

1 February 2022

Critical Infrastructure Centre
National Resilience and Cyber Security Group
Department of Home Affairs
by email: ci.reforms@homeaffairs.gov.au

Re: Exposure Draft Security Legislation Amendment Critical Infrastructure Protection Bill 2022

CitiPower, Powercor and United Energy welcome the opportunity to respond to the Department of Home Affairs (the Department) in relation to the *Exposure Draft Security Legislation Amendment Critical Infrastructure Protection Bill 2022* (SLACIP Bill).

We are supportive of the updated risk management program rules. Our businesses place great importance on ensuring the security of our networks and we recognise the need for an enhanced security framework for critical infrastructure across sectors. We believe the updated draft risk management framework rule (**dated November 2021**) balances enhancing security requirements while minimising unnecessary cost to consumers. In particular, the amended cyber security requirements that allow an entity to comply with a range of appropriate Australian standards and frameworks priorities a robust and efficient approach to managing cyber security.

We have key recommendations we encourage the Department to consider with the progression of the draft SLACPI Bill, including:

1. We recommend a self-assessment and reporting process is adequate for ensuring compliance and avoiding unnecessary costs to customers

The *SLACPI Bill Explanatory Statement* notes the Government intends to provide guidance on meeting the risk management program requirements. We strongly support the Department to develop guidance material on its approach to compliance with the rule, as understanding the compliance regime is key in our interpretation of the rules. We recommend the regulatory framework prescribes a compliance assessment approach that is sufficiently flexible. This will allow entities to use different approaches to demonstrate their initiatives meet the objectives of minimising and mitigating security risks to the level proportionate to the relevant risks and consequences.

We recommend a self-assessment and reporting process is adequate for ensuring compliance and for avoiding unnecessary costs to customers. Information provided on risks typically requires an understanding of our operating context. Similarly, to understand and assess our security risk requires intimate knowledge of our operating context, which why self-assessment is the most effective approach.

We would urge against introducing a regular external audit process which would be overly cumbersome and prescriptive and result in material costs for the Australian public, for little to no additional benefit.

We also urge the Department to coordinate with other agencies who are requesting similar information through a different channel to reduce duplicate effort.

2. We recommend the Department revert to the original timeframe of twelve months for compliance with the risk management framework

We are concerned about the six-month timeframe to develop the risk management programs across the businesses. We foresee material time and effort required to develop these reports and like all essential services, we are continuing to manage the risks that have been driven by the global pandemic. Several of the identified key stakeholders that will need to be involved in the transition process to the new risk management rules are also involved in the COVID-19 response process.

In addition, the pathway to compliance will only be clear once the regulatory regime has been agreed upon and the guidance material from the Department for compliance has been published. While we appreciate

the extensive industry consultation the Department has led, there has been several iterations of the rules and as such, there is confusion on the different versions socialising across industry.

With this in mind, we recommend the Department extend the compliance and reporting timeframe and recommend continued education and communication once a final position has been reached.

3. The scope of the annual reporting to the Department on the risk management framework should be clear to allow for the most efficient process

The *SLACPI Bill Explanatory Statement* notes the annual report is not intended to include reports on day-to-day activities or to include the complete risk management programs. We agree with this approach as it balances reporting with the regulatory burden and costs. The Department notes they will provide further guidance on this obligation which we would welcome, as to ensure the scope of the annual reports are clear.

4. Further consultation is needed with industry on the 'access to system information' cyber requirement


The 'access to system information' cyber security obligation introduces new requirement whereby the Department may require a designated officer to observe a cyber security exercise. The obligation includes the entity preparing an evaluation report relating to the exercise, with the potential for the Department to appoint an external auditor to prepare an evaluation report.

Information provided with respect to cybersecurity is by nature sensitive and requires an understanding of our operating context. Similarly, to understand and assess our security risk requires intimate knowledge of our operating context.

We are concerned about the process for disclosing vulnerability and security content to external auditors. We propose the Government review our existing regulations and collaborate with industry on the existing audit requirements to perhaps leverage the existing processes to minimise the additional sharing of information, as well as the duplication of effort and as such, costs to consumers.

Should you have any queries or wish to discuss our submission further please contact [REDACTED] on [REDACTED] or by email [REDACTED].

Yours sincerely,



Megan Willcox

**Head of Regulatory Performance and Analysis
CitiPower, Powercor and United Energy**