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?** To make Australia the most cyber secure nation by 2030, the strategy should include the establishment of a dedicated cybersecurity commission, implementation of cybersecurity standards, regular monitoring and auditing of compliance, technical assistance and guidance for companies, third-party vendor management, mandatory reporting of significant cybersecurity incidents, protection of personal data, and continuous updating and revising of cybersecurity standards.

2. **What legislative or regulatory reforms should the Government pursue to: enhance cyber resilience across the digital economy?** The government should pursue reforms that establish a comprehensive cybersecurity framework, set mandatory cybersecurity standards for businesses, require the reporting of significant incidents, enforce penalties for non-compliance, and protect personal data.

    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)?** An appropriate mechanism for these reforms would be a combination of legislation and regulation. This would establish a solid legal foundation for mandatory operational cybersecurity standards, while also providing flexibility for adjustments as technology and threats evolve.

    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?** Yes, further reform to the Security of Critical Infrastructure Act is necessary. This should include expanding the definitions of critical assets to cover customer data and systems, ensuring that adequate cybersecurity measures are in place to protect these vital components of the digital economy.

    c. **Should the obligations of company directors specifically address cyber security risks and consequences?** Yes, the obligations of company directors should specifically address cybersecurity risks and consequences. This would emphasise the importance of cybersecurity in corporate governance and hold directors accountable for their organisations' cybersecurity posture.

    d. **Should Australia consider a Cyber Security Act, and what should this include?** Yes, Australia should consider a Cyber Security Act. It should include the establishment of a dedicated cybersecurity commission, mandatory cybersecurity standards for businesses, regular monitoring and auditing of compliance, technical assistance and guidance for companies, third-party vendor management, mandatory reporting of significant cybersecurity incidents, protection of personal data, and continuous updating and revising of cybersecurity standards.

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 establish a monitoring system to assess the regulatory burden on businesses due to legal obligations in cybersecurity. This could include regular consultations with industry stakeholders, collecting feedback from businesses, and conducting impact assessments. Opportunities to streamline existing regulatory frameworks may arise through the consolidation of requirements, simplification of reporting processes, and the provision of clear guidance to businesses.

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?** The government should consider prohibiting the payment of ransoms and extortion demands by both victims of cybercrime and insurers, as it can encourage further criminal activity. Exceptions could be made in cases where non-payment could result in severe consequences, such as loss of life or significant harm to public safety.

    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?** A strict prohibition would put increased pressure on victims, companies, and insurers to invest in robust cybersecurity measures and incident response plans. While it might cause short-term challenges, in the long run, it could lead to a more secure digital ecosystem and discourage cybercriminals from pursuing ransomware attacks. However, there may be instances where the prohibition could cause significant distress or financial harm to victims if they are unable to recover their data or restore their systems.

g. **Should Government clarify its position with respect to payment or nonpayment of ransoms by companies, and the circumstances in which this may constitute a breach of Australian law?** Yes, the government should clarify its position on payment or nonpayment of ransoms by companies. This would provide clear guidance to organisations and help them understand the legal implications of their actions in the event of a ransomware attack.

3. **How can Australia, working with our neighbours, build our regional cyber resilience and better respond to cyber incidents?** Australia can work with its neighbours to build regional cyber resilience by sharing threat intelligence, collaborating on joint cybersecurity initiatives, conducting joint cyber exercises, and providing technical assistance and capacity-building support. This cooperation would help the region better respond to cyber incidents and enhance collective defence against cyber threats.

4. **What opportunities exist for Australia to elevate its existing international bilateral and multilateral partnerships from a cyber security perspective?** Australia can elevate its existing international partnerships by actively participating in cybersecurity forums, collaborating on joint research and development projects, engaging in information sharing, and promoting the adoption of best practices and cybersecurity standards across its partnerships. This would help strengthen global cybersecurity and build a more secure digital environment.

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 cyberspace?** Australia should actively participate in international standards-setting processes by contributing expertise, resources, and best practices. This includes engaging in forums such as the International Organization for Standardization (ISO) and International Telecommunication Union (ITU). Additionally, Australia should work with other nations to develop and promote laws, norms, and standards that uphold responsible state behaviour in cyberspace, such as preventing cyber espionage and cyber attacks on critical infrastructure.

6. **How can Commonwealth Government departments and agencies better demonstrate and deliver cyber security best practice and serve as a model for other entities?** Commonwealth Government departments and agencies can better demonstrate and deliver cybersecurity best practices by implementing robust cybersecurity measures, regularly assessing their security posture, investing in employee training, and actively participating in information sharing with other organisations. By consistently adhering to high standards of cybersecurity, they can serve as a model for other entities to follow.

7. **What can government do to improve information sharing with industry on cyber threats?** The government can improve information sharing with the industry by establishing dedicated communication channels, promoting the use of threat intelligence platforms, organising regular cybersecurity briefings, and providing timely alerts about emerging cyber threats. This will enable businesses to stay informed and better protect themselves against cyber attacks.

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 upon the ASD/ACSC would likely improve engagement with organisations during a cyber incident. This assurance of confidentiality would encourage businesses to share information more openly without fearing that the information will be shared with regulators, leading to a more effective response and mitigation of cyber threats.

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?** Yes, expanding the existing regime for notification of cybersecurity incidents to include mandatory reporting of ransomware or extortion demands would improve public understanding of the nature and scale of these cybercrimes. This increased transparency would help raise awareness and encourage better preparedness and response efforts among organisations.

10. **What best practice models are available for automated threat-blocking at scale?** Best practice models for automated threat-blocking at scale include the use of intrusion prevention systems (IPS), advanced firewall configurations, distributed denial-of-service (DDoS) protection services, and machine learning-based threat detection systems. These technologies can help organisations proactively block threats and minimise their exposure to cyber risks.

11. **Does Australia require a tailored approach to uplifting cyber skills beyond the Government's broader STEM agenda?** Yes, Australia requires a tailored approach to uplifting cyber skills beyond the broader STEM agenda. This includes investing in cybersecurity education programs, offering specialised training and certifications, and promoting cybersecurity as a rewarding career path. A focused effort on developing cyber skills will help build a robust cybersecurity workforce capable of addressing the growing cyber threat landscape.

12. **What more can the Government do to support Australia's cyber security workforce through education, immigration, and accreditation?** The government can support Australia's cybersecurity workforce by providing funding for cybersecurity education programs, offering scholarships and incentives for students pursuing cybersecurity studies, attracting international talent through immigration policies, and establishing accreditation programs for cybersecurity professionals. These initiatives will help develop a skilled workforce and strengthen the nation's cybersecurity capabilities.

13. **How should the government respond to major cyber incidents (beyond existing law enforcement and operational responses) to protect Australians?** The government should respond to major cyber incidents by coordinating multi-agency efforts, providing timely public communication about the incident, offering support and resources to affected organisations, and engaging with international partners to address cross-border cyber threats. This comprehensive approach will ensure a coordinated and effective response to protect Australians from the impact of major cyber incidents.

    a. **Should the government consider a single reporting portal for all cyber incidents, harmonising existing requirements to report separately to multiple regulators?** Yes, the government should consider a single reporting portal for all cyber incidents. This unified system would simplify the reporting process for organisations and streamline the flow of information, enabling a more efficient and coordinated response to cyber threats.

14. **What would an effective post-incident review and consequence management model with industry involve?** An effective post-incident review and consequence management model with the industry would involve a collaborative approach between government and affected organisations to assess the incident, identify lessons learned, implement necessary changes, and share best practices with other organisations. This process would help improve the overall cybersecurity posture of the industry and reduce the likelihood of similar incidents in the future.

15. **How can government and industry work to improve cyber security best practice knowledge and behaviours, and support victims of cybercrime?** Government and industry can work together to improve cybersecurity best practices and support victims of cybercrime by promoting awareness campaigns, providing resources and tools for organisations to strengthen their security posture, and offering assistance to victims through dedicated helplines, financial support, and guidance on recovery efforts.

    a. **What assistance do small businesses need from government to manage their cyber security risks to keep their data and their customers' data safe?** Small businesses need assistance from the government in the form of accessible cybersecurity resources, training, and guidance on best practices. This includes providing affordable tools and services tailored to small businesses, offering workshops and training programs, and establishing a support network to help small businesses manage their cybersecurity risks effectively.

16. **What opportunities are available for the government to enhance Australia's cyber security technologies ecosystem and support the uptake of cyber security services and technologies in Australia?** Opportunities for the government to enhance Australia's cyber security technologies ecosystem include investing in research and development, providing financial incentives for cybersecurity startups, creating public-private partnerships, and supporting the commercialization of cybersecurity innovations. These initiatives will foster a vibrant cybersecurity ecosystem and encourage the adoption of cutting-edge technologies in Australia.

17. **How should we approach future proofing for cyber security technologies out to 2030?** Future proofing for cyber security technologies should involve continuous investment in research and development, nurturing a skilled cybersecurity workforce, fostering public-private collaborations, and staying ahead of emerging threats through regular assessment and updates of cyber security standards and practices. This proactive approach will ensure Australia remains resilient against evolving cyber threats.

18. **Are there opportunities for the 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?** Yes, the government can leverage procurement to support the Australian cyber security ecosystem by prioritising Australian cyber security firms for government contracts, setting minimum cybersecurity standards for procured products and services, and incentivizing the adoption of local cybersecurity solutions. These strategies will create a viable path to market for Australian firms and bolster the domestic cyber security ecosystem.

19. **How should the Strategy evolve to address the cyber security of emerging technologies and promote security by design in new technologies?** The Strategy should evolve by keeping pace with emerging technologies, integrating security by design principles, and fostering collaboration between government, industry, and academia. This will ensure that new technologies are developed and adopted with cybersecurity considerations in mind, reducing vulnerabilities and strengthening overall cyber resilience.

20. **How should the government measure its impact in uplifting national cyber resilience?** Government can measure its impact in uplifting national cyber resilience by tracking key performance indicators (KPIs) such as the reduction in the number of cyber incidents, improvements in organisational compliance with cybersecurity standards, increased adoption of cyber security technologies, and growth in the cybersecurity workforce. These metrics will help assess the effectiveness of government initiatives in enhancing national cyber resilience.

21. **What evaluation measures would support ongoing public transparency and input regarding the implementation of the Strategy?** Evaluation measures to support public transparency and input in the implementation of the Strategy include regular public reporting of progress and performance against KPIs, open consultations with stakeholders, and the establishment of feedback channels for the public to provide input and suggestions. This transparency and engagement will ensure that the Strategy remains relevant and effective in addressing the evolving cybersecurity landscape.