2023 – 2030 AUSTRALIAN CYBER SECURITY STRATEGY: LEGISLATIVE REFORMS

CONSULTATION PAPER

SUBMISSION TO THE DEPARTMENT OF HOME AFFAIRS

March 2024

INTRODUCTION

1. ANZ thanks the Department of Home Affairs (**Department**) for the opportunity to comment on the *2023 – 2030 Australian Cyber Security Strategy: Legislative Reforms* consultation paper (**Paper**).

2. ANZ welcomes the updated cyber security strategy (**Strategy**) and associated action plan including legislative reform. We appreciate the Government's commitment to improving our legislative and regulatory framework for cyber security.

3. To assist the Department to achieve its policy objectives, we have made some observations on selected proposed measures in the Paper.

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

OBSERVATIONS ON SELECTED MEASURES

MEASURE 2: FURTHER UNDERSTANDING CYBER INCIDENTS – RANSOMWARE REPORTING FOR BUSINESS

5. We suggest that the design of any ransom reporting obligation addresses Government's commitment to **simplifying incident reporting**.[1] To that end we make the following observations:

   - We welcome the Department's suggestion to '**acquit the proposed ransomware reporting obligation through existing reporting obligations**'[2] rather than applying a new reporting obligation to entities subject to existing mandatory reporting.[3]

     Existing obligations already require banks to report critical cyber incidents including ransomware or cyber extortion incidents. For example, banks must report incidents under the *Security of Critical Infrastructure Act 2018* (**SOCI Act**), APRA Prudential Standards CPS 234 and CPS 232, and under the *Privacy Act 1988* notifiable data breach scheme where applicable.[4] To the extent that further information is required (e.g., information regarding any ransom payment), our preference would be that this is addressed through modification of existing reporting obligations rather than applying a new ransomware reporting obligation.

   - The US ransomware reporting regime includes **protections for information subject to legal professional privilege** and **excludes the operation of the freedom of information regime**. It also provides assurances for reporting entities regarding **privacy, security and anonymisation** of information.[5] We encourage consideration of a similar approach for any Australian ransomware reporting obligation. Legislation that introduces an obligation could provide that the making of a report does not constitute a

---

[1] Strategy, p 25

[2] Paper, p 15

[3] This approach aligns with that of other jurisdictions. For example, section 2242 of the United States' *Homeland Security Act of 2002* (as amended by the *Cyber Incident Reporting for Critical Infrastructure Act of 2022*) includes a reporting exception for entities required to report substantially similar information to another Federal agency.

[4] Part 2B of the SOCI Act requires notification of critical and other cyber security incidents. The report form requires comprehensive information including when the incident was identified, the impact of the incident, the type of incident (including ransomware), a description of the incident including how it occurred and observed activity and any further details the ACSC may need to understand the effect of the incident. APRA Prudential Standard CPS 232 Business Continuity Management sections 36 and 37.

[5] The United States' *Homeland Security Act of 2002* (as amended by the *Cyber Incident Reporting for Critical Infrastructure Act of 2022*) requires entities to report certain cyber incidents and ransom payments. The Act provides that reports to Government do not constitute a waiver of the reporting entity's applicable privilege or protection provided by law. The Act also provides that reports are exempt from disclosure under federal and state FOI laws or similar laws requiring disclosure of information or records. See section 2245(5)(b).

waiver of privilege, and that reported information is exempt from Commonwealth and State freedom of information laws.

- **No-fault, no-liability protections** should be clear with respect to the application of instruments of crime, anti-money laundering/counter-terrorism financing and sanctions laws. The Paper notes that these protections will 'provide confidence for entities that they will not be prosecuted for making a payment', but that 'entities must still continue to meet their legislative obligations before, during and after a cyber incident'.[6] To help entities understand how the protections would affect their obligations, the protections must clearly identify what they protect, and how.

6. The objectives of a mandatory ransomware reporting obligation include accelerating law enforcement action, enhancing whole-of-economy risk mitigation by contributing to a current threat picture, and helping to tailor victim support services.[7] The Paper notes that it may be appropriate to limit the scope of the reporting obligation to businesses with an annual turnover of more than $10 million per year. We are conscious that excluding smaller businesses from reporting obligations could compromise Government's ability to meet these objectives and may also increase the risk of smaller businesses being targeted by malicious actors. Rather than limit the application of obligations, Government could consider ways in which practical support could be provided to small businesses to assist them in meeting their obligations in the face of a ransom attack.

MEASURE 3: ENCOURAGING ENGAGEMENT DURING CYBER INCIDENTS – LIMITED USE OBLIGATION ON THE AUSTRALIAN SIGNALS DIRECTORATE AND THE NATIONAL CYBER SECURITY COORDINATOR

7. We support the introduction of a legislated limited use and confidentiality obligation (**Limited Use Obligation**). Legislative clarity regarding permitted disclosure and use could help to simplify incident reporting and encourage timely and fulsome information sharing. We make the following observations to support these objectives.[8]

- We encourage Government to clearly define the application of any Limited Use Obligation. Legislation should clearly state **whether it applies to information that is only provided voluntarily**. If it applies more broadly, legislation should address how it

[6] Paper, p 16
[7] Paper, p 13
[8] We note that these observations also apply to to information provided under a Cyber Incident Review Board regime (Paper, Measure 4).

intersects with incident reporting under the SOCI Act and the associated protected information provisions.

- Proposed permitted uses include facilitating 'consequence management'. Government proposes that regulators should not be able to use information as part of an investigation or compliance activity.[9] Accordingly Government may consider **clarifying the scope of 'consequence management'** and expressly excluding investigation and compliance activity from permitted uses.

- We encourage further consideration as to how, in practice or in law, a Limited Use Obligation can prevent a regulator with knowledge of information provided under limited use obtaining the same information for an investigation or compliance activity using its other powers.

MEASURE 6: IMPROVING OUR NATIONAL RESPONSE TO THE CONSEQUENCES OF SIGNIFICANT INCIDENTS – CONSEQUENCE MANAGEMENT POWERS

8. The Paper proposes a consequence management power that would permit Government to issue directions to critical infrastructure entities to *address a consequence* of a cyber security incident that has occurred, is occurring or is imminent, and has had, is having or is likely to have a relevant impact on critical infrastructure.

9. As currently framed, it is difficult to assess the potential scope of the proposed power. For example, the Paper proposes that the Government could direct an entity to do or prohibit from doing a certain thing to prevent or mitigate the consequences of an incident.[10] This is broad and lacks clear boundaries.

10. If implemented, the power should clearly define 'consequence management' (including whether and how it differs from mitigating the impact of an incident as described in section 12P of the SOCI Act). This should also include guidance on how liability will be dealt with for any indirect and/or unintended consequences of such directions.[11]

11. The Paper also proposes that the Government could direct an entity to replace documents of individuals or businesses impacted by the incident.[12] There are some inherent limitations to

[9] Paper, p 20
[10] Paper, p 43
[11] We note that s 35AW of the SOCI Act provides that an entity is 'not liable to an action or other proceeding for damages for or in relation to an act done or omitted in good faith in compliance with a direction' and that the Paper notes that, in implementing the new power, immunities would be provided in the SOCI Act to ensure that entities would not be subject to civil liability when acting lawfully in response to a compulsory legal direction.
[12] Paper, p 43

the effectiveness of such a direction. It is not clear, in some circumstances, the way in which an entity would comply with such a direction. For example, entities would not be able to replace identity documents without the input of the impacted individual, or may not have access to the documents that need to be replaced. We encourage Government to consider other ways to achieve the policy outcome of ensuring individuals or businesses are not unduly impacted in the event of an incident. This could involve the issuance of directions that are more general in nature (for example, to mitigate the risk of identity theft).

12. As an alternative to the introduction of a new power, it may be possible for the objectives of the proposed power to be achieved by modifying the Minister's existing powers under Part 3A of the SOCI Act. These allow the Minister to issue directions to critical infrastructure entities to *mitigate the impact* of a cyber security incident that has occurred, is occurring or is imminent, and has had, is having or is likely to have, a relevant impact (*whether direct or indirect*) on critical infrastructure (**Directions Power**).[13] This impact mitigation could possibly include consequence management.

13. We understand a key driver for the proposal is Government's desire to be able to direct a critical infrastructure entity to take specific actions to mitigate the indirect impact (i.e., secondary consequences) of a cyber security incident that has occurred, is occurring or is imminent in *another* critical infrastructure entity. We suggest the Directions Power could be adjusted to clarify that it extends to directing *any* critical infrastructure entity to mitigate the impact on the availability, reliability, integrity or confidentiality (whether direct or indirect) of any cyber security incident on its critical infrastructure asset. For example, if there is a data breach in one entity (**Entity A**) with indirect relevant impacts for the confidentiality of information stored in the critical infrastructure asset of another entity (**Entity B**) the Government could direct Entity B to take specified actions to mitigate this impact.

ENDS

[13] Section 12P of the SOCI Act states 'mitigating a relevant impact of the incident on a critical infrastructure asset' is an example of responding to a cyber security incident. Section 8G of the SOCI Act specifically includes indirect impacts in the definition of relevant impact.