Australian Government
Department of Home Affairs

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

Certification as Impact Analysis Equivalent – *Critical Telecommunications Assets*

I am writing to certify that the 2022 critical infrastructure risk management program regulation impact statement (the 2022 RIS) along with the attached supplementary analysis has undertaken a process and analysis equivalent to an Impact Analysis (IA).

I certify that this process adequately addresses all seven IA questions for the purposes of informing the Minister's decision to make subordinate legislation under the *Security of Critical Infrastructure Act 2018* (SOCI Act) to introduce a bespoke critical infrastructure risk management program (CIRMP) for critical telecommunications assets.

I am satisfied that the scope of the problem and the recommendations identified in the Impact Analysis Equivalent are substantially the same as the identified problem and recommendations in the policy proposal. To the extent there is a difference, it is that telecommunications assets are already subject to legislated security requirements under the *Telecommunications Act 1997* that are being uplifted into the SOCI Act and clarified and streamlined in the process of extending the CIRMP requirement to them.

Both the 2022 RIS and the supplementary analysis clearly explains the policy problem, which includes an increasing cadence of serious incidents affecting the industry and some confusion caused by regulation under different legislative frameworks. It describes that the problem requires Government intervention because of the increasing incidents and the huge, economy-wide impacts they can generate.

I further certify that fewer than three policy options are examined because these reforms were conducted through a long process of industry co-design, through the Australian Telecommunications Security Reference Group (ATSRG), which identified the proposed policy approach as the preferred policy option for government and industry alike.

These reforms streamline previously disparate telecommunications security into one legislative framework with improvements to clarify compliance requirements. The process of co-design has ensured that the policy option was mutually identified as the most effective and efficient means of realising the shared goals of protecting Australia and its critical infrastructure without imposing undue regulatory burden.

Feedback was obtained through an iterative process in 2024 and 2025 with members of the ATSRG. This feedback significantly shaped the detail and scope of the policy proposal. Further, the Department of Home Affairs (the Department) opened public consultation from 16 December 2024 to 14 February 2025 on the

Security of Critical Infrastructure (Telecommunications Security and Risk Management Program) Rules 2025 (TSRMP).

The Department received 20 submissions on the TSRMP Rules. Following consultation, minor changes have been made to the TSRMP Rules to clarify the operation of section 11, which relates to cyber and information hazards. In particular, the Department has:

- clarified drafting that allows a relevant critical infrastructure asset to comply with an equivalent cyber security framework. This ensures entities can comply with the framework that best mitigates cyber security risks in their operating environment where that framework lacks maturity indicators.
- updated the title of the AS/NZS ISO/IEC 27001 document to reflect the latest version.

Feedback will also shape the development of detailed guidance materials which will clarify compliance and promote a shared, industry-wide understanding of the TSRMP Rules.

Despite government providing industry the chance to submit detailed regulatory costing estimates, no quantitative submissions were made. As a result, no regulatory burden estimate table was produced as it would be insufficiently robust on the basis of its qualitative assumptions.

Despite this, the Department of Home Affairs maintains that the regulatory burden for business is less than was identified in the 2022 RIS, because carriers and carriage service providers have existing security requirements involving risk management activities that other asset classes did not have when that RIS was produced.

As a result, the marginal cost of uplift is smaller than other asset classes as critical telecommunications assets would require significantly less capital investment into governance structures and functions to support the implementation of a CIRMP. The reforms will be implemented with continuous engagement across multiple fronts between industry and government and supported by comprehensive guidance material.

The benefits of more secure and resilient telecommunications assets flow to the entire Australian economy. The reduced frequency of disruptions guarantee that all businesses can continue trading and that Australians have secure and continuous access to internet and communication technology.

The Department's approach to implementation will leverage existing relationships, guidance products and established communications forums to ensure all key stakeholders are aware of the changes. I note that industry is anticipating these obligations being applied due to given the extensive consultation undertaken to date on the ERP Act and the subordinate legislation. These changes will be continuously evaluated by the Department with regular engagement with industry and peak bodies.

Accordingly, I am satisfied that the attached report is consistent with the *Australian Government Guide to Policy Impact Analysis*.

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

28 February 2025