

27 November 2020

Critical Infrastructure Centre  
Department of Home Affairs

Via Online Submission

Dear Sir/Madam

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

TasNetworks welcomes the opportunity to respond to the Department of Home Affairs (**DoHA**) consultation on Protecting Critical Infrastructure and Systems of National Significance Exposure Draft Bill.

TasNetworks is the Transmission Network Service Provider (**TNSP**), Distribution Network Service Provider (**DNSP**) and Jurisdictional Planner in Tasmania. TasNetworks is also the proponent for Marinus Link, a new interconnector between Tasmania and Victoria. The focus in all of these roles is to deliver safe, secure and reliable electricity network services to Tasmanian and National Electricity Market (**NEM**) customers at the lowest sustainable prices. In addition, TasNetworks provides Data Centre, Telephony, Information Technology and Communications services to the broader Tasmanian community, including key government agencies. TasNetworks is therefore supportive of any efforts to ensure Australia's laws, policies and security practices bolster the security and resilience of its critical infrastructure.

The need for increasing security requirements for critical infrastructure is warranted and to be expected. However, the uplift in capability for businesses comes with a cost that inevitably has to be paid for. As a provider of an essential service, TasNetworks is acutely aware of the need to balance increasing security obligations with the impacts on operational efficiency to ensure positive outcomes for customers. Consequently, TasNetworks requests that expectations be clearly articulated so actions taken by the business are commensurate with the risks being mitigated and delivered in the most efficient manner possible.

In considering this, TasNetworks would like to make the following comments with respect to the exposure draft of the Security Legislation Amendment (Critical Infrastructure) Bill 2020.

- Under Section 30DJ the entity may be required to “install a specified computer program on the computer” and “take all reasonable steps to ensure that the computer



is continuously supplied with an internet carriage service that enables the computer program to function". Failing to follow these requirements may attract a civil penalty for non-compliance. TasNetworks is concerned that it may not always be possible to meet these requirements, as the need may arise to put security controls in place which limits the supply of information during a cyber security incident where Internet and/or internal network links are 'severed' as a precautionary response to the incident. TasNetworks considers an entity pre-emptively acting to protect itself during a cyber security incident should not attract civil penalties.

- Section 30AG provides that where a risk management plan is in place, the responsible entity of that critical infrastructure asset must provide an annual report to the Secretary of Home Affairs, or relevant Commonwealth regulator, within 30 days of the end of the financial year. TasNetworks considers that the 30 day timeframe to produce the annual report would be difficult to meet, especially with the requirement to have it signed off by the board, council or other governing body. TasNetworks suggests that a 90 day timeframe would be more appropriate.
- TasNetworks would like to better understand the triggers for the Minister to make a declaration on systems of national significance for the energy sector. Visibility of the timeframes for determination of systems of national significance and approach to 'on-switch' rules will enable TasNetworks to plan to meet these obligations in a timely manner.
- Similarly, in planning to meet the Positive Security Obligations in a timely manner, TasNetworks would like to see further details regarding the implementation of these obligations, particularly in relation to when the Minister will 'on-switch' the rules that are to be made. Details that TasNetworks is interested in include visibility of the timeframes and approach to commencement of the Positive Security Obligations. While TasNetworks will already meet some of these new obligations through the work undertaken in the current security environment, there will be additional cost impacts to modify, expand and enhance current practices to meet additional requirements under the Bill. It is important for TasNetworks to continue to balance increasing security obligations and the impacts on operational efficiency to ensure a positive outcome for customers. This can be achieved through clear articulation of expectations and an understanding by all parties of the implications, cost or otherwise, of implementation.
- The lack of clarity around the timeframe for implementation and the specific obligations that will be imposed on TasNetworks leads to uncertainty regarding cost implications. Until TasNetworks is aware of the extent of its obligations, it will be unable to forecast costs in meeting these new obligations. Forward planning and management of any additional costs is essential in ensuring that cost impacts for customers and the community are well managed. This is particularly important to a regulated business whose revenue allowance is set every five years by a Regulator with only limited ability to alter revenue allowances mid-period.
- TasNetworks is concerned about the implications arising from any determinations that may lead to significantly different obligations being applied to TasNetworks' assets for Transmission and Distribution. Obligations that are introduced would need to be

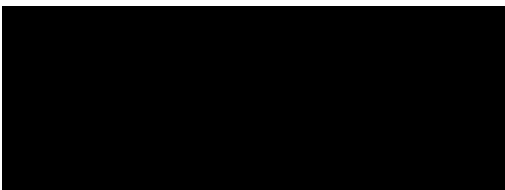
carefully considered from a risk perspective to ensure that they are fit for purpose for different network types while factoring potential impacts in relation to cost and efficiency.

- TasNetworks is concerned with conflicting obligations across legislation, regulations and requirements at both the State and Federal level and the potential liabilities that TasNetworks may be exposed to. With Federal laws taking precedence over State based laws, there are concerns that while complying with the new requirements that TasNetworks may be exposed to liabilities for not meeting State based requirements, such as under the National Electricity Law, or impacts on meeting regulatory requirements. TasNetworks would like to see more clarity around the management of obligations that may conflict between the Federal and State level.
- TasNetworks looks forward to further discussion on an appropriate regulator for the energy industry, noting that there is currently no one regulator for the energy sector that incorporates electricity, gas and liquid fuel. TasNetworks already operates in a heavily regulated environment. To avoid duplication of effort and unnecessary regulatory burden, a regulator for the energy industry would need to take into consideration existing regulators.

TasNetworks would welcome the opportunity to actively participate in the co-design of sector specific requirements. TasNetworks supports working with the Federal and State Governments to develop specific matters to be included in a critical infrastructure risk management program. It is important that the requirements are proportionate to the risk profile of the sector and minimise the regulatory burden that will be imposed to meet the security objectives.

We welcome the opportunity to discuss this submission further. Should you have any questions, please contact Chantal Hopwood, Leader Regulation, via email  or by phone on .

Yours faithfully



Wayne Tucker

General Manager, Regulation, Policy and Strategic Asset Management