# Australian Cyber Security Strategy Discussion Paper

# Response & Comments

**Author:**

**Dated:**

**Contact**:

**Advice on how to respond:**

* **Be specific** – make sure what you argue is based on facts, figures, and direct experience – provide references and context.
* **Demonstrate net benefits** – again prove with facts, figures, and direct experience.
* **Do not assume the reader has a cyber security background** – avoid using jargon without explaining, give plenty of examples.
* **Make sure each answer stands on its own** – it’s quite likely different people will read different answers.

**Post to auscyberstrategy@homeaffairs.gov.au by COB 15 April 2023.**

## Priorities for the 2023-2030 Australian Cyber Security Strategy

**Enhancing and harmonising regulatory frameworks**

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

**Strengthening Australia’s international strategy on cyber security**

*How can Australia, working with our neighbours, build our regional cyber resilience and better respond to cyber incidents? What opportunities exist for Australia to elevate its existing international bilateral and multilateral partnerships from a cyber security perspective? 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?*

**Securing government systems**

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

**Improving public-private mechanisms for cyber threat sharing and blocking**

*What can Government do to improve information sharing with industry on cyber threats? What best practice models are available for automated threat-blocking at scale?*

**Supporting Australia’s cyber security workforce and skills pipeline**

*Does Australia require a tailored approach to uplifting cyber skills beyond the Government’s broader STEM agenda? What more can the Australian Government do to support Australia’s cyber security workforce through education, immigration, and accreditation?*

**National frameworks to respond to major cyber incidents**

*How should the Government respond to major cyber incidents (beyond existing law enforcement and operational responses) to protect Australians? How can Government and industry work to improve cyber security best practice knowledge and behaviours and support victims of cybercrime? What would an effective post-incident review and consequence management model with industry involve?*

**Community awareness and victim support**

*How can Government and industry work to improve cyber security best practice knowledge and behaviours and support victims of cybercrime?*

**Investing in the cyber security ecosystem**

*What opportunities are available for Government to enhance Australia’s domestic cyber security technologies ecosystem and support the uptake of cyber security services and technologies in Australia?*

*How should we approach cyber security technologies future-proofing out to 2030?*

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

**Designing and sustaining security in new technologies**

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

**Implementation governance and ongoing evaluation**

*How should Government measure its impact in uplifting national cyber resilience? What evaluation measures would support ongoing public transparency and input regarding the implementation of the Strategy?*

## Appendix A - Detailed Questions:

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?**
2. **What legislative or regulatory reforms should Government pursue to: enhance cyber resilience across the digital economy?** 
   1. 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)?
   2. 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?
   3. Should the obligations of company directors specifically address cyber security risks and consequences?
   4. Should Australia consider a Cyber Security Act, and what should this include?
   5. 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?
   6. 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?
      1. What impact would a strict prohibition of payment of ransoms and extortion demands by cyber criminals have on victims of cybercrime, companies and insurers?
   7. 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?
3. **How can Australia, working with our neighbours, build our regional cyber resilience and better respond to cyber incidents?**
4. **What opportunities exist for Australia to elevate its existing international bilateral and multilateral partnerships from a cyber security perspective?**
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?**
6. **How can Commonwealth Government departments and agencies better demonstrate and deliver cyber security best practice and serve as a model for other entities?**
7. **What can government do to improve information sharing with industry on cyber threats?**
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?**
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?**
10. **What best practice models are available for automated threat-blocking at scale?**
11. **Does Australia require a tailored approach to uplifting cyber skills beyond the Government’s broader STEM agenda?**
12. **What more can Government do to support Australia’s cyber security workforce through education, immigration, and accreditation?**
13. **How should the government respond to major cyber incidents (beyond existing law enforcement and operational responses) to protect Australians?**
    1. Should government consider a single reporting portal for all cyber incidents, harmonising existing requirements to report separately to multiple regulators?
14. **What would an effective post-incident review and consequence management model with industry involve?**
15. **How can government and industry work to improve cyber security best practice knowledge and behaviours, and support victims of cybercrime?**
    1. What assistance do small businesses need from government to manage their cyber security risks to keep their data and their customers’ data safe?
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?**
17. **How should we approach future proofing for cyber security technologies out to 2030?**
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?**
19. **How should the Strategy evolve to address the cyber security of emerging technologies and promote security by design in new technologies?**
20. **How should government measure its impact in uplifting national cyber resilience?**
21. **What evaluation measures would support ongoing public transparency and input regarding the implementation of the Strategy?**