14 April 2023

Cyber Security Expert Advisory Board
Andrew Penn AO (Chair)
Air Marshall (ret'd) Mel Hupfeld AO DSC
Rachael Falk
Submission made by webform

24-28 Campbell St
Sydney NSW 2000
All mail to
GPO Box 4009
Sydney NSW 2001
T +61 2 13 13 65
ausgrid.com.au

Ausgrid response to the 2023-30 Australian Cyber Security Strategy Discussion Paper

Dear Mr Penn, Air Marshall Hupfeld and Ms Falk,

We welcome the opportunity to respond to the Cyber Security Expert Advisory Board's (**the Board**) *2023-30 Australian Cyber Security Strategy Discussion Paper* (**Discussion Paper**).

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 covers over 22,000 square kilometres from the Sydney CBD to the Upper Hunter. As the most populous network area and financial capital of Australia, over 20 per cent of Australia's GDP is generated within our network area. This means that a cyber-attack on our network, even for a few hours, would severely disrupt lives and livelihoods. In the worst possible case, the economic impact from a complete shutdown of our infrastructure may be as high as $120 million per hour or over $2.9 billion per day.

We support the Board's ambitions for Australia to become the most cyber secure nation in the world by 2030. To achieve this, we make the following key recommendations:

- Targeted engagement forums with industry sectors on specific issues such as organisational and personal cyber security as different energy subsectors will have differing exposure to risks;
- Implement a risk-based framework for compliance against the national cyber security regulatory obligations;
- Consolidate disparate State-based cyber security regulatory obligations into a single national framework; and
- Include Customer Energy Resources (**CER**), such as solar inverters and batteries as well as remotely operable 'smart' meters, as part of the Department's review.

We have included our response to key questions in the Discussion Paper in **Attachment A**. We welcome the opportunity to discuss any aspect of our submission with you. Please contact Shannon Moffitt, Regulatory Strategy Manager, via [redacted]

Regards,

[redacted]

Rob Amphlett Lewis
Acting CEO

Connecting communities,
empowering lives

Attachment A – Ausgrid response to the discussion paper questions

#	Question	Ausgrid's submission
1	What ideas would you like to see included in the Strategy to make Australia the most cyber secure nation in the world by 2030?	We understand that the *2023-30 Cyber Security Strategy* (**Cyber Strategy**) is intended to be broad in scope covering both personal and organisational cyber security. These areas of cyber security (personal and organisational) can face vastly different challenges. For example, the actions required to protect personal information will differ to the actions employed by organisations, particularly critical infrastructure providers, in combating cyber threats that could have widespread impacts for households, businesses and potentially the safety of the community. To navigate the breath of issues, the Board should consider having targeted engagement forums within sectors of industry as different energy subsectors will have differing exposure to risks. Ausgrid would be pleased to take a leading role in working closely with the Board and the Department of Home Affairs (**the Department**) on the key challenges organisations face. This is particularly important when operating critical infrastructure that provides essential services to the community. We would also welcome further engagement with the Board and the Department about our plans to invest $91 million in strengthening our cyber security protections over a five-year period beginning in FY25. This funding plan is subject to Australian Energy Regulator (**AER**) approval.[1] We support risk-based methods in setting out how critical infrastructure providers and other organisations must comply with regulatory obligations relating to cyber security. This would involve each risk being managed 'so far as is reasonably practicable' (**SFAIRP**) rather than a prescriptive approach that deterministically sets uniform standards. To implement this, regulatory obligations should be implemented so that cyber security risks that are so high that they are deemed 'intolerable' risks are addressed through mandated regulatory framework requirements. For other material risks, the regulatory framework should then establish requirements on organisations to reduce or eliminate these other material risks until the disbenefits (e.g. safety, economic losses) are grossly disproportionate to the benefits. Under this SFAIRP approach, this would mean that if there are practicable mitigations that could be reasonably adopted, then would be a risk management plan put in place implementing the mitigations.

[1] As a regulated monopoly distribution network service provider the AER approves our proposed expenditure for upcoming five-yearly periods. We set out our plans for expenditure across the different needs of our network from cyber security to network replacement to general operating expenditure.

2b	Is further reform to the Security of Critical Infrastructure Act required? Should this extend beyond the existing definitions of 'critical assets' so that customer data and 'systems' are included in this definition?	There is an influx of customer-owned energy devices connecting to electricity networks around Australia. These devices potentially provide millions of entry points for cyber threats to infiltrate electricity networks and disrupt the supply of energy to customers. To keep pace with technology change, the Board and the Department should consider whether customer-owned energy devices, such as solar inverters and batteries as well as remotely operable 'smart' meters, should form part of the Cyber Strategy and any resulting regulatory changes.
2e	How should Government seek to monitor the regulatory burden on businesses as a result of legal obligations to cyber security, and are there opportunities to streamline existing regulatory frameworks?	The current level of regulatory burden could be streamlined by removing duplication at the state and federal levels. To do this, we recommend that the Board and the Department explore ways to consolidate disparate State-based cyber security regulatory obligations into a single national framework.
5	How should Australia better contribute to international standards-setting processes in relation to cyber security, and shape laws, norms and standards that uphold responsible state behaviour in cyber space?	The adoption of international standards, relevant to the specific industry sector, will assist in driving greater consistency in supplier and technology controls. This could be progressed through establishing industry working groups to determine and promote adopting relevant standards. Where possible, these standards should be pursued in line with the Department's ambition for Australia to become an international leader in cyber security protections.
16	What opportunities are available for government to enhance Australia's cyber security technologies ecosystem and support the uptake of cyber security services and technologies in Australia?	We support a certification process (or partnership with overseas based agencies) that assists in validating the integrity of information or operational security devices/appliances. For example, knowing that a particular level of certification from an international agency is valid for Australian use would be helpful to add controls to critical systems without need for duplicative and potentially less robust testing locally.
18	Are there opportunities for government to better use procurement as a lever to support and encourage the Australian cyber security ecosystem and ensure that there is a viable path to market for Australian cyber security firms?	The Board should explore a government endorsed device/appliance list. It would help accelerate procurement processes for organisations by providing an independent source for verifying the suitability of devices and appliances. The procurement of approved items would, in turn, strengthen the Australian cyber security ecosystem over time, through investment in devices and appliances that have been independently verified and proven robust.