Australian's 2020 Cyber Security Strategy Questions	QGCIO's responses
What is your view of the cyber threat environment? What threats should Government be focusing on?	Skills shortage and workforce, critical infrastructure, extreme threats (nation state). Should focus on threats which have significant consequence to the economy and population.
Do you agree with our understanding of who is responsible for managing cyber risks in the economy?	Partially agree. The Constitution is fairly clear in allocating responsibility for telecommunications s51(v) to the federal government.
Do you think the way these responsibilities are currently allocated is right? What changes should we consider?	No, clarifying roles and accountabilities.
What role should Government play in addressing the most serious threats to institutions and businesses located in Australia?	Advisory and support, further the role should reflect the role that is played when analogous threats are affected upon organisations in the physical world.
How can Government maintain trust from the Australian community when using its cyber security capabilities?	Transparency, consistent communication, clearly documented and defined processes for ensuring accountability of security agencies. Federal Government needs to clarify when it will share information that will protect Australians at the expense of its intelligence priorities.
What customer protections should apply to the security of cyber goods and services?	Australia has a small population and a middle sized trading nation. It should adopt and promote international standards rather than developing its own. Review and adopt cyber standards for consumer cyber goods and services.
What role can Government and industry play in supporting the cyber security of consumers?	Government should develop a purchasing program to ensure that it uses its purchasing power to only buy goods and services that have met cybersecurity 'tick of approval'. The program should encourage ASX100 companies to participate as well. The 'tick' should be based on meeting minimum international standards.
How can Government and industry sensibly increase the security, quality and effectiveness of cyber security and digital offerings?	Increased participation in international standards process, rewarding adherence to standards, procurement controls and mandates.
Are there functions the Government currently performs that could be safely devolved to the private sector? What would the effect(s) be?	Cyber exercises, consumer minimum security standards (Choice model).
Is the regulatory environment for cyber security appropriate? Why or why not?	No - lack of enforceable legislation for government mandates for minimum standards.
What specific market incentives or regulatory changes should Government consider?	Procurement preference for cyber secure goods and services, panel contract arrangements, strengthening privacy regulations and penalties.
What needs to be done so that cyber security is 'built in' to digital goods and services?	Government needs to create the market and incentive to provide G&S that meets minimum standards. It doesn't need to be perfect (that would be too expensive) it needs to be good.
How could we approach instilling better trust in ICT supply chains?	Legislate a third party compliance framework. Could fund/support test cases in courts to establish liability as an amicus curiae
How can Australian governments and private entities build a market of high quality cyber security professionals in Australia?	Standardize on minimum standards for education and experience. Clarify exactly what their needs are. Cybersecurity is many disciplines, not just one. There are very few people who are expert in all areas. Organisations will generally require people with a mix of skills.
Are there any barriers currently preventing the growth of the cyber insurance market in Australia? If so, how can they be addressed?	The biggest disincentive to the use of cyber insurance has been insurance companies not paying on breaches because the malware allegedly came from an intelligence agency and therefore the breach was an act of war and exempt. Insurance companies being insurance companies, competing with government insurance funds.
How can high-volume, low-sophistication malicious activity targeting Australia be reduced?	Fundamental security controls (E8), enhanced awareness programs, consumer cyber security product standards. Promote the use of a consumer friendly version of the ACSC Top 4. Minimum standards for the sale of IOT devices based on international standards and policed by ACCC.
What changes can Government make to create a hostile environment for malicious cyber actors?	Working with other countries to put pressure on rogue states that support cybercrime. Similar to the work in OECD to minimise tax havens. Offensive security measures, hack back.
How can governments and private entities better proactively identify and remediate cyber risks on essential private networks?	Legislate minimum standards.
What private networks should be considered critical systems that need stronger cyber defences?	Telco's, banking, health care, water, power, transport, Trusted Information Sharing Network (TISN) defined CI areas, emergency services.
What funding models should Government explore for any additional protections provided to the community?	Performance based Cyber Security Budget (at beginning only partial or to achieve outcomes of this strategy). Performance-based budgeting lies beneath the word "result". In this method, the entire planning and budgeting framework is result oriented. There are objectives and activities to achieve these objectives and these form the foundation of the overall evaluation. As the consumer economy moves online, policing will need to increase. Federal Govt has the responsibility under the constitution.

What are the constraints to information sharing between Government and industry on cyber threats and vulnerabilities?	Uniform Information Security Classification and applicability of security controls associated with relevant classification level. Therefore, ability to protect and offer assurance to protect sensitive data/information as per custodian's/owner's expectations across any area that may come in to contact with data. Minimum personnel vetting to the same levels across industry and therefore ensuring that sensitive data/information doesn't find its way to someone that it shouldn't. E.g. Federal government vetting doesn't match State or private organisation's vetting that may hires people from overseas on working visas. Federal Government needs to work harder to reduce Over-Classification as this restricts sharing of information that can be used to protect organisations. The decision on what information gets released needs to be taken out of the hands of the Defence and Intelligence agencies so that the risks of not sharing with the public are adequately considered.
To what extent do you agree that a lack of cyber awareness drives poor consumer choices and/or market offerings?	To some but limited degree. There has to be consumer information available firstly before one can make a choice about the product. For example very few IoT, toys or medical devices with RF technology offerings offer information how secure it is. There needs to be a system that clearly shows level of cyber risk. Very few customers will perform vulnerability, penetration and risk analysis themselves. Perhaps something similar to energy rating on white goods. Refer comments about international standards. Customers are unable to make choices if they are not able to get the information they require.
How can an increased consumer focus on cyber security benefit Australian businesses who create cyber secure products?	Legislation and certification programs similar to these run by the European Union (EU) and United States of America (USA) to provide them with economic advantage in these countries or areas of the world. Promoting the adoption of level playing fields will assist Australian export competitiveness as we can compete on quality of product - rather than a race to the bottom in terms of cost.
What are examples of best practice behavior change campaigns or measures? How did they achieve scale and how were they evaluated?	The best practice behavior change programs are seen in the area of preventative health. Examples are Quit Smoking and Slip, Slop, Slap (sun) The lessons are that the message needs to be simple, clear, have a call to action and be repeated regularly at all levels.
Would you like to see cyber security features prioritized in products and services?	Yes or if there are minimum standards, then it doesn't need to be much more than that.
Is there anything else that Government should consider in developing Australia's 2020 Cyber Security Strategy?	Increased cooperation with all the states and territories but above all, other countries like the US and EU on technical and governance levels. Utilizing their economies of scale and practices while sharing ours. The threats to Australian organisations come mostly from overseas. The vulnerabilities to Australian organisations come mostly from overseas made products. The solutions must come from working with overseas governments and multilateral organisations. The cyber threat is much like piracy in the 1600s. We need something like a cyber version of the international laws of the sea to counter the threats.

https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/cyber-security-strategy-2020/submission-form