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: #11716287
Your Ref: Exposure Draft of the Security Legislation Amendment (Critical Infrastructure) Bill 2020
Contact Officer: Mark Feather
Contact Phone: 03 9290 6958

Mr Michael Pezzullo
Secretary
Department of Home Affairs
6 Chan Street
BELCONNEN ACT 2617

27 November 2020

Dear Mr Pezzullo

Re: Exposure Draft of the Security Legislation Amendment (Critical Infrastructure) Bill 2020

The Australian Energy Regulator (AER) welcomes the opportunity to comment on the exposure draft of the Security Legislation Amendment (Critical Infrastructure) Bill 2020, and more broadly the engagement undertaken by the Department of Home Affairs' (DHA) on the critical infrastructure reforms.

We recognise the importance of uplifting the security and resilience of critical infrastructure and the ongoing work underway in this space.

We remain particularly interested in understanding the impacts to consumers, regulated businesses and the broader energy sector and will continue to engage in the co-design of sector specific obligations and best practice guidance for energy businesses.

In this submission, we highlight the importance of ensuring that the growth of Distributed Energy Resources (DER) take up is taken into account in the design of the critical infrastructure framework specifically with respect to cyber security. We note these were also flagged by other stakeholders in their submissions to the consultation paper.

We also reiterate some of the key points from our previous submission to the consultation paper that we note were common themes in the other energy stakeholder submissions:

- Proportionality and cost implications for consumers
- Benefits of a coordinated regulatory approach and central regulator
- Implementation considerations – timing and maturity

Distributed energy resources and cyber security risks

Various submissions noted that evolving technologies present security challenges for the energy sector that should be considered when developing sector-specific rules.

We consider that the significant take up of DER by households and businesses in Australia represents a critical risk factor for the energy system in relation to cyber security.

Solar PV installations with smart inverters are the norm for DER today. There are over 2 million solar PV installations in Australian homes with a generation capacity of over 10GW. This compares to 2.9GW for Eraring Power Station (the largest single station in the national electricity market).

The growth in DER is expected to continue significantly particularly as battery technology also becomes cheaper. By 2030, AEMO expects approximately 50% of consumers in the National Electricity Market to use some form of DER (solar PV, controllable load, storage, electric vehicles or combination).[1] The 2020 AEMO Integrated System Plan projects investment in a further 10,926 MW of distributed solar generation by 2040 in the central case and double that for the high DER case.[2] AEMO modelling projects that DER could provide 13% to 22% of total underlying annual energy consumption by 2040.[3]

Solar PV inverters have the ability to support both voltage and frequency in the grid. These modes actively inject power into the grid and may also cause unknown problems, especially if the inverter is compromised. Most of the cyber security research focuses on large scale power plants that are connected at transmission level. However, there is a growing body of work that has identified a material risk from compromised inverters.

Specifically, many of these inverters may not carry updated firmware, and manufacturers' cyber protections can vary considerably. Were a malicious actor to gain control of even a small proportion of inverters, they could create a cascading set of events with the potential of a state-wide or even nation-wide system black. The malicious actor could even create problems for the restart of the grid, as the restoration process is very susceptible to uncontrolled load or generation swings.

While there are many different inverter providers, the market share of certain providers would make them ideal targets for malicious actors.

Similarly, energy market retailers and aggregators and other technology providers will increasingly deliver products and services that enable them to remotely control consumer electricity usage, including, for example, through phone based applications to remotely control appliances. If these systems or technology providers were compromised this could also have broader impacts on the operation of the electricity system and may also lead to disruptions.

In commenting on the exposure draft, it is not clear the extent to which DER assets are covered within the proposed definitions, for example, the definitions of "*energy sector*", or the definition of a "*critical electricity asset*". In reviewing the exposure draft, the focus relates to production, distribution and supply of electricity, with the responsible entity for a *critical*

---

[1] *Post 2025 Market Design, Consultation Paper*, Energy Security Board, September 2020
[2] *Integrated System Plan,* AEMO, July 2020,
[3] *Integrated System Plan*, AEMO, July 2020

electricity asset being the holder of a licence, approval or authorisation to "operate the asset to provide the service to be delivered by the asset".

These definitions and their operation appear supply side focussed and we query whether they are sufficiently scoped to take account of increasing levels of DER, demand side response and two way flows of electricity. For example, does the drafting sufficiently take account of demand management services whereby customers agree with an aggregator to turn down their usage of electricity through the use of smart appliances or the remote management of solar PV and batteries. Similarly, it will be important for DHA to determine the extent to which the obligations should be able to cover inverter manufacturers. Whilst the energy sector has been historically characterised by large scale grid sized supply infrastructure, this is increasingly changing with the uptake of more localised DER assets. As such, consideration will need to be given to how these assets are covered under the legislation or framework.

We recommend that in the next phase of co-design, DHA also consider the following issues relating to DER uptake:

- facilitating active monitoring of the supply chain for inverters to safeguard against the tampering of these devices
- coordination between the Commonwealth, jurisdictions and private sector to integrate holistic compliance requirement standards
- government investment and promotion of cybersecurity best practices
- installation of intrusion detection systems
- passive random inspection (of actor command and control); and
- random inspections of imported inverter shipments aimed at identifying any modification not included in the circuit's original design.

We also note that there is ongoing work underway through the Australian Energy Market Commission[4] (AEMC) and existing energy sector working groups which the next co-design phase could leverage.

Besides DER issues, consideration should also be given on how definitions could be updated in the future to keep pace of technology changes. For example, the current definition of "gas"[5] does not include hydrogen or biomethane, which could become more widespread and critical in the future.

Proportionality and cost implications for consumers

We support the DHA's intent to 'develop proportionate requirements that strike a balance between uplifting security, and ensuring businesses remain viable and services remain sustainable, accessible and affordable.'[6]

We also reiterate the importance of proportionality in relation to the costs that will potentially be faced by consumers associated with the new security arrangements, and note that these issues have been raised by numerous energy stakeholders' submissions and in our previous submission.

---

[4] AEMC standards, interoperability and cyber-security working group

[5] Security Legislation Amendment (Critical Infrastructure) Bill 2020, p16

[6] Protecting Critical Infrastructure and Systems of National Significance Consultation Paper, p5.

It is important to not lose sight of the cost implications for consumers. It will be useful to hear consumer views in the next consultation phase to find a balance between security and keeping energy affordable.

We also note that the thresholds governing the application of new obligations are to be considered in the co-design phase and that a reduction in the generation threshold is likely.[7] This will have additional cost implications for new and smaller generators in meeting the new obligations, which in turn is likely to have a flow on effect to consumers.

Benefits of a coordinated regulatory approach and central regulator

A common theme raised by numerous energy stakeholders and in our previous submission was the importance of minimising duplication. We continue to consider that a central regulator across multiple sectors will improve regulatory consistency and outcomes. Specifically, we consider that a central regulator should:

- Minimise duplication and deliver efficiencies relative to a multiple regulator approach
- Facilitate and build expertise and experience
- Deliver consistent regulatory approaches providing certainty to industry stakeholders
- Have a deeper understanding of threats and interdependencies across the sectors
- Deliver efficiencies in reporting and engagement for entities
- Provide broader engagement with consumers

We note that the decisions of the central regulator will need to be taken into account in relation to regulatory determinations issued by the AER for network businesses. We are well placed to advise on what the consequences of alternative standards might be on the prices that consumers pay and we would be willing to assist the central regulator to understand these issues.

Implementation considerations – timing and maturity

We note that through our network regulation processes, we have observed that electricity and gas network businesses have varying levels of security spending. While the energy sector is relatively mature compared to some other sectors, each business will have a different starting point to meeting new obligations.

In the co-design phase, consideration should be given to:

- what the energy sector obligations should involve and how existing frameworks could be leveraged,
- which entities are subject to which obligations,
- how the cyber regulator might have regard to costs in implementing new obligations, and
- whether all obligations take effect from mid-2021 or will they be phased through a transition period.

These considerations will impact on existing AER network regulatory determinations and further work will be needed during the sector design phase to understand the specific

[7] Security Legislation Amendment (Critical Infrastructure) Bill 2020: Explanatory Document, p35.

impacts.[8] There will be a need to consult extensively with industry on sector design and also, as noted above, ongoing consumer engagement so they understand the drivers for increased costs.

For further information on our submission, please do not hesitate to contact myself or Mark Feather, General Manager – Policy and Performance on (03) 9290 6958.

Yours sincerely

Jim Cox
Deputy Chair
Australian Energy Regulator

Sent by web form on: 27.11.2020

[8] Calendar of AER regulatory determinations including regulatory control period and key milestones online: https://www.aer.gov.au/system/files/AER%2010%20year%20regulatory%20determination%20calendar%202018-2027%20%28updated%20December%202019%29.pdf