Charting New Horizons

Developing Horizon 2 of the 2023-2030
Australian Cyber Security Strategy

Australian Government

Policy Discussion Paper – Input for Consideration

August, 2025

On behalf of Trusted Impact Pty Ltd (Trusted**Impact**) I am delighted to present the following input into the **Charting New Horizons** Policy Discussion Paper for submission by 29 August, 2025.

The following input is a consolidated, 19 YEAR perspective gained from helping over 400 disparate organisations with THOUSANDS of cyber 'insight' projects ranging from both TECHNICAL cyber assessments through to defining cyber STRATEGIES and most things in-between.

We are delighted to summarise and synthesize the contemporary and salient cyber issues for Home Affairs based on;

- **Cyber insight spanning nearly TWO DECADES.** Trusted**Impact** was focused exclusively in 'cyber' well before it was a commonly used word for the industry. Our 19-year heritage is unmatched by the vast majority of players in the Australian industry.
- **Cyber insight from a wide BREADTH of perspectives.** With over 400 clients ranging from Australian to International, Large to Small, Government to Commercial organisations. Trusted**Impact** is able to provide cyber insight from nearly ALL industry sectors in Australia.
- **Factually grounded DEPTH of insight from over 4,000 projects.** Trusted**Impact** has a significant repository of factual insight into the technical challenges and strategic and 'leadership' challenges that all organisations face. This insight has been gained from BOTH technical perspectives and business perspectives –and particularly, the important interrelationships between the two.

Our business model is uniquely positioned by being:

- **Independent** consultants – we help organisations mitigate their cyber PROBLEMS – not convince them to buy cyber PRODUCTS.
- With a **singular focus** – information security and 'cyber' is all we do and all we think about.
- Leveraging **experienced** Professionals – our business model is to leverage senior, experienced practitioners with credentials, not hire and train juniors following standardised, low-value checklists.

If anyone would like to discuss any item in the attached submission, please reach out at any point.

Trusted**Impact**
[redacted] Melbourne VIC 3000
[redacted] http: www.trustedimpact.com | X: @trustedimpact | LinkedIn: https://www.linkedin.com/company/trusted-impact/

The following section is structured into the original Sections and specific Questions that were presented in the Policy Discussion Paper with Trusted**Impact** input provided for each question.

2.1. Outlook for Horizon 2

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?

Trusted**Impact** has seen a marked increase in the sophistication that threat actors use to compromise organisations in Australia.

However, the basic 'root causes' of data breaches and cyber incidents have been very constant for the last two decades. For example, most incidents still involve failing to perform simple and fundamental cyber foundational principles such as poor 'access' hygiene (granular identities, poor credential management, limited controls like MFA, etc.), or poor data back-up processes to protect against ransomware.

We suggest the Government need to try to shift the 'conversation' to stop over complicating the threat as savant hackers unable to be stopped, but to highlight that the simple basics can be applied to successfully mitigate a large portion of their cyber risk. We often see clients viewing cyber as if it's all 'TOO HARD' to protect themselves. Because of that 'impression' they often either focus on just 'ticking compliance boxes' or just put it in the 'too hard' category and do little to improve their resilience.

As further evidence, there are way too many, complex, redundant cyber-related frameworks and standards – whether they be Federal (ISM/E8), State (VPDSF), Functionally aligned (PCI-DSS), International (ISO/NIST), or many more. Even the Royal College of General Practitioners (RACGP) has created a separate standard they believe should be applied for GP's[1].

Almost all these standards and frameworks have hundreds of controls. There was a powerful elegance in the original ASD 4, and then the (original) Essential Eight (E8). But frankly, when the E8 was expanded to 4 maturity levels, with a total of nearly 100 unique controls (depending on the latest version), the 'baby was thrown out with the bathwater' and simplicity gave way to additional complexity.

Undoubtedly other submissions will highlight the other essential technology trends like quantum computing and artificial intelligence that will definitely transform our lives. But on a more practical level, Trusted**Impact** suggests that Horizon 2 must attempt to better raise awareness of the benefit for organisations to focus on the basic, often boring, fundamentals (like patching, password hygiene, back up, etc); rather than getting distracted from 'futuristic, sexy sounding' technology or threat actors.

Finally, businesses (including consumers) have voracious appetites to implement and leverage new technologies at considerable speed – often without considering the potential issues or risks associated with that technology. If new technology can demonstrate it will increase revenues, decrease costs, or improve service levels, it'll be adopted, and the people who had the idea will be rewarded by organisation well before something goes wrong because risk was not considered.

Therefore, as part of our suggestion to shift the conversation in awareness, an area that would have measurable impact would be to stress how important it is to consider 'what can go wrong' when adopting new technology (software or hardware).

[1] https://www.racgp.org.au/running-a-practice/practice-standards/standards-5th-edition/standards-for-general-practices-5th-ed/core-standards/core-standard-6/introduction-to-core-standard-6

2.2. Collaborating across all levels of Australian Government

2. Are there initiatives or programs led by State or Territory governments you would like to see expanded or replicated across other levels of government?

To answer the question with a question:

Does the Federal Government have a realistic view of the critical cyber risk(s) that Commonwealth Departments and Agencies face on an aggregated level?

Australia aspires to be a "world leader in cyber security" and this is an obvious 'gap' that Horizon 2 must address. Senior Government leaders should have direct access to a consolidated 'cyber risk register' that provides factual insight into the common and most critical issues faced by Commonwealth organisation on an aggregated level so that they can be mitigated much better than what exists today.

In the last year, Trusted**Impact** partnered with a global consulting firm to design and develop an Enterprise-level AND Federal-level cyber risk management framework for a Country in the Middle East that would provide this perspective. The ability to leverage this Intellectual Property exists and it would be of significant benefit to the Australian Government since it would not have to 'reinvent the wheel' from scratch for this need – but simply tailor it to the idiosyncrasies of Australia. Furthermore, as you know, the Victorian Protective Data Security Framework (VPDSF), which has been in operation since 2016, and could also be utilised to establish this Federal level requirement without starting from scratch.

2.3. Monitoring progress in a changing world—a framework for delivering cyber security outcomes

3. Does the high-level Model resonate, and do you have any suggestions for its refinement?

Respectfully, NO. The high-level model illustrated in the Policy Discussion Paper does NOT resonate with us, as it amplifies the 'complexity issue' we mention in Question #1.

For example:

a) We do not see how a 3-dimensional graphic provides clarity on how the model should, or is intended to operate. We understand the iterative intent, but doing so by adding a third dimension to the picture is superfluous and distracts from the objective and intent for many readers. Consider simplifying to 2 dimensional only.

b) The lack of specificity (i.e., the generic starting and ending bubbles of 'New technology is developed') are so generic, that it's difficult to understand how this model would be used in practical situations. Consider using several simple examples and explain the 'outcome(s)' that would be achieved from following the model. It's far too conceptual to be of practical use at this stage.

Instead of introducing new conceptual models, Trusted**Impact** suggests it might be of value to research a number of other existing models, that can be leveraged. For example, the World Economic Forum, created a range of relational models showing the causal relationships of items relating to cyber security.

These models are at: https://intelligence.weforum.org/topics/a1Gb00000015LbsEAE

4. Can you suggest any existing or new ways to collect data and feedback to monitor these outcomes?

TrustedImpact suggests that creating a 'model' that links ALL outcomes, ALL interventions, etc sounds intellectually interesting, but we believe there is a chance that the model would become too complex, unwieldy and confusing with the large number of potential issues and items that would need to be included.

Therefore, as suggested in response to question #2, if there was a mechanism to identify the MOST IMPORTANT risks faced by the Commonwealth on an aggregated basis, then one could build a working model that appropriately focuses on the major risks facing our Government today (for one application of the 'model'). This is one more reason why we believe the suggestion to develop a 'federal-level' composite cyber risk management framework would be of considerable value.

3.1. Shield 1: Strong businesses and citizens

Consolidate our cyber awareness messages across the economy

5. What could government do better to target and consolidate its cyber awareness message?

TrustedImpact believes that the MOST important step the government can take to improve cyber awareness is to recognise that the challenge is about PEOPLE and their BEHAVIOUR. Thus, it requires a psychological, behaviour-focused approach to impact or change a person's overall behaviour.

Many 'behaviour change' professionals recognise that people learn differently due to their different personality types (see Myers-Briggs for example[2]). However, "Act Now Stay Safe" is a 'generic program' targeted at a 'generic population'. Any attempt to solve a complex issue with one simple, generic solution will likely NOT resonate with all populations, and potentially, those populations or personality types who may be more vulnerable than others.[3] Furthermore, behaviour change programs typically leverage different mediums and methods ranging from using different techniques or approaches (i.e., gamification, operant conditioning, etc.) to more successfully deliver change programs.

We find a similar situation in many of our clients. For example, they often view cyber as an 'IT problem', and thus, have one of their technical staff create the company's 'awareness program', who often lacks the psychological training to understand how to change behaviour. With all the best intentions, the programs often do little to change an employee's appreciation of cyber risk, or social engineering.

TrustedImpact suggests that the Government consider how to better align with these 'behavioural' requirements in Horizon 2. For example, we would suggest a program should be tailored to address how different personality types assimilate information differently.

Furthermore, we also suggest the Government focus more narrowly on 'at risk' populations (i.e., elderly), rather than the entire population with one simple message. To do so, we suspect that IDCARE (https://www.idcare.org/) would have a large amount of data on vulnerable populations to enable a more prioritised and tailored cyber awareness program focused on these groups.

Finally, TrustedImpact suggests that more attention be placed on improving the 'awareness' of younger people. Our firm is helping a well-known Grammar School with awareness for their

[2] https://au.themyersbriggs.com/themyersbriggs-press-2020november-cyberchology.aspx
[3] https://ap.themyersbriggs.com/content/Grow_presentations/Type_Tips_for_Cyber_Security.pdf

entire school, including their STUDENTS. This is contrary from most awareness programs that we see, which focus primarily on adults who are employed as staff of those organisations.

It is rare that we have seen cyber awareness programs focused on younger people as a target population, and yet young people leverage technology as frequently as (if not more than) our older population or employees of organisations.

While there is considerable benefit to having organisations increase the awareness of their staff, we suggest it would also be beneficial to focus on younger people as a target audience. School environments provide a rich educational environment from which to undertake this type of effort, and thus, we suggest the Government should work more with both public and private schools to offer cyber awareness programs focused on younger people via school environments.

Increasing cyber literacy in our schools

6. What programs or pilots have been successful in this context? What additional supports could be developed or scaled-up to address these issues in partnership with both education stakeholders and those with technical cyber security expertise?

As mentioned previously, Trusted**Impact** has assisted a Grammar school with their overall awareness program, which includes 'phishing' their year 8 to 12 students every other quarter.

However, this program is very simple and there is a LOT more that could be done to develop a range of educational courses / curriculum to educate our younger people on how to better protect themselves against a cyber threat.

Creating a concise, yet comprehensive cyber curriculum that could be adopted by (at a minimum) all public schools, and potentially private schools, would be a well-placed investment for the Government.

Target resilience uplift to small and medium-sized entities that cannot adequately protect themselves, including through low or no-cost standards to apply

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.)?

The concept of a "cybersecurity poverty line (CPL)[4]" principally refers to organisations that struggle with security usually because of insufficient budget, expertise, capability, or influence. It's based on the premise that we're besieged by endless hacking campaigns that disproportionately burden under-resourced organisations like small businesses, charities, and community organisations; all whilst our State and Federal agencies are (appropriately) focused on the more serious threats to critical infrastructure. Simply stated, many if not most, SMBs and NFPs do not have the resources to adequately reduce their cyber risk.

Cyber poverty exhibits dynamics very similar to real-world poverty: simply providing money or free expertise does not necessarily address poor technological designs, poor market incentives, misaligned sociocultural attitudes towards security, or other barriers. However, as noted in the above referenced article, cyber poverty poses threats to the entire cyber ecosystem, not just to organisations below the CPL.

Separately and in parallel, many of our Universities and Tafe's are preparing students for professional cyber roles in the cyber industry, and yet many of those students have little to no

[4] https://www.atlanticcouncil.org/content-series/buying-down-risk/cyber-poverty-line/

practical work experience with cyber. We often receive emails from students seeking unpaid work experience or internships to address this gap and to complement their education.

Therefore, we believe there may be an opportunity to address BOTH of those two 'challenges' by considering a similar program that was presented in a relatively recent (2023) Wired Magazine article (https://www.wired.com/story/ut-austin-cybersecurity-clinic-311/).

Simply stated, the University of Texas at Austin and other universities as part of the "Consortium of Cybersecurity clinics" pair cyber students with organisations in need of cyber advice. "*A cybersecurity clinic provides cybersecurity services to community organizations, including small businesses, nonprofits, cities and towns, rural school districts, small utilities and more, while giving students real-world cybersecurity experience. Modeled [sic] after legal and medical school clinics, cybersecurity clinics are typically housed at colleges and universities under the direction of clinical professors. Students from diverse backgrounds and degree paths train to provide free cybersecurity assistance to clients who could not otherwise afford these services. Clinics serve as a skills-based learning environment for students and as a vital local resource for improving the cybersecurity resilience of communities.*[5]"

Please note that as part of a Swinburne University student-led project, Trusted**Impact** has been working with several students to develop an initial plan that would consider if, or how, a similar 'consortium' might work in Australia. More information may be available by the time this input has been received, and we would be happy to share the initial findings with appropriate constituents from the Government.

8. How can industry at all levels and government work together to drive the uptake of cyber security actions by SMBs and the NFP sector to enhance our national cyber resilience? What type of support would be useful and who should provide it?

Please refer to the response to #7, above.

Enhance support for citizens and victims of cybercrime to help them bounce back quicker

Exploring cyber security standards for small businesses and not for profit

9. What existing or developing cyber security standards, could be used to assist cyber uplift for SMBs and NFPs? What role should government play in supporting / endorsing SMB tailored standards?

We believe the fundamental question is whether one 'homogeneous' standard can realistically exist for an extremely 'heterogeneous' combination of organisations with vastly different types of cyber risk. Particularly if it is to be holistic (i.e., across people, process and technology), and 'simple'.

For example, the Essential Eight is primarily a technology-focused standard for mostly 'Windows-based' environments. It under-emphasises the importance of 'People and Process" and does not address the cause of a large percent of cyber incidents – which are people-based.

Therefore, we suggest the effort to identify a 'simple, one -size fits all' standard might be better focused on helping individuals and organisations understand and mitigate the unique cyber risks that are relevant to them, rather than developing an all encompassing list of controls for a standard.

The shift from the Australian Government's ACSI-33 to the ISM, recognised the need to shift from prescriptive controls to choosing controls based on risk. ISO27001 is founded on making risk-based decisions. Furthermore, APRA regulations are risk oriented.

[5] https://cybersecurityclinics.org/about/

We believe that Government should play a role in supporting risk-based decision-making, not simply touting that all controls of a generic standard should be met.

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?

In our opinion, there are no 'unique' challenges that NFP's face.

Access to "resources" (funds, skills, etc.) is the most significant challenge that nearly all NFP's and the vast majority of ALL other organisations face with cyber security.

As you may know, each of the five major banks, have multiple HUNDREDS of staff focused exclusively on security, yet they still fall victim to costly and impactful cyber incidents. Therefore, can we realistically expect small organisations (NFP's or other) to protect themselves when their ENTIRE staff numbers are less than one bank's security team alone?

Cyber is a 'relatively new' concept which many organisations have never had to resource. As one of our clients said "I can go broke trying to be secure", and thus, the attitude of "I haven't spent any money on it in the past, why do I need to do it in the now?" is a prevalent attitude that needs to be adjusted. It's also why a 'risk-based' approach will reinforce that organisations don't simply feel pressured by regulators to implement 'controls', but if done properly, will identify those controls that most effectively mitigate an organisation's most critical cyber risks. Migrating away from 'control-based' approaches to risk-based concepts is inevitable and we need to educate all types of organisations to the benefit of a risk-based approach.

On a totally different note, and from our experience assisting a diverse range of NFP's, we frequently see that most of these organisations will pursue unique/individual technology strategies that support just that specific NFP's activities alone. Most of these technology environments are created individually 'on the smell of an oily rag' and are designed and managed by small Managed Service Providers operating on a limited budget.

We believe there would be significant opportunity to improve the NFP 'Cyber Poverty Line' (refer to answer for question #7) by offering a centralised, yet securely configured and managed 'office technology environment' (like Microsoft Office 365) for small NFP's. Because of scale, these services could be cost effective for the NFP, and if potentially subsidised via the Government, it could be an attractive approach to better 'protect' this group of vulnerable organisations by leveraging a consistent and well configured office technology environment that would likely cover a large portion of their technology needs. The concept of 'approved' NFP's (via the ACNC?) could further be tailored to target those NFP's who, through their work, capture, process and store highly confidential Personally Identifying Information, or other private or confidential data.

The role of cyber insurance in strengthening cyber resilience for businesses and NFPs

11. Do you consider cyber insurance products to be affordable and accessible, particularly for SMBs? If not, what factors are holding back uptake of cyber insurance?

We do not feel we can add a different, insightful idea or unique perspective for this question, or that has not already been made in previous responses.

Ransomware and cyber extortion

12. How well do you consider you understand the threat of ransomware, particularly for individuals and small entities? How is this threat evolving or changing?

From our experience, the threat of ransomware is not well understood by many organisations – particularly individuals or medium to small entities. As criminals get easy access to better information via various Artificial Intelligence programs, the threat will only increase in sophistication and evolve to find more effective ways to access an organisation's data or technology to ransom.

That said, Trusted**Impact** believes that the current 'approach' that the Government has taken to communicate the risk of ransomware, often causes confusion and can lead to inaction. This happens because, we too frequently couch the conversation in obscure or complex terms. For example, by using obscure names like 'Fancy Bear' or 'Volt Typhoon' we create an 'aura of savant hackers' who – irrespective of what an organisation does to protect themselves – can easily bring the company to their knees.

But on a relatively simple level, just having a sound, well maintained (and practiced) 'data backup' plan and process, in many circumstances, will mitigate the ('availability') risk of ransomware for smaller organisations. We believe the Government should focus less on communicating the 'Fear, Uncertainty, and Doubt' of ransomware, and more about the basic, often simple, steps that organisations can take to mitigate this major risk.

13. How could the government further support businesses and individuals to protect themselves from ransomware attacks?

Australia has a useful insurance scheme to support workers who are impacted by work-related accidents via WorkCover. While this topic does not align entirely with our core capability and firm experience, we suspect there may be a worthwhile analogous 'model' to consider for ransomware incidents.

Enhance support for citizens and victims of cybercrime to help them bounce back quicker

14. Have you experienced or researched any vulnerabilities or impacts from cyber security incidents that disproportionately impact your community, cohort or sector? If so, what were the vulnerabilities and impacts that your community faced?

We do not feel we can add a different, insightful idea or unique perspective for this question, or that has not already been made in previous responses.

Strengthening Australia's identity crime response by scaling victim support and exploring systemic protections

15. How can support services for victims of identity crime be designed to be more effective in the context of increasing demand? How can technology be used to support individuals in managing and recovering from identity crime?

We have referred several individuals and small businesses to 'IDCARE'. All mention how helpful the service is for both individuals and organisations who have been impacted. We suspect there would be ways to 'automate' a portion of the assistance process, but note that the ability to get to 'real people' to help with something that can be very traumatic is worthwhile and extremely beneficial.

Harmonise and simplify cyber regulation to promote best practice and efficiency

16. Which regulations do you consider most important in reducing overall cyber risk in Australia?

From our perspective, there are TOO MANY regulators focused narrowly on their legal remit – either as a 'geography' (state-based Info Commissioners), 'function' (ie, Privacy), or as an industry sector (ie, APRA), and many who have vastly different levels of legal authority or the

ability to require organisations to respond appropriately. Simply creating a 'map' of regulators relating to cyber security would highlight this issue.

Furthermore, we see little coordination / harmonisation of what one regulator is doing in relation to the others to either:

a) Reuse or leverage common tools, approaches, advice so that we can be more efficient at regulation (reinventing the wheel over and over), and

b) To be more consistent in the approach, advice, requirements and expectations for different types of regulated organisations.

We believe there would be significant opportunities to improve the situation by rationalising, consolidating, and simplifying the hodgepodge of regulators who have cyber either as a focus or as part of their overall remit. As part of this rationalisation, it would be essential to ensure there was the legal authority and ability to impress action from those regulated.

17. Have regulatory/compliance requirements negatively impacted the cyber maturity of your organisation? How are you currently managing these issues?

Definitely. For many of our clients, their disparate and often overlapping regulatory/compliance requirements have negatively impacted them from their need to iteratively respond to different entities with different frameworks.

Simply keeping the alignment of controls to different frameworks can be a significant effort and is a constant undertaking. The tendency is to focus one's effort on responding to requests for information, rather than spending that time to ensure that controls are effective and that practical risks are being managed.

This challenge is significant if an organisation is an Australian-only organisation, but exponentially increases if they have international business and must align with other country regulators in addition to the Australian regulators.

3.2. Shield 2: Safe technology

Ensure Australians can trust their digital products and software

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?

Although unrelated to 'digital devices' as the category suggests, and as referred to in the answer to question # 2, Trusted**Impact** is partnered with a global consulting firm to design and develop both; an Enterprise-level, AND Federal-level cyber risk management framework for a Country in the Middle East.

This program established something that does NOT exist at a Federal level in Australia – which is the ability to identify cyber risk at an individual departmental or agency level, but more important, to then aggregate these risk registers so that the country's most important risks – at a national, integrated, and aggregated level – can be identified and controls to be put into place to mitigate these risks.

If Australia has aspirations to be a "world leader in cyber security" (per the latest strategy), this is an obvious 'gap' which Horizon 2 must address.

In addition, recent legislation has been announced by the United States regarding better protecting devices categorised as "IoT" and the "Trust Mark" similar to the United Laboratories

marking for electrical devices. It would be worth assessing the applicability of this to Australia. (https://www.fcc.gov/CyberTrustMark)

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?

Please refer to the above for the "Trust Mark" activities occurring in the United States.

20. What additional guidance do you or your organisation need to manage foreign ownership, control or influence risks associated with technology vendors?

We do not feel we can add a different, insightful idea or unique perspective for this question, or that has not already been made in previous responses.

Protect our most valuable datasets

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?

We do not feel we can add a different, insightful idea or unique perspective for this question, or that has not already been made in previous responses.

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?

We do not feel we can add a different, insightful idea or unique perspective for this question, or that has not already been made in previous responses.

Promote the safe use of emerging technology

23. What guidance can government provide to support the safe and responsible uptake of critical and emerging technologies? What do you consider to be the most serious national security risks presented by critical and emerging technologies, such as AI?

We do not feel we can add a different, insightful idea or unique perspective for this question, or that has not already been made in previous responses.

3.3. Shield 3: World-class threat sharing and blocking

Encourage and enable the private sector to block threats and take a more proactive posture against cyber threat actors

24. What could government do to support and empower industry to take a more proactive cyber security posture to ensure the resilience of our cyber security ecosystem? What do you think Australia's proactive cyber security posture should look like for industry?

The establishment of "Information Sharing and Analysis Centres" (ISAC's) – as noted in the document - is a positive step so that common industry groups can share information, etc. Yet we note that there are only TWO ISAC's in Australia – the Critical Infrastructure (CI-ISAC and the newly created, yet to be operational, "Healthcare ISAC 'pilot'".

In comparison, we believe the US has 28 ISAC's. While there would undoubtedly be some Australian organisations participating, that would only be a few of the largest organisations.

These ISAC's are commonly touted by many security professionals as being valuable, and therefore, we should not be 'shy' about creating more then just "one and a half".

25. Does the government need to provide clarity on permissible and non-permissible Active Cyber Defence in the Australian context?

Yes. Clarifying what is and is not permissible for 'Active Cyber Defence' would be very beneficial to better understand how best to repel a common threat.

Amplify existing government and industry models for threat blocking and threat sharing

26. How could government further support industry to block threats at scale?

We do not feel we can add a different, insightful idea or unique perspective for this question, or that has not already been made in previous responses.

27. How could the use of safe browsing and deceptive warning pages be amplified?

We do not feel we can add a different, insightful idea or unique perspective for this question, or that has not already been made in previous responses.

28. What more is needed to support a thriving threat sharing ecosystem in Australia? Are there other low maturity sectors that would require ISACs, and what factors, if any, are holding back their creation?

With a base of over 400 clients, we can easily state that there are LOTS of low maturity sectors. However, we suggest the key is to identify those sectors, that because of the nature of their business, capture and store extremely sensitive data that can be exploited or monetized. We suggest the Government should work to identify, map, and better understand these 'hot spot sectors' in our economy before they are exposed by criminals and so that proactive resilience campaigns can be undertaken to improve their maturity and reduce this extreme risk.

One perfect example, is the real estate industry which captures some of the most highly sensitive Personally Identifying Information (PII) ranging from identity documents to financial information on the very large population of our citizens. However, it is our experience that the maturity of this industry is one of the lowest we've seen over our 19 years. The real estate 'eco-system' is particularly vulnerable when viewed as an integrated whole across all aspects of legal / conveying, financing / lending, estate agents, leasing agents, and overall real estate-technology that captures and stores the information, etc.

This risk is further compounded by the fact that many traditional 'systems' used to process mortgage and related information have been migrated from separate, office-based local server-based applications to consolidated cloud-based applications. What historically was the risk of one physical server in a mortgage providers office with a small database of highly sensitive data on 'hundreds' of customers, is now an huge, internet-exposed, database of 'hundreds of thousands' of customers.

29. How can we better align and operationalise intelligence sharing for cyber security and scams prevention?

We do not feel we can add a different, insightful idea or unique perspective for this question, or that has not already been made in previous responses.

Reviewing policy frameworks as necessary for resilience to a widespread incident, conflict or crisis situations to protect Australia's national interests

30. Are the roles and responsibilities of government and industry clear for cyber

security in a conflict or crisis scenario? What activities, such as cyber exercises, could Government undertake to make you feel better prepared to respond in a cyber conflict or crisis?

Roles and responsibilities for dealing with security in a conflict or crisis have improved significantly with the establishment of the National Cyber Security Coordinator. We applaud that decision.

However, we believe more can be done. A few key suggestions are:

1) For our experience the specific roles, responsibilities between Government and Commercial Organisations at the time of an incident are unclear and not well understood by most organisations. Because of that, we find that companies are hesitant to involve Government in a time of cyber crisis.

2) Many organisations simply do not prioritise the value and benefit from conducting a 'cyber exercise'. To be clear, we help clients with cyber incident planning and simulations, so we are biased in this perspective. Nonetheless, the adage is true that: "one does not 'rise to the occasion' in a time of crisis, they fall to their lowest level of training".

   A large majority of organisations have never considered the ramifications of a cyber incident, have not conducted an exercise, or if an exercise has been conducted, it's often years old or done so infrequently that it's ineffective in a real crisis.

3) SoCI has been very beneficial to impress the importance of undertaking cyber exercises. But to date, the majority of this has been focused on individual businesses and from their perspective only.

   What is lacking, is our need to 'abstract above' individual businesses and consider the broader 'integrated eco-systems' that we rely upon as a country for critical services. For example, one of our largest country assets, superannuation. We appreciate that there has been two 'limited' exercises performed for parts of the superannuation ecosystem (Gateway operators), but this was initiated by an industry body that was chartered with consistency and protection across the Gateways. Individual organisations will not typically identify or see the value to do this, so we suggest that it must be fulfilled by either government or regulators.

Managing vulnerability disclosure

31. How could government better incentivise businesses to adopt vulnerability disclosure policies?

Trusted**Impact** has been performing all types of technical assessments (i.e., vulnerability assessments, penetration testing, white/black/grey hat hacking, ethical hacking, forensic evaluations, configuration assessments, etc., etc.) on a full-time, focused basis across several of our 'researchers' for nearly 20 years.

A comprehensive answer to this question would be extensive and cover a breadth of areas ranging from how 'researchers' are skilled/vetted (how do we know a 'white hat' hacker doesn't moonlight as a 'black hat'?), through to how to disclose flaws or vulnerabilities in a range of practical examples.

For example, a severe, easily exploited vulnerability was recently identified in a cloud / SaaS system while testing on behalf of a local Council – the same flaw would exist for OTHER Councils who were also the clients of the SaaS system – yet, the 'rules' or process of how one goes about trying to resolve this vulnerability on the broader scale are unclear and ineffective.

If the assessors of this document would like to explore this topic in greater depth or understand the wealth of concerns on this topic, Trusted**Impact** would be delighted to meet with the appropriate individuals to provide more concrete examples and suggestions.

32. Does Australia need a vulnerability disclosure program to provide security researchers with a mechanism for safely reporting vulnerabilities?

In our opinion, no. With the international nature of technology and the importance to share vulnerabilities to other 'friendly nations', it would seem to be redundant and not a good use of funds for Australia to create a separate disclosure program focused only in Australia.

3.4. Shield 4: Protected critical infrastructure

Maturation of our regulatory framework for critical infrastructure security

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?

SoCI has been a very positive step in the right direction by establishing legal requirements to improve the resilience of our critical infrastructure.

For our perspective, additional clarification (as appropriate for national defence) on what/who should be considered 'critical infrastructure' would be beneficial. For example, it is often obvious who clearly 'WOULD' be included (i.e., a large, listed electric utility), and who would clearly 'NOT be included' (i.e., a single family home with solar on the roof), but the 'grey area' between those two categories is what is needed to be clarified, as even smaller players may introduce risks to a sector that hasn't been considered.

34. Are there significant cyber security risks that are not adequately addressed under the current framework?

Other than the comments made in Question #30 about needing to 'abstract' above individual companies to protect 'integrated eco-systems', we do not feel we can add an insightful idea or unique perspective for this question.

35. Is the regulatory burden on industry proportionate to the risk and outcomes being sought?

We do not feel we can add a different, insightful idea or unique perspective for this question, or that has not already been made in previous responses.

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?

We do not feel we can add a different, insightful idea or unique perspective for this question, or that has not already been made in previous responses.

Centralising cyber security risk management and prioritising investment and policy interventions for Commonwealth cyber security uplift to drive more coordinated outcomes

37. How can the Australian Government support private sector partners to better engage with government security requirements, including certifications and technical controls?

History has shown that the Australian Government, at the Federal level, either engages with very large, international organisations to assist it with its government security requirements, or utilises local, individual contractors – with very few 'in between'.

We are obviously biased in this perspective, but the truth is, our country's cyber capability would be better if the Federal Government shifted it's 'overwhelming preference' from non-Australian international companies to supporting the local cyber ecosystem.

For example, Trusted**Impact** has been approved and qualified to be part of the Federal 'Digital Marketplace' panel for over 15 years. But over that period of time, we have only had ONE potential opportunity come through that 'channel'. For that reason, we have chosen not to be recertified in the latest round of the Federal Digital Marketplace.

38. How are Australian Government security requirements or frameworks being considered or adopted among private sector partners, including in critical infrastructure?

We do not feel we can add a different, insightful idea or unique perspective for this question, or that has not already been made in previous responses.

3.5. Shield 5: Sovereign capabilities

Promote a sustainable and diverse cyber workforce and business ecosystem

39. What role should government play in supporting the development and growth of Australia's cyber workforce? What initiatives, pilots or policy ideas do you think would best support industry to grow?

Please refer to the response to question #7, which highlights the potential opportunity to help organisations under the 'Cyber Poverty Line' (Not For Profit, Community led organisations, etc.) and in parallel, provide university students with practical 'hands on' experience as part of improving our country's cyber capability.

Trusted**Impact** (pro bono) has been working with a student-led project at Swinburne University to develop an initial plan on how this might work. More information may be available by the time this input has been received, and we would be happy to share the initial findings with appropriate constituents from the Government if desired.

40. What have been the most successful initiatives and programs that support mid-career transitions into the cyber workforce and greater diversity in technology or STEM-fields more broadly?

We do not feel we can add a different, insightful idea or unique perspective for this question, or that has not already been made in previous responses.

41. What are some of the industries with highly transferrable skill sets that could be leveraged to surge into the cyber workforce? Is there any existing research/data that could support these efforts?

We do not feel we can add a different, insightful idea or unique perspective for this question, or that has not already been made in previous responses.

Provide greater support for academic research and strengthen collaboration between academia, industry and Government

42. How can industry, academia, think tanks and government best work together to set research priorities and drive innovation to further our strategic, economic and

community interests and achieve our common goals?

For this to occur, we believe that Government must 'take the lead' to define, structure, orchestrate, and operate open and collaborative forums with specific objectives in mind.

Other than for overall altruistic reasons, the individual 'piece parts' – whether that be a university, business, etc. would typically see little 'direct benefit' to that organisation to undertake the 'setup and operate' aspects of this type of forum. Thus, there would be pressure to focus primarily on the individual priorities of that organisation.

Alternatively, the majority of industry-oriented 'conferences' are expensive to participate in, exclusive by requiring participants to pay for their involvement, and are never focused on fostering collaboration to resolve difficult cyber risk topics.

There have been limited situations where we have seen this occur successfully in the last 19 years (eg RAND orchestrated something like this over a decade ago), but more collaboration with disparate parties would be very beneficial for our sector and the country overall.

43. How can government and academia enhance its direct partnership and promote stronger people-to- people links and collaboration on research and policy development activities?

We do not feel we can add a different, insightful idea or unique perspective for this question, or that has not already been made in previous responses.

Nurture the growth and development of robust sovereign capabilities

44. How would we best identify and prioritise sovereign capabilities for growth and development across government and industry?

In the last two years, two 'previously sovereign' organisations that would have comprised a majority of the 'resources, skills and capability' in cyber, have both been sold to extremely large, international organisations (TNT-Thales and CyberCX-Accenture).

While we appreciate that it is impossible to influence these transactions (other than blocking for anti-competitive reasons), our country nonetheless, has sold a significant portion of the country's cyber capability to organisations who may not prioritise Australia highly in a time of conflict.

45. What are the areas of most concern for ICT concentration and what do you consider would be most effective as mitigation strategies to explore?

A few years ago, Trusted**Impact** undertook a study into the adoption of the cloud and security preparedness by interviewing 30 leaders in the technology and security industry. There were several important findings, but one of the significant observations which was intentionally not highlighted, was the fact that ALL of those leaders were adopting cloud technology and those were primarily concentrated into either AWS or Azure.

If, this was reasonably extrapolated for other organisations in Australia, it is more than probable that the vast majority of our country's 'digital capability' resides in one of two US-based cloud providers. This is a frightening level of concentration from many perspectives that should be understood and mitigated at a Government level.

If interested, a copy of our cloud security report can be found at: http://trustedimpact.com/pdfs/TrustedImpact_AISA_Leadership%20Series_Skys%20the%20Limit_Digital%20Version.pdf

3.6. Shield 6: Strong region and global leadership

Continuing to use all arms of statecraft to deter and impose costs on state and non-state malicious cyber actors

46. Do you view attributions, advisories and sanctions as effective tools for countering growing malicious cyber activity? What other tools of cyber diplomacy and deterrence would you like to see Australia consider for development and use to effectively combat these threats in Horizon 2?

We do not feel we can add a different, insightful idea or unique perspective for this question, or that has not already been made in previous responses.

Strengthening cyber resilience and cooperation on critical technologies in the region and reinforcing Australia's partner of choice status

47. Are there additional ways the Australian Government could engage with Southeast Asia or the Pacific to ensure a holistic approach to regional cyber security?

We do not feel we can add a different, insightful idea or unique perspective for this question, or that has not already been made in previous responses.

48. Is there additional value that Cyber RAPID can provide in the region beyond its current design and scope?

We do not feel we can add a different, insightful idea or unique perspective for this question, or that has not already been made in previous responses.

Continuing to shape, uphold and defend international cyber rules norms and standards in our interests

49. In which forums and on which issues would you like Australia to focus efforts to shape rules, norms and standards in line with its interests most effectively in Horizon 2?

We do not feel we can add a different, insightful idea or unique perspective for this question, or that has not already been made in previous responses.

Driving a program of international regulatory alignment and enhancing regional cyber policy and regulatory capacity

50. What regulatory frameworks or requirements should be prioritised for consideration as part of Australia's efforts on international cyber regulatory alignment?

We often see an over emphasis on 'diplomatic conversations' that may be beneficial in establishing cooperation with other nations over time, but which don't always result in outcomes that are beneficial to the countries involved.

Therefore, we suggest a particular focus should be placed on coordinating law enforcement activities across jurisdictions so that perpetrators can be physically held accountable and exposed to the world as convicted criminals.

For example, do we really think a young intelligent 'hacker' living outside of Australia would be concerned that the Australian Federal Police would ever 'knock on their door'

and punish them from their illegal activity? Doubtful. Until we can reasonably demonstrate that cyber criminals will be punished for their illegal activity, technically astute individuals (young or old), will consider the illegal side of cyber, rather than the legal side.

_____End of Submission.