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 – Second Pass Final Assessment – Amendments to the *Security of Critical Infrastructure Act 2018*

I am writing in relation to the attached Impact Analysis (IA) prepared for amendments to the *Security of Critical Infrastructure Act 2018* (SOCI Act).

I am satisfied that the IA addresses the concerns raised in your letter of 13 August 2024.

In regards to the policy problem of the proposed power to direct an entity to vary their risk management program (RMP) and the process by which the Department would determine serious deficiencies in an RMP, you also asked the Department to better differentiate the proposed power from existing regulatory powers. The IA now addresses these concerns through the inclusion of detail on:

- The Cyber and Infrastructure Security Centre's (CISC) current trial audits into compliance with the critical infrastructure risk management program. Trial results indicate consistent issues of noncompliance, particularly for cyber-related obligations.
- The SOCI National Compliance Plan 2024-25. This document sets out the CISC's approach to regulation, including how the CISC will identify entities for audit. As described by the IA, the proposed powers would be used once an RMP has been found to be seriously deficient through this process or after an incident occurs.
- Enforceable undertakings. Including on how enforceable undertakings are not fit for purpose, costly to obtain, and distinct from the proposed power. Because enforceable undertakings are unfit for purpose and because the risk management program is still reaching maturity, the IA does not discuss previous or anticipated efforts to obtain them.

Your letter also asked the Department to justify the use of break-even analysis and qualitative analysis through the IA. In summary, both types of analysis were used because:

- The anticipated costs and benefits of Option 2 are so uncertain that monetisation of total costs would be vastly inaccurate because of the magnitude and uncertainty of required assumptions.
- The break-even analysis considers costs and benefits with a range of impacts and frequencies to address the uncertainty. Qualitative costs and benefits supplement the break-even analysis.
- Options 1 and 3 use break-even analysis because they are particularly difficult to quantify.

Your letter recommended the Department include a separate regulatory cost estimate for Measure 2 of option 2 and option 3. As discussed between the OIA and the Department, this cost estimate has not been prepared for measure 2 of option 2, consequence management, because of the difficulty in reliably estimating the anticipated cost of the measure. Instead case studies have been used to demonstrate to industry how it is anticipated costs will be incurred.

No regulatory cost estimate was prepared for measure 3 option 3 as there would be no expectation of compliance with guidance through the Trusted Information sharing Network (TISN), as the TISN is a voluntary platform.

Finally, your letter asked the Department to outline more clearly how stakeholder feedback shaped the IA and its options. The IA now more thoroughly describes throughout the two main public consultation processes undertaken to inform the options in the IA and the drafting of relevant provisions in the Bill. The integration of stakeholder feedback is implicit in discussion of the costs and benefits of options throughout the IA and is most explicitly described in tables 31 and 32.

The regulatory costs are as follows -

- For Measure 1: A one-off impact and annual on-going cost within the range of costs already estimated for the Risk Management Program obligations under the SOCI Act, noting the costs of Measure 1 are expected to be low relative to the existing cost of compliance, and the likelihood that many entities already comply with requirements under Measure 1.
- For Measure 2: A cost of between $0.5m to $50m per incident. With an assumed frequency of one incident every three years, the average cost impact is expected to be **between $0.1m and $16.7m per incident per year**. The IA articulates a range of possible cost impacts, noting the potential variance in the frequency and scale of incidents.
- For Measure 3: **No regulatory costs**, as this measure relates to enforcement activities for severely deficient Risk Management Programs.

Overall, the benefits of regulation will be at least (and are expected to be more than) the costs of regulation. This is primarily because the marginal costs of Measures 1 – 3 are expected to be small, relative to existing costs associated with compliance under the SOCI Act and the potential avoided costs of future incidents. The direct cost impacts depend on the frequency of interventions taken by Government to enforce compliance with Measure 2. However, due to the expected frequency of interventions being once every three years, the number of avoided incidents required for total benefits to exceed the cost impact of Option 2 is also low. The IA uses break-even analysis to articulate expected total benefits in further detail.

Accordingly, I am satisfied that the IA is now 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
Department of Home Affairs
10/09/2024