DLC LEGAL

PRECISION NAVIGATION

About DLC Legal

DLC Legal s a boutique provider of virtual and onsite legal, commercial, strategic sourcing, procurement and contract management services to State and Commonwealth governments and private industry. Incorporated in 2021 as an Integrated Legal Practice under the banner Black Ink Legal, the firm specialises in assisting our clients to develop, structure, negotiate and manage strategically important projects and procurements through to deal completion.

DLC Legal specialises in technology and cyber security law, and our lawyers possess a deep understanding of the complex mosaic of the cyber and technology legislative landscape. Our expertise extends to advising a diverse array of clients, ranging from emerging tech startups to established multinational corporations, on a broad spectrum of technology and cyber-related legal issues. This includes AI, data protection and privacy, compliance with local and international cyber security standards, breach response and notification requirements, and the management of cyber risks in contractual agreements. We are proactive in supporting and assisting our clients to navigate the intricacies of the Commonwealth cyber security legislative framework, to safeguard their digital assets and intellectual property, while ensuring their operations align with current and emerging legal frameworks. DLC Legal is passionate about and committed to staying at the forefront of technological advancements and legislative changes to empower our clients to achieve their business objectives with confidence, knowing their legal exposure is minimised and their innovations are protected.

DLC Legal extends its boutique legal and strategic services to Australian managed IT providers, emphasising support in privacy and cybersecurity with clients and partners specialising in technical cyber support and insider threat detection technology. Our advisory services are designed to address the unique challenges faced by the IT and technology sector, offering specialised guidance in navigating the complexities of data protection laws and cybersecurity threats. We understand the critical importance of safeguarding digital assets and personal information in today's interconnected world. By partnering with IT and technology firms, we aim to deliver comprehensive strategies that enhance cybersecurity measures and ensure compliance with Australian privacy laws, thereby fortifying our clients' defences against cyber threats and legal vulnerabilities.

Executive Summary

DLC Legal welcomes the opportunity to comment on the *Exposure Draft of the Security of Critical Infrastructure Legislation Amendment (Enhanced Critical Infrastructure Risk Management Program) Rules 2026 (Exposure Draft Rules)* (**CIRMP Rules**). We support the objective to enhance the resilience of high-risk critical infrastructure assets in light of evolving threats alongside the recommendations of the Independent Review of the *Security of Critical Infrastructure Act 2018* (**SOCI Act**).

We also support the decision to retain an all-hazards, principles-based approach rooted in "so far as is reasonably practicable" rather than moving to a wholly prescriptive regime. However we note that several elements of the Exposure Draft Rules risk undermining the principles-based approach by effectively hard-coding prescriptive expectations that may be difficult or disproportionate to implement for some assets, particularly where there are legacy old technology (**OT**) environments and regulated pricing constraints.

With this in mind, our submission focuses on four themes:

1. Scope and proportionality of enhanced CIRMP requirements.
2. Cyber, Multi Factor Authentication (**MFA**) and network segregation obligations.
3. Personnel, Foreign Ownership, Control or Influence (**FOCI**) and supply chain obligations.
4. Interaction with existing regimes, governance and reporting.

We have also proposed some drafting amendments to address these concerns.

Response to Questions for Consultation

Consideration 1

Scope and proportionality of the enhanced CIRMP requirements.

DLC Legal queries whether the scope and proportionality of the enhanced CIRMP requirements remains genuinely risk-based or drifts into over-regulation. For many operators the key concern is not whether uplift is warranted in principle, but whether the specific asset classes selected for "enhanced" treatment fairly reflect their actual threat profile, interdependencies and existing regulatory obligations. Before examining the detailed drafting in provisions like section 4A of the *Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023*, it is important to test whether the framework clearly explains why some assets are elevated while others with similar systemic importance are not, how the Commonwealth envisages future expansion, and how entities can avoid duplicative efforts where they are already subject to strict regimes. In that sense, proportionality is as much about regulatory coherence and clarity of scope as it is about the intensity of individual obligations.

The proposed asset classes selected for the enhanced CIRMP requirements are based on risk profiling and threat intelligence, with the inclusion of state-sponsored activity in energy, water, freight and communications. We believe that the Exposure Draft Rules and Attachment B provide limited transparency on how specific asset classes were prioritised relative to other interdependent assets and digital infrastructure. DLC legal supports the targeted uplift of the asset classes listed in section 4A(1) but recommend that clearer transparency of the risk criteria used for class selection and attention to how future expansion may be considered. Further, we believe that there is merit to the clarification that a responsible entity may apply another instrument's requirements to a baseline asset and be deemed to have complied with this instrument. However, the drafting could benefit from clearer signalling that this "deemed compliance" is optional and that entities are not expected to adopt multiple overlapping frameworks unnecessarily. Clearly outlining the

obligations of affected entities will allow for better compliancy through the Act. This could simply be addressed by amending the second example for the note in section 4(4) to end with: “This does not prevent the entity from complying with this in another way”. Finally, DLC legal believes that the extension of grace periods under section 4A(6) are a positive addition that will benefit affected entities. The implementation of 6, 18 and 24 month grace periods reflect that the Commonwealth have considered feedback on funding cycles and implementation constraints. However we believe 24 months may be too tight for operational technology segmentation projects and multi-factor authentication deployment, given regulatory price cap resets and outage planning cycles. Where full implementation is not yet practicable, entities should be able to rely on the good faith implementation and documented remediation plans to prevent being branded as non-compliant.

Consideration 2

Cyber, MFA and network segregation obligations.

The cyber, MFA and network segregation obligations are where the Exposure Draft most visibly attempts to translate high-level “reasonably practicable” principles into concrete expectations that can be assessed and enforced. Elevating recognised frameworks (Essential Eight, NIST CSF, C2M2, AESCSF, ISO 27001), introducing phishing-resistant MFA and three-month operational independence benchmarks provides clearer markers for boards and regulators, but also risks hardening flexible standards into arbitrary checklists that may be technically unrealistic in legacy OT environments and may be misaligned with commercial and regulatory constraints. As an entry point to provisions like section 8A, it is useful to frame the question as whether the Rules strike the right balance between prescription and flexibility: do they give entities enough room to adopt compensating controls and staged uplift plans where full compliance is not yet practicable, and is the “equivalent framework” concept sufficiently robust and transparent to accommodate global corporate standards?

Turning our attention to subsection 8A(2), this clause requires entities, “so far as it is reasonably practicable”, to minimise or eliminate specified cyber-related material risks. This is a sensible list, but the interaction between the term “all of” (in the bracketed wording in the Exposure Draft) and the reasonably practicable qualifier could be misread as an expectation of full elimination across all items. The SOCI Act already employs a “so far

as is reasonably practicable" test and we believe that it would be best practice to align the new requirements with the existing framework, which would therefore not imply strict liability upon each risk. Additionally, turning our attention to subsection 8A(3)-(4), DLC Legal believes that requiring alignment with recognised frameworks (Essential Eight, NIST CSF, C2M2, AESCSF, ISO 27001) is a pragmatic way to operationalise the concept of "reasonable practicability". We note that the Exposure Draft is silent on how "equivalent" frameworks under subsection 8A(4) will be assessed, which may introduce uncertainty, especially for multi-national groups already aligned with other standards. If these amendments were to introduce transparent, predictable criteria for "equivalence" alongside a practical approval process, the Commonwealth could better inform affected groups who may find themselves navigating to a new model. We recommend a drafting amendment to 8A(4) that replaces "a framework that is equivalent to" with":

> a framework that provides an equivalent or higher level of risk management maturity to that required by a framework in a document mentioned in subsection (3), having regard to:
>
> (a) the scope of assets and risks covered; and
> (b) the maturity level or security profile achieved; and
> (c) any sector-specific guidance published by the Department.

The addition of a statement outlining the process for entities to notify or seek confirmation that their chosen framework will be treated as equivalent will be necessary to better support active compliancy in the affected sectors.

Phishing resistant MFA is a critical control and attention has been rightfully turned to threats of this nature. The implementation of this control method for legacy OT, vendor systems and some remote access arrangements may be technically infeasible or commercially constrained in the short term. Subsection 8A(7) goes some way to recognising this, but frames compensating controls only in terms of "components or technology that are redundant, unsupported, obsolete or discontinued", which may not capture all practical constraints in an evolving digital threat environment. DLC Legal recommends that a broader scope of compensating controls should be recognised where MFA cannot be implemented due to technical or contractual limitations. Shifting the focus from strictly obsolete technology prevents entities being tied to a narrow construction that may limit the existing and evolving practicalities of compliance. In addition to the above considerations, we support the objective of improving network protection and resilience through segmentation and the boosted ability of restoring critical systems while other networks recover. The practicality of complying with section 8A(9)(b), where critical

systems should “continue to be operational for a period of at least three months” while other networks are in recovery may be unrealistic for some assets, given technical design, safety requirements and economic constraint. We believe a practical solution is to add a qualifier of “so far as reasonably practicable” to cover off scenarios where the risk and cost-benefits are not feasible.

Consideration 3

Personnel, FOCI and supply chain obligations.

The personnel, FOCI and supply chain obligations collectively represent the most significant expansion of the CIRMP’s focus beyond traditional cyber and physical controls into the human and commercial relationships that underpin critical infrastructure. By requiring mapping and vetting of onshore and offshore “critical workers”, explicit FOCI-aware risk assessments, and deep supply chain mapping down to maximum tolerable outage, the Exposure Draft aims to surface and manage vulnerabilities that have historically been under-examined. The threshold question, before turning to sections 6A, 9A and 10A in detail, is whether the proposed mechanisms will drive genuinely better risk decisions or simply increase administrative load and friction with contractors, offshore service providers and vendors. That depends on how flexibly concepts like “unable to meet” AusCheck/NV1 requirements and “so far as reasonably practicable” supply chain mapping are understood in practice, and whether guidance encourages risk-based prioritisation rather than exhaustive documentation for its own sake.

Looking to sections 6A and 10A(5), we believe that elevating the consideration of Commonwealth risk advice and FOCI as part of material risk assessment is a step in the right direction. The current drafting in section 6A(b) (“compromise or impairment … as a result of, or in connection with FOCI”) and the FOCI-related vendor assessment in 10A(5) risk being read as a de-facto bar on engaging entities with certain foreign ownership or exposure to sanctions, particularly where guidance is limited. The Department’s narrative in Attachment B that it does not intend to “whitelist or blacklist specific vendors” is important and should be reflected more clearly in the Rules or Explanatory Statement. We recommend adopting a softer formulation under 6A(b) along the lines of “(b) the potential risk of compromise or impairment of the functions of the CI asset as a result of, or in connection with, FOCI”. Additionally, in considering section 10A(5)(e), reframe the section to clarify the steps that should be taken “where material risks are identified, having regard

to reasonable practicability". One suggestion would be to amend the drafting to say "(e) as far as reasonably practicable to do so—steps to minimise or eliminate material risks identified under paragraphs (a)–(d) and to mitigate the relevant impact of the hazard on the CI asset".

DLC Legal agrees that enhanced personnel security for critical workers is warranted, and we support the general direction of mapping onshore/offshore critical workers and implementing suitability assessments. However:

- the reliance on AusCheck and NV1 clearances may be difficult to operationalise at scale for contractor heavy workforces and for offshore personnel;
- five-year reassessment cycles may not align neatly with project lifecycles and existing sector schemes;
- there is limited guidance on alternative vetting or compensating controls where AusCheck/NV1 is not reasonably available for offshore staff.

A clearer recognition of alternative vetting mechanisms and a more flexible approach for offshore workers, provided entities document and mitigate residual risk would provide better flexibility for critical workers who will be impacted by these enhanced protocols.

The improvement of supply chain resilience is an important objective and we support the mapping of major suppliers and systems. For complex, multi-tier supply chains, we believe that full mapping and determination of maximum tolerable outage for every critical system and supplier will be multi-year work, and in some cases limited by contractual and commercial confidentiality constraints. There should be an emphasis on risk-based and staged implementation that prioritises the most critical suppliers and systems first, recognising practical constraints on information. As has been a theme for our response, addressing the practicality of implementing these standards is important to assure compliancy by affected entities. For this reason, support section 10A but consider that under section 10A(2), the addition of "so far is reasonably practicable" will protect the affected entities and offer a risk-based approach.

Consideration 4

Interaction with existing regimes, governance and reporting.

The interaction with existing regimes, governance and reporting raises the question of how the enhanced CIRMP framework will sit within an already crowded regulatory landscape, including state, sectoral and corporate obligations, and how boards can realistically discharge their oversight responsibilities. Many operators are already subject to detailed physical security, WHS, dam safety, cyber and business continuity requirements, and boards are already grappling with overlapping reporting and assurance expectations; layering enhanced CIRMP duties and possible new implementation-update reporting under section 30AG onto this mix carries a real risk of duplication and "form over substance" compliance. Before delving into provisions like section 11A or the contemplated reporting amendments, it is important to frame the theme around two core questions: can compliance with existing equivalent frameworks or licences be recognised to reduce duplication, and can governance expectations be articulated in a way that allows boards to rely on internal and external assurance without being forced into box-ticking public disclosures that might themselves create security or confidentiality risks? That lens should guide the more granular comments that follow.

Operators are already parties to robust physical security regimes, including state planning, WHS, dam safety and sector-specific frameworks. Section 11A is generally aligned with these frameworks, but there are risks of duplication and an administrative burden if compliance with existing equivalent frameworks is not recognised. As was the case in our consideration of section 4(4), we believe that compliance with an equivalent physical security framework should be treated as compliance for the purposes of 11A. This would offer consistency to the manner in which the Department have drafted their amendments but also offers flexibility and accessibility by affected entities. Beyond this, the requirement for implementation updates in section 30AG reports is understandable, but it risks increasing the sensitivity of public reporting and may create tension with confidentiality and security considerations. This will also highlight the broader issue of how boards can reasonably assure themselves of compliance with detailed enhanced obligations. DLC Legal recommends that the proportionate reporting of CIRMP implementation progress should:

- limit public detail to high-level status and indicators;
- allow sensitive operation details to be provided separately through secure channels; and
- clarify that boards may rely on internal assurance functions and external certifications.

A way of capturing these recommendations would be to amend the drafting to ensure that any new provision explicitly allows certain information to be provided in a non-public annex where disclosure would prejudice security.

Conclusion

DLC Legal commends the Department for retaining a principles-based, all-hazards approach and for extending grace periods in response to industry feedback, particularly in recognition of funding cycles, legacy technology constraints and the realities of regulated pricing frameworks. A measured, risk-based uplift, anchored in the "so far as reasonably practicable" standard and supported by recognised cyber and physical security frameworks, is far more likely to produce durable improvements in resilience than a rigid, one-size-fits-all rule set. With targeted refinements of the kind outlined above—clarifying the treatment of FOCI, calibrating MFA and network segregation expectations, recognising equivalent state and sector regimes, and giving greater comfort around staged implementation and compensating controls—the enhanced CIRMP framework can better align Commonwealth risk reduction objectives with the operational, contractual and governance realities facing critical infrastructure operators nationally. That alignment is crucial if boards and executives are to make informed trade-offs, invest early in the right areas and avoid treating the framework as a compliance checklist divorced from their existing risk management systems.

We welcome the opportunity to participate in further co-design of guidance material and supporting artefacts, including sector-specific case studies and worked examples that illustrate how the enhanced requirements can be implemented proportionately in different asset classes and organisational contexts. In our view, the ultimate success of the regime will turn less on the words of the Rules themselves and more on how those words are interpreted and operationalised—through regulator guidance, assurance expectations, information-sharing mechanisms and the accommodation of existing state, sectoral and corporate frameworks. Collaborative development of guidance on acceptable staged implementation, compensating controls (particularly for OT and offshore workforces), determination of maximum tolerable outage, and interactions with other regulatory instruments would give entities the certainty they need to commit to multi-year uplift programs. DLC Legal would be pleased to contribute to that process through targeted working groups, scenario testing and the sharing of practical lessons from large-scale infrastructure projects and operations in Queensland and across Australia.