Response to Charting New Horizons Policy Discussion Paper

Date: 29/08/2025

xAmplify Services Pty Ltd

[redacted]

w www.xamplify.com.au

Authorisation

Authorised by:	Contact for further Information:
[redacted] [redacted] xAmplify Pty Ltd Email: [redacted]	[redacted] [redacted] xAmplify Pty Ltd Email: [redacted]

Conditions and Assumptions:

This document is being provided to the Department of Home Affairs in response to the request for feedback and comment on the Policy Discussion Paper *Charting New Horizons – Horizon* 2

The feedback, suggestions and recommendations provided in this response have been collated from the collective experience and knowledge of our personnel who have deep experience in this area from a technical perspective, and from policy and implementation of action plans points of view.

Table of Contents

Overview

Thank you for the opportunity to put forward our views on the *Charting New Horizons – Horizon 2 Policy Discussion Paper* (the paper). We strongly agree with the intent expressed in the Minister's foreword, "*… to further embed cyber messaging, standards capability and efforts across society, empowering our businesses and citizens to protect themselves*".

The building of and embedding cyber security practices into the fabric of our nation's operations, so people don't even think about it other than just normal practice, is essential to achieve and sustain the goal of the government's *2023–2030 Australian Cyber Security Strategy* (the strategy), "*We envisage a future where stronger cyber defences enable our citizens and businesses to prosper, and to bounce back quickly following a cyber-attack*".

Through our experience providing strategic, operational and tactical level cyber security advice and services in the public and private sectors, we have seen firsthand the gaps in the understanding and appreciation of what it takes to secure and then maintain effective cybersecurity. The cause of those gaps varies, but organisational factors feature more than technical ones.

It is heartening to see a range of questions in the paper that look at the organisational factors, either through extending cyber awareness and support to Small and Medium Businesses (SMB) and the Not-For-Profit (NFP) sectors, as they will need tailored support. The focus on developing and educating a cyber security workforce will also be critical, in having the right size and shape workforce with the right skills to support the strategy's outcomes.

We agree that government has a key role, but it must be truly cooperative with the private, academic and NFP sectors. There will be challenges in establishing the roles and responsibilities of the different sectors, but they can be overcome through clear communications, ongoing dialogue, and by building trust. In our response, we have highlighted the need for change impact and management to be integral to implementation of the strategy.

We have been selective with our responses, focusing on questions where we have the expertise to provide insights informed by real world experience and highlight the areas that we believe will provide the greatest impact and most valuable to contribution to support the government's objectives. In the following *Framework for our Response* section we have provided a summary of our views across the Shields to provide context, before providing observations, suggestions, and recommended actions in the detailed responses to the *Responses to Questions* section.

About xAmplify

xAmplify is a 100% Australian owned and operated business that specialises in solving real world problems by aligning strategy, people, and technology to create transformation that lasts. We integrate human capability with AI and automation to deliver practical solutions that generate value today and keep organisations ready for tomorrow. The result is measurable business impact, sustained performance, and long-term customer value.

We bring an Australian approach to using business transformation, technology services, and enterprise platforms to help organisations stay ahead of rapid technological change. Our human-centred approach ensures transformation is fast, sustainable, and focused on business impact.

We have a deep technical understanding of the cyber security landscape, through our work helping organisations to mature their cyber security capability. We also have members of our team who have worked in senior executive roles across the public, SMB and NFP sectors, so we can bring their real-life experience and practical understanding of the challenges those sectors face.

Framework for our Response

Approach

To provide a practical response to the department's request for feedback, comment and suggestions that will support identifying and developing policy options, we have structured it to establish a holistic view of the government's objectives, and the main challenges and risks we consider that the future policies will have to address.

We have identified challenges, themes and key considerations under each of the main headings in the paper, to set the scene for and provide linkages to the specific questions, as follows.

Developing our vision for Horizon 2

The policy discussion paper sets out a clear and achievable direction, yet its impact will be greatest if five critical challenges are addressed.

1. Adopt an outcomes-focused approach.

   The central objective should be to strengthen Australia's national cyber resilience and uplift cyber security across all sectors. Rather than relying on a prescriptive regulatory model and a compliance-based approach, government should focus on setting clear, outcome-based goals grounded in appropriate and commensurate risk management. This approach enables a consistent regulatory baseline while allowing organisations and sectors to tailor their strategies and controls to their unique risk profiles and operational contexts. It promotes flexibility, innovation, and accountability—ensuring all entities contribute meaningfully to the national cyber security agenda without being constrained by rigid, one-size-fits-all rules.
2. Establish an underpinning governance and assurance framework.

   Effective implementation requires robust structures for planning, oversight, review, and reporting. A governance and assurance framework should underpin delivery of the strategy, drawing on the guidance and processes of leading examples in this area, like the EU's Digital Operational Resilience Act (DORA), as an initial reference point.
3. Build resilience through flexible regulation and policy.

   Given the rapidly evolving technical, societal, and business environment, cybersecurity related legislative, regulations and policies must be capable of continuous monitoring, assessment, and adjustment. Responsiveness will be critical to ensuring the strategy remains relevant and effective through to 2030 and beyond.
4. Embed change management practices.

   Implementation of the policy will directly or indirectly impact organisations and individuals, creating uncertainty and potential resistance. Success therefore depends on embedding change management practices into both planning and monitoring processes, closely connected with the underpinning governance and assurance framework described above.
5. Use Evidence-Based Decision Making.

   Government policy and planning must be grounded in evidence, supported by systematic data collection, performance metrics, and clear evaluation criteria. Continuous monitoring and assessment will ensure that strategic objectives are being met and allow for timely adjustments. Industry must contribute relevant data and insights and demonstrate how actions support the achievement of national cyber security outcomes. Where negative impacts are identified, both government and industry must respond with agile, informed adjustments.

6. Bridge the gap between policy and practice with practical patterns and guidance.

   High-level policy settings and regulatory frameworks are critical, but in our experience by themselves will not drive consistent and effective cyber resilience. Organisations faced with resource constraints struggle to translate abstract requirements into practical actions.

   Government should collaborate with industry, standards bodies, and academia to co-develop reference patterns, playbooks, and practical guidance for common challenges. Areas to focus on could include mitigating risks from legacy applications, managing end-of-life technologies, securing multi-cloud deployments, or uplifting identity and access management in resource-constrained environments.

   These resources would

   - provide repeatable, industry-aligned solutions to well-known risks
   - reduce duplication of effort across sectors
   - enable organisations to act with confidence that their measures are consistent with national objectives, and
   - help overcome barriers stemming from capability gap by creating a set of "ready-to-adopt" approaches that can be implemented without deep specialist expertise.

Shield 1: Strong businesses and citizens (Q5-17)

In the discussion points and questions under Shield 1, the references to the different industry sectors makes it difficult to describe specific actions or recommendations, as they will vary according to the size, nature and maturity of the industry sectors. For the purposes of providing responses to the questions related to Shield 2 we have applied the following assumptions:

- organisations included under the existing definitions of Critical Infrastructure have support networks and mechanisms in place under the *Security of Critical Infrastructure Act 2018* and provided by Cyber and Infrastructure Security Centre, although they can vary according to the size of the operator
- the SMB sector is well supported through the Cyber Warden program, managed through the Council of Small Business Organisations of Australia (COSBOA), which provides tailored guidance and resources, and
- the NFP sector does not have a coordinated approach and is comparatively under-resourced to develop its cyber and operational resilience. There are no dedicated, large-scale national program focused purely on NFP cyber resilience. However, given the extremely sensitive data held by, for example, NFP organisations operating in the health sector, the impact from any unauthorised release of data would be extreme.

Our responses to Questions 7, 8, 9, 10, 16 and 17 are set against the above assumptions.

Shield 2: Safe technology (Q18-23)

Recent reforms to the *Privacy Act 1988* and the *Cyber Security Act 2024* mark a significant step forward in aligning Australia's legislative and regulatory frameworks with internationally recognised best practices, particularly those adopted in the UK and European Union. While these jurisdictions operate under different legislative structures and cultural norms—making direct comparisons complex—their frameworks offer valuable insights that Australia has begun to incorporate. These changes enhance Australia's ability to participate in global efforts to strengthen privacy and cybersecurity.

However, there remains an opportunity to further improve Australia's approach by shifting toward more outcomes-focused regulatory language, which would promote a more flexible and innovative risk-based approach and more effective compliance across sectors. Our response to Questions 18 and 22 provides more details and suggestions considering the setting above.

Shield 3: World-class threat sharing and blocking (Q24-32)

In reviewing the paper and the questions posed under this section, the key theme that we identified was "trust". To achieve the desired outcomes, government will have to establish a sense of trust with industry and the community, to avoid unnecessary worries or fears of government overreach – which ties in with the challenge noted under the earlier part *Developing our vision for Horizon 2*, assessing the impact of change.

Our responses to Questions 26, 28 and 30 Part 2 provide highlights on where trust needs to be established, and suggestions for actions.

Shield 4: Protected critical infrastructure (Q33-38)

The discussion points in the paper and the structure of the questions suggest that the government is viewing industry and private sector partners as a homogenous group. The danger for the government is that businesses and other organisations range from very large, to very small, and different approaches will have to be developed and implemented. In the earlier Questions Q7-10 inclusive, the SMB and NFP sectors were highlighted, especially the unique challenges they might face.

Our responses to Questions 36 and 37 highlight where government will need to tailor its approaches, and bridge current gaps.

Shield 5: Sovereign capabilities (Q39-45)

The concept of "Sovereign Capabilities" is a current topic that is receiving a lot of attention in the Defence sector, and there are parallels that can be drawn and applied to this paper. One key element is what makes an Australian Sovereign Capability and the definitions that will be applied to set the appropriate level of coverage, and ability to access resources and funding from the government.

Our responses to Questions 44 and 45 put forward suggestions for how those definitions can be developed and applied.

Shield 6: Strong region and global leadership (Q46-50)

We commend the Australian Government's proactive initiatives to strengthen our presence and influence within international standards-setting bodies, as outlined in the Cyber Security Strategy. The focus areas identified under initiative 20 reflect a strategic commitment to shaping global norms and fostering regional cyber resilience. At this stage, we have no further comments or suggestions, other than to express our full support for the key objectives and themes presented.

Responses to Questions

Developing our vision 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?*

While it is difficult to predict the exact nature of future technological trends such as the rapid emergence of generative AI tools, the pace of innovation is accelerating, and with it, the complexity and scale of cyber threats. These developments have already expanded the attack surface and enabled more sophisticated criminal activities.

Rather than attempting to forecast specific technologies, government should prioritise agility in its cyber security strategy. This means embedding flexibility, responsiveness, and resilience into policy and planning frameworks to ensure Australia can adapt quickly to emerging technologies. The risk of failing to adopt and integrate new technologies is not just missed opportunity, it could expose critical systems to significant cybersecurity vulnerabilities.

Current strategic approaches often rely on static assumptions (e.g., "if we do X, Y will happen"), which are insufficient in a dynamic threat landscape. Government must shift toward adaptive models that allow for continuous monitoring, rapid response, and iterative improvement. The only certainty is that the rate of technological change will continue to accelerate, and cyber security strategies must evolve accordingly to safeguard national interests.

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

In the paper *Figure 5. Cyber Security Policy Evaluation Model* p11, presents a good coverage of the key areas. However, it could be improved by incorporating another element next to the existing blue circle "Code of Practice for App Stores and Developers" at the bottom right, with an additional one for "Code of Practice for those who hold or manage Data".

We suggest that the government develop a practical Code of Practice for this element, to bring together the different principles and responsibilities under relevant Acts and Regulations into a single statement.

Shield 1: Strong businesses and citizens

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.)?*

To build a more resilient and digitally capable economy, government must lead a cultural shift that encourages small and medium-sized businesses and not-for-profit organisations to critically assess how they use connected digital services. These services should be consumed responsibly and strategically to support core organisational objectives.

Programs such as *Cyber Wardens* demonstrate how practical initiatives can build digital confidence and cyber awareness. Research from this program shows that 17 percent of small businesses have experienced data leaks due to breaches in other organisations, and 10 percent have had accounts or passwords compromised highlighting shared vulnerabilities across sectors.

While small businesses benefit from strong representation and tailored support, the not-for-profit sector lacks a coordinating body with an operational focus. The Australian Charities and Not-for-

profits Commission plays a regulatory compliance role but does not appear to provide practical guidance on cybersecurity or digital service consumption.

Given the interconnected nature of digital systems, many challenges and solutions are not sector specific. This presents an opportunity to develop shared support mechanisms that are accessible to all organisations, regardless of size, mission, or maturity. Rather than creating new frameworks for each sector, government should expand proven models like *Cyber Wardens* to ensure inclusive, scalable support across the economy.

This approach promotes responsible digital consumption and embeds cybersecurity into broader business continuity and disaster recovery planning, helping all organisations build the resilience needed to thrive in a connected environment.

8. How can industry at all levels and government work together to drive the uptake of cyber security actions by SMEs and the NFP sector to enhance our national cyber resilience?

To meaningfully enhance Australia's national cyber resilience, a cultural shift is required. A shift that champions the adoption of outcomes-based cybersecurity principles across all sectors. This shift must move beyond traditional compliance models and instead promote a mindset of continuous evaluation. This requires every organisation to take active responsibility for ensuring that the digital services and technologies used directly support the organisation's strategic objectives.

Only through this approach can government and industry demonstrate that they are genuinely supporting the needs of organisations in a way that is proportionate to their scale and risk profile. By embedding cybersecurity as a strategic enabler rather than a technical afterthought, and by fostering a shared responsibility model, Australia can develop a resilient, inclusive, and adaptive cybersecurity ecosystem. This cultural transformation is not optional it is essential to securing the national interest.

9. What existing or developing cyber security standards, could be used to assist cyber uplift for SMBs and NFP's?

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?

Small businesses contribute over one-third of Australia's GDP and comprise 98% of all enterprises, according to the Australian Small Business and Family Enterprise Ombudsman. Similarly, Australia's 57,000+ not-for-profit organisations generate over $200 billion annually, delivering vital services across education, health, environmental protection, and more.

Despite their importance, SMBs and NFPs face growing cyber threats. The Australian Cyber Security Centre (ACSC) reports a steady rise in incidents, with phishing, scams, and malware among the most common. These threats are often preventable, yet many organisations remain vulnerable.

This issue doesn't necessarily require new standards; existing resources from the ACSC already offer robust guidance but in our experience are underutilised. What's needed is a mindset shift: SMBs and NFPs must take ownership of their cyber resilience. Given their diversity in size, risk, and resources, a one-size-fits-all approach is impractical. An outcomes-based certification model, like

the UK's Cyber Essentials, could better support organisations to critically assess services, tailor security to their context, and avoid superficial compliance.

NFPs face unique challenges, including limited funding, varied operational models, and a lack of commercial incentives to invest in cybersecurity. Government interventions that would have the most impact include subsidised certification schemes, targeted education, and clearer guidance on managing outsourced ICT risks. These measures would support meaningful cyber maturity while preserving service delivery.

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

The most important legal and policy instruments contributing to the reduction of cyber risk in Australia include

- *Security of Critical Infrastructure Act 2018*
- *Data Availability and Transparency Act 2022*
- *Cyber Security Act 2024*
- *Privacy Act 1988*
- Protective Security Policy Framework (PSPF)
- Australian Government Hosting Certification Standard, and
- Information Security Manual (ISM).

These instruments provide a robust foundation for national cyber resilience, setting essential baselines for security and data protection across both government and non-government sectors. Their value lies not only in establishing minimum standards but also in their potential to evolve into outcome-focused, adaptive regulatory models that support innovation, sector-specific risk management, and long-term resilience.

To ensure these instruments remain effective and future-ready, it is critical to embed transparent, evidence-informed policy evaluation practices. Leveraging tools such as the OECD Public Policy Evaluation Toolkit and the Commonwealth Evaluation Toolkit can support a structured, principles-based approach to assessing regulatory performance. These toolkits emphasise the importance of

- clear policy objectives and logic models
- stakeholder engagement and cross-sector collaboration
- data-driven insights and performance measurement, and
- continuous improvement and policy learning.

By applying these evaluation toolkits, government agencies can ensure that cybersecurity related instruments are not only fit for purpose, but also capable of adapting to emerging threats, technologies, and operational realities. Putting in place an ongoing evaluative program also helps build public trust because it demonstrates that government is committed to continuous improvements in cybersecurity to protect the national interest.

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

In some cases, regulatory and compliance requirements have unintentionally constrained cyber maturity in organisations that we work with by reinforcing a compliance-centric culture. This can

lead to a focus on meeting prescriptive standards and the misapplication of scarce resources, rather than the achievement of strategic, risk-informed security outcomes. Such an approach may limit agility, reduce innovation, and result in suboptimal allocation of resources.

To address these challenges, a more outcome-oriented, adaptive and risk-based approach to cybersecurity governance is required. This includes

- aligning cyber related regulatory and legislative practices with the principles outlined in the OECD Public Policy Evaluation Toolkit and the Commonwealth Evaluation Toolkit, which emphasise transparency, stakeholder engagement, and the use of evidence to inform continuous improvement
- regularly reviewing the effectiveness of cybersecurity controls and cyber services providers, ensuring they remain responsive to evolving threats and operational needs.
- embedding evaluation and learning into cyber risk management processes, enabling a cultural shift beyond static compliance and toward risk-based continuous improvement, and
- encouraging cross-sector collaboration and knowledge sharing, to ensure that regulatory compliance also contributes to broader national security and resilience objectives.

By integrating these practical evaluation actions into its cybersecurity agenda, the government will be better positioned to ensure that compliance efforts are not only met but also leveraged to drive meaningful improvements in cyber maturity and public value.

Shield 2: Safe technology

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?

Frameworks such as the US NIST Cybersecurity Framework and the EU's NIS2 Directive offer outcome-based models that focus on setting clear security objectives, rather than prescribing specific controls. For edge devices, consumer energy resources (CER), and operational technology (OT), the approach embedded in these models would enable Australia to define targeted outcomes, while allowing industries to tailor implementation to their unique risk profiles.

International best practice also highlights the importance of robust governance and assurance. The EU's DORA provides a strong example of how assurance mechanisms can be embedded in critical infrastructure regulation. Australia should consider a governance framework that includes CER providers, OT operators, and device manufacturers, supported by audits, shared threat intelligence platforms, and independent oversight.

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 does Government and Industry work together to achieve this aim in an evolving global threat environment?

Initiatives like the Cyber Threat Intelligence Sharing (CTIS) partnership and collaborations between the Australian Signals Directorate (ASD) and major technology providers underscore Australia's growing commitment to proactive threat intelligence sharing and cybersecurity enforcement.

To build on this momentum, Australia should adopt clear, outcome-driven public policy security objectives that empower businesses to innovate confidently and cost-effectively considering the

risk and threat environment. Crucially this must be accompanied by a clear commitment to not being constrained by vendor lock-in. Some example objectives are set out below.

1. Interoperable Data Ecosystems

   Government should further facilitate secure data exchange across public and private sectors to enhance real-time detection and coordinated responses to fraud, cyber threats, and other digital risks.

2. Scalable Threat Detection Infrastructure.

   Invest in the development and deployment of adaptive, anomaly detection systems that can operate across diverse industries and evolve in response to emerging cyber threats.

3. Privacy-Preserving Data Collaboration.

   Encourage the adoption of privacy-enhancing technologies in machine learning, including federated learning and homomorphic encryption, to enable collaborative analytics on sensitive data without compromising individual or organisational confidentiality. Government can lead the way by incorporating these technologies into its own operations.

4. Cyber Resilience Benchmarks.

   Develop and implement standardised metrics and frameworks to assess, compare, and improve the cyber resilience of organisations across sectors. This could start by taking the PSPF reporting and assurance model and trialling it in government service delivery adjacent sectors.

By focusing on resilience, adaptability, and continuous improvement rather than rigid compliance, these objectives promote vendor neutrality and solutions that can be tailored to diverse risk profiles.

Shield 3: World-class threat sharing and blocking

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

Australia has taken significant steps to strengthen national cybersecurity through legislative instruments such as the *Security of Critical Infrastructure Act 2018* and the *Cybersecurity Act 2024*. These frameworks impose mandatory reporting obligations for cyber incidents and ransomware payments, enhancing visibility of threats and enabling coordinated responses across sectors. To build on this foundation, the government could define enforceable outcomes that apply across both public and private sectors. This could extend to using procurement practices and supply chain transparency to further drive secure technology adoption and reduce systemic risk.

For government support to be effective, it must be both practical and grounded in trust. Establishing clear roles and responsibilities between government and industry is essential to avoid perceptions of overreach. Defining what constitutes “threats at scale” will help clarify triggers for action and align them with those roles.

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?

To support a thriving threat sharing ecosystem, government will need to continually communicate and engender trust with industry, particularly with the low maturity sectors (e.g. the NFP sector),

but done in a manner that it appropriate to the different sectors (i.e. avoid a one-size-fits-all approach).

The NFP sector should have its own Information Sharing and Analysis Centre (ISAC) model, as it has unique characteristics, and unfortunately, in places low levels of understanding of the threat vectors and impacts. To minimise overhead and maximise reach, the government should use multiple communication channels (e.g. email bulletins, webinars, social media, and community networks) to distribute sector-agnostic threat intelligence and best practices. Messaging must be inclusive and carefully crafted to resonate across the broad spectrum of NFP sector organisations, as highlighted in our Shield 2 overview.

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

Desktop trials/tests of scenarios are valuable (e.g. wargaming) and can be a valuable tool to provide practical insight to the public of the cybersecurity environment. These are conducted internally by different organisations to identify any vulnerabilities, but there is a role for them to be used as an educational tool.

To have the most impact, the following considerations for conducting simulated or hybrid simulated/real exercises should be included in the planning processes.

- Extend the existing ASD Exercises in a Box model, micro-services examples to include cross industry and cross sector relationships and reflect the cross-dependencies and complexity of real-world situations.
- Create a playbook of scenarios, each covering different circumstances, environments and expected outcomes, relevant to the different industry and NFP groups.
    - Identify educational outcomes for each scenario and link them to the broader policy-based outcomes.
- Consider how to maximise the exposure and impact of conducting the desktop trials, across the relevant sector groups, which may include real, virtual or hybrid settings, and how participants can raise questions or be involved.
- Record and document the desktop trials, to provide ongoing educational resources.

Shield 4: Protected critical infrastructure

36. What support would assist critical infrastructure [(CI)] 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?

The current enforcement framework under the *Security of Critical Infrastructure Act 2018* relies heavily on prescriptive obligations and regulatory intervention. It includes powers for government to compel remediation of deficient risk management programs and respond to incidents through direct assistance. While this approach provides clarity and control, it can limit flexibility and innovation, particularly for smaller CI operators with diverse risk profiles. To support a proactive maturing of cyber and operational resilience, government should transition toward outcomes-oriented policy objectives, supported by continuous assurance mechanisms to evaluate effectiveness and inform refinement. Enforcement should focus on achieving measurable resilience outcomes, enabling CI operators to adopt tailored, risk-based approaches. This model

promotes continuous improvement, encourages innovation, and ensures all CI operators can contribute meaningfully to national resilience.

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

The government should continue to embed structured review and oversight mechanisms into its approach. The *Cyber Security Act 2024* provides a strong model, with mandated legislative reviews and the establishment of the Cyber Incident Review Board ensuring that requirements remain relevant, transparent, and responsive to industry feedback. Applying this approach to technical frameworks like the ISM and related guidance would improve clarity and adaptability. In and of itself this would make it easier for businesses to align with government's expectations. Regular reviews and stakeholder consultations would build trust, reduce compliance friction, and encourage proactive engagement from industry.

In addition, the government should have a clear definition of what are "private sector partners". The paper treats these "partners" as a homogenous group, which is not the reality. As highlighted in other parts of our response, to be successful government needs to

- map the sectors likely to be impacted by breakdowns in cyber security, to get a full appreciation of the coverage and nature of the different sectors – tied to our response to Question 44 below.
- establish a framework like the Chartered Institute for Information Security (CIISec) skills framework to align the essential skills sets required for people working in the different sectors, and
- conduct a gap analysis to clearly identify the size and nature of any capability gaps, and work with the relevant sectors to determine the most practical and appropriate actions they should implement for them to mature their cyber and operational resilience practices.

Shield 5: Sovereign capabilities

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

In our view, there are several activities government can undertake to achieve its goal of prioritising sovereign capabilities for growth and development across government and industry. There is an opportunity for the department to collaborate closely with the Department of Industry, Science and Research, the Department of Employment and Workplace Relations and the Department of Education on this issue.

- Set a small number of clear national cyber goals where Australia must lead or be self-reliant, like secure digital identity, critical infrastructure resilience, quantum-safe cryptography, safe artificial intelligence, and rapid incident response. Put one coordinating body in charge to line up federal, and state and territory efforts, cut overlap, and set simple "sovereign" tests for each goal (e.g. local design control, reliable local supply of key hardware, local response capacity, and Australian control of sensitive data). The government should also treat research and development (R&D) broadly, so it includes software, data, services, and ways of working, from early research through to real-world use.

- Map the full cybersecurity landscape to find weak spots and where Australia can build scale. Create hands-on translation hubs for cybersecurity with longer funding windows that fit fast-moving technologies. This includes putting in place stable, long-term funding for essentials such as high-performance computing, secure data platforms, testing ranges, and hardware security labs.
- Pull solutions into use with better incentives and smarter buying. Make government an early, significant customer through challenge-based buying and easier SME access, with stronger requirements for procurement of Australian-made, mission-aligned tools and services delivered by 100% Australian owned and operate companies.
- Build and keep talent with industry-embedded PhDs, short-term moves between sectors, and more secure early-career roles. Lift inclusion (e.g. women and First Nations) in higher education cybersecurity-related degrees and teach commercial and product skills alongside research.