AUSTRALIAN ENERGY
REGULATOR

Level 17, Casselden
2 Lonsdale Street
Melbourne Vic 3000

GPO Box 520
Melbourne Vic 3001

tel: (03) 9290 1800

www.aer.gov.au

Our Ref: #12,659,421
Your Ref: Strengthening Australia's cyber security regulations and incentives
Contact Officer: Mark Feather
Contact Phone: [redacted]

27 August 2021

Cyber, Digital and Technology Policy Division
Department of Home Affairs
6 Chan Street
BELCONNEN ACT 2617

Dear Department of Home Affairs

## Re: Strengthening Australia's cyber security regulations and incentives: a call for views

The Australian Energy Regulator (AER) supports these efforts to uplift Australia's cyber security incentives. We also recognise the extensive consultation efforts across a broad range of stakeholders and the diverse views and perspectives on these initiatives.

There are important links between cyber security and energy. The AER is interested in understanding the impacts to consumers, regulated businesses and the broader energy sector. In particular, the standards (Chapter 6) and labelling (Chapter 7) for smart devices are of particular relevance to the AER as smart devices include distributed energy resources (DER).

Cyber security will become increasingly relevant in an energy context with anticipated increases in DER penetration including rooftop solar, electric vehicles, smart appliances and batteries. The future will see more consumer devices and DER connected to the broader energy system with a portion of DER participating in electricity wholesale markets (via exports and imports on the grid) through their retailers and aggregators.

### *Standards and labelling for smart devices*

The proposed standards and labelling for smart devices are an important first step to address potential risks from growing interconnectedness between devices, households, service providers, networks and energy markets. There are also important links to other work already underway within the energy sector on cyber security including standards for DER interoperability.

As the discussion paper has identified, consumers bear negative externalities and have to contend with information asymmetries. With more DER and consumer devices forming part of the interconnected cyber security picture in the future, it will be increasingly vital to educate and involve consumers who will be a critical part of the solution. A secure by design approach is more likely to become prevalent if consumers understand and attribute value to cyber security.

We support labelling to help consumers assess the security and value of smart devices. Though we note that there will be a range of issues for further consideration:

- Potential for a proportional or tiered approach noting the wide variety of devices with varying complexity, life cycles and values
- Whether the label will include associated software and applications
- Whether a live and updated label will help keep pace with rapidly changing technology
- Labelling will need to be tested with consumers to ensure effectiveness and usefulness (the Department's testing work underway with the Behavioural Economics Team of the Australian Government will be informative)
- Labelling should be accompanied by consumer engagement and education
- Compliance to ensure consistent labelling and transparency

The AER also supports standards for smart devices as an effective way to achieve a baseline level of security uplift for all consumers regardless of whether they are able make cyber secure choices or engage with labels. There would be a range of implementation issues requiring further consideration:

- Whether there are opportunities for cooperation and alignment with international standards and practice as a way to mitigate the risk of unintentionally creating a barrier to innovation or products being available to the Australian market
- How will these standards interact with other existing work and standards that touch on cyber security?
- How will compliance be tested and monitored?

Standards and labelling will be important tools within the cyber security toolkit. These regulatory responses should be supported by a resourced regulator with cyber security expertise and a clear remit to uplift cyber security.

### *Cyber security standards for energy infrastructure owners*

The AER also notes that separate work is being led by the Department of Home Affairs through the proposed amendments to the *Security of Critical Infrastructure Act 2018* to introduce mandatory requirements on critical infrastructure businesses including cyber security. The AER has made separate submissions into this process. The AER is supportive of uplifting these requirements, however would reiterate that it is important that the cumulative costs to consumers are carefully considered. The AER would also note that energy network businesses are subject to economic regulation frameworks administered by the AER, which ensure that only the efficient costs of meeting regulatory obligations are passed through to consumers.

We look forward to seeing these cyber security initiatives develop and continue to provide input to measures affecting the energy sector. If you require further information, please do not hesitate to contact me at [redacted] or on [redacted].

Yours sincerely

[redacted]

Mark Feather
General Manager, Strategic Policy and Energy Systems Innovation
Australian Energy Regulator

Sent by online form on: 27.08.2021