similar to AusCERT, be established as a hub for sharing information about the cyber threat environment. This information sharing hub should work to collate information shared from multiple sources and manage the information securely and in a way that maintains the anonymity of the organisations providing the information. Timely and meaningful threat information sharing is still a gap in the market that existing efforts are yet to fill.

KPMG considers that it is important to take into account the confidentiality needs of impacted organisations to be protected from reputational damage as well as exposure to the further risk of targeted attacks. Confidentiality will encourage

voluntary incident reporting. The potential for organisations to be identified or for their confidential information to be disclosed as part of a cyber incident report, may inhibit voluntary reporting. KPMG considers that there can be a better balance struck between transparency and data anonymisation that seeks to achieve the public policy objective of intelligence gathering and remediating harm caused by breaches, while also limiting the cost through reputational damage.

This information could help government and businesses make informed decisions about their digital and cyber security investments as well as the development of targeted policy approaches. It would also demonstrate if regulatory reforms and business practices are having any impact on reducing the number of cyber incidents. KPMG supports incentives for organisations that do voluntarily report incidents, given the additional investment organisations are making to do so.

Measure 8: Enforcing critical infrastructure risk management obligations – Review and remedy powers

42. How would the proposed review and remedy power impact your approach to preventative risk?

KPMG response Q42

It would be positive to introduce a formal, written directions power, managed by appropriate oversight mechanisms, particularly if exercised by exception and with education as the first line of resort.

Measure 9: Consolidating telecommunication security requirements – Telecommunications sector security under the SOCI Act

43. What security standards are most relevant for the development of an RMP?
44. How do other state, territory or Commonwealth requirements interact with the development of an RMP?
45. How can outlining material risks help you adopt a more uniform approach to the notification obligation?
46. What are the main barriers to engaging with government through the notification process as it is currently enforced? How can the obligation to notify be clarified?
47. How do your procurement and network change management processes align with the existing and proposed notification arrangements? Can you suggest improvements to accommodate industry practice?

KPMG response Q43-47

The *Telecommunications Sector Security reforms and the SOCI Act* amendments seek to uplift security resilience, including cyber, across critical infrastructure sectors. The Australian Government should consider reviewing how customer data is more explicitly captured across critical sectors.

KPMG also recommends greater alignment with regulatory requirements which would reduce ambiguity and provide consistency across critical infrastructure sectors.

Another recommendation would be for greater transparency around critical risks so far as reasonably practical. This will make a substantive contribution across driving resilience across the Australian economy. Ambiguity and inconsistent interpretations of these foundational concepts represent the greatest risk for the policy reform program going forward.