Ausgrid Submission

Protecting Critical Infrastructure and Systems of National Significance

16 September 2020

16 September 2020

24-28 Campbell St
Sydney NSW 2000
All mail to
GPO Box 4009
Sydney NSW 2001
T +61 2 131 525
ausgrid.com.au

Mr Andrew Kiley
Assistant Secretary, Assurance, Risk and Engagement Branch
Critical Infrastructure Security Division
Department of Home Affairs

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

Dear Mr Kiley,

We welcome the opportunity to comment on the Critical Infrastructure Centre's consultation paper - Protecting Critical Infrastructure and Systems of National Significance and contribute to the development of reforms to the Security of Critical Infrastructure Act (2018) and the supporting regulations.

We recognise the need for an enhanced critical infrastructure framework. Our shared distribution network supplies energy to over 4 million people living and working in and around Sydney every day. The network not only provides an essential service to our customers; it is a critical enabler of a significant part of the Australian economy.

Our submission provides views on various matters covered in the consultation paper, including the costs and potential customer impact of any reforms, and the possible duplication of requirements between state and federal jurisdictions – these matters are covered in greater detail in Attachment 1 to our submission. In our view, there should be a consistent framework for equivalent critical infrastructure operators. We support the development of a new energy sector standard, which all network businesses in the sector would need to comply with.

It is important that customers are included in these conversations, as any changes in obligations could lead to increased costs for the operators of critical assets. Recognising the sensitivity of these issues, we are seeking the views of customers on these issues through our new Technical Review Committee. These conversations allow us to explain the drivers and detail behind the proposed security obligations.

Given the sensitive nature of our responses to the consultation questions, we request that Attachment 1 to our submission is kept confidential in accordance with the Department's call for submissions – a redacted version of this submission without Attachment 1 is also provided. If Attachment 1 is to be tendered or otherwise made available to any party other than Ausgrid, we would be grateful if the Department would provide us with advance notification, so that we may take the appropriate steps.

We appreciate the Department's consultative approach on these issues. If you have any questions contact me on [redacted] or Andy Chauhan, Chief Information Security Officer on [redacted] or by email [redacted].

Yours sincerely,

[redacted]

Richard Gross
Chief Executive Officer

Executive Overview

Cyber security and cyber terrorism are receiving increased focus in today's digital age. Electricity distribution assets are recognised as critical infrastructure by the Critical Infrastructure Centre. Cyber security is vital if Ausgrid is to protect its network against cyber-attack and continue to deliver a safe and reliable energy supply to our customers.

We recognise the need for an enhanced critical infrastructure framework. Our submission provides responses to each of the questions in the consultation paper, as well as highlighting two key issues:

- the costs and potential customer impact of any reforms; and
- duplication of requirements between state and federal jurisdictions.

About Ausgrid

Ausgrid operates a shared electricity network that powers the homes and businesses of more than 4 million Australians living and working in an area that stretches over 22,000 square kilometres from the Sydney CBD to the Upper Hunter. As the provider of an essential service, we recognise the important role we play, not just in our customers' lives, but in enabling a significant part of the Australian economy.

Day-to-day, we are responsible for operating, maintaining, repairing and building our network of substations, overhead power lines, underground cables and supporting infrastructure. We are working to ensure the network is ready for a future where renewables play a major role in the power mix, and households and businesses can generate their own electricity and sell it back through the grid.

Ensuring the security of our network is critical for the current and future delivery of services to our customers and communities. We are committed to providing a safe and reliable energy supply. Our network is designed and operated to meet our customers' expectations and ensure customer data and control of our infrastructure cannot fall into the wrong hands.

Ausgrid Network

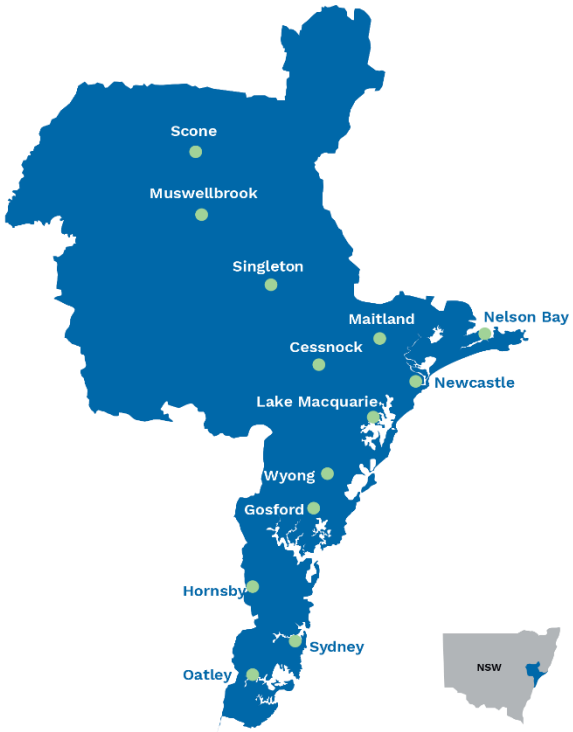
20%
of Australia's GDP

16%
of Australia's jobs

1,200
Schools

105
Hospitals

3980
Employees



Cost and customer engagement

Our customers have asked for greater visibility and justification of our cyber security expenditure. To support information sharing and understanding of cyber requirements we established a specialist customer consultation group named the Technical Review Committee (TRC).

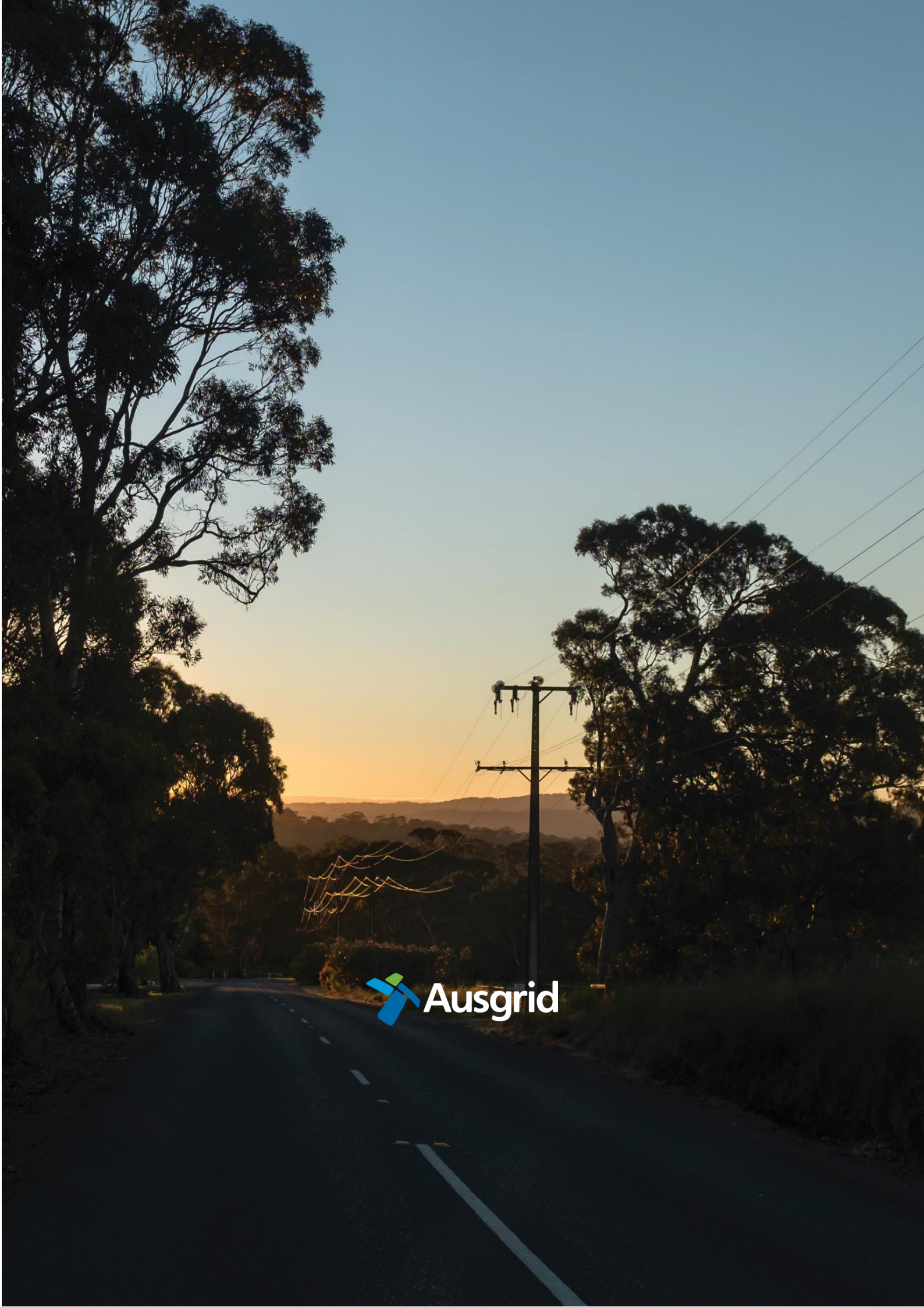
Customer engagement is critical in the development of a new framework for the protection of critical infrastructure. Operators of critical assets are likely to incur additional capital and operating costs to ensure they are compliant with any new obligations. These costs include up-front costs to make systems and infrastructure compliant with the new obligations, as well as ongoing costs to ensure continued compliance and associated regulatory reporting.

The costs incurred will depend on the nature of the obligations, their impact on existing practices and our infrastructure, and the effort required to sustain and report on the new obligations. Given these implications, it is important that customer views are sought as part of the development. We will continue to engage with customers through our TRC during the development of the new framework.

Duplication of requirements between state and federal jurisdictions

Ausgrid is currently subject to Distributor's Licence conditions imposed by the New South Wales Government under the Electricity Supply Act, 1995 (NSW) that regulate Ausgrid's critical infrastructure protections. Additionally, over the last 2 years we have been assessing the maturity of our critical infrastructure protections against the proposed Australian Energy Sector Cyber Security Framework (AESCSF).

We support the development of a new energy sector standard, which all network businesses in the sector would need to comply with. Having one set of requirements at a national level is more likely to avoid duplication with existing jurisdictional requirements. This may require Ausgrid's NSW Distributor's Licence to be varied to remove or modify the critical infrastructure licence conditions, to remove inconsistency or unnecessary duplication. Consultation with the NSW Government and the NSW Independent Pricing and Regulatory Tribunal (IPART), which administers the Distributor's Licence, will be needed to ensure the desired outcome is achieved.


Ausgrid