Insurance Council of Australia

2 September 2025

Department of Home Affairs

By upload

Dear sir/madam

Horizon 2 of the 2023-2030 Australian Cyber Security Strategy

The Insurance Council of Australia (Insurance Council) welcomes the opportunity to comment on this important topic.

The Insurance Council is the representative body of the general insurance industry in Australia and represents approximately 85 per cent of private sector general insurers. As a foundational component of the Australian economy, the general insurance industry employs approximately 60,000 people and on average pays out $147 million in claims each working day ($36.5 billion per year).

We provide the comments in this submission on behalf of our membership whose interest in cyber security spans two distinct categories:

1. Insurers hold significant amounts of sensitive information and provide critical financial services. For these reasons insurers operate in a heavily regulated environment including supervision by the Australian Prudential Regulation Authority and coverage under the *Security of Critical Infrastructure Act 2018* (SOCI Act).
2. Insurers of cyber risk. Many of our members offer cyber insurance products and have a strong interest in improving insurability of Australia's cyber risk.

Given these two impetuses, the Insurance Council and our members have an interest improving Australia's cyber security at the individual, business and aggregate levels. We acknowledge that from a business perspective, cyber best practice involves not just individual firms but their supply chains, employees and customer bases. Given this, we commend the Government for its national approach to improving cyber security and welcome the opportunity to contribute.

Since the Australian Government released its 2023-230 Cyber Security Strategy, Australia's national digitisation has continued with pace. Digitisation has brough significant opportunities for the national economy. However, it has also brought increased risk as greater digitisation increases digital touchpoints and cyber security exposure. Given this, the Department of Home Affairs' (the Department) *Charting New Horizons: Developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy policy discussion paper* (the Discussion paper) is timely.

At the appendix we provide specific responses to the Discussion paper's questions.

Australia is maturing its cyber security practices, but much work remains.

We support the Government's *Act Now Stay Secure* campaign and the Small Business Cyber Resilience Service. We agree with the Government's focus on small and medium businesses (SMBs) and not-for-profits (NFPs) and would welcome further initiatives that raise cyber awareness amongst these cohorts.

Insurance Council of Australia

If you have any questions relating to our submission, please contact Eamon Sloane, Adviser, Strategic Policy at [redacted]

Regards

[redacted]

Insurance Council of Australia

Appendix: Discussion paper responses

Outlook for horizon 2

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?

We recognise that technology continues to evolve and suggest the following technologies as ones that may warrant consideration for Horizon 2:

- Consumer managed personal data stores and digital vaults that give individuals direct control over their personal data storage, sharing permissions and usage tracking across all services.
- Guaranteed identity systems.
- Quantum computing and cryptography.

We also raise Artificial intelligence (AI) as another significant emerging technology. AI is likely to bring further advancements in direct cyber threats such as deep fakes and automated malware. Other issues associated with AI that should be monitored include privacy issues associated with open-source AI tools and highly distributed data processing reaching across multiple external entities and locations. The Department will need to consider how Horizon 2 will interact with other Government initiatives including the *Voluntary AI Safety Standard*, of which Guardrail 3 is particularly relevant to Horizon 2.

There are important lessons we can learn from how AI adoption has been managed and discussed nationally. Before the explosion of interest in AI associated with ChatGPT's 2022 breakthrough, the use of large language models and other AI tools had been tracking well. ChatGPT's breakthrough saw a significant focus on generative AI and entities vacillated between blocking and embracing its adoption.

Finally, we agree geo-politics is likely to influence how cyber technologies are deployed, including in cyber warfare, cyber espionage and lower level targeted cyber-attacks such as supply chain disruptions. Monitoring geo-political shifts and their likely influence on cyber risk over the coming years can assist in informing the Government's outlook.

Collaborating across all levels of Australian Government

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

It is critical that any national cyber security arrangements apply without duplication at the state/territory level. For example, we note the confusion caused for businesses by the *South Australia's Cyber Security Framework* and its interaction with the *Security of Critical Infrastructure Act 2018*. Duplication such as this leads to confusion, increased regulatory burden, and ultimately costs to consumers.

Strong businesses and citizens

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 Government could collaborate with large entities including private businesses to identify touchpoints with SMBs and NFPs (for example, when an SMBs takes out or renews an insurance policy). These touchpoints could then be used to communicate key messaging on cyber security (provided by the Government to ensure consistency) to these smaller entities. Similarly, large entities

could be encouraged to host redirections to the Government's key cyber resources for SMBs and NFPs.

The Government could consider how to promote and support the rotation or secondments of cyber security professionals (from government and large entities) through SMBs and NFPs to assist with adoption of sustainable cyber practices. It may be appropriate for these secondments to be to third parties who support SMBs rather than directly into SMBs. Secondments could provide critical work experience for early career cyber professionals, and provide the opportunity for meaningful work for individuals impacted by organisational change (role redundancies) and transitioning to different work stages, such as retirement planning.

Finally, the Government should consider greater obligations for technology providers to ensure the security of their products and services. Significant numbers of SMBs and NFPs will be using off-the-shelf technology, and often low-cost or free versions given financial constraints. The developers and providers of these technologies must be leveraged earlier in the value chain, to reduce the direct cyber burden on SMBs and NFPs. A Government endorsement scheme may support this outcome.

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?

Government and larger businesses should view their supply chains and customer bases as opportunities to contribute to a national cybersecurity approach with education being key. It is incumbent on large organisations (government and private) to ensure cyber security material is relevant to and digestible by SMBs. This includes understanding that most SMBs will not have an IT Security resource in house, rather they will most likely operate on an outsourced model. Given this, large organisations need to help SMBs understand what they can do in the environment in which they operate.

Additionally, we suggest considering:

- Providing standardised template contracts for SMBs dealing with outsourced service providers.
- Enabling entities regulated under the *SOCI Act* to confidentially integrate and maintain SMB vendors through standardised supply chain security assurance programs.

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

A principles-based standard, akin to the Australian Prudential Regulation Authority's (APRA) *CPS234* with supporting guidance contextualised to SMB and NFP operations may be useful. However, a standard without accompanying monitoring and compliance may not carry sufficient impetus for SMBs and NFPs to adhere, so the Government may wish to consider if a standard is the best approach. Additionally, the Government should consider how these standards will interact with requirements under the *Privacy Act 1988*, if the Government progresses with removing the small business exemption as part of its privacy reforms.

An alternative approach could be considering how to make the *Essential Eight* more relevant and approachable for SMBs and NFPs.

Additionally, we suggest that the Government consider how the Australian Signals Directorate's Cyber Hygiene Improvement Programs might be extended to support SMBs.

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

Insurance Council of Australia

We suggest that a low understanding of cyber risk and limited awareness of cyber insurance are factors impacting the uptake of cyber insurance.

We note that that the intrinsic value of cyber insurance can be difficult for an SMB operator to determine, particularly where SMB decision-makers have a limited understanding of their digital risk profile. Additionally, those considering cyber insurance for the first time, may not completely recognise or understand the value of the pre, during and post-incident support many cyber insurers offer. Value-added services may range from threat intelligence, security assessments and network scanning resources to workshops and cyber data and information insights. Access to relevant vendors, risk management tools and advice on these services may also be offered.

Importantly, cyber insurance must be considered as one part of SMBs cyber defence, not the entire cyber security defence for a business. This is an important message for SMBs to understand so they can rationalise their cyber security budget, balancing insurance costs with preventive measures (which can positively influence insurance costs). Improving SMBs cyber literacy will help SMB decision makers in their cyber insurance journey, from purchasing through to claims.

While cyber insurance pricing may also be a factor when considering the purchase of cyber insurance, we note premiums are influenced by both the nature of the risk being underwritten as well as broader market dynamics. Insurers will typically place a strong focus on a customer's risk management and cyber security controls when reviewing, assessing, and pricing the risk. Consideration is also typically given to the nature of the business/industry sector, the volume and nature of data being handled, third-party and supply chain risks, and claims history. Broader market dynamics such as competition in the market and rising claims at an industry level (e.g. due to ransomware or other events) can also put pressure on pricing.

The Insurance Council would welcome the opportunity to undertake a research project in collaboration with Government to gain insights into SMBs' awareness of cyber insurance and market penetration in Australia. We currently undertake a similar, annual project with the Department of Foreign Affairs and Trade on travel insurance.[1] Gathering a greater understanding of the awareness of, and appetite for, cyber insurance across SMBs would enable the identification of opportunities to drive enhanced resilience and insurance penetration.

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

The insurance industry, comprised of APRA-regulated businesses, has a solid understanding of the threat posed by ransomware. We note that the insurance industry is an active contributor to the public literature on cyber risks, including ransomware.[2]

Observations provided by our members include:

- Ransomware remains among the most common cyber exposures for SMBs, alongside business email compromise. SMBs may think they are unlikely to be specifically targeted but may often have limited or no understanding of the use of automated malware which can mean they are easily targeted as part of a larger campaign. SMB literacy around these risks typically remains low.

[1] The 2024 results can be found here.
[2] Munich Re. 2025. *Cyber Insurance: Risks and Trends 2025*; QBE. 2024. *Managing cyber security risks for Australian businesses*.

Insurance Council of Australia

- There is a move from single to double and sometimes triple extortions (i.e. threat actors leveraging their attack and data stolen from the initial victim to extort individuals or entities whose data or assets were breached), which is increasing the impacts on individuals.
- Some reductions in threat actors being able to encrypt systems due to the evolution and uptake of security technologies. However, we expect that this is more reflective of large organisations with the financial resources to invest is such technological capabilities.

It is reasonable to assume that knowledge of ransomware and how it can manifest, potential impacts, and ways to defend and recover would be lower among individuals and small entities. For example, the Insurance Council understands that many insurance customers do not distinguish between scams, fraud and cyber-attacks, suggesting their understanding of ransomware is likely to be limited.

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

Any security advice for businesses and individuals must keep pace with how ransomware attacks are evolving. Recently for example, there has been a growth in the use of social engineering techniques to stage ransomware attacks, so current guidance on how to identify, defend against, and respond or recover should reflect these realities. The Government needs to consider how it can move as quickly as possible from identifying a new risk or ransomware technique to disseminating advice.

For SMBs specifically we suggest the Government could utilise the relationship businesses have with managed service providers (MSPs). Baseline cybersecurity requirements could be made mandatory in commercial contracts and procurement agreements for IT MSPs.

It may also be appropriate to review mandatory data retention requirements and reduce the time for which organisations must retain data to mitigate the risk of data exfiltration.

Finally, the Government could consider how it can undertake dark web scanning, find breached data and quickly provide information on the necessary response to impacted Australians.

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

We believe ransomware reporting obligations will improve visibility of our national cyber risk profile and help reduce our risk. Given this, we would support an expansion of the obligation to include a broader cohort so that the data better reflects the actual state of ransomware attacks experienced across Australia. We do acknowledge that an extension of ransomware reporting obligations will burden newly captured entities. However, mechanisms that support the sharing of collected data can help businesses and Government better understand the threat landscape and respond accordingly.

The insurance and broader financial services sector are subject to a high standard of regulation by APRA through the recently implemented CPS 234. The Insurance Council acknowledges this has required an often-significant uplift in cyber risk management practices across the industry with the aim of minimising the likelihood and impact of cyber incidents.

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

We have concerns that some audit firms working with insurers have transformed risk-based security standards into checkbox compliance exercises, applying rigid enterprise frameworks regardless of organisational size, context, or actual threat landscape. This has resulted in an erosion of risk-based scoping and the tailoring of control standards to individual entities. We note that this has also occurred

Insurance Council of Australia

against a backdrop of significant, multi-layered regulation including but not limited to APRA supervision, the *SOCI Act* and the *Privacy Act 1988*.

Safe technology

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?

The Government could promote standardised formats and protocols for organisations to share information about their vulnerabilities, critical assets, and supply chain dependencies. We also refer to earlier answers that can or would approve overall cyber awareness in Australia as actions would support individual consumers.

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?

The Government should overlay a data lens across the map of critical infrastructure assets, which will help demonstrate movement paths for critical data and concentration of data risk across key suppliers.

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?

There may be opportunities for collaboration between Government and the private sector on open standards.

World class threat sharing and blocking

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?

Within the national business community, SMBs have the greatest vulnerability. We note that with the financial services sector, regulators such as APRA not only regulate but also provide insights. There may be scope for other regulators to replicate these efforts to better support their regulated entities. The Government could also consider how it can help industry associations (particularly those whose members are largely SMBs) to perform a similar role.

The Government must support NFP and community-led security initiatives, ensuring the independence of these organisations from Government and business is respected. Opportunities to partner with Government on discreet opportunities and deliver initiatives on behalf of Government help grow industry's confidence in and visibility of such entities.[3]

Does the government need to scope and define what Australia's proactive cyber security posture should look like for industry?

We would welcome all industries, irrespective of their size, having a baseline cybersecurity posture. These could be tiered using a number of measures such as revenue. We would be open to consulting further on this.

[3] An example is Health Cyber Sharing Network Pilot funded by the Department and delivered by CI-ISAC.

Insurance Council of Australia

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?

Investment in Australia's cybersecurity workforce and sovereign capabilities will over time, grow our ecosystem organically and provide the resources needed for the creation of ISACs. However, Government investment in pilot opportunities will give nascent but well-functioning ISACs a quicker pathway to sustainable development and success.

Protected critical infrastructure

How effective do you consider the SOCI Act at protecting Australia's critical infrastructure? Are the current obligations proportionate, well-understood, and enforceable?

We are supportive of the *SOCI Act 2018*. We believe amendments made over the last few years have increased proportionality and been implemented with nuance.

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

Our industry is comfortable with the outcomes of the *SOCI Act 2018* although we note the regulatory overlap with APRA requirements and would welcome work to reduce overlap while maintaining cyber security.

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?

The Government should host more cross sectoral exercises to encourage greater operational resilience. We welcome ongoing dissemination of observations from exercises completed across various sectors, for the benefit of shared learning and to inform uplift of incident response processes within Australian organisations and would also welcome most sector-specific guidance.

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

The Government should make available material that has analysed the overlap of Government-applicable security requirements with regulatory and better practice obligations applicable to private sectors. This would support compliance but enable businesses to benchmark against Government-only security requirements and identify areas requiring greater focus.

The provision of insights and recommendations on practical considerations for implementation, such as priority order for implementation and lessons learnt, would also support better engagement.

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

We are aware that some Insurance Council members monitor government-applicable obligations, to inform best practice where relevant. Further, insurers have APRA standards and guides that set internal governance requirements.

Sovereign capabilities

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?

As above, the Government could play a coordinating role for programs of cross sector placements. Placement programs offer individuals the opportunity of exposure and development in varying

industries and enables smaller entities to gain the benefit of skills and expertise of staff from organisations with more mature capabilities.

We also recommend the Government consider how traditional information technology (IT) workers, with significant knowledge of entire IT ecosystems, not just cybersecurity, can be better brought into the cybersecurity fold.

Collectively, Australian governments should agree on and consistently adopt a cyber curriculum for school.

The Government has a role to play in ensuring the cybersecurity workforce represents the diversity of the Australian population. It is critical that cyber security professionals have the soft skills necessary to communicate and educate other parts of the workforce and diversity is a key input for this outcome.

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?

There may be value in the Government considering how successful schemes from other industries, such as mature aged apprentices, can be deployed to encourage growth in the cyber security workforce.

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?

Industries with highly transferable skills include:

- engineering
- law enforcement
- military
- privacy and legal
- governance, risk and compliance.

We also note a lot of traditional IT roles are being disbanded because of moves towards automation. Many of the individuals displaced by these processes will have highly transferable skills.

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

Grow entry level, Australian-based IT jobs which leverage emerging technologies including AI. This would in turn grow our national cyber workforce and contribute to the growth of our next generation of cyber security entrepreneurs who will in turn help develop sovereign capabilities.

We also recommend the Government consider how to negate the offshoring of cybersecurity roles. Doing so would shape the thinking of Australia's private sector, encouraging creativity on investment in sovereign cyber capabilities.

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

Insurance Council members have flagged concerns about audit firms' focus on using *Systems and Organisation Controls 2* (SOC2) and the concentration this may be causing among larger firms that have the resources to implement SOC2. Financial audit requirements for SOC2 terms overlap with at

Insurance Council of Australia

least 9 months of a given financial year, further contributing to concentration. American based firms, who work to a September-ending financial year, are unable to meet this overlap requirement without additional compliance investment, reducing the pool of possible vendors.