Appendix A: List of questions to consider when making a submission

How to engage with us

We welcome responses to the questions consolidated below and any additional matters relevant to the Strategy by **29 August 2025**.

Please send any questions to:
CSSH2@homeaffairs.gov.au

Submissions should be made in PDF via the Horizon 2 Discussion Paper webform at:
homeaffairs.gov.au

This Discussion Paper is only the first step in our consultation on Horizon 2. There will be further opportunities to engage with us, including on the development of specific actions and initiatives to achieve these outcomes.

Please see our website **homeaffairs.gov.au** for a schedule of other engagement forums you can engage in to continue the discussion such as live online town halls.

List of questions to consider when making a submission to the Horizon 2 Public Discussion Paper

2. Developing our vision for Horizon 2

2.1 Outlook for Horizon 2

1. *What trends or technology developments will shape the outlook over the next few years and what other strategic factors should Government be exploring for cyber security under Horizon 2?*

2.2 Collaborating across all levels of Australian Government

2. *Are there initiatives or programs led by State or Territory governments you would like to see expanded or replicated across other levels of government?*

2.3 Monitoring progress in a changing world – a conceptual framework for evaluating cyber security outcomes

3. *Does the high-level Model resonate and do you have any suggestions for its refinement?*
4. *Can you suggest any existing or new ways to collect data and feedback to monitor these outcomes?*

3. Shield-level focus for Horizon 2

3.1 Shield 1: Strong businesses and citizens

5. *What could government to do better target and consolidate its cyber awareness message?*

6. *What programs or pilots have been successful in this context? What additional supports could be developed or scaled-up to address these issues in partnership with both education stakeholders and those with technical cyber security expertise?*

7. *How can Government encourage SMBs and NFPs to uptake existing cyber resources (i.e. Small Business Cyber Resilience Service, Cyber Wardens, ACNC guidance etc.)?*

8. *How can industry at all levels and government work together to drive the uptake of cyber security actions by SMEs and the NFP sector to enhance our national cyber resilience?*

9. *What existing or developing cyber security standards, could be used to assist cyber uplift for SMBs and NFP's?*

10. *What are the unique challenges that NFP entities face for cyber security compared to the broader business sector and what interventions from government would have the most impact in the NFP sector?*

11. *Do you consider cyber insurance products to be affordable and accessible, particularly for small entities? If not, what factors are holding back uptake of cyber insurance?*

12. *How well do you consider you understand the threat of ransomware, particularly for individuals and small entities? How is this threat evolving or changing?*

13. *How could the government further support businesses and individuals to protect themselves from ransomware attacks?*

14. *Have you experienced or researched any vulnerabilities or impacts from cyber security incidents that disproportionately impact your community, cohort or sector? If so, what were the vulnerabilities and impacts that your community faced?*

15. *How can support services for victims of identity crime be designed to be more effective in the context of increasing demand? and*

16. *Which regulations do you consider most important in reducing overall cyber risk in Australia?*

17. *Have regulatory/compliance requirements negatively impacted the cyber maturity of your organisation? How are you currently managing these issues?*

3.2 Shield 2: Safe technology

18. *What are best practice examples internationally that Australia should consider for enhancing our secure technology standards and frameworks? In particular, what approach do you consider would work best for edge devices, CER and operational technology?*

19. *How should the government work with you to support consumers and end-users to be more informed about cyber security in their products and protect themselves from cyber threats?*

20. *What additional guidance do you or your organisation need to manage foreign ownership, control or influence risks associated with technology vendors?*

21. *How could government better work with industry to understand data access and transfer across the economy to inform policies around secure data sharing and limit data exploitation from malicious actors?*

22. *Boosting innovation and economic prosperity is enabled when data is shared with trust and not accessed exploited by malicious actors (e.g. IP theft). How does Government and Industry work together to achieve this aim in an evolving global threat environment?*

23. *What guidance can government provide to support the safe and responsible uptake of critical and emerging technologies?*

3.3 Shield 3: World-class threat sharing and blocking

24. *What could government do to support and empower industry to take a more proactive cyber security posture to ensure the resilience of our cyber security ecosystem? What do you think Australia's proactive cyber security posture should look like for industry?*
25. *Does the government need to scope and define what Australia's proactive cyber security posture should look like for industry?*
26. *How could government further support industry to block threats at scale?*
27. *How could the use of safe browsing and deceptive warning pages be amplified?*
28. *What more is needed to support a thriving threat sharing ecosystem in Australia? Are there other low maturity sectors that would require ISACs, and what factors, if any, are holding back their creation?*
29. *How can we better align and operationalise intelligence sharing for cyber security and scams prevention?*
30. *Are the roles and responsibilities of government and industry clear for cyber security in a conflict or crisis scenario? What activities, such as cyber exercises, could Government undertake to make you feel better prepared to respond in a cyber conflict or crisis?*
31. *How could government better incentivise businesses to adopt vulnerability disclosure policies?*
32. *Does Australia need a vulnerability disclosure program to provide security researchers with a mechanism for safely reporting vulnerabilities?*

3.4 Shield 4: Protected critical infrastructure

33. *How effective do you consider the SOCI Act at protecting Australia's critical infrastructure? Are the current obligations proportionate, well-understood, and enforceable?*
34. *Are there significant cyber security risks that are not adequately addressed under the current framework?*
35. *Is the regulatory burden on industry proportionate to the risk and outcomes being sought?*
36. *What support would assist critical infrastructure owners and operators to mature their cyber and operational resilience practices? What role should government play in enabling uplift, including through tools, guidance or incentives?*
37. *How can the Australian Government support private sector partners to better engage with government security requirements, including certifications and technical controls?*
38. *How are Australian Government security requirements or frameworks being considered or adopted among private sector partners, including in critical infrastructure?*

3.5 Shield 5: Sovereign capabilities

39. *What role should government play in supporting the development and growth of Australia's cyber workforce? What initiatives, pilots or policy ideas do you think would best support industry to grow?*
40. *What have been the most successful initiatives and programs that support mid-career transitions into the cyber workforce and greater diversity in technology or STEM-fields more broadly?*
41. *What are some of the industries with highly transferrable skill sets that could be leveraged to surge into the cyber workforce? Is there any existing research/data that could support these efforts?*
42. *How can industry, academia, think tanks and government best work together to set research priorities and drive innovation to further our strategic, economic and community interests and achieve our common goals?*

43. *How can government and academia enhance its partnership and promote stronger people-to-people links and collaboration on research and policy development activities?*

44. *How would we best identify and prioritise sovereign capabilities for growth and development across government and industry?*

45. *What are the areas of most concern for ICT concentration and what do you consider would be most effective as mitigation strategies to explore?*

3.6 Shield 6: Strong region and global leadership

46. *Do you view attributions, advisories and sanctions effective tools for countering growing malicious cyber activity? What other tools of cyber diplomacy and deterrence would you like to see Australia consider for development and use to effectively combat these threats in Horizon 2?*

47. *Are there additional ways the Australian Government could engage with Southeast Asia or the Pacific to ensure a holistic approach to regional cyber security?*

48. *Is there additional value that Cyber RAPID can provide in the region beyond its current design and scope?*

49. *In which forums and on which issues would you like Australia to focus efforts to shape rules, norms and standards in line with its interests most effectively in Horizon 2?*

50. *What regulatory frameworks or requirements should be prioritised for consideration as part of Australia's efforts on international cyber regulatory alignment?*