2023 – 2030 AUSTRALIAN CYBER SECURITY STRATEGY

DISCUSSION PAPER

SUBMISSION TO THE EXPERT ADVISORY BOARD

April 2023

INTRODUCTION

1. ANZ thanks the Expert Advisory Board (**Board**) for the opportunity to comment on the *2023 – 2030 Australian Cyber Security Strategy* discussion paper (**Paper**).

2. ANZ welcomes the development of an updated cyber security strategy (**Strategy**). The nation's cyber security and resilience will benefit from a comprehensive, long-term strategy that provides clarity on the Government's policy objectives and priorities.

3. To assist the Board to achieve its policy objectives, we have made some observations on selected questions in the Paper. These comments are made within the context of our overall support for the development of a Strategy which provides a clear roadmap to maintain and advance Australia's cyber security and resilience. Our key points for the Board's consideration are set out in the response to question 1.

4. We look forward to the next steps in the Board's review and would welcome the opportunity to discuss the points in this submission if this would be useful.

OBSERVATIONS ON SELECTED QUESTIONS

1. What ideas would you like to see included in the Strategy to make Australia the most cyber secure nation in the world by 2030?

5. To the extent not already contemplated, we recommend that the Strategy includes:

- A plan to **expedite** Australia's cyber resilience development.

  With the increase in cyber activity it is vital that we advance whole-of-society cyber resilience at speed. While there has been progress on initiatives such as the Cyber Threat Intelligence Sharing platform (**CTIS**) there is opportunity to move faster. The Strategy should sequence and prioritise key initiatives to be delivered in the short-term including effective threat intelligence and incident sharing.

- A **government led economy wide anonymised threat intelligence and incident sharing** regime.

  Industry intelligence sharing already exists in certain sectors. For example, the major banks share intelligence regarding active threats to support each other and the broader economy. The Government could co-ordinate anonymised two-way sharing across the economy, involving smaller organisations, via the Australian Cyber Security Centre (using the CTIS) and the National Anti-Scams Centre.

  Government may also consider the opportunity to share appropriately anonymised intelligence insights from existing incident reporting data (for example reporting under the *Security of Critical Infrastructure Act 2018* (**SOCI Act**) and APRA Prudential Standard CPS 234 (**CPS 234**)).

- A regular program of **coordinated economy wide incident response exercises** exploring different scenarios, industry sectors and regulatory agencies. Scenarios could model attacks causing major disruptions across the economy, including ransomware attacks on third parties in an organisation's supply chain.

  Exercises enhance understanding of potential economic impacts and help us plan how we work together across the economy and identify opportunities for improvement.

  We welcome the Government's April 2023 announcement concerning the launch of a series of cyber exercises to respond to attacks on critical infrastructure.

- A Government led program of **education and awareness** backed by behavioural science research. This should be simple, consistent and actionable messaging that Government, agencies and industry can target to different groups including large

corporates, small and medium enterprises (**SMEs**) and individual customers to raise cyber security and scams defences across the economy.

- Development of a **national digital ID** system to help minimise the volume of identity documents collected and stored.

- **Alignment with other digital economy reforms.**

  We encourage the Strategy to ensure alignment between cyber resilience initiatives and broader reforms, like *Privacy Act 1988* (**Privacy Act**) reform, scams policy and the development of the strategic plan for the payments system. This will support efficient, consistent reform implementation.

2. What legislative or regulatory reforms should Government pursue to enhance cyber resilience across the digital economy?

2.a. What is the appropriate mechanism for reforms to improve mandatory operational cyber security standards across the economy (e.g. legislation, regulation, or further regulatory guidance)?

6. We suggest Government prioritises measures to support less mature organisations to help lift cyber security standards across the economy.

7. Government could consider:

   - Further regulatory guidance on **best practice compliance** with directors' duties concerning cyber security. There is a range of resources available from Government and regulators.[1] It may be helpful to review and revise current guidance to ensure there is simple, consistent 'one-stop' messaging clarifying minimum standards and best practice.

   - A voluntary **cyber security accreditation regime**, including ongoing audit, to support organisations to efficiently demonstrate cyber security risk management credentials to customers. Currently, many corporate customers require suppliers to complete cyber security assurance reviews and ongoing audits involving significant cost, particularly for SMEs.

2.b. Is further reform to the Security of Critical Infrastructure Act required? Should this extend beyond the existing definitions of 'critical assets' so that customer data and 'systems' are included in this definition?

[1] The Australian Securities and Investments Commission (**ASIC**) offers cyber resilience guidance. The Australian Competition and Consumer Commission (**ACCC**) offers scam guidance. The Australian Cyber Security Centre (**ACSC**) offers guidelines on various topics and guidance on cyber resilience and scams.

8. Before considering further reform of the SOCI Act, to the extent not already contemplated, Government could conduct:

   - **Post incident reviews** of recent significant data breach incidents with representatives from relevant regulatory agencies and relevant industry representatives. See the response to question 14 below.
   - **Coordinated economy wide incident response exercises** as identified above at question 1.

9. This could help identify necessary regulatory change and whether that should be addressed via amendments to existing legislation like the SOCI Act or the Privacy Act, or via a new Cyber Security Act.

10. For example, one area that may benefit from legislative amendment is permitting limited data sharing with appropriate safeguards where that would be helpful to prevent fraud following a major data incident. This may be addressed via amendments to privacy or other existing legislation. Similarly, if it is considered that organisations are not adequately securing personal information, further guidance regarding compliance with Australian Privacy Principle 11 (concerning the security of personal information) may be the most appropriate solution.

2.c. Should the obligations of company directors specifically address cyber security risks and consequences?

11. We do not support directors' duties explicitly addressing cyber security risk and consequences. Existing directors' duties, including the duty 'to act with due care and diligence' and the duty 'to act in good faith in the best interests of the company', address cyber security and other evolving risks such as climate change.[2]

12. Directors of Australian Financial Services Licensees (**AFSL**) must also be mindful of AFSL obligations under Chapter 7 of the Corps Act including under section 912A(1). Importantly, in *ASIC v RI Advice Group Pty Ltd* [2022] FCA 496 the Court held that RI Advice contravened ss912A(1)(a) and (h) as a result of its failure to have documentation and controls in respect of cybersecurity and cyber resilience in place that were adequate to manage these risks.

13. We further note the Banking Executive Accountability Regime (**BEAR**) set out in Part IIAA of the *Banking Act 1959* that applies to authorised deposit-taking institutions (**ADIs**) in

[2] See section 180 (duty to act with care and diligence) and section 181 (duty to act in good faith in the best interests of the company) of the *Corporations Act 2001* (**Corps Act**).

Australia. It also includes accountability obligations for those with responsibility for overall risk controls and/or overall risk management arrangements and information management (including information technology and security) of the ADI.

14. The Financial Accountability Regime Bill 2023 introduced into Parliament in March 2023, if passed, will replace the BEAR requirements (including equivalent accountability obligations) and will make a number of changes including applying the regime to *all* APRA-regulated entities.

15. While we do not see a need for directors' duties to explicitly address cyber security, directors may benefit from further guidance to support risk-based decision making regarding cyber security.

2.d. Should Australia consider a Cyber Security Act, and what should this include?

16. We refer to the response to question 2.b. above.

2.e. How should Government seek to monitor the regulatory burden on businesses as a result of legal obligations to cyber security, and are there opportunities to streamline existing regulatory frameworks?

17. Government should consider opportunities to harmonise and streamline regulatory reporting obligations.

18. Many organisations have overlapping obligations to report incidents to multiple Australian regulators in addition to reporting obligations in other jurisdictions. For example, in Australia entities may be required to report under the SOCI Act, CPS 234, the Privacy Act and others. Extensive reporting obligations can divert resources from responding to and managing incidents.

19. Government could consider a consistent framework for reporting an incident and a single channel for regulatory reporting and subsequent regulatory engagement.

2.f. Should the Government prohibit the payment of ransoms and extortion demands by cyber criminals by: (a) victims of cybercrime; and/or (b) insurers? If so, under what circumstances?

i. What impact would a strict prohibition of payment of ransoms and extortion demands by cyber criminals have on victims of cybercrime, companies and insurers?

20. If Government does elect to prohibit ransom payments it will be important for it to:

- **Offer practical support** to organisations to enable them to meet their obligations to customers and shareholders in the face of a ransom attack. For example, Government could offer governance expertise and a clear path to law enforcement responses. In the

US the FBI disrupted the Hive ransomware group that targeted victims around the world.[3]

- **Consider providing safe harbour** for a ransom payment in certain circumstances. For example, it has been suggested there should be a safe harbour "…to ensure the company is not guilty of an offence if, for example, it notifies the Australian Cyber Security Centre on a confidential basis before paying the ransom, and it believes, in good faith and on reasonable grounds, that paying the ransom is reasonably necessary to enable the company to continue to provide essential services, to lessen or prevent a serious threat to the life, health or safety of any individual, or to protect public health or safety."[4]

14. What would an effective post-incident review and consequence management model with industry involve?

21. Post incident reviews (**PIR**) of significant cyber incidents that provide opportunity for wider learning and capability improvement should involve representatives from relevant regulatory agencies and relevant industry representatives. A PIR could identify remedial actions, improving government and industry cooperation to respond to significant incidents, including appropriate, timely data sharing.

22. Appropriate safe harbour protections could be considered to encourage an open and constructive approach.

ENDS

[3] US Department of Justice Disrupts Hive Ransomware Variant

[4] Australian Financial Review *Making cyber ransom payments unlawful would help boards* 21 November 2022