Friday, 13 February 2026

Submission: Consultation on enhancements to the Critical Infrastructure Risk Management Program (CIRMP) Rules

Department of Home Affairs

To Whom it May Concern

The Clean Energy Council (CEC) is the peak body for the clean energy industry in Australia, representing nearly 1,000 leading businesses across renewable energy, energy storage, and renewable hydrogen. We are committed to accelerating Australia's transition to a clean energy future as rapidly as possible while maintaining a secure and reliable electricity supply for customers.

The CEC welcomes the opportunity to provide feedback to the Department of Home Affairs about the enhancements to the Critical Infrastructure Risk Management Program (CIRMP) Rules. This submission reflects feedback received from our members, as well as independent analysis. It reflects practical implementation constraints, proportionality concerns, budget timing impacts and asset-specific challenges across cyber, personnel and physical security domains.

The CEC supports targeted enhancements to the CIRMP Rules where they are proportionate, risk-based, and demonstrably effective in reducing material security risks. However, several proposed amendments—particularly those relating to foreign ownership, control and influence, supply chain obligations, personnel security requirements and cyber maturity uplift—risk imposing significant cost, delay and operational burden on the energy sector without a commensurate improvement in national security outcomes.

The clean energy sector operates within global supply chains characterised by limited OEM diversity, high capital intensity, and time-critical delivery pathways. Without appropriate flexibility, clarification and proportionality, aspects of the proposed amendments risk unintentionally constraining investment and delaying delivery of critical generation capacity required for Australia's energy transition.

The CEC's submission provides detailed, constructive feedback and proposes refinements to ensure the CIRMP framework remains fit-for-purpose, aligned with the AFAIRP principle, and capable of supporting both national security and energy system reliability objectives.

We welcome ongoing engagement with the Department as these proposals are refined.

1) Overarching Position – Proportionality & Transition Risk

Members acknowledge risks across all hazard areas. However, regulatory settings must balance national security objectives with other national interests, including maintaining momentum in the energy transition and avoiding avoidable cost impacts to consumers.

The proposed rule changes collectively introduce significant upfront investment within a short timeframe (18 months). For many asset operators, implementation would fall largely within a single financial year, creating budgetary, procurement and workforce constraints.

Without refinement, industry-wide cost increases are likely to flow through to electricity pricing.

Members also seek clearer definitions of:

- Critical Components
- Critical Workers

Phone: +61 3 9929 4100
Fax: +61 3 9929 4101
info@cleanenergycouncil.org.au

Level 20, 180 Lonsdale
Street, Melbourne, VIC
3000, Australia

cleanenergycouncil.org.au

ABN: 84 127 102 443

- Critical Systems

Greater clarity will materially improve consistent and risk-based application of the rules.

2) Security Must Be Risk-Based and Tiered

As currently drafted, the bundle of proposed rule changes is not proportionate to the threat profile of all assets.

The renewable sector includes distributed generation across multiple landholders under shared-use models. The governance, procedural and technical sophistication proposed may be appropriate for System of National Significance (SoNS) assets but is disproportionate for many distributed or lower-consequence assets.

CEC Recommendation:

- Introduce a tiered approach aligned with asset consequence.
- Consider AESCSF Security Profile levels aligned to AEMO guidance.
- Review the 30MW entry threshold for Critical Asset designation.
- Consider a new intermediate tier of criticality.

3) CYBER-1 – AESCSF v2 Security Profile Requirements

CEC supports the transition to AESCSF Version 2. However:

- SP-2 represents a substantial uplift (275 practices; 152 additional high-maturity controls).
- All additional SP-2 practices require high maturity; many require the highest maturity level.
- The 18-month timeframe risks rushed implementation that may introduce new vulnerabilities.

CEC Recommendation:

- Mandate SP-1 (v2) for all Critical Infrastructure entities.
- Apply SP-2 only to SoNS or higher-tier assets.
- Allow staged transition beyond 18 months where justified.

Barrier to Entry Risk:

For smaller renewable developers, SP-2 requirements combined with the 30MW critical asset threshold may unintentionally deter new entrants – which itself poses energy security and transition risk.

4) CYBER-4 – Published Cyber Risk Advice

Greater clarity is needed regarding how prescriptive published advice will be. Overly restrictive interpretations may unintentionally limit supply chain options in already concentrated OEM markets.

5) PERSONNEL-2 – Strengthened Background Checking

The proposal to require AusCheck for all onshore Critical Workers presents operational and legal challenges:

- Many critical workers are contractor employees, not direct employees of the Responsible Entity.

- Responsible Entities may lack legal authority to access or manage AusCheck for non-employees.
- Privacy Act and employment law considerations complicate implementation.

CEC Recommendation:

- Risk-tier worker cohorts.
- Allow contractor-managed checks.
- Permit third-party administrators.
- Ensure <20 business day turnaround times.

6) PHYSICAL-1 – Physical Security Plan Requirements

Large-scale renewable assets are often distributed across multiple landholders under shared-use agreements.

Site-wide fencing, CCTV, alarms and monitoring may:

- Be prohibitively costly.
- Create contractual complexity.
- Undermine landholder and community trust.

CEC Recommendation:

- Apply proportionate, risk-based physical security requirements.
- Recognise distributed asset models.
- Avoid blanket site-wide mandates where threat profile does not justify them.

7) Implementation Timing & Budget Impact

Working back from the proposed June 2028 compliance date implies a January 2027 commencement, effectively allowing one financial year to complete all uplift.

For many entities, this is operationally unrealistic and risks either:

- Incomplete implementation; or
- Diversion of capital from generation delivery.

CEC Recommendation:

- Extend implementation timeframes.
- Allow phased compliance.
- Align major uplift requirements with normal investment cycles.

8) Conclusion

The CEC supports strengthening Australia's critical infrastructure security framework. However, proportionality, tiering and implementation realism are essential to ensure the rules strengthen national security without materially undermining the energy transition.

Phone: +61 3 9929 4100
Fax: +61 3 9929 4101
info@cleanenergycouncil.org.au

Level 20, 180 Lonsdale
Street, Melbourne, VIC
3000, Australia

cleanenergycouncil.org.au

ABN: 84 127 102 443