22 December 2025

Department of Home Affairs
PO Box 25
BELCONNEN ACT 2616

Online submission

Dear Dr Slay,

Independent Review of Security of Critical Infrastructure Act 2018

AEMO welcomes the opportunity to provide input into the independent review of the *Security of Critical Infrastructure Act 2018* (SOCI Act) and the rules made under the SOCI Act (SOCI Rules). AEMO strongly supports the objectives of the SOCI Act as a cornerstone for safeguarding Australia's essential services.

The SOCI Act plays a vital role in strengthening resilience against evolving threats, in the energy sector and sectors on which energy is dependent, such as communications, data storage and processing. Government and industry alike are aware that this legislative framework will have to evolve to respond to the changing threat environment, as is demonstrated by current consultation on enhancements to the Critical Infrastructure Risk Management Program (CIRMP) Rules.

Recognising that amendments to the SOCI Act in 2021 and 2022 have uplifted the security posture of critical infrastructure entities, AEMO considers that the intended objectives of the SOCI Act could be better achieved. In considering whether the legislative framework is functioning as intended, the review should consider potential enhancements to both the scope / scale of the sectors captured and the obligations that apply to these sectors. AEMO provides some high-level comments in relation to the energy sector only for consideration.

Application of SOCI Act

AEMO strongly recommends a review of the critical electricity assets definition to ensure it remains fit-for-purpose through the energy transition. This definition needs to accommodate a more diversified electricity system, comprising of more renewable energy generators, that are firmed by storage and backed up by gas-fired generation.

AEMO recommends that the review considers the explicit inclusion of large grid-scale storage (or batteries) within the scope of the SOCI Act (including via the applicable Rules). Storage is an important contributor to maintaining both a reliable and secure electricity system. Batteries can offer energy services to meet reliability requirements and essential system services to ensure a secure operating system. AEMO and industry are collaborating to validate battery capabilities to provide system services, noting system services range across system strength, inertia, system restart and voltage control. This is highlighted for instance in South Australia where at least six major grid-scale batteries are operational with a combined capacity exceeding 793 megawatts and over 1,181 megawatt hours of storage, delivering critical reliability and security services. The terms used in the SOCI Act and SOCI Rules, that is *electricity generation station* and *electricity generator* are not defined, while similar terminology with specific meanings are provided for under the National Electricity Rules (applied to the National Electricity Market (NEM)) on the east coast) and the

Electricity Market and System Rules (applied to Western Australia's South West Interconnected System (SWIS)). As such AEMO considers the legislative framework could benefit from this clarification.

The energy transition is well underway with businesses and households investing heavily in Consumer Energy Resources (CER) particularly rooftop solar photovoltaic (solar PV) cells, but increasingly electric vehicles (EV) and small-scale batteries, albeit from a much lower basis. Today some 25 gigawatts (GW) of solar PV are connected in the NEM regions[1] meeting 12% of the NEM's energy needs[2] while Western Australia's SWIS hosts close to 3GWs of solar PV. AEMO's draft 2026 Integrated System Plan (ISP) assumes that CER continues to form an important part of the generation mix, with CER forecast to reach over a third of the NEM's installed generation capacity by 2050[3]. In WA the take-up of solar PV is expected to continue to 6.5GWs of capacity by 2033-34[4].

The take-up of CER that can be orchestrated means that aggregated CER is rapidly reaching critical infrastructure status. Aggregated CER through Virtual Power Plants (VPP) is expected to become Australia's largest power plants, while VPP operators, referred to as aggregators, will effectively become critical infrastructure responsible entities (via their ability to coordinate CER en masse). Other jurisdictions are progressing reforms to recognise and better manage the security risks posed by CER. For example, in the UK where the critical infrastructure security framework is primarily governed by the Network and Information Systems (NIS) Regulations 2018, the Government is seeking to strengthen this framework through the Cyber Security and Resilience Bill by expanding the scope to include data centres and large load controllers (≥300 MW control capability threshold)[5]. This reflects a broader effort to bring consumer-led flexibility into the regulatory framework, ensuring that aggregated control of CER and distributed assets does not introduce system-wide cyber risks. AEMO strongly encourages this review consider the role of and risks presented by aggregated CER to the energy sector and broader economy and consult on how best to mitigate these.

Requirements of the SOCI Act

AEMO has consistently supported a calibrated, criticality-based and sector specific approach to protecting critical infrastructure wherever possible. Recent SOCI reforms have focussed on establishing a broad baseline and general uplift across all critical infrastructure sectors, cognisant of the dependencies between sectors. However, AEMO considers that more nuanced requirements are needed for the energy sector going forward.

Ideally the Australian Energy Sector Cyber Security Framework (AESCSF), which is AEMO's preferred energy sector-specific cyber maturity model and selected by most responsible energy entities, would be mandated. The AESCSF is a self-assessment tool developed by AEMO[6] to allow energy entities to measure and improve their cyber-security maturity against industry best practices and regulatory expectations. Mandating the AESCSF would ensure a specific and contemporary 'standard' be applied consistently, improve benchmark reporting and identifying gaps. AEMO has also advocated for energy sector entities having to meet criticality-based security profiles under the AESCSF and notes that the Department of Home Affairs consultation paper on enhancing the CIRMP rules proposes that responsible energy sector entities comply with maturity Level 2. This consultation process will likely canvass some of AEMO's concerns that relate to remote access and control of critical energy assets.

[1] draft-2026-integrated-system-plan.pdf, p85
[2] Supporting secure operation with high levels of distributed resources Q4 2024, p15
[3] draft-2026-integrated-system-plan.pdf, p84
[4] wem-esoo-infographic-2024-v05
[5] Cyber Security and Resilience Bill - GOV.UK
[6] AEMO | AESCSF framework and resources

Enforcement, Flexibility and Complementary Frameworks and Proportionality

AEMO recognises the significant progress through SOCI reforms to better protect Australia's critical infrastructure in recent years. Having established a broad baseline across sectors and allowed sufficient time for responsible entities to embed requirements, AEMO recommends this review considers stronger oversight and enforcement.

As foreshadowed, the Government requires the ability to amend the SOCI legislative framework in response to a changing threat environment. The existing legislative architecture provides flexibility in that the Minister can make rules relating to definitions under the SOCI Act (including critical energy assets) which determines requirements and the application of the CIRMP obligations. AEMO considers that the existing architecture generally strikes the right balance between the primary legislation and the legislative instrument to provide sufficient flexibility. One improvement could be to include a more enduring reference to the AESCSF framework in clause 30ANA of the SOCI Act, noting that AEMO released version 2 in 2021-22.

For the energy sector the SOCI framework is complemented by and interacts with other legislation, guidance and policy work, including the previously mentioned AESCSF, Australian Signals Directorate guidance referred to as CI Fortify[7], the National Electricity Rules and the Cyber Security Act. Moreover, the Minister for Climate Change & Energy recently submitted a rule change request to the AEMC to establish gas cyber security roles and responsible for AEMO under the National Gas Rules[8]. AEMO emphasises the importance that this suite of legislation, guidance and policy development is coherent, harmonised and reinforces effective risk management practices.

Finally, proportionality is it is important feature of any effective legislative framework. AEMO understands that the SOCI Act compliance costs are significant and ongoing and that these costs are ultimately met by consumers. AEMO is conscious that cost of living concerns are enduring and that benefits of effective risk management need to be balanced against the costs.

AEMO remains committed to working with the Government and stakeholders to ensure the SOCI framework continues to protect Australia's energy infrastructure while enabling innovation and operational efficiency. Should you wish to discuss this submission further, please do not hesitate to contact [redacted], [redacted] on [redacted].

Yours sincerely,

[redacted]

[redacted]

[redacted]

[redacted]

[7] CI Fortify | Cyber.gov.au

[8] Gas cyber security roles and responsibilities for AEMO | AEMC