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?

   a. Defend all sections of government, industry, and academia as one.

   b. Use legislation and regulatory guidance to establish laws, and standards which will allow government, critical infrastructure, industry, and academia to hastily react and stay pace with changes in cyber.

   c. Develop the right cyber security skillset and culture nationally.

2. What legislative or regulatory reforms should Government pursue to: enhance cyber resilience across the digital economy?
   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)? This should be a combination of legislation, regulation, or further regulatory guidance. Legislation statue designed to state what is a cyber crime and how it should be handled. Regulation or regulation reform to promote openness and sharing of information between Inter-government, industry, and academia. Regulatory guidance on what protocols, standards and frameworks can enhance cyber security posture, and best practice implementation.
   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? The definition should only extend to customer data and systems if the customer data and system are part of the critical infrastructure itself, and is required for proper operation of the critical infrastructure.
   c. Yes
   d. No comment provided
   e. No comment provided
   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? Government should not prohibit private citizens from making such payments, but should advise them of their options. However, if the ransoms and extortion demands are related or tied to a government employee, system, or process then the government should have the option to prohibit payment.
3. How can Australia, working with our neighbors, build our regional cyber resilience and better respond to cyber incidents? Establish international laws in the region that transcend physical boarders to aid cyber-crime investigations. Establish binding agreements to work with each other on cyber security related operations to strengthen sovereign and regional security posture. Perform periodical exercises to practice, build trust, and improve on areas of weakness. These things will help with building cyber resilience and better response to cyber incidents.
4. What opportunities exist for Australia to elevate its existing international bilateral and multilateral partnerships from a cyber security perspective? There are public-private partnership cybersecurity opportunities, international formalized bilateral cyber partnership – like the one between the US, and Israel. Through such partnerships there is the opportunity to conduct bi-lateral and multilateral

military cyber exercise to strengthen the nations cyber defenses and improve it cybersecurity posture.

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 behavior in cyber space? There are several Cybersecurity consortiums organizations which are dedicated to the international standards-setting processes in relation to cyber security. These consortiums transcend borders and provide partnerships, knowledge sharing and many other benefits to the international cyber community.
6. How can Commonwealth Government departments and agencies better demonstrate and deliver cyber security best practice and serve as a model for other entities? All six states and federal government should be working from the same script. Which means they should follow approved government guidelines for how to execute on matters of cybersecurity. Government should also explicitly outline what information can be shared and how it should be handled, and based on the circumstances, which authorities are in-charge. This should also include international agreements with allied countries.
7. What can government do to improve information sharing with industry on cyber threats? Policy-wise, establish agreements with rules for what can be shared, sensitivity levels, circumstances, and authorities. Technical-wise, ensure there are secure means to guarantee the confidentiality, Integrity, and availability of the information being shared, and that any data shared will continue to be safe when at rest.
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 organizations that experience a cyber incident so as to allow information to be shared between the organization and ASD/ACSC without the concern that this will be shared with regulators? An explicit obligation of confidentiality will build trust, and promotes inter-agency information sharing, which are both good things in the event of a cyber 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? Yes, it would improve the public's awareness and understanding, but it should not be made mandatory. Victims of this type of crime are sometimes ashamed and embarrassed and should be allow to report as they seem fit without penalty.
10. What best practice models are available for automated threat-blocking at scale? Intelligence blocking built into technology like SD-WAN which learn network traffic and applications behavior to automate blocking attacks has been the latest industry trend. There are a number of product that implement this type of gateway security, but this is the method by which it is executed.
11. Does Australia require a tailored approach to uplifting cyber skills beyond the Government's broader STEM agenda? With over AU$1 billion invested, the Government's broader STEM agenda seems sufficient. However, the program should not be limited to those seeking STEM degrees or in STEM studies. There should be other incentivize programs in place to identify those with the aptitude for cyber.
12. What more can Government do to support Australia's cyber security workforce through education, immigration, and accreditation? Start STEM training in early childhood, incentivize more cyber

professional to stay or migrate to Australia to work or teach the next generation of cyber professionals.

13. How should the government respond to major cyber incidents (beyond existing law enforcement and operational responses) to protect Australians?
    a. Should government consider a single reporting portal for all cyber incidents, harmonizing existing requirements to report separately to multiple regulators? There should a single reporting portal for all cyber incidents with proper access controls for the organizations which need access. This will ensure a single source of truth, and less confusion. This also helps with inter-agency collaboration.
14. What would an effective post-incident review and consequence management model with industry involve? Working with a group like MITRE and its MITRE ATTACK framework, a good model would involve following the cyber kill-chain to identify the actions that addressed each of the issues that allowed the threat actor to succeed. This collection of data can then be use to strengthen the organization's security posture.
15. How can government and industry work to improve cyber security best practice knowledge and behaviors, and support victims of cybercrime? a. What assistance do small businesses need from government to manage their cyber security risks to keep their data and their customers' data safe? Government can make cybersecurity cost more manageable for small business. By allowing for effective but variance in the way cybersecurity measures is deployed by small businesses. Essentially, cybersecurity regulations cannot be so cumbersome to small business that they become a financial burden. Instead, they must enable small business to mitigate cybersecurity risks and keep their data and customer's data safe, while turning a profit.
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? Cybersecurity technologies must be developed to a standard where software is agnostic of the hardware and vice versa. The data and protocols should be what matters the most and cybersecurity solutions must be interoperable with any data set or protocol. Also, develop a fast and agile framework for procurement of cybersecurity technologies. There are consequences for having a slow process for procurement as cybersecurity requires quick action.
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? Yes, first, identify systematic risks in government supply chain and implement and acquisition strategy to deal with the risks. The government should mandate an acquisition and design strategy that prioritize the use of open standards-based technology for cybersecurity technologies. The Government should also ensure it does not constraint its cybersecurity firms with unrealistic compliance protocols which cause overspending and go to market slow-down.
19. How should the Strategy evolve to address the cyber security of emerging technologies and promote security by design in new technologies? The strategy must have some flexibility built into its implementation. It should evolve over time with strong governance, a standardized procurement strategy with enhance supply chain pipeline security, a meaningful evaluation framework to ensure compliance is being met, collaborative ventures with academia and industry to address current and new challenges, and consistent readiness testing of the establish cybersecurity criteria. Lessons

learned from these parts should be evaluated and used to improve and evolve the cyber security strategy.

20. How should government measure its impact in uplifting national cyber resilience? Government should Identify its critical systems and infrastructure to include any mission data that are critical to the economy and national security. Establish a baseline security posture by assessing its current state to the adopted cybersecurity framework. Measure periodically to ensure compliance and improved cybersecurity posture are being achieved, and that the goals of the cybersecurity strategy are being met. In conjunction, government should also use KPIs that pull from the strategy's objectives and will guide the delivery of the strategy.
21. What evaluation measures would support ongoing public transparency and input regarding the implementation of the Strategy? The evaluation measures should be a phased approached highlighting short-term, medium-term, and long-term initiatives as they relate to the spending plan. Periodical review is required to ensure spending towards initiatives are continuously aligned to the overall strategic plan. This will ensure that the strategic goals are being met within budget.

Prepared by Marlon Walker
Principle Security Strategist
Global Government and Critical Infrastructure, Forcepoint