Response to Discussion Paper: Horizon 2

Submitted by:

Name	[redacted]
Email Address	[redacted]
Mobile	[redacted]
LinkedIn	[redacted]
Previous Submission to Strategy	[redacted]

Preface and Introduction

Thank you for the engagement for the discussion paper on Horizon 2. It is heartening to see the steps government is taking to safeguard Australia and continue to do that.

Technology and Processes can be aligned, refined and governed. As always, people are the weakest link, especially the vulnerable cohorts with lower digital literacy should be paid special consideration throughout. ***We can patch systems not our people easily…***

While we continue to address the weakness , however, defining and encouraging some more values in the cyber journey- such as "**simplicity**" to use and adopt for all cohorts. Cyber should be **intuitive** for people to make decisions in their daily lives, Cybersafety should be easily **identifiable** as **trustworthy**, products and services across Australia are intuitive and **empowers** people to take Cyber sensitive decisions with ease.

And Cyber exemptions should not be allowed to all cohorts because it needs exemption for a small cohort.

Once again thanks for giving the change to contribute, I am always passionate about CyberSecurity in any way or form. I would like to and continuously engage in this journey if appropriate.

Thank you.

1.	What trends or technology developments will shape the outlook over the next few years and what other strategic factors should Government be exploring for cyber security under Horizon 2?
Response	In addition to the existing considerations , it may be valuable to consider the following technology developments , considering they are likely to shape the Cyber Threats and Attack surface. a) **Industry Specific AI Approach not generic AI**: • Since 2012, the decade or so was all about foundation of AI and it was really on how to make computers learn and how to develop AI. The next decade will be **application** of AI across industries.IT is just a small sector of AI and the CyberThreat landscape. **AI will be applied to automotive, factories, home appliance and so on. The Cyber Threat surface will be across industries** and requires industry specific focus for Cyber and Safety convergence. • Government must act early towards **specific Cross Functional Sectors for AI use**. While handling Generative AI in general is ok and a thought of the past, the next steps should be **how do we ensure its Safe for use across industries and citizens**. Specific focus must be provided industry wide for industry specific regulations when comingled with AI and Cyber. • For instance AI's current anticipated biggest change is not in IT but in **automative, healthcare, finance, gaming and wireless networks**. Early thought in embedding cyber must be considered as an important strategic factor with not a generic approach to AI but industry specific use case and cyber challenges. **Gaps in these field can not just be Cyber but the Cyber Gaps can have impact on citizens life and health.** • Consider promoting enforcing AI governance frameworks, use of explainable AI and with specific attention to industry. b) **6G is set to be launched by ~2030** : • **And combined with explosion of devices- IOT** and, special consideration to wearable technology boom. News from yesterday- facebook believes AI glasses will surpass/replace mobile phones for instance.Government must give early consideration to 6G and its potential Cyber impact and planning, IOT in isolation may not suffice the planning. • **6G changes Attack surface** and has different architecture- It is important to plan Cyber for 6G as it's architecture is open and distributed and not centralized. • And has **features like reconfigurable intelligent surfaces** (RIS), cell-free massive MIMO, visible light communication (VLC). These will evolve new Cyber Threats. • **Again AI embedded with 6G** will bring in new cyber Threats- Government must plan , be appraised and potentially contribute for a secure-by-design and/or standardization of it when released from a Cyber viewpoint. **c) Proactive- Not reactive Phased adoption of Post-Quantum-Cryptography**

	• We must consider the **planning** towards enforcing **Post Quantum Cryptography in Public Sectors and Critical Infrastructure**. It will not be an easy change hence waiting for NIST and other agencies to simply release more standards will be a reactive approach. • Proactive approach must be considered on plan to enforce and what industries must be regulated, must be considered in advance. **d) Convergence of Digital and Physical** • **Smart cities,** autonomous transport, energy grids, and robotics will converge- (digital + physical**). Real world impact and threats likely possible.** • Industry Standards must **integrate *safety AND cybersecurity by design***, ensuring that a cyber event cannot compromise physical safety. • **Combined certifications and standards** be developed for these emerging convergence.It is good to see government promoting Zero Trust which does reduce the likelihood of Cyber Threats. • Recovery and Resilience- Must be uplifted as focus today is on protection.
4.	Section 2.3 Monitoring progress in a changing world—a framework for delivering cyber security outcomes Question -Can you suggest any existing or new ways to collect data and feedback to monitor these outcomes?
Response	In addition to the develop metrics, and address data and evidence gaps in partnership with industry, academia, data agencies, and the community. Consider : • Citizen and community engagement-specially track awareness of cyber hygiene. • Cyber Incident Metrics-KPIs and trend of major Cyber Incidents in Australia - prevented, contained, responded, succeeded etc. • Maturity benchmarks- How many Critical Infrastructure organizations have moved to higher maturity models for ASD Essential 8 or equivalent such as NIST. • Consider reporting the Maturity Level and slowly introducing a direction to increase maturity level, else maturity level 1 will remain a compliant and stagnant level and wont promote continuous uplift. • Capture Economic Indicators- Track cyber workforce numbers, SME adoption of cyber insurance, cyber industry revenue growth. • Compare Australia's progress wi.r.t data -against OECD, EU, US or Asia-Pacific peers. • Consider Red teaming exercises- and their results as a trend for a set of organizations such as with Critical infrastructure.
5.	What could government do better to target and consolidate its cyber awareness message?
Response	Cyberaraewness should be learnt from other countries also to complement the already work in progress initiatives.

	• Such as – **Estonia** leads CyberAwareness-after its massive 2007 CyberAttaks, it mandated cyber education **at primary school**. • Estonia citizens use **digital ID** and e-government services daily, making awareness a lived experience. **annual cyber drills** with NATO and has the **NATO Cooperative Cyber Defence Centre of Excellence** in Tallinn. • Public cyber hygiene is high; phishing and digital fraud rates are lower compared to EU averages. **Israel**- is another good example, it has a Strong industry with government and military collaboration and with heavy investment in **cyber startups and education.** • Another example is Finland- replicate its awareness programmes. • Citizens already score highly on digital skills, making cyber hygiene more natural. **Impact: It has a v**ery high adoption of secure practices like **electronic ID, strong passwords, and phishing avoidance.**
7.	How can Government encourage SMBs and NFPs to uptake existing cyber resources (i.e. Small Business Cyber Resilience Service, Cyber Wardens, ACNC guidance etc.)?
Response	There are several steps that can be done here specially with NFP is really patchy in Australia. Consider the following: • Incentives or Rewards/Recognition-On similar lines as UK, where it has UK's *Cyber Essentials*, create a **lightweight certification** for SMBs/NFPs completing the Cyber Wardens program. • Provide **Badge**- such as **Safe to trade** to these and promote Cyber. • Work with Insurance companies- help Companies consider discounts to SMBs that are Cybersafe and provide government grants etc. • **Offer some tax relief if Cyber Safe? Rating mechanism- it will be effective and SMBs will be after Cyber for their own benefit.** • For NFPs, prompts could be tied to **ACNC annual reporting**. • Many SMBs/NFPs trust their **accountants, IT providers, and insurers** more than government. Governments can equip these intermediaries to "push" the resources for Cyber cause.
10.	What are the unique challenges that NFP entities face for cyber security compared to the broader business sector and what interventions from government would have the most impact in the NFP sector?
Response	NPFs are really patchy and they really don't have a motive to be CyberSafe in Asutralia. Because of challenges such as: • **budgets constraints,** • **margins,** • **dependency on volunteers,** • **non-tech workforce, and so on but they still hold** **Sensitive data** sometimes such as health records, disability information etc. they are high risk and sensitive data hubs. Government should consider the following for **Not for Profit organizations and Cyber in them:**

	• Awareness with custom and specific functions- print, lecture, etc Such as but not limited to -"Cyber in Disability Services", "Cyber in Faith Communities", etc...start that practice • **A voluntary reporting of cyber -simple 2-3 things such as has your organization implemnetd MFA?** Do you take and restore from backups- a simple check boxes without complicating things. • This can be included in their existing reports **ACNC Annual Information** Statement Prompt or wherever appropriate. • Consider **grant conditions to Cyber Hygine**- They will definitely adopt Cyber in that case as its all about money end of the day for organizations. • **Small vouchers for NFPs to pay for MFA setup, backups**, or training. • **Insurance premium to go down with Cyber maturity.** Or Partner with insurers to provide reduced premiums for NFPs that adopt Cyber Wardens or ACSC guidance.
13	How could the government further support businesses and individuals to protect themselves from ransomware attacks?
Response	**In addition to some of the actions listed in response 10 above,** • **Secure-by-Design tech**:Work with ISPs and cloud providers to push **automatic patching, DNS filtering, MFA prompts**, and safe email defaults for SMB and residential customers. • **Offer** Provide affordable "cyber starter packs" (backup tools, endpoint protection, MFA hardware tokens) subsidised for small operators? And highlight the benefit of it- make t compelling for them to invest in it.
16.	Which regulations do you consider most important in reducing overall cyber risk in Australia?
Response	It is actually not bringing new regulations, for instance ASD Essential 8 is great. Problem is organizations that are required to be SOCI complaint sign off they are but they aren't. • Do we audit the organizations with critical infrastructure against ISM Controls? NO, and that's a GAP. • **Today all big 4 banks in Australia don't even have a mandatory MFA on login. Excuse is user cohorts** but for the people that are young, tech savvy, and want to implement MFA even cannot have MFA. Try calling your bank and ask them that you want mandatory MFA- they will say NO. And that's a real shame**. Even some smaller and economically weaker countries which are far behind Australia** have MFA mandatory and even you take 5 dollars out of ATM, there is a immediate SMS. How will we prevent fraud without foundation. It is not about framweorks but because organizations are able to find a way to bypass these frameworks is the problem.
18	What are best practice examples internationally that Australia should consider for enhancing our secure technology standards and frameworks? In particular, what

	approach do you consider would work best for edge devices, CER and operational technology?
Response	• **Edge has its own challenge** of distributed attack surface Where as CER has high dependency on timind ie when incident occurs And OT standards were largely designed for availability and safe and Cyber in mind. • Consider using convergency through : enforce Zero Trust + lifecycle management for **edge devices.** Invest in integrated platforms, playbooks, and redundant comms for **CER** Focus on segmentation, passive monitoring, and compensating controls for **OT**. The best approach is **convergence**: Unify IT/OT/edge telemetry into CER, backed by **Zero Trust + resilience-first governance**.
19	How should the government work with you to support consumers and end-users to be more informed about cyber security in their products and protect themselves from cyber threats?
Response	There are several things that government can do here. In addition to the work it is doing on IOT and raising cyber standards on devices, consider: • **Why don't we have a simple 5 Star rating on products sold – across JB Hifis Chinese shops, and everywhere- Simple like a Kids "up and go" has a health star rating- a system to have a "Cyber Rating" on these products. That allows our old children (our old Australians) to just see starts and buy product without worrying much about security as they are not tech savyy.** • We don't want to teach cyber to old people in their old age- isn't it? Just a "Cyber Star rating" is good for them.I would want to relax when I am old , stress free..and Cyber could be stress for them. • **Replicating UK with Acts such as -**Product Security and Telecommunications Infrastructure Act (2022) that mandates ***minimum security standards for smart/IoT device****s*, including banning default passwords, clear vulnerability disclosure, and update transparency.
21.	How could government better work with industry to understand data access and transfer across the economy to inform policies around secure data sharing and limit data exploitation from malicious actors?
Response	• There are existing policies regulated across industries within Australia and globally to address Data access, privacy and security of data. **The problem lies in organizations that do not understand or endeavour to understand** or if if they understand they do not comply with those policies proactively. • This is specially **with small business, small industries , NFP and unethical companies.** • Government should consider understanding WHY this problem occurs and address those . Some of these problems , not necessarily limited to are:

	• Organizations without IT/ Legal background needs a simple way to understand the complex legal policies around data. Low Cyber Literacy, Low motivation to comply, Low regulatory fear, "**we wont have this problem" mindset, cost and profit, siloed ownership, etc.** • Or even if Organizations want to comply, their supply chain model doesn't allow to comply with data regulations completely. Now what can government do is address those reasons for non-compliance such as : • **Plain English** and non legal terms guidance for small scale business, NFP organizations, or even large organizations with weak Cyber Culture. • Provide **Toolkits**- Policy Creation guidance, data handling Standard Operating procedures that can be customized for their industry use. • **Self assessment** kits- for compliance , enabling them manage their data regulations. • Community outreach, work with vendors for secure by design, by default encouragement across the tool sets used. • Require basic data privacy/security attestations for government tenders, grants, and **NFP funding**. • **Publish case studies of penalties** (anonymised for SMEs if needed) to show that non-compliance has consequences. • Partner and help change the mindset of compliance from legal requirement to how **it attracts their business value** by building customer trust and customer value for their brand.
22	Boosting innovation and economic prosperity is enabled when data is shared with trust and not accessed exploited by malicious actors (e.g. IP theft). How can government and industry work better together to achieve this aim in an evolving global threat environment?
Response	• The aim and vision mentioned in this question is really good for us as Cyber professionals. How do we make this equally appealing to industry or enabling them to meet this is the key. • How can we partner with industries to work on: ---**Review what data do they store or process?** **---Is that necessary for them to store or process?** **---Can government provide alternatives to organizations** to store or process the data? For instance can government allow companies to leverage Digital ID (stored and processed at Government) rather than creating copies of data locally at the companies? ----Can government suggest alternative ways of fulfilling the function that requires them to store data- such as authentication, verification, preference etc. And help get funding to move away from that local storage models that can lead to data theft? • Work with regulators such as OAIC, APRA to push large firms to **collect less data retain less data and encrypt more**. • **For SOCI obligated organizations**, consider them reporting not just compliance annually but reporting on what is their plan to move to higher security maturity levels, such as roadmap for ASD essential 8 maturity level 2 and . This will

	commit them to maturity and will also make it difficult for threat actors to deal data with controls of higher maturity levels. • **Consider for non-SOCI obligated**, large size organizations introduction of a framework for mandatory , transparent , audit covering their cyber security maturity with their board's signoff.
26	How could government further support industry to block threats at scale?
Response	There are some good initiatives that government has started since the strategy, it is heartening to see them bening thought and developed.Further consider: • Learning from **Singapore**- Cyber Security Agency of Singapore works with ISPs to provide DNS filtering at National level- blocks websites before users can access those sites. • Encourage **and promote ISPs to block network level malware/phishing and C2 domains.** • This single change at **ISPs will protect millions of Australians**. • Create a **framework if not a playbook with SLAs** to suspend malicious domains- fake government domains, phishing, malware and so on. • Harden the email ecosystem which is one of biggest attack surface. Tie KPIs to government and supplier domains with spoofed reduction in phishing reaching mailboxes. • Promote **RPKI/ROV** adoption across Australian autonomous systems. • Share/provide funding for telcom sector **scrubbing capacity** for public interest services such as but not limited to healthcare, education, emergency -state and national. • Encourage Australian **consumer IoT baseline** such as with no default passwords, automatic enable update policies, vulnerability disclosure) and label compliance. • With ISPs, ship **managed home routers** with auto-updates, WPA3, and default DNS protection; provide SMB SKUs with the same features.
27.	How could the use of safe browsing and deceptive warning pages be amplified?
Response	• Government should partner with **other countries and influence the key vendors to have - browsers,operating systems, and mobile app stores** to integrate real-time safe browsing feeds (malware, phishing, scams). • Move towards a **shared global blocklist consortium** • Bring SIMPLE Clear Messages for Vulnerable people that don't understand technology, such as **Replace** "This connection is not private" with plain-language warnings: ***"Scammers may steal your banking details if you continue."*** • ***This should be reflected in browsers*** • Force extra clicks or have browser vendors design steps to make bypassing warnings psychologically harder. • Can **Citizen reporting built-in** be worked with the help of browser vendors? Where a simple option by browser vendors allows global (and Australian) citizens to click and report phishing/scamming websites and global playbooks work on them?

	• Mobile First Focus- can you link SMS originates, and Sources that originate broswers in mobile device to go through security checks before lauching the website?
28.	How can we better align and operationalise intelligence sharing for cyber security and scams prevention?
Response	• Enhance international partnership and **playbooks** applicable to ensure scams seen outside Australia are blocked in minutes in Australia. • Use **AI for anomalies detection across Telco and Banking** to flag mule accounts and scam campaigns proactively. • Build mandatory data satndards for feeds, can you have All partners publish scams and cyber threat indicators in **STIX/TAXII or MISP-compatible feeds**. • Consider creating sector specific partnerships and operational controls across sectors such as Superannuation and Agecare. • Small Business, consider **Scam alerts embedded in ATO Business Portal, ASIC Connect, and ACNC portals.**
31.	How could government better incentivise businesses to adopt vulnerability disclosure policies?
Response	The key here is to make vulnerability disclosure "attractive" for organizations. Either through incentive or through recognition or other ways. Government can consider some of the following • **Financial Advantage**- make vulnerability disclosure mandatory in government contracts and tenders to start with. • Work with **insurers** for benefits of vulnerability disclosure. • Annual **rewards** for Vulnerability Disclosure in public sector. • **Partner** and **delegate** touch points for Vulnerability disclosure at banks, healthcare, supply chains, etc. • Consider **appropriate SOCI Uplift to disclose vulnerabilities**?
33	How effective do you consider the SOCI Act is at protecting Australia's critical infrastructure from cyber-attack? Are the current obligations proportionate, well-understood, and enforceable?
Response	Effectiveness of SOCI can only be measured for Critical infrastructure. But Cyber Attacks can go on critical infrastructure and beyond. So, firstly effecviveness question is only valid for critical infrastructure, unless government considers complementary existing and new obligations for non-SOCI obligated organisations. In my personal view, SOCI Act is partially effective because: • **Data of Cyber breach in Australia confirms that organizations that signed of compliance for SOCI (ASD essential 8) were still targets of major data breaches or Cyber Attacks**. • It is not just because there will always be threats and attacks but also due to the fact that SOCI obligations **and especially CIRMP under SOCI, gives a way out to obligated parties to not meet some of the challen**ging requirements. They end up raising risk and getting green tick against compliance. The risk raised is again internal and not standardized centrally across Australia but depends upon the organizations Risk Management program.

	• Secondly, **a lot of industries such as banks, give priority to Sales (which they would obviously)** for instance ANZ, CBA, NAB, WestPAC- non of them have a mandatory MFA. And neither can a user that wants MFA to secure his account get it enabled.WHY- because they find an excuse of usability/disability and don't enforce it. • Why Does not SOCI/CRIMP or Essential 8 clearly imply Things such as -" the obligated parties under SOCI, must ensure that they are offer security requirements listed under the frameworks such as ASD essential 8 NIST CSF, to all users where the decision **is not to enforce a control due to smaller user cohorts (accessibility, etc).** • Why should **security of 99% of users be compromised for 1% of users (accessible) and banks don't enforce** it because they see it as a friction point that can potentially reduce their revenue. How are they even complaint and they sign off every year without mandatory MFA? • There are several other examples where organizations obligated under SOCI do it and SOCI becomes ineffective....
34.	Are there significant cyber security risks that are not adequately addressed under the current framework?
Response	See response to Question 33 and in addition: • It is difficult for organizations to Report and manage critical infrastructure assets as per SOCI because , organizations have limited understanding of **supply chain**, and third parties, especially in Food groceries etc. • Similarly with **energy sectors, they have OT blind spots**. • Would it be valuable to consider linking Security frameworks under SOCI (such as ASD essential 8) **to industry specific controls as well**? • Align to realistic -threats and applicable controls? • Would you consider a **consistent improvement** , moving towards higher maturity model as a mandate or some way to promote that? • How can SOCI encourage **Cyberuplify beyond compliance**? Can you consider some considerations- that encourage organizations to not just stop at SOCI (essential 8 controls) but use complementing controls as required.
36.	What support would assist critical infrastructure owners and operators to mature their cyber and operational resilience practices? What role should government play in enabling uplift, including through tools, guidance or incentives?
Response	For the large organizations (and with a benchmarked financial turnover), that own critical infrastructure- Consider : • **Developing How to Guides**- something very similar to **ASD's Cloud Blue print (that covers Azure EntraID).** In partnership with product vendors, publish how to meet essential 8 maturity levels on leading domain products used in Cyber.

	• Develop **Guides on how to move from level 1 maturity level to level 2.** • Develop guides on what other **controls other than SOCI implied (such as ASD essential 8)-** what other controls than it , owners of critical infrastructure must have.
50	What regulatory frameworks or requirements should be prioritised for consideration as part of Australia's efforts on international cyber regulatory alignment?
Response	Thera are two parts to this : **One** : Select the best regulations from leading countries, in the areas where they are best.(examples listed below). **Two**: Build Australia's own fit for purpose, futuristic-Frameworks for the Cyber Challenges that we foresee in the future in Australia. **<u>For One: consider :</u>** • Australia's work on **Consumer IOT** Cyber- can have UK PTSI- standards. • Australia's consumer **IOT-ETSI EN** for device security and benchmarked security in IOT. • US has "**Cyber trust Mark**" , where qualifying consumer smart products that meet robust cybersecurity standards.**Australia should build our own Cyber trust Rating- like a Cyber Star Rating- similar to food health rating.** • **EU Cyber Resilience Act** – for helping with areas such as but limited to vulnerability handling. • For state of maturity in software transparency and supply chain security, consider **CISA's 2025 minimum** elements for software bill of materials. • Build Australia's own identity framework or replicate some elements from **European Digital Identity Framework.** **<u>For Two: consider</u>** • Build Frameworks that handles Cyber problems in Australis largely same as other countries, but we differ in • economy, regulations, digital literacy, digital adoption, • average age of population • Cyber Skills shortage. Hence the frameworks we create for Australia must consider some of the factors(not mutually exhaustive) as above.