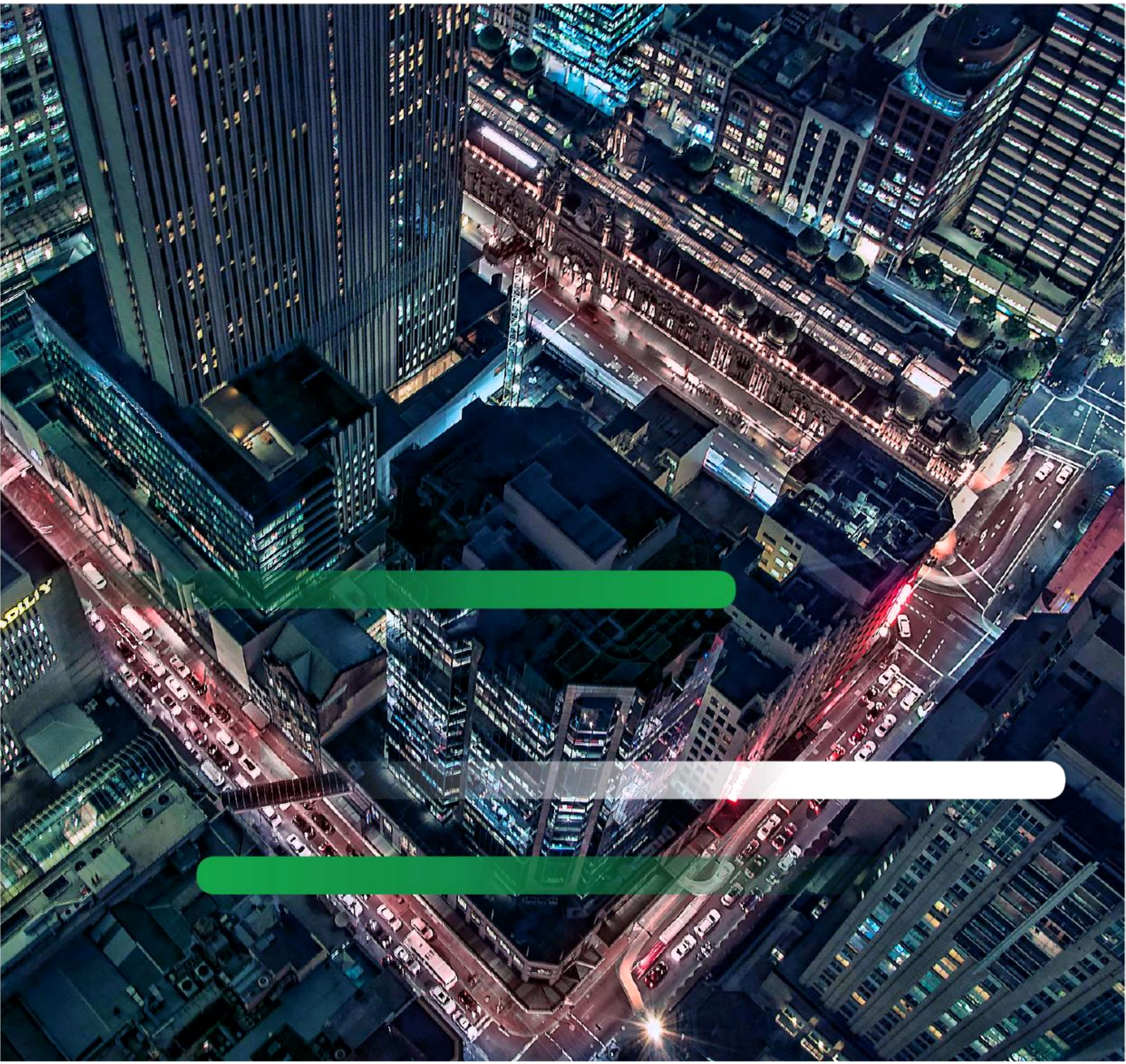
Transurban

Response to Australia's 2020 Cyber Security Strategy – a call for views



Response to the call for views

The Transurban Group is pleased to respond to the Department of Home Affairs' call for views for the 2020 Cyber Security Strategy. Planning for the future of cyber security in Australia is critical for keeping Australia safe and prosperous.

1. Comments on individual consultation questions

The Transurban Group's comments on specific questions posed in the call for views are included over the next few pages. The Transurban Group hopes these comments provide constructive feedback on a complex set of issues and help find a path to an appropriate regime for both government and industry.

Question	Comment
1. *What is your view of the cyber threat environment? What threats should Government be focusing on?*	The Transurban Group sees the cyber threat environment as evolving in nature and including the full range of threats, from opportunistic and low sophistication, to targeted attacks requiring highly coordinated and skilled threat actors. The Transurban Group feels that while private enterprise and the available security defence capabilities are able to manage the risk of the lower levels of sophisticated threats, highly sophisticated and potentially state-backed threat actors should be the focus of Australia's cyber defence capabilities for enterprise. The Transurban Group predicts the convergence of cyber and physical risks will be an area of increasing concern and government should take a lead in providing policy framework and advisory assistance in this area. The Federal Government should also continue to inform and educate the Australian public on cyber safety initiatives to lower the impact of opportunity-based, low sophistication attacks.
2. *Do you agree with our understanding of who is responsible for managing cyber risks in the economy?*	The Transurban Group is of the view that Government should continue acting in an advisory role and raising security awareness in industry and community. Government and industry should continue working together to support communities in this endeavour. The allocation of risk should be in line with international norms and agreements.
3. *Do you think the way these responsibilities are currently allocated is right? What changes should we consider?*	The Transurban Group views cyber security as a shared responsibility between government, industry and consumers. For industry especially, a balance between competitiveness and protecting consumers must be struck. Accordingly, the Transurban Group is of the view that the current responsibility allocation should be maintained but that opportunities for industry to improve their capabilities should be explored.

4. What role should Government play in addressing the most serious threats to institutions and businesses located in Australia?	The Government's advisory in Information Technology and Operations Technology (OT) has been of assistance to the Transurban Group. Timely and industry-specific threat intelligence sharing, like the alert system utilised by the Department of Homeland Security in the United States (US), would improve the utility of the Government's current threat intelligence services.
5. How can Government maintain trust from the Australian community when using its cyber security capabilities?	No comment.
6. What customer protections should apply to the security of cyber goods and services?	The *Privacy Act 1988* (Cth) and data protection generally are closely interlinked with consumer rights and consumer protection. On a broader note, the Transurban Group is of the view that the existing Schedule 2, Volume 3 *Competition and Consumer Act 2010* (Cth), also known as the Australian Consumer Law (ACL), can be extended to include the security of cyber goods and services, too, if not already.
7. What role can Government and industry play in supporting the cyber security of consumers?	The Transurban Group views cyber security as a shared responsibility between Government, industry and consumers. Accordingly, the Transurban Group endorses the Government's current model of acting in an advisory role to industry and taking part in raising industry and consumer security awareness. Opportunities to improve can be explored but the Transurban Group perceives that the existing roles are appropriately balanced.
8. How can Government and industry sensibly increase the security, quality and effectiveness of cyber security and digital offerings?	No comment.
9. Are there functions the Government currently performs that could be safely devolved to the private sector? What would the effect(s) be?	Privatisation of the timely and industry-specific threat intelligence sharing would have a minimal impact on industry. The Transurban Group makes this suggestion in reference to the American not-for-profit Information Technology-Information Sharing and Analysis Centre (IT-ISAC), which acts as a point of contact for on-demand operations, knowledge sharing and physical security for its members.
10. Is the regulatory environment for cyber security appropriate? Why or why not?	The Transurban Group is of the view that the existing Schedule 2, Volume 3 *Competition and Consumer Act 2010* (Cth), also known as the Australian Consumer Law (ACL), can be extended to include the security of cyber goods and services, too, if not already.
11. What specific market incentives or regulatory changes should Government consider?	The Transurban Group endorses the Government's investment in the start-up and cyber security scene. The Transurban Group especially wishes to endorse the work of Data61 and Australian Cyber Security Growth Network (AustCyber) in furthering Australian industry competitiveness.

12. *What needs to be done so that cyber security is 'built in' to digital goods and services?*	Voluntary accreditation or certification for digital goods and services with international standards would provide assurance of whether cyber security was 'built in' to digital goods and services. A combination of market-based and regulatory mechanisms could encourage cyber security by design. One example where a combination of market-based and regulatory mechanisms has improved cyber security is mandatory data breach notification in the Australian privacy law regime.
13. *How can we approach instilling better trust in ICT supply chains?*	Voluntary accreditation or certification for digital goods and services with international standards would provide assurance and sufficient information to consumers in order to allow industry and consumers to make informed decisions in relation to the cyber security of goods and services. In the Transurban Group's experience, during the Information and Communications Technology supply chain risk management process, it is common practice to refer to as many publicly available, reputable sources as possible, such as vulnerability databases, public data sets, international news and the Evaluated Products List. More specific information on supply chain risk management matters and guidance on the Government's use of certain products or vendors would be helpful.
14. *How can Australian governments and private entities build a market of high-quality cyber security professionals in Australia?*	Governments should continue to work together with industry to build cyber-related subjects into industry-based learning and to make industry-based learning in cyber security a nationally offered program at tertiary and TAFE-level. Further, cyber security subjects in secondary education, similar to the Israeli education system, should be considered. Additionally, governments should consider supporting more postgraduate cyber security research through grants. Minimum standards of knowledge for cyber security-related professions should be devised, similar to the work completed by the Department of Homeland Security in the US. This would provide a reference point and greater assurance when hiring candidates for industry.
15. *Are there any barriers currently preventing the growth of the cyber insurance market in Australia? If so, how can they be addressed?*	Insurance providers may need to draw on qualified data in order to accurately assess risk. Reliable public data sets in relation to cyber security topics would assist insurers as well as other stakeholders in assessing risk.
16. *How can high-volume, low-sophistication malicious activity targeting Australia be reduced?*	High-volume, low-sophistication malicious activity is an issue for all Australians and industry. Accordingly, the Transurban Group believes that better cyber security awareness and education, as well as the continuing existence of services like iDcare could assist in reducing the impact of these types of attacks.

17. What changes can Government make to create a hostile environment for malicious cyber actors?	Government should continue to conduct operational activities that raise the overall cost of attack to malicious cyber actors. This cost could be diplomatic, economic or other. Increased cyber security awareness in the Australian community would also make the target environment more robust.
18. How can governments and private entities better proactively identify and remediate cyber risks on essential private networks?	Since the Transurban Group views the role of governments in cyber security as advisory, the Transurban Group believes that the provision of a safe forum with "Chatham House" rules to share confidential information on threats and other matters of relevance could assist governments and industry to better identify and remediate cyber risks on essential private networks.
19. What private networks should be considered critical systems that need stronger cyber defences?	Essential service networks.
20. What funding models should Government explore for any additional protections provided to the community?	No comment.
21. What are the constraints to information sharing between Government and industry on cyber threats and vulnerabilities?	Timely and substantive information sharing is critical to effective incident response. Over the past year the Australian Cyber Security Centre (ACSC) has become more active in sharing threat intelligence, however the following improvements could be made: • timelier and industry-specific threat intelligence sharing, similar to the alert system utilised by the Department of Homeland Security in the US; • more learnings after the fact, such as what happened and what the lessons learned are; and • a more trusted forum, perhaps with "Chatham House" rules, for industry to safely voice their experiences in. The ACSC's OT forum is a current and working model that meets the needs described above.
22. To what extent do you agree that a lack of cyber awareness drives poor consumer choices and/or market offerings?	No comment.
23. How can an increased consumer focus on cyber security benefit Australian businesses who create cyber secure products?	If cyber security becomes an increased consumer focus, then businesses with a more cyber secure service or product offering would as a result become more competitive than businesses that are perceived to be less cyber secure. It may lead to an overall prioritisation of cyber security in production and service provision across Australia as well as additional side benefits.

24. What are examples of best practice behaviour change campaigns or measures? How did they achieve scale and how were they evaluated?	Some successful campaigns that made certain behaviours societally unacceptable and accordingly encouraged behavioural change are: • campaign against drunk driving; • campaign against speeding; • campaign against texting while driving; • campaign against smoking; and • health campaign, encouraging people to do a little bit every day. The Transurban Group feels that the use of emotional appeal (fear, curiosity, urgency) is effective in scaling and embedding the message into common social discourse. Also, nudging behaviour through intuitive design can be effective.
25. Would you like to see cyber security features prioritised in products and services?	Since the Transurban Group relies on third party products and services in order to operate its roads, the overall prioritisation of cyber security in products and services within this supply chain would benefit the Transurban Group.
26. Is there anything else that Government should consider in developing Australia's 2020 Cyber Security Strategy?	The Transurban Group predicts that in coming years, technological development will change the way its roads are used. Currently, an increasing number of standard vehicles are fitted with low levels of automation, such as adaptive cruise control and lane-keep assist. As the Transurban Group moves into the 2030s, Transurban expects the adoption rates of highly automated vehicles to increase significantly. This significantly changes the way users interact with roads and will increase the interconnectivity between users and roads, including the Transurban Group's roads. The Transurban Group is preparing for this transition and is committed to providing secure and reliable roads. Open standards and integrated security protocols would assist in this transition. Additionally, the 2020 cyber security strategy could consider the creation of a framework for continually assessing emerging technologies and their impacts on society including any cyber security implications.

-ENDS-

CONTACT

Acting Head of Cyber and Information Security

Andre Bertrand

Email [redacted]