PUBLIC SUBMISSION ON CYBER SECURITY LEGISLATIVE PACKAGE

Prepared by: **Kat McCrabb, Flame Tree Cyber**

Date: **12 February 2025**

Flame Tree Cyber

Public Submission on Cyber Security Legislative Package

Flame Tree Cyber welcomes the opportunity to provide feedback on the proposed:

- Cyber Security (Security Standards for Smart Devices) Rules 2024
- Cyber Security (Ransomware Reporting) Rules 2024, and
- Cyber Security (Cyber Incident Review Board) Rules 2024.

While these rules represent important steps toward strengthening Australia's cyber security posture, the following areas warrant further consideration.

Cyber Security (Security Standards for Smart Devices) Rules 2024

The exclusion of devices used by businesses as point-of-sale (POS) terminals is a missed opportunity to enhance the security of payment infrastructure. POS terminals are a known target for cyber criminals seeking to compromise financial data. Expanding the scope of the rules to include these devices would provide greater protection against such threats.

Additionally, it is recommended that the rules establish controls to mitigate brute force attacks including:

- minimum password length requirement and
- maximum allowable password attempts over a given time.

Passwords should be able to be reset to protect against devices become unusable if an account is locked out. These controls improve baseline security measures across all applicable devices.

Cyber Security (Ransomware Reporting) Rules 2024

The current reporting requirements focus on incidents but do not capture financial transactions related to ransomware payments. Expanding reporting obligations to include payment account details used in ransom transactions would enhance the ability of law enforcement agencies to track and disrupt cybercrime financial flows.

Cyber Security (Cyber Incident Review Board) Rules 2024

The requirement for the Minister's approval of the Cyber Incident Review Board (CIRB) Terms of Reference introduces a risk of government oversight influencing the Board's operations. To ensure the CIRB remains independent and focused on community interests, its governance framework should clearly define its autonomy while maintaining appropriate accountability mechanisms.

These recommendations seek to strengthen the effectiveness of the proposed rules in enhancing national cyber security resilience. I appreciate the opportunity to contribute to this consultation and encourage further refinement of the legislative framework to ensure robust protections for businesses and the community.