

Minister Tony Burke
Department of Home Affairs
PO Box 25
Belconnen ACT 2616
Australia

February 13, 2025

Re: Comments on Cyber Security (Ransomware) Reporting Rules

Dear Minister Burke,

We appreciate the opportunity to submit comments on the Cyber Security (Ransomware) Reporting Rules.

Coalition Insurance Solutions Pty Ltd. operates as an AFSL-licensed insurance intermediary and cyber risk management firm. Our mission is to help *solve cyber risk* by strengthening organizations' digital resilience. As a leading provider of cyber insurance, Coalition assists organizations before, during, and after cyber incidents. We leverage data and tools to accurately underwrite and proactively manage risk both for individual policyholders and across our aggregated portfolio of insureds. Through affiliated entities under Coalition's corporate structure, we equip policyholders with risk management tools, including customized alerts for critical vulnerabilities affecting their systems, and offer real-time technical support to mitigate risks. We believe our model advances digital resilience and represents the future of cyber insurance — a belief supported by data. Coalition policyholders experience 65% fewer claims than the market average.

We commend the rule's thoughtful approach and recognize that mandatory reporting can enhance the government's understanding of ransomware attacks, payment trends, and Australia's digital resilience.

We appreciate your consideration of the following comments:

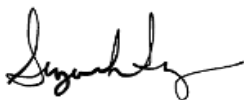
1. **Reporting entities and third parties:** The rule should clarify that reporting responsibility remains with the designated entity, even if a third party

(e.g., an insurer or incident response firm) makes a payment on its behalf in connection with a ransomware or extortion demand.

2. **Turnover threshold:** The draft rule defines reporting entities as those that (a) manage critical infrastructure assets covered under Part 2B of the *Security of Critical Infrastructure Act 2018*, or (b) generate annual gross revenue exceeding AUD \$3 million. We agree this threshold appropriately balances the need to limit the reporting burden on small businesses while ensuring the government collects meaningful insights into ransomware activity and related payments. Currently, fewer than 7% of registered businesses meet this threshold, though that may change over time. The draft rule would benefit from an acknowledgment that the turnover threshold will be reassessed periodically — and adjusted if necessary — to ensure reporting requirements remain focused on Australia's largest businesses.
3. **The 72-hour reporting window may be overly ambitious:** While other countries have proposed or adopted a 72-hour reporting timeframe, our experience with incident recovery suggests that meeting this deadline may be challenging for some organizations. Even when the 72-hour clock starts upon making or becoming aware of a payment, the immediate hours and days following a ransomware event are critical. Incident response and recovery efforts often take weeks or months, and a strict 72-hour deadline could divert attention from essential remediation. We offer this observation for future consideration as laws and policies evolve. However, we recognize that the *Cyber Security Act 2024* establishes the 72-hour timeline, making immediate changes unlikely.

Thank you for considering our views. We look forward to continuing our partnership.

Sincerely,



Sezaneh Seymour
VP and Head of Regulatory Risk & Policy