27 November 2020

Critical Infrastructure Centre
Cyber, Digital and Technology Policy Division
Department of Home Affairs
[redacted]

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

Exposure Draft Security Legislation Amendment (Critical Infrastructure) Bill 2020

Alinta Energy welcomes the opportunity to respond to the Department of Home Affairs exposure draft of the *Critical Infrastructure Bill*.

Alinta Energy, as an active investor in energy markets across Australia with an owned and contracted generation portfolio of nearly 3,000MW and more than 1.1 million electricity and gas customers has a strong interest in the development of the exposure draft and the obligations and impacts it will have in the energy sector in particular.

We maintain support of the Government's objectives to protect Australia's critical infrastructure and systems from emerging threats such as cyber-attacks and the recognition that achieving this across different sectors of the economy requires a flexible approach.

Definition of critical electricity asset

We note that point 206 of the explanatory document defines a critical electricity asset (with respect to generation) as:

> *"an electricity generation asset that is critical to ensuring the security and reliability of electricity networks or electricity systems in a state or territory"*[1]

The Department has indicated it will work with industry participants to identify appropriate thresholds regarding generation capacity and system restart functions. Alinta Energy welcomes further discussion with the Department on this definition as it will have a material compliance impact on regulated electricity assets. A definition consistent with the energy rules in the specific jurisdiction (i.e. National Electricity Rules or WA Wholesale Electricity Market Rules) would eliminate confusion over whether nameplate capacity, registered capacity or any other definition should be applied.

We maintain the view from our response to the consultation paper in September that credible

[1] Critical Infrastructure Centre (2020), Security Legislation Amendment (Critical Infrastructure) Bill 2020 – Explanatory Document, page 34.

contingency events determined by AEMO are an appropriate means of identifying electricity assets that are critical and therefore provide guidance on an appropriate threshold to satisfy the definition above.

Section 12M - Definition of cyber security incident

While broad, the definition of a cyber security incident aligns with the Australian Energy Sector Cyber Security Framework (AES-CSF). Alinta Energy expects the definitions in practice to mature over time.

Section 12F(3) - Obligations to notify data storage and processing service providers

It is not clear how a notice to a data storage or processing service provider will alter the arrangements in place between a responsible entity and the service provider (if the service provider is not covered by 8D(b) "Data storage or processing sector". In the energy (and other sectors) storage as a service (SaaS) and other related services may be provided by many commercial entities under agreed contractual terms. The effect of the notice required by section 12F(3) may not obligate these service providers to take any action or deviate from the contractual terms they have in place with a responsible entity. It is not clear if this section will impact on existing contractual arrangements and obligations agreed commercially.

We welcome further discussion with the Department in relation to the exposure draft. Please contact David Calder on [redacted] in the first instance.

Yours sincerely

[redacted]

Graeme Hamilton
General Manager, Regulatory & Government Affairs