AUSTRALIAN ENERGY COUNCIL

Critical Infrastructure Centre
Cyber, Digital and Technology Policy Division
Department of Home Affairs
4 National Circuit
BARTON ACT 2600

17th September 2020

Submitted online to:
https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/protecting-critical-infrastructure-systems

Dear Sir/Madam,

Protecting Critical Infrastructure and Systems of National Significance

The Australian Energy Council (the "**Energy Council**") welcomes the opportunity to make a submission in response to the Critical Infrastructure Centre's *Protecting Critical Infrastructure and Systems of National Significance Consultation Paper*.

The Energy Council is the industry body representing 22 electricity and downstream natural gas businesses operating in the competitive wholesale and retail energy markets. These businesses collectively generate the overwhelming majority of electricity in Australia, sell gas and electricity to over ten million homes and businesses, and are major investors in renewable energy generation.

Introduction

The *Security of Critical Infrastructure Act 2018* sets out a framework for managing risks to national security relating to critical infrastructure. Critical electricity assets are defined in the regulations according to the following table.[1]

Minimum installed capacity of a synchronous electricity generator		
Item	**State or Territory**	**Amount (in megawatts)**
1	New South Wales	1,400
2	Victoria	1,200
3	Queensland	1,300
4	Western Australia	600
5	South Australia	600
6	Tasmania	700
7	Northern Territory	300

In addition, generators contracted to provide system restart ancillary services are also included as critical electricity assets.[2]

Critical gas assets are defined in the Act according to their maximum daily quantities.

[1] *Security of Critical Infrastructure Rules 2018*, Section 6(1)(b)
[2] *Security of Critical Infrastructure Rules 2018*, Section 6(1)(a)

Level 14, 50 Market Street
Melbourne 3000
GPO Box 1823 Melbourne Victoria 3001

P +61 3 9205 3100
E info@energycouncil.com.au
W energycouncil.com.au

ABN 92 608 495 307

The Consultation Paper proposes to enhance the critical infrastructure framework by imposing:

- a Positive Security Obligation;
- enhanced cyber security obligations; and
- Government assistance for entities the target of a cyber attack.

The Energy Council is supportive of the Government's efforts to counter this growing threat, and assist industry should it be the victim of an attack. In addition, industry supports the Australian Energy Market Operator ("**AEMO**") continuing to develop its Australian Energy Sector Cyber Security Framework.[3] This should form the basis of any industry-specific regulations, noting that the *National Electricity Rules* (and in Western Australia the *Wholesale Electricity Market Rules*) already include obligations for managing the risks associated with the secure operation of the power system.

The paper seeks to broaden the electricity and gas infrastructure which will be subject to the Act and its associated regulations, by defining "critical infrastructure entities", "regulated critical infrastructure entities" and "systems of national significance".

This expansion of definitions needs to be balanced against the additional compliance burdens to be placed on entities, and the risks associated with expanding the generators captured by the new obligations to those which have immaterial effects on the power system.

It will also be important for implementation of the framework to occur in a reasonable timeframe. The energy industry is currently undergoing significant system changes (for example the Five Minute Settlement Implementation Programme) and any additional obligations and system changes need to be achievable within the foreshadowed implementation period. To this end the Sector-specific Co-design Period will be critical for establishing industry engagement and developing the necessary plans and budgets.

Critical Infrastructure Assets

The workshop proposed that "critical infrastructure assets" be defined as "entities involved in the production, transmission, distribution and sale of gas, electricity and liquid fuels".

This is an enormously broad definition. As distributed energy resources become widespread, unless a sensible threshold accompanies the definition, there is a likelihood that very small businesses, for example those exporting excess solar power back to the power system, will be captured by the definition. Not only are such generators individually immaterial to the operation of the power system, but the regulatory and administrative burden of including them will be significant.

Regulated Critical Infrastructure Assets

The workshop suggested that 30MW generators in the NEM (10MW in other power systems) should be regulated critical infrastructure assets.

While 30MW is the threshold below which the AEMO will automatically grant a generator registration exemption,[4] this is for unit dispatch and pricing purposes, and is not pertinent to whether a cyber attack on the generator would have widespread grid impacts. Interference to the operation of units of 30MW in size is unlikely to have significant effects on the stability and security of the power system. Instead the Energy Council suggests that the threshold should be measured across a power station rather than a unit, and a consequentially much larger threshold would be more suitable for the proposed framework. The Energy Council suggests that the appropriate threshold should be developed in consultation with industry and AEMO, to determine the size of power station which will have power system effects should it be targeted by a cyber attack. For example this could be set as

[3] Available at https://aemo.com.au/initiatives/major-programs/cyber-security/aescsf-framework-and-resources
[4] unless the market participant intends registering a battery, in which case the threshold is 5MW

Level 14, 50 Market Street
Melbourne 3000
GPO Box 1823 Melbourne Victoria 3001

Phone +61 3 9205 3100
Email info@energycouncil.com.au
Website www.energycouncil.com.au

ABN 92 608 495 307

the largest single contingency expected to affect power system security. (Note that different jurisdictions may need different thresholds, due to the differences in their supply-demand balances and interconnections with other states.)

In addition, while the 30MW threshold is inappropriately low, there is also the issue of the generator characteristics. For example, there are a number of variable renewable energy generators which exceed the 30MW threshold. Therefore generator technology may also be a relevant factor to consider in the framework, as intermittent generators are less critical to reliability. For those units, the threshold could be higher again.

Furthermore, the generation mix in the power system will change over time, therefore the thresholds may need reviewing in a number of years' time. The Energy Council therefore suggests that the framework include provision for a regular review, and consideration of aggregation across a portfolio or technology class. For example, if a particular type of generator was installed widely, and its control system became susceptible to cyber attack, classification as a critical infrastructure asset may be necessary.

Incident Reporting

One issue which hasn't been addressed by the consultation paper is the definition of a "cyber incident". It is proposed that assets affected by cyber incidents will have an obligation to report same, but there needs to be detail and a materiality test made clear, to ensure that trivial matters such as phishing e-mails do not trigger an onerous reporting obligation.

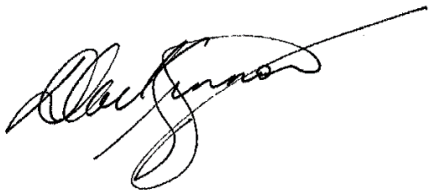
An appropriate regulator

While the energy industry operates under a myriad of different laws, rules and regulations, primary supervision in the National Electricity Market is the responsibility of the Australian Energy Regulator ("**AER**"), which is a subsidiary of the Australian Competition & Consumer Commission. In Western Australia it is the responsibility of the Economic Regulation Authority ("**ERA**").

The Energy Council suggests the AER and the ERA are the appropriate bodies to oversee the energy industry's obligations under the critical infrastructure framework, but drawing on specialist advice from the Australian Cyber Security Centre.

Any questions about this submission should be addressed to the writer, by e-mail to Duncan.MacKinnon@energycouncil.com.au.

Yours faithfully,



Duncan MacKinnon
Wholesale Policy Manager
Australian Energy Council

Level 14, 50 Market Street
Melbourne 3000
GPO Box 1823 Melbourne Victoria 3001

Phone +61 3 9205 3100
Email info@energycouncil.com.au
Website www.energycouncil.com.au

ABN 92 608 495 307