01 May 2026

Department of Home Affairs

Via email: CI.Strategy.Guidance@homeaffairs.gov.au

Consultation on the Exposure Draft of the Critical Infrastructure Risk Management Program Rules

Alinta Energy welcomes the opportunity to provide feedback to the Department of Home Affairs on the Exposure Draft of the *Critical Infrastructure Risk Management Program Rules*.

Alinta Energy recognises the Department's efforts to incorporate feedback but recommends further refinements are required to ensure that the new requirements are genuinely risk-based.

In our initial submission, Alinta Energy, and as recognised by the Department, many other respondents, emphasised that the CIRMP rules should be principles-based and avoid undue prescription, noting that responsible entities (particularly in the electricity sector) are best placed to identify relevant risks and appropriate mitigations given their specific assets, operating environments and existing obligations.

Alinta Energy recognises the Department's efforts to reflect this feedback in the Exposure Draft, including through the use of the qualifier *"in so far as reasonably practicable"*.

This formulation appropriately limits compliance exposure where the implementation of systems or processes would be infeasible. However, it does not clearly address circumstances raised in industry feedback where a prescribed risk or mitigation is not relevant or not necessary at all, having regard to the specific circumstances and structure of an asset's critical systems and supply chains, an entity's existing regulatory, market and operational controls.

In the electricity sector, participants already operate within a mature and highly regulated framework comprising licensing conditions, technical and performance standards, contingency and reserve arrangements, and ongoing monitoring and reporting obligations, reinforced by strong commercial and market incentives to remain available. Where these frameworks already manage a risk to an immaterial level, additional centrally prescribed CIRMP requirements may add compliance burden without corresponding risk reduction.

We recommend that further refinement is required to ensure the rules expressly permit responsible entities to determine that certain prescribed requirements do not need to be applied where implementing the requirement is not relevant to the asset's risk exposure, or the risks are not material or are already adequately mitigated, consistent with a genuinely risk-based and principles-focused framework.

Notwithstanding the above recommendation, we expect that the costs and resources associated with implementing and maintaining compliance under the proposed CIRMP Rules to be significant. We note that the implementation burden and result costs may be particularly pronounced for electricity companies, as the framework encompasses a broad

range of assets. We also note that any cost increases may impact consumers.

We make the following further recommendations to support a risk-based and principles-focused framework by preserving the intent of the enhanced CIRMP requirements, while minimising unnecessary duplication and compliance burden. This approach seeks to ensure that regulatory effort, cost and operational focus are directed to areas where they will have the greatest impact on reducing material risks to critical infrastructure.

Further detailed recommendations

Material risk

- **We recommend that the requirements under proposed section 6A be narrowed to risks not already identified and addressed within the CIRMP to avoid unnecessary duplication.**

Cyber and information security hazard measures

We recommend that:

- **The requirement for multi-factor authentication is narrowed to users of critical systems.**
- **Subsection 8A(8) requires refinement to avoid requiring the segregation of critical systems from networks in all cases and ensure requirements are risk-based.**
- **In relation to the requirement to identify risks in deploying new technologies (8A(2)(d) and 8A(2)(e)), it should clarified that entities have discretion as to how they define the technologies they will consider.**
- **Further clarity and transitional flexibility is required in section 8A to ensure obligations are proportionate and deliverable.**
- **A grace period should be permitted where cyber security frameworks are updated.**

Supply chain hazard measures

We recommend that:

- **The requirement to identify maximum tolerable outages should be limited to critical systems of a CI asset.**
- **The risks identified to suppliers should be reasonably foreseeable and material.**
- **The grace period to comply should be extended to 48 months due to the significant complexity associated with compliance.**

- **A tiered approach should be applied based on supplier criticality to the CI assets.**

Personnel security hazard measures

- **As drafted, the background check requirements in 9A could disrupt critical energy operations, which often need specialised workers on short notice. We recommend these checks only be required when practical and when they do not interfere with asset operation (including in emergency circumstances).**

Physical and natural hazards

- **Several of the requirements in 11A are duplicative and should be consolidated.**

Material risk

The requirements under 6A should be narrowed to risks not already identified and addressed within the CIRMP.

As currently drafted, section 6A risks duplicating existing risk identification requirements, particularly in relation to system impairment and FOCI-related risks which are already captured under broader CIRMP obligations. We recommend narrowing the scope of section 6A so that it applies only to material risks not already identified or addressed elsewhere in the CIRMP. This would avoid unnecessary duplication, and ensure regulatory effort is focused on genuinely incremental or heightened risks that warrant enhanced treatment.

Cyber and Information Security Hazard measures

The requirement for multi-factor authentication should be narrowed to users of critical systems.

As currently drafted, the requirement to apply MFA across all “networks and systems” is overly broad and may capture non-critical systems that have no material bearing on the operation or security of the critical infrastructure asset. Extending MFA to non-critical systems would add compliance burden without proportionate security benefits and would not advance the underlying objectives of the reforms.

Subsection 8A(8) requires refinement to avoid requiring the segregation of critical systems from networks in all cases and ensure requirements are risk-based.

The updated requirement should instead ensure that critical systems *are capable of* operating independently from networks where it is practicable to do so, and where this would genuinely reduce the risk of material disruptions.

We recommend refining the requirement under 8A(8)(b) to only mandate operating critical systems separately from networks if those networks are essential for the system's operation or present a significant risk to it. This would ensure that the obligation matches the actual risk, supporting the resilience of critical systems without placing unnecessary or excessive requirements on supporting or low-risk networks.

The requirement to recover a critical system under 8A(8)(c) should also be narrowed so that it applies only where there is a reasonable risk that a network issue could necessitate such recovery. This would ensure the obligation is targeted to credible risk scenarios, aligning recovery requirements with their intended purpose while avoiding unnecessary or disproportionate compliance burdens.

In relation to the requirement to identify risks in deploying new technologies (8A(2)(d) and 8A(2)(e)), it should clarified that entities have discretion as to how they define the technologies they will consider.

Permitting entities this discretion will support management plans being risk-based and avoiding an unnecessary compliance burden that does not serve the CIRMP objectives.

The requirements under 8A(2) should not apply to the extent that they are already met in compliance with a sanctioned cyber security framework.

Further, we recommend that these requirements are edited to remove overlap with these frameworks, or otherwise, areas of potential overlap are highlighted. Greater clarity on areas of overlap would assist responsible entities in understanding how compliance with established frameworks can be leveraged to meet CIRMP obligations and avoid duplication.

We recommend extending the timeframe for section 8A8A

We consider that the proposed 24-month implementation period for section 8A is insufficient, particularly for complex capabilities such as disaster recovery under subsection 8A(10). We consider that the proposed 24-month implementation period for section 8A is insufficient, particularly for complex capabilities such as disaster recovery under subsection 8A(10).

We recommend extending the compliance timeframe to at least 36 months, recognising the scale, cost and operational complexity associated with designing, building and testing effective recovery and restoration arrangements for critical systems.

A grace period should be permitted where cyber security frameworks are updated.

Section 8A(2) notes that cyber frameworks are incorporated “as in force from time to time”, which creates a moving baseline for compliance.

This approach introduces uncertainty for compliance assurance, audit processes and long-term investment planning, as framework updates could materially change obligations without regulatory amendment.

We recommend:

- introducing grace or transition periods following material framework updates; and
- confirming that entities will be assessed against the version of the relevant framework that was in force at the time of assessment or implementation, rather than retrospectively against updated requirements.

These clarifications and adjustments would materially improve regulatory certainty and workability, while still supporting the policy objective of strengthening cyber resilience for critical infrastructure assets.

Supply Chain Hazard measures

The requirement to identify maximum tolerable outages should be limited to critical systems of a CI asset.

Section 10A should be amended so the obligation to identify maximum tolerable outages within both supply chain mapping under 10A(3)(b) and vendor assessment under 10A(5)(d) applies only to critical systems of a CI asset that are *reasonably contingent on supply chain dependencies*, consistent with a risk-based and proportionate approach.

The risks identified to suppliers should be reasonably foreseeable and material.

Section 10A(4)(5) should be amended to limit the obligation to identify risks to major suppliers (including legal and FOCI-related risks) to risks that are reasonably foreseeable and material. This obligation should be expressly subject to the "so far as is reasonably practicable" threshold, as for other requirements.

The grace period to comply should be extended to 48 months.

We recommend that the grace period for complying with the enhanced supply chain requirements in section 10A be extended from 18 months to 48 months. The current timeframe is insufficient to implement the extensive mapping, risk assessment and mitigation activities required, particularly given the scale and complexity of supply chains for many CI assets. And particularly energy infrastructure assets.

A tiered approach should be applied based on supplier criticality to the CI assets.

We recommend that the enhanced supply chain requirements in section 10A be implemented on a staged and tiered basis, rather than applying uniformly to all 'major suppliers'. As currently drafted, the broad definition of major supplier, combined with requirements to assess jurisdictional laws, sanctions regimes, access and control over CI assets, and the potential to exceed maximum tolerable outage, creates a substantial compliance burden and risks disproportionate effort being directed to low-risk vendors.

Supply chain obligations should instead be tiered based on supplier criticality and level of access or control over critical systems, with deeper assessment reserved for suppliers whose failure could reasonably result in material disruption to the CI asset. This approach would better align with the principles-based intent of the CIRMP framework and ensure compliance effort is directed toward the highest-risk supply chain dependencies.

Personnel Security Hazard measures

The background check requirements under proposed section 9A require refinement to avoid threatening the ongoing operation of critical assets.

As drafted, the background check requirements under proposed Rule 9A risk undermining the ongoing operation of critical energy assets, particularly where specialised workers or contractors must be deployed at short notice, during outages or in emergency circumstances.

Electricity generation assets rely heavily on a limited pool of highly specialised onshore and offshore personnel, including OEM contractors, to maintain safety, availability and system reliability.

This risk arises in part due to the breadth of the definition of "critical worker", which

includes individuals who have access to any critical component of an asset.

Requiring background checks in all such circumstances, without adequate flexibility, risks delaying maintenance, fault response or contingency actions in ways that may increase operational and system risk rather than mitigate it.

Alinta Energy considers the Rules should expressly provide carve-outs where it is not practicable to obtain these checks, or where waiting for checks to be completed would threaten the safe or continuous operation of a facility, including in emergency or contingency situations.

This is particularly important for offshore and specialist workers mobilised through OEMs, where entities may have limited visibility over the identity of the specific individuals attending site and where mobilisation timelines are often constrained. In these cases, it may be more efficient and effective to operationalise background assurance through existing procurement and/or visa and immigration processes, rather than through potentially duplicative, asset-specific checking regimes.

As a complementary measure, Alinta Energy also recommends that background checks should not be required for workers who are appropriately supervised by personnel who have already satisfied the relevant checking requirements, with supervision calibrated to the nature of the task and the level of access involved.

Together, these changes would support a risk-based and proportionate application of Rule 9A, ensuring that security outcomes are achieved without introducing unnecessary compliance burden or avoidable operational risk.

Further, the drafting of the requirements should also recognise practical limitations in emergency or unforeseen circumstances. For example, where emergency services require immediate access to a site – including critical components or areas where critical systems are accessible (such as in response to a fire), it would not be feasible for a responsible entity to obtain clearances in advance. The requirements should explicitly reflect such scenarios.

Alinta Energy recommends that subsection 9A be redrafted to minimise the extent of cross-referencing, noting that the current drafting requires responsible entities to navigate extensive cross-references across multiple provisions of the Rules, as well as external Acts and legislation, in order to understand the full suite of background check requirements. Consolidating these obligations into a clearer and more self-contained provision would improve clarity, reduce interpretive risk and support more efficient compliance, without altering the underlying policy intent.

Physical and Natural Hazards

Several of the requirements in 11A are duplicative and should be consolidated.

The drafting of the requirements under 11A(1)(b) to:

> "as far as it is reasonably practicable to do so—minimise or eliminate the risk associated with physical security consequences arising from the occurrence of both physical or other hazards, including cyber and information security hazards, personnel hazards and supply chain hazards"

appears duplicative and should be incorporated in the relevant sections pertaining to those hazards. For instance:

- 8A(2)(a) specifies a requirement to eliminate material risks including replacing and updating hardware and other critical components; and
- 9A(2) requires entities to minimise or eliminate materials risks associated with physical access to critical systems.

Additionally, Section 11A(2)(d) is duplicative with the enhanced cyber and information security hazard requirements under *Multi-factor Authentication* - 8A(5) - and the enhanced Personnel hazards requirements under 9A(2).

Thank you for your consideration of [redacted]

Yours sincerely,

[redacted]