

16 September 2020

Department of Home Affairs
email: ci.reforms@homeaffairs.gov.au

Protecting Critical Infrastructure and Systems of National Significance

Energy Networks Australia welcomes the opportunity to provide a response to the Department of Home Affairs (the Department) consultation on *Protecting Critical Infrastructure and Systems of National Significance*.

Energy Networks Australia is the national industry body representing Australia's electricity transmission and distribution and gas distribution networks. Our members provide more than 16 million electricity and gas connections to almost every home and business across Australia.

Energy Networks Australia and its members recognise that the energy networks of Australia deliver an essential service that supports the businesses and residents of Australia. Network service providers, regulated by the Australian Energy Regulator (AER) and jurisdictional regulators, take a proactive approach to securing their assets and operations to ensure that energy is delivered securely, reliably and safely to all consumers, at an efficient cost.

Proposal

The Department proposes a framework that would set:

1. Positive Security Obligation, including:
 - a. set and enforced baseline protections against all hazards for critical infrastructure and systems, implemented through sector-specific standards proportionate to risk.
2. Enhanced cyber security obligations that establish:
 - a. the ability for Government to request information to contribute to a near real-time national threat picture;
 - b. owner and operator participation in preparatory activities with Government; and
 - c. the co-development of a scenario based 'playbook' that sets out response arrangements.

3. Government assistance for entities that are the target or victim of a cyber attack, through the establishment of a Government capability and authorities to disrupt and respond to threats in an emergency

Security frameworks

Network service providers, working with the Australian Energy Market Operator (AEMO), currently participate in the simulations of threat scenarios (Item 2). They have also collaborated with AEMO on the Australian Energy System Cyber Security Framework (AESCSF). Any additional cyber security framework developed by the Department should closely align with and leverage this existing Framework.

While the AESCSF currently only applies to cyber security, the principle of leveraging an existing framework also applies to other areas of security (e.g. Protective Security Policy Framework for physical security) for critical infrastructure.

The Department will also need to recognise that while national requirements are highly desirable, particularly for a sector where networks cross jurisdictional boundaries, there are likely to be specific jurisdictional requirements and programs of work (such as the NSW Government Cyber Security Standards Harmonisation Taskforce) that will need to be aligned to avoid duplication.

Energy networks are keen to work with the Department to determine the status of key energy infrastructure, particularly in determining what assets are classified as “nationally significant”.

Cost recovery

Network service providers recognise the need to secure critical infrastructure, but the Positive Security Obligation is likely to place additional costs on regulated businesses, which are ultimately borne by consumers through their utility bills. It is essential that the benefits of any obligations outweigh the cost to businesses and consumers, and careful consideration is needed to ensure that network service providers have the ability to recover their efficient costs through the regulatory framework.

It would also be beneficial for the Department to work with the industry regulator, the AER, to ensure that they have a clear understanding of the requirements and rationale of the Positive Security Obligation, to assist with their expenditure assessments.

Compliance.

It is not immediately clear which regulator will be best placed to oversee compliance. The Critical Infrastructure Centre (CIC) is one option and while the CIC is well placed to assess the security requirements for critical infrastructure, there will be little understanding of the existing energy regulatory framework.

The AER, with extensive experience in the energy regulatory framework, is unlikely to have the knowledge and capacity to oversee security compliance, particularly any compliance related to cyber security. Jurisdictional regulators may also not have the

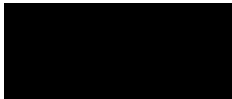
capacity, and therefore significant support, including secondment, may be required to ensure that these regulators develop the necessary capacity.

Regardless, care will be needed to develop efficient regulatory oversight, avoiding the risk of duplication and competing requirements from multiple regulators, which would create complexity and elevate costs.

Energy Networks Australia and its members, as key stakeholders, look forward to continuing to engage with the Department as it develops the Frameworks and progresses towards legislation and implementation.

If you require further information please contact Jill Caine, General Manager Networks (████████████████████).

Yours sincerely,



Andrew Dillon
Chief Executive Officer