Resilience NSW

Reference:

Mr Hamish Hansford
Group Manager
Cyber and Infrastructure Security Centre
Department of Home Affairs
Australian Government

Via email: ci.reforms@homeaffairs.gov.au

Dear Mr Hansford,

Response to Critical Infrastructure reforms – proposed risk management program (RMP) Rules and Guidance

Resilience NSW is pleased to see the progress of the *Security of Critical Infrastructure Act 2018 (SOCI Act)* reforms and the range of engagement material and activities made available to industry and governments.

A function of Resilience NSW is to collaborate with government agencies, industry and non-government sectors to minimise the risk of disruption during and after disasters. Our Agency administers the Critical Infrastructure Resilience Advisory Group (CIRAG) made up of relevant State government agencies to assist in providing coordinated advice on critical infrastructure resilience. Accordingly, members of the CIRAG have provided us with comments on the Draft RMP, which are attached in a summary table.

The intention of the RMP outcomes is conveyed well in the Draft Rules and Stakeholder Guidance document. The logic applied to address the potential critical infrastructure risks that could cause significant harm to the nation and states, appears sound.

To enhance compliance with the RMP and improve its likelihood of successful implementation, we recommend that guidance on the RMP is made clearer. This will ensure obligations are easier to understand and the Program, simpler to apply in practice - particularly in the context of responsible entities' other obligations.

Agencies are finding it difficult to interpret how the risk management process is to be applied and integrated into their existing risk management systems. This appears to be due to mixed messaging within the draft material and terminology differences with existing risk management frameworks.

For instance, the terminology and order of process in ISO 31000 uses a stepped process of analysis and a risk matrix approach to determine the risk rating based on likelihood and consequence. The

National Emergency Risk Management Guidelines (NERAG) for natural hazards also follows this standard.

To address these concerns, Resilience NSW suggests it may be beneficial for your Department to consider including in the Guidelines:

- a variety of critical infrastructure risk scenarios which could guide responsible entities in testing the integration and interpretation of risks;
- a process chart that shows how the measures set out under the Act/Rules are integrated and enhance security obligations; and,
- a clear definitions table.

Further enquiries on this submission can be directed to

Yours sincerely,

Samuel Toohey
A/ Executive Director
Strategy, Policy, & Programs

18/11/2022