Ausgrid Submission

Exposure Draft of the Security Legislation Amendment (Critical Infrastructure) Bill 2020

27 November 2020

27 November 2020

24-28 Campbell St
Sydney NSW 2000
All mail to
GPO Box 4009
Sydney NSW 2001
T +61 2 131 525
ausgrid.com.au

[redacted]
[redacted]
Critical Infrastructure Security Division
Department of Home Affairs

Lodged via: https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/protecting-critical-infrastructure-systems/submission-form

Dear Mr Kiley,

We welcome the opportunity to comment on the Exposure Draft of the Security Legislation Amendment Bill 2020 (**Exposure Draft**).

We recognise the need for an enhanced critical infrastructure framework and an update of the Critical Infrastructure bill.

However, we believe some obligations and expectations outlined in the Exposure Draft would benefit from further clarification to ensure more effective governance and compliance. For example:

- Separate state and federal requirements create a potential for overlapping accountabilities, unclear compliance obligations and additional compliance costs.
- [Proposed] enhanced cyber security obligations will require extensive consultation with the energy sector, our customers, stakeholders and the proposed energy sector regulator to ensure these obligations minimise risk for our customers and stakeholders, are cost effective and practical

Whilst the Exposure Draft takes an all-hazards approach, our understanding is that this will be based on the risk assessment relevant to each organization. More specifically we have the following questions and suggestions:

- Are the personnel employed by a Critical infrastructure provider required to undergo an AusCheck background check or will there be a subset of checks relating to personnel with privileged levels of access to identified critical assets?
- Definition of “significant impact” in reference to security incidents needs more clarification to ensure compliance to the requirement.
- The incident response timeframe should follow a “tiering” methodology wherein incident response times are commensurate with the impact of the incident.

We appreciate the Department’s consultative approach on these issues. If you have any questions please contact Andy Chauhan, Chief Information Security Officer on [redacted] or by email [redacted].

Yours sincerely,

[redacted]

Richard Gross
Chief Executive Officer


Ausgrid