As a trusted government partner and corporate citizen, Transurban Limited, on behalf of itself and the Transurban Group (**Transurban**), welcomes the opportunity to provide feedback on the 2023-2030 Australian Cyber Security Strategy Discussion Paper (**Discussion Paper**).

Our feedback on specific questions is set out below.

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?**

   Stronger Collaboration: Foster greater collaboration between government, industry, and academia to share knowledge, resources, and threat intelligence. This will help to create a more comprehensive and coordinated approach to cybersecurity.

   Improved Public Cyber Awareness: Increase cybersecurity and fraud awareness and knowledge at all levels of society, to empower individuals to better protect themselves and their digital assets.

   Defined Cyber Education Accreditation: Create accredited and nationally recognised cyber education pathways for a full range of cyber skill requirements including individuals' cross skilling or changing career paths.

   Collaboration with International Partners: Work closely with international partners to share best practices and coordinate responses to cyber threats.

   Single Digital Identity: Establish a secure and single digital identity, maintained by the Government, so businesses do not have to hold personal data for customer identification purposes. This view is also reflected in the Productivity Commission Report's recommendation (recommendation 4.2) for expanding application of a secure, single digital identity.

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

   Our answer to this overarching question is captured by each of the answers to the sub-questions set out below.

   As a general comment, any reforms should focus on building cyber resilience, be outcome based, and seek to be proactive and not merely reactive, as well as establish specific regimes to disincentivise individual and group criminals and protect Australia against state-sponsored actors.

   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)?**

      Any mechanism will need to balance specificity with technical neutrality and be capable of being quickly updated to keep pace with technological changes.

      As such, we suggest that a combination of overarching, technological agnostic legislation with regulations and/or binding guidance that is regularly updated to reflect technological changes and the changing threat landscape will be the appropriate mechanism.

      We also note a major source of risk is data retained longer than may actually be necessary (and this played a factor in the severity of the Optus, Medibank and Latitude Financial breaches). Government should seek to clarify retention periods so that businesses have confidence in establishing regular data destruction programs in accordance with law.

      Any new mandatory requirements should include suitable grace periods to allow appropriate time for businesses to procure and safely implement complex and high risk technology changes to their core processes and systems and allow for the financial budgeting of such implementation (for example, a 36 month period to allow for uplifts).

      See also our comments in relation to question 2(d) below.

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?**

In our view, further reform of the Security of Critical Infrastructure Act (**SOCI Act)** is not the appropriate mechanism to enact reforms to enhance cyber resilience across the digital economy. The spirit of the SOCI Act is to intervene when a critical supply has been disrupted. Extending this to cover customer data is beyond the spirit of the SOCI Act. Any reforms relating to customer data are more appropriately governed as part of the *Privacy Act 1988* (Cth) and the *Competition and Consumer Act 2010* (Cth) (in relation to consumer data).

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

No, as this is sufficiently addressed already.

Directors' duties and obligations are adequately addressed in the *Corporations Act 2001* (Cth), as well as the ASX Corporate Governance Council's Corporate Governance Principles and Recommendations (which specifically cover risk). Cyber security risks should not be treated any differently to other business risks, all of which need to be appropriately identified and managed.

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

A separate Cyber Security Act may be helpful, but only to the extent such an Act does not duplicate what already exists and is not inconsistent with existing regulations. We also note our answer to 2(a) above. Furthermore, any new legislation should have a practical and positive impact and compliance with new legislation (i.e. reporting and notification obligations) should not impose an undue burden.

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?**

The Government should continue to engage with and consult industry on development of any new or amended regulations to identify areas of potential impact.

Seeking to streamline existing frameworks, such as harmonising data breach notification requirements, should be explored further as part of the various regulatory reviews taking place. Increased cooperation between existing regulators will also assist in streamlining.

Self-monitoring and self-reporting by industry, with appropriate regulatory powers to independently investigate and/or audit compliance, can also help with the regulatory burden.

As noted in response to question 1 above, Transurban strongly supports the creation of a single digital identity. This single digital identity will minimise the collection of personal data by businesses, which will result in businesses having a reduced burden in relation to costly and complex data retention systems and will deter cyber-attacks on businesses as there is less valuable information to be obtained from such attacks.

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?**

Transurban generally supports the prohibition of ransom / extortion payments with appropriate, limited exceptions. Regard should be had to learnings from any jurisdictions that have already enacted such prohibition regimes.

Ransom or extortion payments should not be prohibited if there is an overriding public safety concern. For example, if the incident response determines that it will take an unacceptable amount of time to return control of safety systems which control a critical function (such as ventilation of a tunnel), then a payment should be permitted.

Prohibiting ransom or extortion payments also punishes the ‘victim’. An alternative approach is one more outcome based, by imposing a penalty on the individuals or businesses that benefited from (or sought to benefit) from the data. This penalty should apply to any individual and/or business that benefited (or sought to benefit) from the compromised data, capturing persons who may not have been part of the original attack (for example, a person that knowingly bought a stolen data set).

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

Strict prohibition on payment of ransoms and extortion demands could negatively impact victims and companies.

For companies, a strict prohibition could result in public backlash and a perception that the company is using the prohibition as an ‘excuse’ not to do everything it can.

Strict prohibition may also make certain targets more vulnerable (for example, if certain businesses or individuals are exempt from the general prohibition).

Strict prohibition of payment would also limit law enforcement from counter ‘sting’ activities, and the ability to track and trace criminal organisations.

g. **Should Government clarify its position with respect to payment or non-payment of ransoms by companies, and the circumstances in which this may constitute a breach of Australian law?**

Yes – in absence of express legislation, clear guidance from government would be beneficial.

3. **How can Australia, working with our neighbours, build our regional cyber resilience and better respond to cyber incidents?**

Australia should seek to deepen its links with allied cyber security agencies. This should include practices and threat sharing, as well as seeking consistency between jurisdictions.

4. **What opportunities exist for Australia to elevate its existing international bilateral and multilateral partnerships from a cyber security perspective?**

No response.

5. **How should Australia better contribute to international standards-setting processes in relation to cyber security, and shape laws, norms and standards that uphold responsible state behaviour in cyber space?**

Global standards that are not nation-specific lower the costs of meeting cyber security requirements in a global market. Industry or national standards that do not equate to internationally agreed standards increase the cost of business and lead to conflicting cyber risk outcomes. As such, Australia should seek to actively contribute to the development of such global standards.

6. **How can Commonwealth Government departments and agencies better demonstrate and deliver cyber security best practice and serve as a model for other entities?**

No response.

7. **What can government do to improve information sharing with industry on cyber threats?**

Agreed disclosure rules and legal protections comprising a standardised and timely information sharing framework would increase the level for participation and value of cyber collaboration between entities. We note that non-government industry groups already share data on threats, which is used to then provide protections to industry organisations. These non-government groups have been borne out of necessity and are a reflection of the intermittent investment and commitment of the Government to establish and maintain a sustainable cyber threat sharing function.

8. **During a cyber incident, would an explicit obligation of confidentiality upon the Australian Signals Directorate (ASD) Australian Cyber Security Centre (ACSC) improve engagement with organisations that experience a cyber incident so as to allow information to be shared between the organisation and ASD/ACSC without the concern that this will be shared with regulators?**

   Yes, an explicit obligation of confidentiality enables more fulsome and candid disclosure. This supports faster response and potentially mitigates the impact of a cyber incident, particularly where multiple organisations are impacted by the same incident.

9. **Would expanding the existing regime for notification of cyber security incidents (e.g. to require mandatory reporting of ransomware or extortion demands) improve the public understanding of the nature and scale of ransomware and extortion as a cybercrime type?**

   We do not consider expanding the existing regime for notification would benefit public understanding. Notification fatigue is a legitimate concern and has driven the materiality thresholds of mandatory notification regimes (such as the eligible data breach notification process under the *Privacy Act 1988* (Cth)).

   Any increase in notification needs to also consider the interrelationship between notifications to government (federal and State/Territory), insurance, and the market and what would potentially be revealed to threat actors.

10. **What best practice models are available for automated threat-blocking at scale?**

    No response.

11. **Does Australia require a tailored approach to uplifting cyber skills beyond the Government's broader STEM agenda?**

    No response.

12. **What more can Government do to support Australia's cyber security workforce through education, immigration, and accreditation?**

    No response.

13. **How should the government respond to major cyber incidents (beyond existing law enforcement and operational responses) to protect Australians?**

    Until investigations conclude, it should be assumed that the business subject to a major cyber incident is a victim of crime and the government should provide support to mitigate damage that could be suffered by such business victims. This will be particularly important where the perpetrators are state-sponsored actors as businesses will not have the funds, resourcing, or appropriate political power to defend themselves against such well-funded enterprises.

    Appropriate government services should be capable of quickly scaling up to assist individuals impacted by a major cyber incident, including ability to change business-as-usual processes. For example, the Passport Office may need to increase resources if a major incident impacts a large number of Australian passports.

    While Transurban does not consider step-in to be appropriate in most circumstances, providing expert support for companies without appropriate cyber security maturity or sophistication could be another way for government to provide assistance to protect Australians.

a. **Should government consider a single reporting portal for all cyber incidents, harmonising existing requirements to report separately to multiple regulators?**

Yes. As recommended in the Productivity Commission's *5-year Productivity Inquiry: Advancing Prosperity* (Recommendation 4.5), a single reporting portal would assist with streamlining the multiple existing reporting obligations.

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

A post-incident review and consequence management model between government and industry should be limited to major, large-scale incidents (such as the 2022 Optus and Medibank incidents) that have resulted in significant harm to many Australians.

The focus should be on lessons learnt, with a no fault "Chatham House Rules" (ie, confidential) approach to encourage fulsome and candid disclosure. Consideration should be had to the risks to insurance claims and/or prejudice to any actions (including class actions) arising from any documentation of a post-incident review. An example of a model already employed is the United States Cyber Safety Review Board's initial report on Log4j.

15. **How can government and industry work to improve cyber security best practice knowledge and behaviours, and support victims of cybercrime?**

Funding of services like IDCare and public service announcement campaigns by government would support public awareness and support victims. We note industry is very active in putting out messaging around being aware / vigilant of potential scam communications.

a. **What assistance do small businesses need from government to manage their cyber security risks to keep their data and their customers' data safe?**

No response.

16. **What opportunities are available for government to enhance Australia's cyber security technologies ecosystem and support the uptake of cyber security services and technologies in Australia?**

No response.

17. **How should we approach future proofing for cyber security technologies out to 2030?**

No response.

18. **Are there opportunities for government to better use procurement as a lever to support and encourage the Australian cyber security ecosystem and ensure that there is a viable path to market for Australian cyber security firms?**

No response.

19. **How should the Strategy evolve to address the cyber security of emerging technologies and promote security by design in new technologies?**

We consider the Securing the Internet of Things for Consumers Code of Practice, developed by the Department of Home Affairs and ACSC, is an example of a good starting point on how the government can promote security by design in new technologies.

The Strategy should support the development of such codes of practice (and similar frameworks), with continuous engagement with industry to ensure emerging technology is accounted for and addressed as appropriate.

20. **How should government measure its impact in uplifting national cyber resilience?**

In measuring the impact, metrics and reporting need to be holistic and repeatable. An example of that approach is not just measuring and reporting on the number of cyber attacks affecting a sector, but also the response and impact. If the number of attacks does not change but the harm arising from those attacks is reduced, then that would indicate a positive impact of uplift.

21. What evaluation measures would support ongoing public transparency and input regarding the implementation of the Strategy?

Regular reviews and publishing of progress based on an agreed set of consumable and internationally comparable metrics (eg, number of major attacks, loss of consumer money to scams, etc) would support ongoing public transparency and support.