AUSTRALIA'S 2020 CYBER SECURITY STRATEGY

RSA is pleased to provide the following inputs to the Australian 2020 Cyber Security Strategy document. We have selectively provided suggestions and feedback to questions we thought appropriate for our response. The document is well thought out and comprehensive and should provide relevant inputs to help Australia raise its overall cybersecurity posture in 2020 and beyond.

1. **What is your view of the cyber threat environment? What threats should Government be focused on?** The cyber threat around the globe endangers freedoms, economic growth and national security for all nations. So much of the world's business, government, and communications functions rely wholly on the internet to function. This is a double-edged sword, in that the continued digital adoption and transformation of business functions necessitates a cybersecurity review and risk management approach to ensure they are safely executed. Current investments and strategies in protecting information and information systems around the globe is not yet keeping pace with the threats faced. RSA would recommend that Australia apply resources to threats that endanger: government/Defense, energy, telecommunications, transportation, and financial sectors (all critical infrastructure).

   There currently does not exist a ratified operational plan for the management and execution of national cyber security incidents. When it comes to critical infrastructure, this will be significant in being able to defend, protect and recover from such events. The specific threats are wide and varied but range from simple DDOS attacks to intricate spear phishing attacks on local government employees. A digital risk management prioritization of the application of limited resources will focus on five areas: Identity assurance; improved cyber hygiene, network visibility, forensics and resiliency.

2. **Do you agree with our understanding of who is responsible for managing cyber risks in the economy?** Yes. We believe that the government / industry (those who have resources to scale across the country) play and should continue to play a very strong role in providing for mechanisms for everyone to be successful using the internet. Additionally, we recommend ensuring accountable individuals are resourced sufficiently to achieve success. We also recommend more centralized management and oversight of the cybersecurity challenge in Australia. The government is uniquely positioning to oversee standards, execution and priorities for this now ubiquitous tool.

3. **Do you think the way these responsibilities are currently allocated is right? What changes should we consider?** Yes. Although, government and industry possess resources to improve the country's cybersecurity ecosystem, whereas the population does not. The future actions and expectations do need to account for the citizen population as a major component. For example, cybersecurity research and development activities conducted by both government and industry should be aimed at bettering organizations and individuals alike. Additionally, we recommend ensuring accountable individuals (those charged with this task) are resourced sufficiently to achieve success. Lastly, accountable organizations as well as critical infrastructure components, should possess a network of resilience and back up in order to provide necessary services during and after cyber events.

4. **What role should government play in addressing the most serious threats to institutions and businesses located in Australia?** We believe that the government should: establish standards of performance and behavior and for security of network systems commensurate with the criticality of the system to the nation. This framework will ensure that necessary risk management actions can be planned, developed, deployed and maintained and can also assist in most efficient use of resources. The government can also decide when national security is at risk, and when government resources will be brought to bear on a cyber related incident in industry. Government must consider how it helps to protect both large and small institutions/businesses as smaller organizations cannot afford a full suite of cybersecurity protections.

5. **How can Government maintain trust from the Australian community when using its cyber capabilities?** This trust is only delivered through consistent demonstrations of the highest ideals of Australian society. Additionally, we believe that legislative/policy restrictions must be in place to ensure that cyber capability usage is framed in a way to the population such that absent a criminal act that warrants requiring the use of these capabilities, the population's trust is earned and kept. Privacy of the citizen population is of utmost importance.

6. **What customer protections should apply to the security of cyber good and services?** Customers should be afforded reasonable assurance that the products they purchase will perform as advertised. Effecting a "Seal of approval" from a qualified laboratory could be a way to deliver some level of assurance that the end item will perform as advertised. Provision of cyber security good and services could come under a licensing structure. Adopting a leaf from the Singapore Cybersecurity Act, where they require the providers of certain cyber security services to be licensed. This will go a long way to ensuring a required standard and capability is considered.

7. **What role can government and industry play in supporting the cybersecurity of consumers?** We believe that industry can help the population be providing easy to use tools supporting internet-based commerce. Government can leverage industry best practices in identity management/multi-factor authentication, encryption, and other technologies that provide surety to the consumer regarding the transactions. Additionally, government can institute education for the internet starting at in elementary schools and completing in secondary school. How to engage the internet securely, has become as important as reading, writing, and mathematics.

8. **How can government and industry sensibly increase the security, quality and effectiveness of cybersecurity and digital offerings?** We believe that the government can take several actions in this area. First, the government may establish an approved products list which contains those products acceptable for use. Second, government can sponsor cyber ranges where architectures and tools can be exercised (simulating key environments from the sectors listed above) data to demonstrate capabilities in a contested environment.

9. **Are their functions the Government currently performs that could be safely devolved to the private sector? What would the effects be?** Absolutely, industry could be tapped to provide more cybersecurity services on behalf of the Government as a managed security service. The Government would need to establish levels of service levels, incentives and penalties associated with specific work packages. In buying a service from a cybersecurity industry, the government would always have the latest tools is it's no longer buying an end items, but rather a capability. The effects should be mostly transparent to the Government and result in more effective service delivery.

10. **Is the regulatory environment for cyber security appropriate? Why or why not?**

11. **What specific market incentives or regulatory changes should Government consider?**

12. **What needs to be done so that cyber security is build in to digital good and services?** Legislative, policy and regulation are required to affect this level of change. However, these requirements will come with an added cost for the end item and that increase must be considered. When it comes to cybersecurity goods, there are few suggestions: Commodity products should come 'out-of-the-box' closed. That is only upon installation are the necessary configurations undertaken to open such things as specific ports and/or services. Purchase of such products should be made aware of the required level of competency for the installation of such products. Much the same of electrical products and

components such as wall sockets etc. These require licensed persons to perform the installation. Providers of good/products need to implement a higher level of security into especially commodity products. This could be by way of a standard for production. Such a standard could include for example, products should not have hard coded passwords into the admin console and vendors should be required to provide notifications of new vulnerabilities and patches in a timely manner.

13. **How could we approach instilling better trust in ICT supply chains?** Supply Chain Management must be a focus of the Government to instill regulations and policy that supports a trusted ICT environment. Procurements of ICT hardware and software should perform to design expectations…possessing and upper and lower control limit for performance…with no functionality than planned. This can be achieved with detailed quality control procedures as well as implementing functional lot testing programs. Expectations are that whatever comes up on a computer screen (for nearly every citizen) is generally implicitly trusted. Recognize that most CI is underpinned by ICT and technology these days and growing. With the majority of CI owned by the private sector, there needs to a considered and balance approach between Government and the private sector around cybersecurity. An unduly heavy hand by Government risk that the private sector will abdicate leaving Government to shoulder most of the work and responsibility. Agree with the point around funding to provide such services in supporting sustainable services to these critical systems. The focus should be on cost recovery. Additionally, the government should consider requiring Supply Chain Risk Management practices be part of ICT procurements (for both government and industry), thereby ensuring that this facet of cybersecurity (which represents industry best practices) is executed.

14. **How can Australian Governments and private entities build a market of high-quality cyber security professionals in Australia?** In 2019, there is a worldwide shortage of cybersecurity professionals. Given that inequity between supply and demand, an few options remain to be successful. First, develop a comprehensive plan of what/how many skills are needed. Two, initiate education programs as referenced above as early as possible and incentivize colleges to offer associate, bachelor, and advanced degrees. Incentivize participants in the programs through jobs and pay. The strategy proposes and expansion of Government functional roles. While admirable, the reality is that Government continues to struggle to attract and retain good cyber folk. There needs to be a concerted focus on how to address this problem to enable Government to effectively compete for these scare resources. Arguably the cyber security industry is fast developing into a 'professional' industry. Consideration should be given to minimum education standards for identified roles within the industry, much like other professional industries such as Law, Accounting, Medicine, etc. In many cases, cyber leads for organizations (both public sector

and non-public sector) sadly lack the necessary education, knowledge and experience i.e. time at the coal face, that goes into making a competent and well-rounded leader in cyber security.

15. **Are there any barriers currently preventing the growth of the cyber insurance market in Australia?**

16. **How can high volume, low-sophistication malicious activity targeting Australia be reduced?** Capabilities to detect malicious behavior crossing the borders as well as emanating from in Australia should be enhanced to minimize the low-sophistication threats. Enhancement of the statistical information for data breaches by way of incorporation of healthcare data breaches would provide a more comprehensive view on the state of data breaches. As it stands, Healthcare data breaches are reported separately. Additionally, it has been noted that of the reported breaches, there has not been a single instance of public sector entities. This is particularly curious when looking at other industry reports e.g. Verizon's Data Breach Investigations report and the UK Office of the Information Commissioner – where both have recorded instances of public sector entities. Are Australian public sector agencies that good?

17. **What changes can government make to create a hostile environment for malicious cyber actors?** The government can create a 5-10-year plan to invest in and grow the cyber security defense capabilities of the government and share with the ICT industry. Law enforcement needs to be equipped with enough resources and authorities to investigate and punish offenders. Expanding partnerships with global allies for information sharing, cyber solutions and prosecution will aid in this effort. Similarly, Australia can leverage and empower the ICT industry as cybersecurity enablers, as they are positioned to observe, detect, protect and remediate most internet-based threats faced.

18. **How can governments and private entities better proactivity identify and remediate risks on essential private networks?** By requiring and instituting a digital risk management strategy so that the network, applications, data, and organizational mission/business processes are priorities and adequately considered and cyber resources are allocated. The digital transformation imperative, and the digital risk it brings, are paving the way for a convergence of risk and security today. Some organizations are developing security strategies in a broader business context, seeking to inform security with specific information about business objectives and values. Organizations looking to adopt such an approach should consider a few key recommendations:
The CISO should be part of the strategic team that sets business objectives, initiatives and priorities. It's the only way to ensure alignment of security strategy and business priorities from the start—the only way to ensure security strategy has a business context. Security teams, from top to bottom, must have a

fundamental understanding of business risk. Working closely together, risk management and security leaders can pursue decisions that accelerate the business while identifying and managing digital risks to that business. Security operations center (SOC) teams need to have business context for preventing, detecting and remediating threats. For example, is a threat targeting essential tech infrastructure, or just the server that hosts the cafeteria menu? Without the benefit of context, they may find it difficult to set priorities, make effective decisions, follow the right leads and communicate the relevant details—all while being inundated with alerts during an attack.

19. **What private networks should be considered critical systems that need stronger cyber defense?** First, the mission or business outcome of that network or system needs to be assesses and prioritized. For example, banking networks and energy grid control networks should be overtly labeled as critical systems, necessitating investment and oversight from the requisite authority.

20. **What funding models should Government explore for any additional protections provided to the community?** There are several paths available to provide for the investment to protect citizens on the internet. The Australian economy is bolstered in a large part by digital commerce. Sources of revenue could be taxes, tax breaks, use of managed security services, or some could be citizen funded in an "opt-in" approach. The ICT carriers also may provide cybersecurity services to consumers on a "opt in" basis.

21. **What are the constraints to information sharing between Government and Industry on cyber threats and vulnerabilities?** The constraints, as they exist around the globe, are the potential sensitivity / classification / attribution of the malware. There are ways to share with industry by providing a mechanism to allow industry to qualify to hold and share sensitive information with Government, thus greatly expanding the sensor ecosystem for the country. Also required is an incident reporting schema and a response mechanism.

22. **To what extent do you agree that a lack of cyber awareness drives poor consumer choices and/or market offerings?** To a very great extent. Never has the individual user been required to have a baseline of knowledge to safely engage the internet. Absent of what's required, or ICT providers inserting protections on behalf of citizens, much of the population can be considered cyber-unaware. Government owes its constituents to shape these market-based choices so that slowly, vulnerabilities are reduced.

23. **How can an increased consumer focus on cyber security benefit Australian business who create cyber secure products?**

24. **What are examples of best practice behavior change campaigns or measures? How did they achieve scale and how were they evaluated?** There currently does not exist any punitive repercussions for poor cyber hygiene. The document makes the point through the example of driver education and the provision of seat belts. There is however a law requirement to wear a seat belt but not one for the application of patches, education, mobile security etc. i.e. good cyber hygiene. This makes enforcement of good cyber hygiene rather difficult. However, making the public aware is of importance.

    The issue is one of application once awareness has been created. This lack of application is across the board including many large businesses. One must look at the many examples that enable such cyber-attacks such as Notpetya with the Eternalblue exploit such to organizations still having an old deprecated SMB v1.0 protocol.

25. Would you like to see cyber security features prioritized in products and services? Yes

26. **Is there anything else that Government should consider in developing Australia's 2020 Cyber Security Strategy?** a. There has been a notable shift/increase from just focusing on the financial and monetary aspects of cyber-crime towards 'disruption' and towards 'destruction'. We can see this with the advent of new malware such as Triton/Trisis, Shamoon and Darkseoul which only have a purpose to destroy. This needs to be recognized and factored into the strategy.

    b. The strategy also needs to recognize and include Universities and Academia as an area of focus. The last few years has seen a significant increase in cyber-attacks on Universities as they hold significant information and data beyond just PII. This include IP and specialize research with other entities including Defense research. Several Australian universities have been targeted in the last few years including the Australian National University.

    c. JCSCs are a great step in the right direction in aiming to bring the community together and enhance information sharing and collaboration. It would be good to undertake an exercise to evaluate the actual usage of these centers and by what segments of the cyber community.

    d. Much has been made about cyber resilience and while this is true, we advocate adopting the strategy of cyber resistance – this being the incorporation of strong cyber practices into organizational strategic assets to enable cyber resilience.

e. We also note that the World Economic Forum now list Cyber-attacks at No.3 f or Likelihood and No. 6 for Impact.

f. We believe that the EU NIS Directive and adopting something like it could enhance national capability and maturity. The requirement to provide oversight on the providers of critical services and infrastructures. Additionally, the requirement to perform regular testing and exercise of their capability could be something that the Government, through the ACSC, have oversight on. In doing so, they can set the standard for such exercises and use the results to validate areas which need improvements.

Any question or comments regarding the contents of this paper can be referred to Antoine LeTard ([redacted]), Leonard Kleinman ([redacted]) and or Robert Carey ([redacted]. We look forward to helping the government of Australia strengthen its cybersecurity posture in 2020 and beyond.