COALITION INSURANCE SOLUTIONS PTY LTD.
[redacted]

Department of Home Affairs
PO Box 25
Belconnen ACT 2616
Australia
CSSH2@homeaffairs.gov.au

August 18, 2025

Re: Response to Horizon 2 Public Discussion Paper

Dear Horizon 2 Consultation Team,

Coalition Insurance Solutions Pty Ltd (Coalition) appreciates the opportunity to share our views on the Horizon 2 Policy Discussion Paper. We value the Government's commitment to an open and collaborative consultation process. We look forward to participating in the forthcoming co-design process aimed at developing targeted actions and initiatives for Horizon 2.

Please do not hesitate to contact us if you require any further information, clarification, or additional input from us as the process progresses. Coalition remains ready to assist in supporting the Government's efforts towards building a robust and secure digital environment.

Sincerely,

[redacted]

Coalition Responses to Horizon 2 Policy Discussion Paper

Question 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?

Cyber insurance uptake among Australian SMBs remains modest, even though most products are both affordable and accessible for businesses that seek them. Public statistics indicate that only about 20 percent of Australian SMBs hold standalone cyber policies, and we believe this estimate to be high. Our estimate is closer to 10 percent. We find that barriers on the demand side, rather than on the supply side, are the primary reason for slow adoption.

First, a few words about affordability and accessibility, which have nuanced meanings in the cyber insurance market. Affordability refers to the price or premium that an organisation pays for coverage. Insurers set these premiums after thoroughly assessing a company's business risk, which includes sector, revenue, claims history, and investment in cyber controls. Businesses that use multifactor authentication, maintain reliable data backups, and provide staff training, for example, typically receive lower premiums. Coalition also uses technology, including a proprietary external scanning engine, to identify critical vulnerabilities and other security issues in potential policyholders which our data shows are likely to lead to insurance claims, and we use that data to benchmark businesses against their peers.

Businesses do not need to achieve perfect security to qualify for coverage. However, we require policyholders to address any critical vulnerabilities we identify during the underwriting process. Our data shows that leaving even one critical vulnerability unaddressed makes a business 33% more likely to experience a claim within the next year, compared to businesses without such vulnerabilities. By remediating these high-risk exposures, policyholders significantly reduce their chances of a costly incident and increase their resilience against ransomware and other cyber threats.

It is difficult to draw generalisations about premium pricing as policies are specialised and organisational risks are specific; premiums will vary depending on company size, industry, existing security controls, and individual claims history.

This risk-based pricing structure actively encourages better digital safety practices, an important incentive when nearly half of Australian SMBs report spending less than $500 annually on cyber security. As more organisations enhance their cyber hygiene, the entire market benefits through reduced risk and lower collective premiums.

Accessibility relates to the coverage limits that insurers offer. Coalition offers coverage to over 95% of Australian applicants. Most Australian SMBs can obtain policies with limits ranging from $100,000 to $1 million, which provides baseline coverage for high frequency cyber claims related to business email compromise or funds transfer fraud. SMBs can also elect coverage for catastrophic/high severity events where a $1 million limit may not be adequate (e.g. certain ransomware or data breach claims). Larger firms that seek to transfer greater financial risk may need to negotiate complex, multi-layered policies, as insurers may not offer the very high limits they seek in a single policy.

Two main factors explain the limited adoption of cyber insurance policies despite the range of affordable and accessible products available. Many SMB owners underestimate their risk or are unaware of the value of cyber insurance. Recent surveys, including from ACSC and ASIC, show that almost half of SMBs assess their understanding of cybersecurity as average or below average, and many assume that only large organisations are targets. As a result, many small businesses either wrongly believe that cyber insurance is not meant for them, or that it's unaffordable. Even where coverage is within reach, the combination of a knowledge gap and a tendency to underestimate risk causes many to undervalue the product.

Second, the Australian cyber insurance market lacks the broad structural incentives seen in other lines of insurance. Unlike property insurance, where mortgage lenders often make loans contingent on coverage, cyber insurance has no significant external market mandates that drive demand. Although some organisations purchase cyber policies to meet specific contractual obligations, such as doing business within certain sectors or with government entities, these requirements remain the exception rather than the rule. As a result, broader adoption of cyber insurance still relies largely on business leaders proactively recognising the importance of protection.

In summary, affordability and accessibility rarely present barriers to obtaining cyber cover. Instead, low demand remains the chief challenge to broader cyber insurance adoption among Australian SMBs, driven by a combination of limited understanding of cyber risk, lack of education on the value of cyber insurance,

policy complexity, and the lack of material regulatory requirements play a more significant role in slowing adoption. By increasing education, continuing to raise risk awareness, and potential public policy incentives designed to increase demand for coverage, Australia can unlock more widespread protection and ensure that SMBs benefit from the accessible and affordable coverage already available in the market.

Question 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?

As a modern cyber insurer, Coalition maintains an exceptionally deep and continuously evolving understanding of ransomware threats to small entities, drawing on a broad array of proprietary and industry-leading data sources.

Coalition operates global honeypots that gather real-time intelligence on emerging ransomware tactics, techniques, and attacker infrastructure. This live telemetry enables us to detect shifts in ransomware campaigns as they occur, often before significant public impact is felt, and enables us to encourage our customers to adopt specific security measures to protect against these shifts in campaigns. Our claims data from many tens of thousands of small business policyholders provides quantitative insight into the frequency, attack vectors, impact severity, and financial losses associated with real ransomware events. Industry reporting and our own data indicate that small businesses increasingly face these attacks: in the last year, ransomware accounted for over 20% of all reported cyber insurance claims for SMBs, with an average incident cost exceeding $100,000. Our global Digital Forensics and Incident Response (DFIR) teams investigate a wide range of ransomware cases, allowing us to identify patterns in root causes, attacker behaviors, and the specific business operations most at risk.
We supplement our internal intelligence with curated external feeds and close monitoring of criminal forums, enabling us to anticipate not only how ransomware groups are innovating but also which sectors or organisational profiles they are likely to target next. Our intelligence reveals that threat actors now heavily leverage ransomware-as-a-service (RaaS) platforms. These platforms lower the barrier to entry, fueling an ecosystem where technical expertise is no longer required to orchestrate sophisticated ransomware attacks. As a result, ransomware incidents have become more widespread and opportunistic, with automation allowing attackers to cast wider nets and exploit mass vulnerabilities.

Ransomware tactics have also evolved: double extortion has become the norm, with attackers exfiltrating data and threatening public exposure alongside file encryption. Our data shows that 70% of ransomware events we investigate involve a data exfiltration component, and this statistic is consistent with those released by Verizon, among others. (That number is up from 57% in 2021.) Remote work, reliance on cloud-based business tools, and persistent use of weak or reused passwords and unpatched systems continue to present easy entry points for these attackers. In our incident analysis, credential compromise and remote desktop protocol exposure remain leading factors for successful attacks on small businesses.

By combining live attacker intelligence, direct claims and incident response data, and external threat feeds, Coalition maintains a uniquely comprehensive, timely view of the ransomware risk landscape. This allows us to not only anticipate shifts in attacker tactics but also to deliver targeted guidance on prevention and effective coverage for the specific threats SMBs face today.

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

To help individuals and businesses better protect themselves from ransomware, we recommend that the government adopt a multi-faceted approach:

1. *Expand Awareness and Education:* The government should invest in targeted awareness campaigns that reach both SMBs and the public. These campaigns must address the misconception that only large organisations are at risk and focus on actionable steps, such as enabling multi-factor authentication, maintaining routine backups, and providing regular cyber safety training for both staff and families. Existing resources, such as ACSC's Small Business Cyber Security Guide, deserve broader distribution and frequent updates. Coalition offers similar resources and stands ready to collaborate with government initiatives.
2. *Promote Risk-Based Incentives:* The government can introduce incentives like tax credits or grants to encourage businesses to strengthen cyber defences by investing in measures like modern backups, endpoint protection, and employee training. Tax credits for SMBs purchasing cyber insurance for the first time can both improve economic resilience and prompt business owners to engage meaningfully with their true level of

cyber risk. By linking financial benefits to first-time participation, such incentives not only lower the cost barrier but also create long-term engagement with cyber risk management. Insurers should continue using risk-based pricing to reward strong cyber hygiene.

3. *Boost Incident Response Resources:* Additional investment in rapid-response support, such as hotlines, recovery guides, and directories of vetted recovery providers, could help small businesses and the public recover faster and limit economic loss after a cyber incident. These services are essential while cyber insurance market penetration remains low among SMBs. As adoption grows, insurers will increasingly provide these services directly; until then, public support ensures that all organisations can access expert assistance in a crisis.
4. *Support Accessible Cyber Insurance Markets:* The government should make it easier for SMBs and individuals to access clear, unbiased information about cyber insurance. This includes creating straightforward educational materials, demystifying the application process, and exploring regulatory frameworks that improve market stability.
5. *Encourage Secure Technology Design:* The government can extend minimum security standards for core digital services and common business software. Encouraging software makers and IT service providers to deliver regular security updates and enable secure default settings will ease the burden on end-users, especially those less able to manage complex cyber risks.
6. *Share Data on Emerging/Evolving Threats with the Cybersecurity Industry:* To the extent possible, increased collaboration between government and private industry, such that private industry can be aware of emerging threats to Australian businesses and rapidly iterate on solutions, would be broadly beneficial in developing new shields to protect against evolving ransomware tactics (both in Australia and globally).