Responses to the Discussion Paper on Australian Cyber Security Strategy 2023-2030.

Submitted by:

Name	Ashish Ahluwalia
Email	[redacted]
Mobile	[redacted]
LinkedIn	[redacted]

Preface and Introduction

Dear Hon. Clare O'Neil MP, Andrew Penn, Mel Hupfield and Rachael Falk,

It is heartening to see that we are targeting Australia to be a world leader in the cyber security by 2030 and reminds me of a famous quote from Robert Frost for you, your extended team and everyone involved "Woods are lovely, dark, and deep, But I have promises to keep, And miles to go before I sleep, And miles to go before I sleep…"

I, being a common Australian and from cybersecurity domain, feel proud of the goal that you have defined, and perhaps could feel the hard work and commitment you and everyone involved would be endeavoring in this journey.

Please find below my responses to the questions outlined in the Attachment A of the Discussion Paper: 2023-2030 Australian Cyber Security Strategy. The responses are based upon my **individual learnings** in the cyber security domain for the last 17+ years. I understand that some of the questions in the discussion paper need a deep view of the Australia's current international partnerships or current state which may not be public information. Due to the lack of time and other constraints I have **selectively responded** to the questions.

Before I submit the answers to the questions, in my view, **the single most deciding factor** to achieve the goal, for us or for any cyber security strategy is to **strengthen the weakest link in cyber security- humans.** While the strategy discussion paper does cover different ways to strengthen the weakest link in the cyber security, it would be vital to revolutionize the way every common Australian think, relate and behave in their daily lives in the cyber ecosystem.

Please find below the responses to the question in the discussion paper:

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?
Response	The following Ideas should be included in the Strategy: a) Consideration about **"Made in Australia" for CyberSecurity (products and services)**- It may be too early to achieve it by 2030 but the work in this direction and aligned to CyberSecurity Strategy will help in many ways. It must go in tandem with the cyber security strategy execution and act as a supporting force when implementing the cybersecurity strategy 2023-2030. It will not only help Australian economy but competency, skills, engage masses, cyber development, research and development. We should define a vision for not just made in Australia consumer goods we target today but CyberSecurity products and Services, brining same or even confidence across globe with "Made in Australia" b) Consideration about **"Make in Australia" for CyberSecurity**- Encourage product vendors, International bodies, System Integrations, RnD Centres to make in Australia. This will tie with Cyber Economics and also make Australia a cyber Hub and will automatically instill Cyber culture and driving forces, innovation across technology and its adoption. **Australia should have a Cyber Silicon Valley , world's preeminent cyber innovation and technology hub.** It may be too optimistic for 2030 but we must consider that vision and tie it to our strategy. c) How would our **Strategy be adaptive (**to an extent) Some areas to consider – a) Ability to adapt to the change in **geo conditions/ technology disruptions/new threats/ external forces etc**. For instance, one way to achieve could be: Lead Through Volatility With Adaptive Strategy (gartner.com) (please see the changes and exploring uncertainty illustration). Further, how our strategy **execution** will start early and levers to expedite it's execution. Some areas to consider for a very brief touch on- (Decision Rights, Structure, Parties involved and their roles, Milestones, Communication etc)These areas can also apply to the adaptive parameters of the strategy. d) How do we establish **ongoing engagement channels to enhance cybersecurity maturity for Australia with the help of Cybersecurity market leading product/services vendors** (such as Microsoft, Mandiant,Palo Alto, McAfee, Zscaler, CrowdStrike, Cisco and so on) e) The strategy must have a direction/special mention of **the Cyber Threats Australia faces today or expected**- Inputs from ACSC, ASD, Global threat Reports and publications. On the same lines- Strategy must be wholistic and expandable during implementation on some of the real-world use cases as below or more: • How do we **standardize, enforce security controls, educate masses, on right IOT Devices**, especially with more and more Australians adopting Smart homes, heterogeneous home devices. Retail market is booming with IOT from small independent retailers selling non-regulated chinese products to standard retailers from Bunnings to Woolworths to JBHiFi's and so on. Most of these could be

used by the scammers and malicious users and can become a threat, especially for non IT background Australians.
A Code of Practice that was released by Australia previously is a recommendation but doesnot necessarily enforce the recommendations stated at :
Code of Practice, Securing the Internet of Things for Consumers (homeaffairs.gov.au)

A consideration for us could be to follow UK on BSI Kitemark for product testing - UK product and service quality certification mark | BSI (bsigroup.com)

- Similarly with the government encouraging Electric vehicles- the strategy and planning with a solid foundation is required to handle the EV boom.

NIST is preparing Cybersecurity framework for EV Extreme fast charging infrastructure- a national risk based approach.
Cybersecurity Framework Profile for Electric Vehicle Extreme Fast Charging Infrastructure | NCCoE (nist.gov)
Australia should plan on the similar lines to keep up with the EV boom expected in Australia, especially with the government encouraging the EVs.

- Strategy must consider not just IOT or EVs, but how would we equip **Australians for daily digital lives**.- Motivation, engagement, knowledge, skills, interest and **digital habits.**

f) The CyberSecurity Strategy should consider gaps in **Telecom Sector**, Telecom Regulations- in Australia the telecom sector can play a vital role in preventing Australians from being scammed every day, integrate with financial institutions, ACSC, ASD and Australia can **proactively use offensive** against the scam hubs through international diplomacy where these scam hubs are located overseas.

g) The CyberSecurity Strategy should indicate – how we adapt to **ongoing challenges (current)** and how would we handle for similar challenge in future- adaptive.
To name a few- **Geopolitics, Remote workforce, Quantum Computing , AI Attacks, Blockchaain and Cryptocurrency attacks.**

h) **Consider the Cryptocurrency challenges** as it provides **anonymity** to ransomware demands- Australia must have strictest Policies or **simply ban ransomware payments in Cryptocurrency**. This should at least reduce the interest of hackers in targeting Australia.

i) While the discussion paper does have some views on Laws and Regulations, we know that its takes time to develop regulations and standardization and enforcement will **take its due course of time**,
Where as the **cyberattack can occur within seconds**. The non-compliance to the regulations (existing or any new through the strategy) must enforce heavy fines on the Public and Private sector , we must clearly define the **strict times to comply, assessment must be quick**.

j) Strategy must have a process **to instil a change of mindset** for small, medium and large organizations, a change to realize that Cybersecurity is the duty of the

	board/top management of each organization, align leadership at each organization through enforcements outlines in strategy. k) **Cyberinsurance** providers for Australian organizations (public and private) must also ensure that organizations completely comply with security compliance requirements to be eligible for Insurance. The Insurance providers must not simply raise the insurance price for lack of controls. There must be an **obligation** for CyberInsurance providers too, to report the gaps to Government while insuring an organization, Australia can enforce a **standard security scoring model** for every organization that gets Cyberinsurance. l) Consider the **CyberSecurity Strategy for world's top 5 most Cyber Secure countries**, engage and learn best practices and challenges they faced in execution of strategy.

7.	What can government do to improve information sharing with industry on cyber threats?
Response	a) Mandate the government and private organizations (based upon size or sensitivity)- to become a member of ACSC for alerts and advisories. b) Demonstrate that these organizations have a process and have acted timely when ACSC issued an Alert or a Cyber Threat. It must be a part of Regulatory requirement, assessed, improved, automated and matured. c) Government **must join global dots** through international partnership and also **leverage SMEs from Product and vendor companies to improve depth and details when issuing advisories.** d) ACSC may advice to apply a patch for a vulnerability, but often applying a patch for a vulnerability may not be straight forward for an organization. It should not be assumed that organizations will call or reach out to ACSC for help on the remediation of advisory threats. For instance, the advise to apply patch must have **as much information as possible for a deeper and quicker help to organizations**- it can actually **have detailed step by step procedure on how to apply that patch** (wherever possible- though with disclaimers) and the **Verification steps** for the patch allied or verification steps that vulnerability has been addressed. A **typical example is when Log4j vulnerability** was reported lot of organizations were not able to find all the places of their exposures. ASCS must try to release or with help of Product vendors or international cooperation Release toolkits to identify all the exposure places for an organization, patch apply detailed steps, Patch verification detailed steps. e) ACSC should **exchange best practices and run models** from other countries such as CISA, enhance and fill the gaps. It is specially not just around a public threat but also on the latest best practices. For instance a comparison of CISA with ASCS will indicate CISA is more agile, advanced and releases advise on more latest threats when compared with ACSC.

	A small yet powerful example is MFA(multi factor authentication)- CISA recommended number matching MFA Implementing Number Matching in MFA Applications (cisa.gov) Or Phishing resistant MFA such as CISA Releases Guidance on Phishing-Resistant and Numbers Matching Multifactor Authentication | CISA long time ago. But ASCS is still on the recommending the use of MFA and doesn't explicitly compare the models or specific risks with each MFA method. ACSC should release a matrix with recommended methods to be used with a comparison of MFAs. This would help organizations to go to the best MFAs in their security maturity journey.in summary ACSC should be more advanced, agile and release in depth guidance.

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?
Response	Absolutely correct and one of the purposes of the engagement between organizations and ASD/ACSC is to achieve security maturity, encourage and instil a **welcoming culture for organizations to report more and more cyber incidents.** The organizations should feel welcomed and being helped to recover and restore and lastly get guidance on building the processes to avoid cyber incidents. Trust should be built between the Australian organizations to openly engage ASD or ACSC with a **commitment of confidentiality.**

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?
Response	Yes it will improve the understanding of the ransomware attacks. But the key question that **how would government encourage this practice**? What would the organization undergoing ransomware going to achieve by doing so? What is their **benefit** (not just Government's cyber benefit) in following the mandatory reporting? It must again be a **compelling and nurturing engagement** rather than a mandate enforced on organizations. How would government and its agencies help when the organizations report and take government into their confidence? How can **confidentiality** here be trusted to ensure there is no reputational loss or financial loss due to **stocks fall because of media/social?**

	What role would government play? **Answers to these and similar broader questions be standardized to create a culture of mutual trust even though if we chose to make a mandate.**

10.	What best practice models are available for automated threat-blocking at scale?
Response	Even before answering this, the broader objective that would address the cause of these problems would be how Government can enforce the **S3 Principles- "Secure by Scale" "Secure by Design" "Secure by Future".** **NIST and other agencies does have recommendations on the above principles but Australia should incorporate them by uplifting the compliance model for the critical and public infrastructure and platforms**. **Similarly zero trust must be mandated** (not just recommended) for critical infrastructure, with the help of zero trust maturity assessment. For the automated threat-blocking at scale:- a) Understand the pattern of large scale threats – Historic and Futuristic. b) Enforce S3 or Zero Trust and similar principles in the solutions and technologies encompassing the critical assets. c) Leverage the relevant and applicable product vendors, make them and the system integrators accountable (through regulations)to ensure secure, resilient services are provided to critical assets. d) Government must mandate frameworks based upon NIST CSF or ASD equivalent against large scale attacks and model to identify, detect, protect respond and recover. e) Work with Vendors (such as CSPs- Google, Amazon, MS, product vendors – Crowstrike, Paloalto, Akamai, etc), SIEM and SOAR vendors for security orchestration, Leverage Analysts such as Gartner, Forester on everchanging/ latest offerings f) Government must further standardize and mandate detailed and a separate incidents response plan for large scale incidents/threats.
14.	What would an effective post-incident review and consequence management model with industry involve?
Response	a) Formulate and enforce a revamped post incident review with a hybrid from **UK's and USA'PIR** plans and enhance it with technology and product vendors and academia engagement. b) Only by Enforcing its usage by government and private businesses will solve the purpose. c) Keeping it adaptive with external factors and changing technology to help incident response is the key.

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?
Response	a) Government must encourage and drive "**Made in Australia**" and "**Make in Australia**" for CyberSecurity, this will automatically help technology ecosystem, innovation and CyberSecurity culture. b) Help Australia become a natural hub for Product vendors to establish their development and **RnD** Centres. c) **Guide, nurture or provide subsidies/support** to private organizations for modernization of cybersecurity technologies. Obviously, this has to be evaluated, scored (such as against ASD essential 8 Maturity) for a subsidy eligibility and maturation d) Encourage or enforce organizations to **modernize the underlying infrastructure and security architectures** (secure by design) which is a pre-requisite for building any new digital services. e) Build a **continuous engagement model with Product vendors** and SI for explicit and pinpointed goals rather than generic engagement across for keeping update on and Cyber technologies ecosystem. f) For instance a lot of WoVG solutions would leverage Microsoft Cloud for IAAS or SAAS, **but enforcing a strong and measurable security solution**, right from the architecture design to implementation, scoring against the CISA or OEM security playbooks (MS in this case as it is the original equipment manufacturer), having enforced security framework(s) rather than recommended framework(s) makes the difference to the security outcomes.

17.	How should we approach future proofing for cyber security technologies out to 2030?
Response	a) By appointing a **separate cyber security technology body**, to keep abreast on the evolving trends and technologies, external forces and can advise and support the government cyber entities and private businesses on it. b) Ensuring and empowering the Australian cyber technology body to **partner with the international partners, national and international academia through diplomatic relations, foreign policy and so on.** c) Participate and represent Australian businesses and organizations in World Economic Forum and review and possible act upon what the forum thinks as a ongoing process. 7 trends that could shape the future of cybersecurity in 2030 | World Economic Forum (weforum.org) WEF_Global_Security_Outlook_Report_2023.pdf (weforum.org) d) Look out for partners who can help the cyber technology body on how the **security standards and frameworks are getting shaped for the emerging technologies,** if we cannot drive that in Australia.

	e) Ensuring the cyber technology body works in **coordination with all other government and private cyber agencies and may be business also with a common goal to make Australia a cyber security world leader**. f) Running **sprints** for the cyber security strategy 2023-2030 (not just one time strategy but the continuous scanning and real time insights) into technology. g) Making the cyber strategy **adaptive** to ensure the threats due to changes in technologies and external forces are timely and effectively addressed.

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?
Response	a) **Engage and learn from India** where their Prime Minister drove "**Make in India**" and even "**Made in India"** and helped boost several sectors. Australia must case study this and re-use the knowledge from India for establishing similar CyberSecurity firms in Australia. b) **Subsidize, encourage, partner, collaborate, help and empower the Australian cybersecurity firms**- across Product, Services and Consulting offerings. c) Help these Australian cyber security forms to **leverage analysts** such as Gartner and Forester to help the firms **RnD and roadmap for capability offerings** across these cyber security firms, ensuring they stay abreast and offer best in the breed when it comes to cyber sector. d) **Compel an evolution of cyber security start-ups** in Australia- by clearly defined goals and a win-win for the firms and the Australian cyber security objectives.

19.	How should the Strategy evolve to address the cyber security of emerging technologies and promote security by design in new technologies?
Response	**Refer to answer 17**
20.	How should government measure its impact in uplifting national cyber resilience?
Response	a) Global cyber security Index b) National cyber security index c) Basel AMl Index d) Cybersecurity exposure index e) Global Cybercrime Reports f) Global threat reports g) Or create Australia's own global index with engaging academia such as : NCPI_2020.pdf (belfercenter.org) It is imperative that any of the indexes would indicate the same direction Australia is heading towards over a period of time.

Ending Note:

With this, I end my responses to the questions in the discussion paper for the Australian Cyber Security Strategy 2023-2030.
I wish you and your team a great success in not just meeting but surpassing the goal. It is a privilege for anyone to be a part of this journey in any way.

I am sure you would have many more engagements with the Australian cybersecurity community and a common cybersecurity professional like me would be able to contribute on the ground whenever given a chance.

Warm regards,

Ashish Ahluwalia
Email: [redacted]
Mobile: [redacted]
Place: [redacted]