AUSTRALIAN ENERGY REGULATOR

1 February 2022

The Hon Karen Andrews MP
Minister for Home Affairs

Sent by email to: CI.Reforms@homeaffairs.gov.au

Dear Ms Andrews

Submission on the Exposure Draft of the Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022

I refer to the latest developments around the *Security of Critical Infrastructure Act 2018* (SOCI Act), with the *Security Legislation Amendment (Critical Infrastructure) Act 2021* (SLACI Act) commencing on 2 December 2021 and the *Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022* (SLACIP Bill) to be considered in 2022.

The AER has been closely following the legislative developments including discussions with the Department of Home Affairs staff on specific aspects of the SOCI Act. We thank the Department for its constructive engagement with us to date and appreciate the further opportunity to comment on the SLACIP Bill. We also appreciate the Department taking our previous feedback on board and reflecting our concerns in the exposure draft SLACIP Bill.

After reviewing the exposure draft SLACIP Bill, there is one issue that we would like to bring to the Department's attention; that greater clarity be included in the draft Rules and SLACIP Bill about how material risks and relevant impacts are defined and identified. In particular, certain aspects of the exposure draft may not align with the economic principles within the National Electricity Objective (NEO) and National Gas Objective (NGO). These seek to promote efficient investment in, and efficient operation and use of, electricity and gas services for the long-term interests of energy consumers.

We consider that the implications of the current drafting of the Risk Management Program Rules (draft Rules) could be detrimental to consumers. In particular, the definition of materiality of the risk and therefore the degree of investment required to mitigate that risk is at the discretion of the responsible entity. This may conflict with the NEO/NGO.

We consider that the draft Rules and SLACIP Bill would benefit from the proposed amendments we have set out below. This would better align the NEO/NGO and the SOCI Act so that Australian consumers' interests are at the forefront of responsible entities' decision-making. In particular, we believe the proposed changes ensure the intent of the SOCI Act to protect Australia's critical infrastructure and systems of national significance is retained, but does so in a way that is likely to reduce the risk of unnecessarily high compliance costs to consumers of energy services.

Definitions of material risk and relevant impact

We propose that greater clarity be included in the draft Rules and SLACIP Bill about how material risks and relevant impacts are defined and identified so it is consistent with the economic principles in the NEO/NGO.

The draft Rules contain provisions relating to the identification of material risks:[1]

> 1. [The SLACI Act] requires responsible entities to continue to identify and mitigate **material risks** that have a substantial impact on the availability, integrity and reliability of a critical infrastructure asset.
>
> 2. Responsible entities for critical infrastructure assets must consider **all** relevant **material risks** to their business.
>
> 3. Responsible entities for critical infrastructure assets are responsible for determining if a risk is a **material risk**.

Our concern is that the draft Rules do not provide clear guidance on what is material and places the discretion on the responsible entity to determine the materiality of the risk to be mitigated. We consider that the lack of clarity around materiality, and the discretion conferred on responsible entities, has the potential to give rise to very large compliance costs without regard for the balance between those costs and the benefits of the risk reduction.

We note that in the SLACI Act, when considering if a cyber security incident is a material risk the Minister will have regard to whether:[2]

> …the incident has seriously prejudiced, is seriously prejudicing, or is likely to seriously prejudice:
>
> (i) the social or economic stability of Australia or its people; or
>
> (ii) the defence of Australia; or
>
> (iii) national security.

We consider that the matters identified in the above provision are reasonable guiding considerations as to whether a risk is a material risk for the purposes of the Rules. While clause 4a of the "Definition of Material Risk" section in the draft Rules uses similar language to the first Bill, the draft Rules definition adds other considerations such as:

- a stoppage or major slowdown of a critical infrastructure asset's functioning for an unmanageable period (4b.)
- interference with technology essential to the functioning of a critical infrastructure asset (4d.), or
- any other material risk that goes to the substance of the functioning of the critical infrastructure asset (4g.).

Our concern is that these other considerations in the draft Rules substantially broaden the character of a material risk and act to reduce the materiality threshold from that contemplated by the wording in the SLACI Act. Our view is that, to reasonably characterise the degree of materiality that the responsible entities should consider, a definition of material risk consistent with the cyber security provisions of the SLACI Act be used in the draft Rules. This would ensure that even though the responsible entity decides what is material, there is clarity around what is material risk and the high threshold is consistent with the requirements of the NEO/NGO.

We also note that section 30AH(7) of the SLACIP Bill states:

> ….in determining whether a risk is a material risk, regard must be had to:
>
> (a) the likelihood of the hazard occurring; and
>
> (b) the relevant impact of the hazard on the asset if the hazard were to occur.

---

[1] Department of Home Affairs, *Risk Management Program Rules*, 26 November 2021, p. 4.

[2] *Security Legislation Amendment (Critical Infrastructure) Act 2021*, Division 2, s. 35AB(1)(c).

With respect to section 30AH(7)(b), the term “regard must be had to the relevant impact” could be construed as referring to the existence of the impact, regardless of how trivial it might be. In particular, as drafted, it could cover any impact on the availability, integrity or reliability of the asset, or on the confidentiality of information about the asset or that is stored in the asset. This seems to suggest that any prolonged outage or impairment of electricity or gas supply is itself a material risk, without any consideration of the extent of the outage or impairment. To ensure there is consideration of the degree of the impact of the hazard, we propose that section 30AH(7)(b) include the following additional words (in italics):

(b) *the extent of* the relevant impact of the hazard on the asset if the hazard were to occur.

We welcome any further dialogue with the Department on the contents of this submission or related matters.

If you would like to discuss any of the issues raised above or have any questions or queries please do not hesitate to contact Dr Kris Funston, Executive General Manager, Network Regulation on [redacted]

Yours sincerely

Clare Savage
AER Chair