TasNetworks
Delivering your power

Tasmanian Networks Pty Ltd
ABN 24 167 357 299
PO Box 606
Moonah TAS 7009

16 September 2020

Critical Infrastructure Centre
Department of Home Affairs

Via Online Submission

Dear Sir/Madam

RE Protecting Critical Infrastructure and Systems of National Significance

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

TasNetworks is the Transmission Networks Service Provider (**TNSP**), Distribution Network Service Provider (**DNSP**) and Jurisdictional Planner for transmission and distribution 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, IT and Communications services to the broader Tasmanian community, including key government agencies. Therefore, TasNetworks is supportive of any efforts to ensure Australia's security practices, policies and laws bolster the security and resilience of its critical infrastructure.

Similar to other Network Service Providers (**NSPs**), TasNetworks is continuously improving its business risk management processes. TasNetworks acknowledges the importance of identifying and mitigating the risks it faces due to the essential nature of the services provided. However, TasNetworks is also acutely aware of the cost impacts and the affect increased electricity costs have on the Tasmanian community and customers in the wider NEM. TasNetworks therefore attempts to balance the impact on operational efficiency from increasing security obligations to ensure the best outcome for its customers.

One way TasNetworks does this is through working with Australian Energy Market Operator (**AEMO**) and other energy sector entities in developing the Australian Energy Sector Cyber Security Framework (**AESCSF**). This voluntary arrangement allows for benchmarking against similar businesses to gauge the level of maturity of its risk management. There is also a

collegial sharing of information and skills allowing for a sector wide improvement in capability.

Like other NSPs, TasNetworks operates in a heavily regulated environment. It is critical that regulators work in unison, being aware of each other's objectives, thereby avoiding duplication and the imposition of unnecessary regulatory burden. There is a risk that a Critical Infrastructure regulator may require what are rightfully identified as critical reforms while an Economic Regulator (in our case the Australian Energy Regulator (**AER**)) aims to set revenues so that energy consumers pay no more than necessary for the safe and reliable delivery of an essential service. TasNetworks therefore requests a balanced and coordinated approach where regulators understand each other's objectives and provide a consistent set of drivers to businesses.

TasNetworks is also aware that a large proportion of the cost to manage security risks are not dependent on the size of the entity or a NSP's customer base. This could lead to a disproportionate impact on Tasmanian customers arising from an increase in obligations. There are also concerns about how a business, that may have some functions declared as critical and some not, will be able to manage costs. There will be situations where to meet a positive security obligation may require implementing a solution across the entire business, including part of the business not declared as critical. There are questions as to how a business would be able to assign all the costs of meeting the obligation to just those areas formally required to meet those obligations. The alternative would see some costs unduly apportioned to a business unit potentially unable to recover those costs due to competitive pressures.

TasNetworks recognises the importance of cyber security. There is no substitute to having appropriate protections in place. However, TasNetworks views it as critical that the cost impacts for customers and the community from responding to changing security risks are well managed. Government must support the investments required by business by ensuring the costs are reflective of the risks and have a benefit for customers.

Government could help minimise costs by, amongst other things, providing:

- assistance in identifying security and supply chain risks, especially in other sectors of the economy;
- regular updates on risks;
- appropriate training opportunities; and
- guidance on priorities and appropriate timeframes to implement security improvements.

It would also be of assistance if the Government was to provide guidance on best practice risk management approaches that businesses could consider adopting. This would be especially beneficial for businesses with multiple functions such as both electricity distribution/transmission and telecommunications. Some of this assistance could be efficiently delivered through broad based sector specific Trusted Information Sharing Networks (**TISNs**).

This support and guidance combined with clear and realistic expectations established by ensuring regulators are working collaboratively will assist businesses meet security obligations while managing the end impact on customers.

TasNetworks responses to individual questions are provided below. We welcome the opportunity to discuss this submission further with you. Should you have any questions, please contact Chantal Hopwood, Leader Regulation, via email [redacted]r by phone on [redacted].

Yours faithfully

[redacted]

Wayne Tucker

General Manager, Regulation, Policy and Strategic Asset Management

Responses to Questions

1. **Do the sectors above capture the functions that are vital to Australia's economy, security and sovereignty? Are there any other sectors that you think should be considered as part of these reforms (e.g. manufacturing)?**

   The outlined sectors, including energy, adequately cover the areas vital to the Australian economy and security. One sector that TasNetworks considers should be included as a critical infrastructure sector by DoHA is the justice sector due to the impacts a breakdown in law and order has on society.

2. **Do you think current definition of Critical Infrastructure is still fit for purpose?**

   TasNetworks is of the view that the current definition of Critical Infrastructure is still fit for purpose. The definition broadly states the types of services that if negatively impacted would affect Australia. This definition would still be applicable even if the reforms broadened the range of sectors to which an enhanced regulatory framework would apply.

3. **Are there factors in addition to interdependency with other functions and consequence of compromise that should be considered when identifying and prioritising critical entities and entity classes?**

   The Consultation Paper adequately identified the main factors to consider when identifying and prioritising critical entities and entity classes.

   Full consideration of the mapping process for entities with business functions that sit across multiple sectors will be critical.

4. **What are the common threats you routinely prepare for and those you have faced/experienced as a business?**

   TasNetworks is faced with the standard threats that any other business, particularly in the electricity supply and telecommunications industry, faces. These threats include natural disasters, asset failures and cyber attacks.

5. **How should criticality be assessed to ensure the most important entities are covered by the framework?**

   The criticality of an entity is appropriately assessed in terms of the impact it may have on both up and down stream markets. Extensive supply chain mapping is necessary to identify less obvious but critical providers within a supply chain. There is a risk that an obviously critical industry (like an electricity network) may be reliant on access to a key product, the provider of which would not seem like a critical entity.

While the Cyber Supply Chain Risk Management Practitioner Guide is a useful tool for businesses to assess their own supply chain risks there is risk in relying on self-assessment. TasNetworks would prefer that DoHA undertake a regular assessment of economy wide supply-chains in consultation with sectors to assist entities in undertaking their own assessment.

TasNetworks is interested in better understanding the approach to businesses that provide multiple functions, only part of which is defined as critical. Clarity needs to be provided as to how a business, that may have some functions declared as critical and some not, will be able to manage costs. There will be situations where to meet a positive security obligation may require implementing a solution across the entire business, including part of the business not declared as critical (examples could be IT systems or physical protections like fences or gates). There are questions as to how a business would be able to assign all the costs of meeting the obligation to just those areas formally required to meet those obligations. The alternative would see some costs unduly apportioned to a business unit potentially unable to recover those costs due to competitive pressures. This could be particularly important for businesses with regulated incomes, which are less able to absorb costs.

6. **Which entities would you expect to be owners and operators of systems of national significance?**

TasNetworks has no view on this issue.

7. **How do you think a revised TISN and Critical Infrastructure Resilience Strategy would support the reforms proposed in this Consultation Paper?**

TasNetworks supports the proposed reforms, including a "reinvigorated TISN". TasNetworks is particularly interested in Individualised Vulnerability Assessments as outlined in the Consultation Paper (page 15) and would like to explore this further due to likely operational impacts. TISN would need to work more closely with regulators and enhance all hazards approaches through collective and expert threat horizon scanning, education, training, exercising, vulnerability assessments, research, analysis and evaluation. TasNetworks identifies benefits from added linkages to the expanded National Exercise Program.

8. **What might this new TISN model look like, and what entities should be included?**

TasNetworks supports maintaining the sector oriented structure. To support the action proposed by DoHA in the Consultation Paper (page 15), "Boards of critical infrastructure entities have visibility of, and are responsible for planning and actively managing security and resilience", TasNetworks recommends a broad membership on TISN is required. TasNetworks recommends membership of TISN minimally includes entities identified as Critical, Regulated Critical and Systems of National Significance (Consultation Paper page 13).

9. **How else should government support critical infrastructure entities to effectively understand and manage risks, particularly in relation to cross sector dependencies? What specific activities should be the focus?**

   Government support could include the provision of information on other sectors' risks, trends and vulnerabilities especially where that information is not generally available. Assistance would also come from provision of sector specific frameworks, maturity targets and reporting mechanisms. TasNetworks notes the benefit it has from working with AEMO and other energy sector entities in developing the AESCSF and would encourage the continuing cooperation and support shown by DoHA with this work.

   It is also critical that Government acknowledge and support the investment needed to obtain and retain the specialist skills and knowledge required for critical infrastructure protection. This can be a particular challenge in smaller jurisdictions and could be partially alleviated by an Australian Cyber Security Centre (**ACSC**)/Joint Cyber Security Centre (**JCSC**) being established in these jurisdictions.

10. **Are the principles sufficiently broad to consider all aspects of security risk across sectors you are familiar with?**

    The principles-based outcomes listed on page 18 of the Consultation Paper provide a comprehensive description of the framework businesses should follow to manage risks.

11. **Do you think the security requirements strike the best balance between providing clear expectations and the ability to customise for sectoral needs?**

    TasNetworks considers that the security requirements on pages 19 and 20 of the Consultation Paper provide clear high-level expectations. These security requirements have the flexibility to allow for customisation for the expanded range of sectors.

    However, more detail is required to fully explore the sector specific expectations.

12. **Are organisations you are familiar with already operating in-line with these principles, or do you think there would be a significant time and/or financial cost to meet these principles?**

    Similar to other TNSPs, TasNetworks is continuously improving its business risk management processes. The principles on page 18 of the Consultation Paper are the basis for the approach to developing both the business' Risk Management and Emergency Risk Management frameworks.

    TasNetworks, together with AEMO and other energy sector entities have adopted the AESCSF. This voluntary arrangement allows for benchmarking against similar businesses to gauge the level of maturity of its arrangements. There is also a collegial sharing of information and skills allowing for a sector wide improvement in capability.

This voluntary framework allows each business to target a level of maturity consistent with its criticality and the ability of its customer base to fund it through tariffs. TasNetworks is vitally aware of the potential impact on operational efficiency from increasing security obligations being incorporated in business as usual operations and works to balance the need to manage security and cost implications to our customers.

13. What costs would organisations take on to meet these new obligations?

It will not be possible to move from voluntary obligations to mandated obligations without either an increase in costs for end consumers or diverting resources from other priority focus areas for the business.

TasNetworks notes that a large proportion of the cost to manage security risks and meet new obligations are not dependent on the size of the entity. TasNetworks is concerned that the ability to pass on these costs may have a disproportionate impact on customers in smaller jurisdictions.

Another challenge faces businesses operating in less competitive environments. This could be a particular issue for TasNetworks. Operating in an island state comes with risks to the supply chain. If TasNetworks is required to meet certain obligations with regards to the security of some of its providers it could face substantial cost increases as it searches for providers willing to either operate in Tasmania or meet increased security requirements. This may well result in the costs to meet new security obligations being higher than in markets with greater competition.

Government needs to support businesses wherever possible in ensuring costs are prudent to the appropriate consideration of risk. TasNetworks recognises the importance of cyber security. There is no substitute to having appropriate protections in place. However, TasNetworks views it as critical that the cost impacts for customers and the community from responding to changing security risks are well managed.

Some opportunities for Government that would assist in managing costs are included in the response to question 19. In addition, it would also be of assistance if the Government was to provide guidance on best practice risk management approaches that businesses could consider adopting. This would be especially beneficial for businesses with multiple functions such as both electricity distribution/transmission and telecommunications.

This support and guidance combined with clear and realistic expectations established by ensuring regulators are working collaboratively will assist businesses meet security obligations while managing the end impact on customers.

14. Are any sectors currently subject to a security obligation in-line with these principles? If so, what are the costs associated with meeting this obligation? Does this obligation meet all principles, or are enhancements required? If so, what?

TasNetworks is unaware of any other sectors' detailed security obligations, across the four security obligations.

15. **Would the proposed regulatory model avoid duplication with existing oversight requirements?**

    TasNetworks considers that the proposed regulatory model has the potential to avoid duplication with existing oversight requirements. This would be dependent on, when it came to the Commonwealth designating regulators (step 2), the Commonwealth working with the current regulator(s) for the relevant sector.

16. **The sector regulator will provide guidance to entities on how to meet their obligation. Are there particular things you would like to see included in this guidance, or broader communication and engagement strategies of the regulator?**

    In the guidance provided to entities around meeting their obligations, TasNetworks would like to include the regulation of the AESCSF across the sector. There would also need to be engagement with the current regulator(s) for the sector to remove duplication of obligations and expectations, and streamline with any engagement strategies. This would assist in reducing additional burdens and costs on entities when dealing with additional obligations and expectations.

17. **Who would you consider is best placed to undertake the regulatory role for sectors you are familiar with? Does the regulator already have a security-related regulatory role? What might be the limitations to that organisation taking on the role?**

    TasNetworks' main concern is not with who the regulator is but the potential for duplication in function and the lack of coordination between the various regulatory bodies TasNetworks and other NSPs interact with. Duplication or conflicting obligations arising from multiple regulators will result in unnecessary additional regulatory burden, thereby increasing costs to customers.

    There is a risk that a Critical Infrastructure regulator may require what are rightfully identified as critical reforms while an Economic Regulator (the AER) aims to set revenues so that energy consumers pay no more than necessary for the safe and reliable delivery of an essential service. TasNetworks therefore requests a balanced approach where regulators understand each other's objectives and provide a consistent set of drivers to businesses.

18. **What kind of support would be beneficial for sector regulators to understand their additional responsibilities as regulators?**

    It would be beneficial for sector regulators to be provided with a clear articulation of their responsibilities, security and cost implications. In situations where the regulator for the positive security obligations (**PSOs**) is not the same body that is regulating costs, it would be essential to provide a requirement for an understanding of the cost consequences on customers to be factored into any decisions on increasing security obligations.

19. How can Government better support critical infrastructure in managing their security risks?

The Government could support critical infrastructure through:

- setting clear responsibilities in legislation;
- providing clarity on definitions of critical infrastructure and systems of national significance and likely obligations flowing from them;
- recognising the cost impacts that will flow through to customers by either tailoring obligations or setting realistic timeframes wherever possible;
- sharing information, especially on risks in other sectors that may impact the energy sector;
- using existing energy security frameworks (for example the AESCSF);
- providing support to assist smaller business reach increased security expectations, especially when their customer base cannot accept cost increases;
- facilitating through bodies like TISN, sectorial collaboration and identification of synergies that realise investment efficiencies; and
- increasing investment and expanding the ACSC/JCSC to all States and Territories.

20. In the AusCheck scheme potential and ongoing employees in the aviation, maritime, health and major national event security sectors undergo regular national security assessments by the Australian Security Intelligence Organisation and criminal history assessments to mitigate the risk of insider threats. How could this scheme or a similar model be useful in the sectors you are familiar with?

TasNetworks supports personnel security checks for those employees and contractors who have access to assets. We consider the most appropriate standard is *Baseline Vetting,* as outlined in the Australian Government's Protective Security Policy Framework (**PSPF**). This provides the most appropriate balance between cost and security control.

21. Do you have any other comments you would like to make regarding the PSO?

There needs to be greater clarity and definition underpinning the PSO principles that clearly articulate what entities must have in place and what is a minimum requirement for meeting the obligation. If an expectation to audit against obligations is introduced, more detail will need to be provided, for example through a framework or mitigation strategies.

TasNetworks prefers that the Federal Government has a role in improving Supply Chain Security outcomes (Consultation Paper page 20). It is important that vendor risk be managed in a coherent and compelling manner. This could include mandating the use of security standards for technical asset compliance for Critical Infrastructure supply chains.

22. Do you think there are other preparatory activities that would assist in proactively identifying and remediating cyber vulnerabilities?

TasNetworks considers DoHA could assist in the following areas:

- sharing of threat intelligence information;

- identifying supply chain vulnerabilities;
- holding workshops (specific to a single topic – for example, Cyber Security Incident Response); and
- providing or supporting industry relevant cyber specific training courses.

23. What information would you like to see shared with industry by Government? What benefits would you expect from greater sharing?

TasNetworks considers that the business can be best protected from cyber security attack through effective and confidential information sharing including sharing specific industry threat intelligence and approaches with the Federal Government.

24. What could you currently contribute to a threat picture? Would you be willing to provide that information on a voluntary basis? What would the cost implications be?

In principle, TasNetworks is interested in developing two-way confidential information sharing arrangements with relevant Federal authorities.

It is not possible to comment on cost implications until a draft plan is agreed.

25. What methods should be involved to identify vulnerabilities at the perimeter of critical networks?

Vulnerabilities in any perimeter-facing equipment are currently widely disseminated and generally quite detailed. Identifying such vulnerabilities should be the focus of entities like the ACSC working in partnership with vendors and industry. Federal agencies could assist critical infrastructure operators with early notification and targeted assistance to help detect exploitation of such vulnerabilities.

26. What are the barriers to owners and operators acting on information alerts from Government?

For TasNetworks, the two biggest barriers to acting on information alerts from Government are the timeliness of the alerts and the availability of both internal skills and systems to allow the timely ingestion and analysis of the information alerts. The alerts must be clear and easily actionable.

27. What information would you like to see included in playbooks? Are there any barriers to co-developing playbooks with Government?

TasNetworks identifies DoHA as providing practical input on the nature and shape of playbooks, including:

- provide standard playbook templates and approaches;
- the provision of a Cyber Security specific Incident Response Framework that is easily able to be integrated into and support existing internal and external incident response plans and procedures;

- consistency of language terminology and techniques between TISN, State based government agency obligations and internal incident response and emergency management processes and procedures; and
- integration of cyber security elements with an 'All Hazards' approach.

28. What safeguards or assurances would you expect to see for information provided to Government?

TasNetworks considers that confidentiality of information is essential. Further consultation would be required to ensure that any information sharing solutions and processes are effective in managing security risk.

29. In what extreme situations should Government be able to take direct action in the national interest? What actions should be permissible?

TasNetworks considers that Government has a role in both the detection and prevention of cyber security events in the national interest. Further consultation is required on the specifics of what might constitute direct action when considered in the context of TasNetworks' existing regulatory, non-regulatory and state based energy and communications specific obligations.

30. Who do you think should have the power to declare such an emergency? In making this declaration, who should they receive advice from first?

The energy sector has a robust emergency management framework. AEMO's Power System Emergency Management Plan (**PSEMP**) defines the parties who can declare an emergency in the electricity sector. In this plan, technical advice is received from the 'Responsible Officer' (**RO**) of the jurisdiction where the initial incident occurs in consultation with ROs of the other NEM jurisdictions. This collaboration recognises the interdependency of the NEM members during emergencies arising from the ability to transfer electrical power between the States. From this advice a decision on the level of and lead authority for the emergency will be determined collaboratively. There is scope for an agency like DoHA to be involved in this process particularly when cyber security issues have an adverse impact on energy supply.

31. Who should oversee the Government's use of these powers?

TasNetworks considers that the Judiciary should fill the role of oversight of the Government's use of these powers, via the Commonwealth Judicial Review Act.

32. If, in an exceptional circumstance, Government needs to disrupt the perpetrator to stop a cyber attack, do you think there should be different actions for attackers depending on their location?

TasNetworks has no view on this issue.

33. What sort of legal protections should officers (both industry and Government) undertaking emergency actions be afforded?

TasNetworks considers that there should be provisions for statutory immunities for officers. This would result in no personal liability attaching to a person for any act or omission in good faith in the performance or exercise of a power, function, duty or direction under the Act.

34. What safeguards and oversight measures would you expect to ensure the necessary level of accountability for these type of powers?

TasNetworks considers that the Secretary of DoHA must stay the effect of a relevant decision that is subject to administrative review or appeal, while the Judiciary must review the disputed decision.

35. What are the risks to industry? What are the costs and how can we overcome them? Are there sovereign risks to investment that we should be aware of?

Given the importance of the electricity sector and the well tested framework described in the PSEMP, there is minimal risk of the Government taking emergency action having an impact on the electricity industry.

36. Does this mix of obligations and assistance reflect the roles and responsibilities of Government and industry in protecting critical infrastructure? How would private sector management of risk change with the proposed increased role for Government?

TasNetworks has no view on this issue.