

31 January 2022

Cyber and Infrastructure Security Centre  
Department of Home Affairs

Submitted via email by [REDACTED] to [ci.reforms@homeaffairs.gov.au](mailto:ci.reforms@homeaffairs.gov.au)

### **Exposure Draft of the Security Legislation Amendment (Critical Infrastructure Protection) Bill 2022 (the SLACIP Bill)**

The Australian Energy Council (the “AEC”) welcomes the opportunity to make a submission to the Department of Home Affairs on the SLACIP Bill.

The AEC is the industry body representing 20 electricity and downstream natural gas businesses operating in the competitive wholesale and retail energy markets. These businesses collectively generate the overwhelming majority of electricity in Australia and sell gas and electricity to over 10 million homes and businesses.

#### **Critical Infrastructure Risk Management Programs**

The AEC supports the Australian Government’s efforts to protect essential services by uplifting the security and resilience of critical infrastructure and systems of national significance. The Department of Home Affairs had initially proposed sector-specific Risk Management Program (“RMP”) rules to assist in achieving this objective. While the requirements of the sector-specific rules could have proved challenging for some stakeholders in the energy sector, this approach would have assisted the Department of Home Affairs in delivering an uplift in the security of critical electricity assets.

Nonetheless, the Department of Home Affairs shifted from a sector-specific rules-based approach to a principles-based approach that covered all sectors. The details of this new principles-based approach was outlined to the energy sector in a town hall virtual meeting on 11 November 2021. There was strong feedback in that town hall meeting that the change to a principles-based approach would not support the uplift in the security of critical electricity assets because the standards had been ‘watered down’. Indeed, this new principles-based approach appears to provide minimum standards that, generally speaking, do not support the energy sector to boost their security capability. This move away towards a broad principles-based approach will also limit the collective pressure the electricity sector can put on manufacturers and suppliers to offer products and services that meet the required standards to uplift security.

The AEC’s main concern with the principle-based approach is that it is not prescriptive enough. The Explanatory Document notes that the “Government’s intention is that responsible entities would have discretion as to how they construct their Risk Management Program.”<sup>1</sup> The Explanatory Document goes on to say that:

---

<sup>1</sup> See p12, [Security Legislation Amendment \(Critical Infrastructure Protection\) Bill 2022: Explanatory Document](#)

“Sections 30AE and 30AF would provide that the entity is also required to review the program on a regular basis and take all reasonable steps to ensure it is kept up to date ... The Exposure Draft does not define the frequency with which the review required in section 30AE would need to occur, but rather simply would provide that it would need to occur on a regular basis ... The Exposure Draft also does not define ‘reasonable steps’ in section 30AF, as it would depend on the individual circumstances of each entity.”<sup>2</sup>

The principle-based approach has created ambiguity and owners of critical electricity assets now have the discretion to create their own RMP without the opportunity for sector benchmarking or comparison. It is also difficult to envisage how a regulator will provide a consistent industry benchmark assessment if different standards are selected by different critical asset owners. In short, it’s difficult for critical asset owners to know what a “good” RMP looks like under the new principles-based approach.

The Explanatory Document does state that “the process for developing a Risk Management Program would be supported by consultation with industry and additional guidance provided by Government.”<sup>3</sup> The AEC considers that this guidance is necessary to ensure that the RMPs developed by critical assets owners meet the expectations of the Department of Home Affairs and there is some amount of consistency across the RMPs to facilitate benchmarking. This guidance is required as soon as possible.

### **Timeframe for compliance**

The town hall virtual meeting on 11 November 2021 indicated that critical asset owners have 6 months to establish their RMP and provide details on how they will address each rule. This is an extremely short timeframe, particularly given the ambiguous nature of the requirements and the need to consider such a wide variety of potential hazards, the links and risks in each supply chain, and measures to address each all of the risks. It is exacerbated by asset owners being forced to wait for further guidance on the RMPs from the Department of Home Affairs.

The AEC suggests that compressing the timeframe to only 6 months may have the unintended consequence of RMPs lacking the necessary substance to be effective in uplifting the security of critical assets. In other words, there is a real prospect that RMPs will be hastily put together to meet a deadline instead of the programs being well considered and a benefit to protecting the asset. For RMPs to be truly considered and detailed, the deadline for critical electricity asset owners to produce their RMPs should be extended to 12 months.

### **Background checking**

The AEC previously expressed its concerns about the proposed background checking. Compulsory AusCheck background checks on existing staff would have proven onerous in terms of time and costs, and potentially inconsistent with anti-discrimination and fair work legislation. As such, the AEC welcomes further detail in the Explanatory Document that now “this is not a mandatory background check for critical infrastructure.”<sup>4</sup>

The optional background checking outlined in the Explanatory Document is supported by the AEC because it will:

- Avoid unnecessary costs;
- Prevent delays from responding to security threats (such as mobilising international staff to respond to an unexpected outage at an electricity generation asset); and
- Avert potential issues with fair work legislation.

---

<sup>2</sup> See p12, [Security Legislation Amendment \(Critical Infrastructure Protection\) Bill 2022: Explanatory Document](#)

<sup>3</sup> See p12-13, [Security Legislation Amendment \(Critical Infrastructure Protection\) Bill 2022: Explanatory Document](#)

<sup>4</sup> See p15, [Security Legislation Amendment \(Critical Infrastructure Protection\) Bill 2022: Explanatory Document](#)

## Conclusion

The AEC appreciates this opportunity to provide feedback on the SLACIP Bill and encourages the Department of Home Affairs to consider the issues raised above.

Please do not hesitate to contact Graham Pearson, Western Australia Policy Manager by email on [REDACTED] or by telephone on [REDACTED] should you wish to discuss this further.

Yours sincerely,

**Graham Pearson**  
Policy Manager, Western Australia  
Australian Energy Council