13 February 2026

Sophie Bazzana
Acting Assistant Secretary
Department of Home Affairs

Submitted online: https://www.homeaffairs.gov.au/

Dear Ms Bazzana,

Enhancing the Critical Infrastructure Risk Management Program (CIRMP) Rules – Consultation Paper and Addendum

Origin Energy Limited (Origin) welcomes the opportunity to provide feedback on the Enhancing the Critical Infrastructure Risk Management Program (CIRMP) Rules Consultation Paper and Addendum. Origin supports elements of the proposed reforms, including the uplift to cyber security maturity, where these measures are proportionate and targeted to the most material risks.

However, Origin is concerned that aspects of the proposed foreign ownership, control and influence (FOCI), supply chain and personnel hazard enhancements are, in some cases, disproportionate, overly prescriptive and would be difficult to implement in practice. These measures could impose significant administrative, operational and investment costs that are not commensurate with the expected improvements in risk management outcomes. In particular, certain requirements do not adequately reflect the operational realities of the energy sector, including limited original equipment manufacturer (OEM) availability, which means that alternatives may not be commercially or operationally viable.

During a period of significant asset investment and transition to a lower emissions energy system, there is a risk that some proposed measures could delay projects and increase costs without delivering a commensurate reduction in risk to critical infrastructure assets. To address these concerns, Origin recommends that the Department adopt a flexible, risk-based approach to implementation, minimise overly prescriptive requirements, and allow compliance to be demonstrated through existing frameworks and processes. We also suggest that implementation be staged, with priority given to key cyber security enhancements.

Further detail on Origin's concerns and recommended refinements to specific hazards is set out in Attachment I, including the following key points:

- Vendors of concerns / FOCI risks: The obligations should allow for flexibility where no commercially or operationally viable alternatives exist and avoid requirements that would materially constrain project delivery in limited OEM markets.
- Personnel background checks: The rules should apply a risk-based approach to applying the checks to critical workers; enable third parties to independently meet or administer background check requirements; and ensure the process is adequately resourced to avoid delays.

Should you have any questions or wish to discuss this submission further, please contact me at [redacted] or on [redacted].

Yours sincerely,

[redacted]
Sarah-Jane Derby
Group Manager, Regulatory Policy

Origin Energy Limited ABN 30 000 051 696 • Level 32, Tower 1, 100 Barangaroo Avenue, Barangaroo NSW 2000
GPO Box 5376, Barangaroo NSW 2000 • Telephone (02) 8345 5000 • Facsimile (02) 9252 9244 • www.originenergy.com.au

General comments

The energy sector operates within a highly-regulated environment and has mature, well-established risk management frameworks to manage material risks. As providers of essential services, energy entities are already subject to extensive regulatory obligations that drive a high standard of risk management and operational resilience. For example, where a generation asset is unavailable, energy suppliers are required to comply with National Electricity Rules (NER) obligations and incentivised to respond to market price signals to support continuity of supply. Consistent with these obligations, and the existing Critical Infrastructure Risk Management Program (CIRMP) requirements, Origin has implemented robust, risk-based processes across its operations.

Origin generally supports the proposed uplift to cyber security hazard requirements (subject to our detailed comments in Table 1), as these measures target the most significant risks under the Security of Critical Infrastructure (SOCI) framework. However, we consider that aspects of the proposed supply chain and personnel hazard enhancements are, in some cases, disproportionate, overly prescriptive and challenging to implement in practice.

In particular, certain uplifts do not reflect risk-based approaches and could create unnecessary duplication, particularly where differing terminology or frameworks apply across regulatory regimes, such as the Australian Sustainability Reporting Standards (ASRS) and the NER. The implied emphasis on site-based risk assessments is also likely to be difficult to operationalise during a period of significant asset investment and transition and would impose a substantial administrative burden.

Given the scope of the proposed uplifts, implementation would involve material costs for critical infrastructure entities, including Origin, as well as for suppliers and other related parties subject to additional compliance obligations. This would ultimately have implications for the cost of the energy transition and for energy supply more broadly.

To address our concerns regarding proportionality and cost, Origin proposes the following for the Department's consideration.

A flexible approach to implementation should be adopted

The rules should enable Responsible Entities (RE) to demonstrate compliance by leveraging existing frameworks and processes, rather than requiring the establishment of parallel systems. This can be achieved by avoiding overly prescriptive requirements and allowing flexibility in how the enhanced obligations are met. Where practicable, terminology should align with related regulatory regimes, recognising that alignment may not always be feasible given the breadth of sectors captured by the CIRMP.

The rules should also permit broader, whole-of-organisation risk assessments where this is more appropriate and effective, rather than imposing site-based risk assessment expectations that would create significant administrative burden.

In addition, the Department should consider developing detailed guidance material, including case studies and practical examples, consistent with approaches adopted by work health and safety (WHS) regulators. Where prescription is necessary, including in relation to specific cyber security standards or foreign ownership, control and influence (FOCI) requirements, key terms should be clearly defined to reduce ambiguity and compliance uncertainty.

Enhancements should be prioritised

The Department should prioritise implementation of the critical cyber security enhancements, with further consultation undertaken on the remaining measures to ensure they are appropriately calibrated to risk and operational realities.

Origin Energy Limited ABN 30 000 051 696 • Level 32, Tower 1, 100 Barangaroo Avenue, Barangaroo NSW 2000
GPO Box 5376, Barangaroo NSW 2000 • Telephone (02) 8345 5000 • Facsimile (02) 9252 9244 • www.originenergy.com.au

Implementation timeframes

If the Department proceeds with all proposed reforms rather than prioritisation, Origin considers that a staged approach to implementation is necessary to appropriately reflect the administrative burden of the proposed uplifts. Further detail on where additional time may be required is provided in Table 1.

Noting this, a compliance date of 30 June 2028 appears to provide a reasonable preparation period, particularly where implementation of the more burdensome obligations is staged. In relation to the proposed requirement to include a documented plan within the CIRMP outlining how compliance will be achieved during the attestation periods leading up to September 2028, Origin suggests that this obligation allow for a degree of flexibility. In particular, the plan should be capable of being high-level or 'open-ended', enabling entities to refine and mature their approach over time in a manner consistent with best practice.

In addition, Origin seeks clarity on how implementation will be assessed for energy sector projects with long delivery lead times, where procurement decisions are often made several years prior to commercial operation. Changes to requirements during this period create uncertainty for project development, particularly where it is unclear which framework will apply to the assessment of vendor risks once an asset becomes operational. This risk arises where procurement decisions are made under an existing framework, but the rules are amended prior to commercial operations. The Department should therefore consider appropriate transitional arrangements for projects where contractual commitments have already been made at the time the rules are finalised.

Scope of application

The enhanced CIRMP obligations are proposed to apply to the energy, communications, water and sewerage and transport sectors. The Consultation Paper indicates that, for communications, the relevant asset classes are intended to capture critical broadcasting and domain name system assets, while noting that telecommunications assets, including carriers and Carriage Service Providers (CSPs) with more than 20,000 active services, are regulated under the Security of Critical Infrastructure (Telecommunications Security and Risk Management Program) Rules 2025. It is therefore unclear whether the uplifts are intended to apply to CSPs, including broadband retailers such as Origin.

Origin considers that the enhanced obligations should not apply to CSPs. CSPs do not own critical infrastructure (CI) assets and are therefore not in a position to manage risks associated with those assets. Extending the enhanced CIRMP obligations to broadband retailers would impose disproportionate administrative burden and costs, without delivering a commensurate improvement in critical infrastructure risk management outcomes.

Proposed enhancements to the CIRMP

Table 1 offers comprehensive feedback regarding the proposed uplifts, noting areas where additional time may be required for implementation and identifying instances where the recommended obligations may lack proportionality or alignment with a risk-based methodology.

Table 1: Origin feedback

Proposed uplift	OE comments
All-hazard measures	
Consideration of specified risk advice	Origin currently receives a significant volume of risk advice, notices and related communications, which vary in their relevance and materiality. If the Department were to issue multiple advisories throughout the year, the proposed requirement could result in substantial administrative burden, including repeated updates to CIRMPs that are not proportionate to the risks presented. To ensure proportionality, the rules should limit this obligation to advice that has a material impact on the relevant critical infrastructure asset. In addition, the implementation approach should be flexible. While the Consultation Paper indicates that RE will have 12 months from risk identification to comply, this timeframe may not be feasible in all circumstances, including where advice

	relates to operational technology hardware or complex components such as wind turbine systems. The rules should therefore allow the Department to specify longer compliance periods where appropriate.
All-hazards material risks – foreign ownership, control and influence	Origin acknowledges that FOCI represents a material risk and supports its consideration within the CIRMP framework. We note that controls to manage FOCI risks are already embedded within our organisation and across existing CIRMP hazards. To minimise duplication, the Department should reconsider whether a standalone all-hazards FOCI obligation is necessary. A more efficient approach would be to focus on whether FOCI risks have been appropriately identified and managed across the CIRMP as a whole. Our experience with assessing FOCI risks has highlighted that the current framework lacks clarity, which has led to implementation uncertainty. In particular, limited guidance has resulted in organisations relying on internal risk appetite and judgement on matters such as complex geopolitical considerations, which may not align with the Department's own risk tolerance. This creates uncertainty for decision-making and compliance. To address this, the Department should provide further guidance, where practicable, to reduce ambiguity. While we acknowledge that blacklists or whitelists are not proposed, greater guidance on assessment methodology, such as referencing publicly available Five Eyes resources, would assist RE to better align with the Department's risk expectations and make more informed decisions on matters of national security.
Cyber and information security hazards measures	
Cyber security framework uplift & Multi-factor authentication (MFA)	Origin is supportive in principle of the intent to uplift these two frameworks.
Critical systems network protection	Energy sector assets, including wind turbines and battery energy storage systems (BESS), commonly rely on remote diagnostics, monitoring and analytics to maintain safe and reliable operations. There is a risk that overly prescriptive network segregation requirements could undermine essential operational functionality, including access to software updates, and materially increase operating costs across the sector. The rules should therefore include appropriate guardrails to ensure flexibility for energy sector operating models, such as exemptions for operating models that are standard across industry. In addition, clear guidance should be provided on what constitutes the "greatest practical level" of segregation, consistent with a risk-based rather than prescriptive approach.
Enhancing cyber material risks	Origin recognises the value of forward-looking risk management, including planning for emerging technology hazards, and does not oppose this measure in principle. However, additional information is required regarding the scope and expectations of this requirement to assess its practical implementation, particularly given the rapidly evolving nature of advanced and emerging technologies.
Supply chain hazard measures	
Supply chain vulnerability mapping	Given existing supply chains, this proposed change could be burdensome particularly the requirement for suppliers to disclose if they are a critical supplier for other CI entities. Achieving this would likely necessitate legislative amendments mandating supplier disclosure, as visibility is currently limited beyond tier 1 (direct) suppliers and our capacity to influence upstream supplier operations is restricted, including their ability to provide services.

	Effective implementation would likely require corresponding obligations on suppliers to disclose relevant information, potentially through legislative change. Absent this, compliance would be impractical. In addition, reliance on tools (e.g. software as a service solutions) that are not yet developed introduces further uncertainty. Origin recommends deferring this requirement until there is reasonable assurance that industry can comply through appropriate supply-chain-wide obligations. If the requirement proceeds, the rules should clearly define the expected scope, depth and frequency of supply chain mapping to support consistent and efficient implementation.
Vendors of concern	Origin currently assesses FOCI risks associated with vendors through its procurement framework and recognises the importance of managing this risk, as previously noted. However, the proposed changes may be difficult to implement in the context of the energy sector's limited vendor landscape. While we support the stated intent not to prohibit the use of vendors where no practical alternatives exist, the requirement to implement additional security measures in such circumstances is not clearly defined. Given the current OEM landscape, overly stringent requirements could significantly constrain project delivery and competition. Addressing these challenges would require a fundamental shift in the global OEM market, which is unlikely in the near term. The rules should therefore allow flexibility in the application of additional security measures where no commercially or operationally viable alternatives exist, or where requirements would materially distort competition.
Personnel security hazard	
Personnel security plan	Origin favours a flexible approach to meeting this obligation. Compliance should be achievable through existing organisational plans and processes, rather than requiring a standalone SOCI-specific plan. This would minimise administrative complexity and support efficient implementation.
Strengthened background checking	Requiring AusCheck background checks for all critical workers would be administratively burdensome. If the Department proceeds with this requirement, the rules should allow for: • Responsible Entities to categorise their Critical Worker Cohort according to risk, and apply additional background checking requirements as a control for the highest risk cohort, when appropriate; • Contractors to meet the AusCheck requirement for their staff independently of the CI Responsible Entity; • Third parties to administer the Responsible Entity AusCheck administrative processes on behalf of the CI Responsible Entity; and • The Department to provide advice on suitable similar processes and standards for contractors employed in countries other than Australia. The Department should also consider developing and resourcing the AusCheck process to ensure checks can be carried out in a timely manner, ideally with a turnaround of fewer than 20 working days. Longer processing times risk workforce attrition and require additional interim risk controls.

Enhancing personnel material risks	The proposed implementation timeline may be appropriate for administrative controls such as training and process development. However, engineering controls may require additional time and incur significant costs. A flexible, risk-based approach should therefore be adopted, allowing extended timeframes where requirements are more complex.
Physical hazards	
Physical security plan	Origin already maintains a physical security plan. While some proposed enhancements may be beneficial, certain elements would be duplicative or difficult to implement. In particular, requirements relating to ownership, tenancy and asset availability impairments may result in the plan being classified as protected information, necessitating parallel documentation and increasing administrative burden. Continuous monitoring requirements may also be impractical for all components and could involve significant cost and engineering changes. Monitoring obligations should be limited to components that can reasonably be monitored. Several key terms also require clarification to support efficient implementation, including the meaning of “whole asset or organisation”, the intended scope of an “incident response plan” with respect to physical hazards, and several references to what is considered “appropriate”. As with other measures, requirements should remain aligned with a risk-based approach and avoid unnecessary prescription. Compliance by June 2028 may be challenging given the scope of the proposed enhancements, particularly when considering older or legacy sites. Additional time should be considered to reflect cost pressures and practical implementation constraints.