Ms Joanna Abhayaratna
Executive Director
Office of Impact Analysis
Department of the Prime Minister and Cabinet
1 National Circuit
BARTON ACT 2600

Email: helpdesk-OIA@pmc.gov.au

Dear Ms Abhayaratna

Impact Analysis – Mandatory Ransomware Reporting Obligation for Businesses – Second Pass Final Assessment

I am writing in relation to the attached Impact Analysis (IA) prepared for a proposal to introduce mandatory ransomware reporting for certain businesses as part of a proposed Cyber Security Bill 2024.

I am satisfied that the IA addresses the concerns raised in Mr Daniel Craig's letter of 17 April 2024, as follows.

1. **Better articulating the objectives, and why government intervention is needed to achieve them**

The IA has been amended to better articulate the objectives of the proposal and why government intervention is needed. Section 1.2 provides evidence from a range of sources to indicate the financial cost of ransomware incidents to businesses globally. The financial cost to Australian businesses however, is difficult to quantify without adequate data. Requiring businesses to report when they have paid a ransom will assist the Australian Government in building in understanding of threat picture and true cost to the Australian economy.

With the ransomware and cyber extortion reporting data, the Government can better provide support to businesses experiencing ransomware attacks, and build industry resilience against such threats. From publicly reported instances, the IA sets out evidence that the cost to businesses experiencing ransomware attacks is significant. This includes not only financial burden on the business to respond to an incident, but the impact to their delivery of services and managing the cascading consequences for the broader economy.

Section 1.3 sets out the inconsistencies in current reporting data. Differing methodologies to assess the rates of reporting make it inherently difficult to assess the amount of unreported ransomware incidents. Underreporting of ransomware impedes Government's ability to build an accurate understanding of the threat landscape and to understand industry's needs for Government support.

2. **Proving a more granular description of the options being considered**

All options set out in the IA have been bolstered with further detail. This includes outlines of the types of information business would report to Government under each option. Case studies have been included to set out how each option would operate in practice.

3. **Providing more quantification of costs and benefits**

More quantification of costs and benefits of the proposal have also been included. This includes regulatory costs. The initial administrative costs for captured entities to familiarise themselves with their obligations was

calculated to be $276.80 per entity. The IA notes that for an entity with an annual turnover of $3 million (the lowest threshold set out in the options) this initial administrative cost accounts for less than 0.001 per cent of turnover. Quantification of the ongoing cost during a cyber incident to report a ransomware payment, sees approximately 3 hours of labour costing $255.51 per incident.

Each option in the IA provides more granular detail on the costs and benefits specific to that option.

4. **Better articulating implementation steps, key measurable and any risks to success**

Finally, the steps for implementation of Option 3 (preferred) have been further detailed in Section 6. The Department of Home Affairs would be responsible for implementation, with support from the Australian Signals Directorate.

Key measures for success are set out in Section 2 and Section 7. Some of these measures include a significant increase in the volume and scope of data reported to Government, the development of anonymised and actionable threat reports, and an increase in businesses receiving assistance from Government.

An internal post-implementation review of the mandatory ransomware and cyber extortion reporting regime should occur no later than two years after implementation in line with other measures brought forward in the same legislative package, as outlined under the 2023-2030 Australian Cyber Security Strategy.

Implementation risks have been set out at Section 6.2, including the risk of non-compliance with the proposed regime. Engagement and consultation on the legislation would commence prior to, and continue following, the legislation entering into force to ensure that entities are ready to meet their obligations.

Accordingly, I am satisfied that the IA is consistent with the six principles for Australian Government policy makers as specified in the *Australian Government Guide to Policy Impact Analysis*.

I submit the IA to the Office of Impact Analysis for formal final assessment.

Yours sincerely

Hamish Hansford
Deputy Secretary
Cyber and Infrastructure Security Group
Department of Home Affairs

6 September 2024