Ref: REG19010232-2006-1

13 February 2026

Department of Home Affairs
By webform / email
CI.Strategy.Guidance@homeaffairs.gov.au

Proposed amendments to the Critical Infrastructure Risk Management Program Rules for high-risk asset classes

Essential Energy welcomes the opportunity to participate in the above consultation process and supports continued strengthening of the principles-based risk management approach in the Critical Infrastructure Risk Management Program ("CIRMP") Rules.

The final CIRMP Rules would benefit from additional clarification to support effective, efficient, and consistent implementation across entities in response to the evolving threat environment. In particular, alignment of definitions, and supplementary guidance would support the object of the *Security of Critical Infrastructure Act 2018* (Cth) ("SOCI Act") and the intent of the proposed amendments.

Definitions generally

The consultation paper includes references to critical systems as being or including 'vital' or 'important' technology and systems. It also includes references to critical systems that are adjacent to but separate from references to 'operational technology control systems'.

To avoid ambiguity and unnecessary complexity, the definitions in existing legislation and rules (such as for critical components, and major suppliers) should be used wherever possible in any amended CIRMP Rules. Additional guidance and examples would also assist in consistent interpretation and adoption.

Consideration of specified risk advice

Specified risk advice assists entities in identifying, minimising or eliminating risks to critical infrastructure. Essential Energy notes that existing advice provided to government entities under the Protective Security Policy Framework ("PSPF") in some cases refers to specific processes and functions for government entities, and may require amendment or the provision of equivalent advice for critical infrastructure sectors.

Cyber security framework uplift; critical systems network protection; and enhancing cyber material risks.

Essential Energy supports continued strengthening of cyber security practices across critical infrastructure sectors. Aggregated maturity measures are most useful when establishing minimum baseline practices, but are less effective as a measure of risk mitigation when moving beyond baseline

compliance and adopting a risk-based approach focused on protecting and segregating areas of highest risk.

Examples and guidance targeting higher minimum standards for practices applicable to highest risk systems (for example, operational technology control systems) would support a commensurate focus on these areas.

Essential Energy notes that the proposed requirements and specific material risks are in some cases reflected in existing detailed cyber security frameworks such as the Australian Energy Sector Cyber Security Framework. The terminology in these frameworks should be aligned to the terminology in the CIRMP Rules wherever possible. If terminology is not aligned, maintaining and complying with a separate set of practices is likely to create additional and unnecessary delay, cost and complexity.

Where entities have already adopted detailed frameworks, alignment would allow for these requirements to be met with reference to existing practices and anti-patterns. Alignment of terminology may also assist entities that have adopted other less detailed frameworks to selectively uplift and obtain assurance on specific additional practices.

Additional specific material risks arising from technology management practices (for example, remote access) or advanced and emerging technology should also be addressed through minimum standards in relevant cyber security frameworks where possible.

The proposal would benefit from additional clarification on how the material risk requirements interact with the cyber security framework requirements, and if or how the requirement to have a plan to completely rebuild critical systems interacts with system segregation and isolation requirements.

Foreign ownership, control and influence ("FOCI"); supply chain vulnerability mapping; and vendors of concern

Existing PSPF guidance to Australian government entities on FOCI risks focuses on requirements "when undertaking procurement of technology assets". In general, FOCI risk assessment, supply chain vulnerability mapping, and vendor due diligence are most effective when integrated into procurement and supplier selection processes. Outside of these processes, additional assessments and mitigations are often necessarily more limited in scope.

Identification of specific products or vendors (as has been provided for example with Deepseek, and Kaspersky Lab products and services) allows entities to rapidly respond to identified risks and should continue to be shared with critical infrastructure entities and expanded over time.

Given the scale and complexity of critical infrastructure supply chains, clear guidance on expectations for managing existing arrangements where there is no specific identified concern would assist entities in adopting an approach that is reasonable and practical, particularly within the relatively short 6 month period proposed in the consultation.

The proposal would benefit from additional clarification on how the general all-hazards FOCI requirements (proposed to be implemented within 6 months following consultation) interact with the vendors of concern requirements (proposed to be implemented by 30 June 2028) particularly where the examples focus on FOCI risks.

Next steps

Essential Energy looks forward to participating in the next stages of the consultation process. If you have any questions in relation to this submission, please contact Mr Dean Saunders, Head of Risk and Compliance via email at dean.saunders@essentialenergy.com.au

Yours sincerely,

Martin English
General Counsel and Company Secretary