AUSTRALIAN ENERGY COUNCIL

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

Submitted via email: ci.reforms@homeaffairs.gov.au.

14 May 2021

Critical Infrastructure Asset Definition Rules

The Australian Energy Council ('AEC') welcomes the opportunity to make a submission to the Department of Home Affairs' consultation on the Critical Infrastructure Asset Definition Rules ('Definition Rules').

The Energy Council is the industry body representing 21 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.

The AEC supports the intent of the legislation to bolster the resilience of Australia's critical infrastructure to external threats. Our members recognise that the reliable provision of energy is essential to the social and economic wellbeing of Australia and have existing, and sophisticated, security and IT systems in place already to ensure this. Furthermore, AEMO has developed its own Australian Energy Sector Cyber Security Framework to foster industry collaboration in managing cyber risks. It is important the Department acknowledges the sophistication of these existing systems when developing its Risk Management Program for generators. This Program should be seen as supplementary to, rather than the foundation of, how energy generators minimise their risk exposure to cyber-attacks.

The AEC makes the general observation that the most critical part of the power system with respect to external threats is the grid itself, which internationally has been the main target for malicious attacks.[1] In that regard, the AEC supports the focus to date on ensuring that electricity networks and AEMO develop robust and secure systems.

Generation is inherently less vulnerable because it is distributed across relatively small individual contributions and carries substantial redundancy across the fleet. To disrupt the community, a malicious actor would need to simultaneously attack many generators, each employing different informational technologies. Even if successful, the impact would, at worst, result in a period of rolling load-shedding rather than a widespread blackout as might occur with a network attack.

Noting the above, the AEC understands the Department's reasoning for lowering the threshold for what constitutes critical infrastructure in the energy sector to recognise both the move towards a

[1] See, for example: Chris Vallance, 'Ukraine cyber-attacks could happen to UK', BBC News, 29 February 2016, https://www.bbc.com/news/technology-35686493.

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

more distributed energy system and the emergence of new threats to Australia's sovereignty. Any new threshold should be cognisant of the regulatory burden the proposed obligations place on generators and should not capture generators that have an immaterial influence on the reliability and security of the power system.

Setting a Proportionate Threshold

The threshold proposed in the Definition Rules is 30MW. While there is no explanation for why 30MW has been selected, it appears to reflect the scheduling and semi-scheduling threshold that AEMO uses when classifying generators in the National Electricity Market ('NEM'), although not in the Western Australian Wholesale Electricity Market ('WEM'). This is an unusual benchmark to follow because this threshold exists for market dispatch and pricing purposes; it is not a directly relevant consideration to system security. The AEC remains concerned that this unrelated threshold has been chosen for expedience only and will impose an unnecessary regulatory burden on smaller generators for which the compliance cost will far exceed any security benefit.

Noting the sentiment expressed by the Department in the Explanatory Document that it 'will work with industry participants to identify appropriate thresholds…',[2] the AEC has considered alternatives that can deliver the same outcomes to system security without imposing an unnecessary regulatory burden on generators. One viable alternative solution is to align with the approach AEMO has taken to provide mandatory primary frequency response ('PFR'). PFR is a technical, but essential, service that generators provide to 'support the secure operation of the power system'.[3] This provision of system security is analogous to the intent of the Critical Infrastructure Bill and therefore arguably a more appropriate model to replicate.

AEMO determined that the most optimal way to implement PFR, and ensure system security, is through a three-stage tranche approach:

- Tranche 1 covers generation with a nameplate capacity above 200MW.
- Tranche 2 covers generation with a nameplate capacity between 80MW and 200MW.
- Tranche 3 covers generation with a nameplate capacity below 80MW.

AEMO's three tranches are progressively introduced over time with intersecting periods for learning and reporting. By taking such an approach, the first tranche provides immediate "bang for buck" but also an opportunity to monitor progress and identify issues that can be resolved before involving more numerous, but smaller parties with less of an ability to absorb costs.

This learning opportunity will serve to identify the true costs of compliance and what facets of the Risk Management Program are a) most important to system security and b) most costly to implement. This knowledge can then be used to inform the focus of the requirements placed on the smaller tranches. Rather than locking in 30MW at this time, it would be more appropriate to set a higher

[2] Department of Home Affairs, 'Security Legislation Amendment (Critical Infrastructure) Bill 2020 Explanatory Document', November 2020, p35, https://www.homeaffairs.gov.au/reports-and-pubs/files/exposure-draft-bill/exposure-draft-security-legislation-amendment-critical-infrastructure-bill-2020-explanatory-document.pdf.

[3] AEMO, 'Primary Frequency Response', 6 May 2021, https://aemo.com.au/en/initiatives/major-programs/primary-frequency-response.

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

threshold for the first tranche, such as 200MW, with an intent to lower this threshold following the first learning period.

Taking practical steps like this to minimise compliance costs is especially important in light of the concern raised from the Australian Energy Regulator in its previous submissions that the rule change, as proposed, may have undesirable cost implications for customers.[4] Likewise, the Department has stated that it wants 'proportionate requirements' that 'strike a balance' between security and affordability.[5] A tranche approach better achieves these objectives.

The Department should also make it clear in its Definition Rules that:

- The Bill only applies to operational assets. An asset is operational once it is connected and fully registered by AEMO.
- The threshold is measured by generation unit and is not cumulative.

Scope of the Bill

The rationale in the Definition Rules states 'the intent of lowering the threshold to 30MW nationally is … to drive a broad uplift in sector resilience given the interconnected nature of the electricity network'.[6]

Two issues emerge with respect to this statement:

- The imposition of an increased compliance regime should be in response to clear evidence of shortcomings in existing resilience, and the new provisions should directly target those shortcomings. A justification of "broad uplift" does not provide industry with confidence that this has occurred, instead suggesting the exercise is being conducted purely to demonstrate action.
- The rationale does not specify clearly what form of resilience it seeks to achieve. Resilience is a broad term and one that is common in the energy sector to refer to a range of natural events, most commonly extreme weather. To avoid ambiguity, the AEC recommends the rationale be revised to: '…bolster sector resilience against malicious action given the interconnected nature of the electricity network'.

Monitoring Compliance

If the Department opts to persist with a 30MW threshold, it is important that the regulator takes a collaborative approach to monitoring compliance. This should include clearly defined transitional arrangements, the process for generators with units above 30MW but identify as non-critical and want to develop a modified Risk Management Program, and a no-fault feedback loop between

[4] Australian Energy Regulator, 'Submission to Exposure Draft of the Security Legislation Amendment (Critical Infrastructure) Bill 2020', 27 November 2020, p3-4, https://www.homeaffairs.gov.au/reports-and-pubs/files/critical-infrastructure-consultation-submissions/EDS078-CISoNS-AustralianEnergyRegulator.PDF.

[5] Department of Home Affairs, 'Protecting Critical Infrastructure and Systems of National Significance Consultation Paper', August 2020, p5, https://www.homeaffairs.gov.au/reports-and-pubs/files/protecting-critical-infrastructure-systems-consultation-paper.pdf.

[6] Department of Home Affairs, 'Protecting Critical Infrastructure and Systems of National Significance Draft Critical Infrastructure Asset Definition Rules', April 2021, p8, https://www.homeaffairs.gov.au/reports-and-pubs/files/critical-infrastructure-asset-definition-rules-paper.pdf.

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

regulators and generators to encourage confidential, upfront reporting of gaps or errors in a generator's security protocols.

The AEC reiterates its view that the Australian Energy Regulator and Western Australia's Economic Regulation Authority are the appropriate regulatory bodies to oversee these obligations, with support from the Australian Cyber Security Centre.

Any questions about this submission should be addressed to Rhys Thomas, by email to Rhys.Thomas@energycouncil.com.au or by telephone on (03) 9205 3111.

Yours sincerely,

Ben Skinner
GM Policy
Australian Energy Council

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