The Trustee for Anchoram Consulting
ABN 85 197 062 817
Level 1, Suite 3, 16 Napier Close
Deakin, ACT 2600
Tel: +61 1300 042 833
www.anchoramconsulting.com.au

Mr Hamish Hansford
Head of National Security
Home Affairs
Canberra ACT 3000
Australia

Dear Hamish,

Anchoram Consulting welcomes the proposed amendments to the Ministerial Directions powers in Part 3 of the Security of Critical Infrastructure Act 2018. The proposed reforms are a timely and practical response to a threat environment that is increasingly dynamic, diverse and degraded, including heightened cyber risk, foreign ownership, control or influence risks, governance failures, and supply chain vulnerabilities affecting critical infrastructure operators.

Anchoram Consulting has deep experience supporting owners and operators across the critical infrastructure ecosystem on security governance, operational technology and cyber risk, critical infrastructure compliance, supply chain assurance, risk management, and security uplift programs. From that perspective, the proposed changes are welcomed because they improve the Government's ability to act early, proportionately and with clearer statutory authority where serious national security risks cannot be adequately addressed through existing mechanisms alone.

The consultation paper correctly identifies that the SOCI Act has established a strong baseline for critical infrastructure security, but that practical experience has shown aspects of the current Part 3 framework are difficult to apply in practice, create legal uncertainty, and may delay action where threats are time sensitive. Anchoram supports the Government's objective of refining the framework so that it is agile, operationally robust and legally durable, while preserving safeguards, accountability, consultation requirements, and judicial review.

The proposed package is also welcome because it adopts a more graduated and risk-based intervention model. In practice, critical infrastructure risk treatment often requires a spectrum of tools, beginning with voluntary uplift and existing regulatory obligations, but escalating where governance failures, vendor dependencies, hostile state-linked exposure, or persistent cyber risk remain unresolved. The proposed reforms better reflect that operational reality.

Measure 1

Anchoram strongly supports the proposed amendments to the existing directions power in section 32. The current requirement for the Minister to receive an Adverse Security Assessment and to be satisfied that no other regulatory system could be used to eliminate or reduce the risk can create avoidable delay and procedural contest in circumstances where timely intervention may be necessary to manage material national security risk.

The proposal to replace the existing ASA requirement with a requirement to obtain and have regard to tailored ASIO advice is sensible and proportionate. It preserves the centrality of intelligence advice while allowing the Minister to make a broader national-interest assessment that also considers regulatory, economic, commercial and social factors relevant to any direction. This is particularly important in complex critical infrastructure environments where operational continuity, supply chain realities, and sector-specific regulatory dependencies must be weighed alongside threat intelligence.

Anchoram also supports recalibrating the current "regulatory exhaustion" threshold so the Minister must consider whether other mechanisms could more effectively address the risk, rather than proving that no existing system could do so.

The Trustee for Anchoram Consulting
ABN 85 197 062 817
Level 1, Suite 3, 16 Napier Close
Deakin, ACT 2600
Tel: +61 1300 042 833
www.anchoramconsulting.com.au

This change is practical and necessary. In real-world environments, waiting to exhaust every possible regulatory pathway can create material delay, increase residual exposure, and invite process-focused disputes instead of risk-focused resolution.

The retention of statutory thresholds, proportionality requirements, good-faith negotiation expectations, consultation with affected entities, and judicial review provides an appropriate safeguard set. The additional proposal to expand consultation to relevant Commonwealth Ministers and agencies, while retaining State and Territory consultation requirements, is also supported because it strengthens whole-of-government coordination without undermining the operational utility of the power.

Measure 2

Anchoram welcomes the proposed Conditions Power. The consultation paper rightly identifies that governance and control arrangements, whether foreign or domestic, can create pathways for coercion, interference, compromised decision-making, and weakened compliance with security obligations. These are not theoretical issues; in practice, governance settings, board access, observer rights, privileged personnel arrangements, and cross-border control structures can materially affect the resilience and trustworthiness of critical infrastructure entities.

A dedicated conditions power is preferable to relying on repeated or open-ended use of the general directions power in section 32. The proposed ability to impose tailored, fit-for-purpose, time-bound conditions on matters such as access controls, personnel security, board governance, committee structures, cyber security baselines, segregation of critical systems, and independent audit provides a more precise and proportionate mechanism for managing persistent governance-related risks.

Anchoram particularly supports the paper's recognition that this power should complement rather than duplicate the Foreign Acquisitions and Takeovers Act framework, and that some governance risks may emerge or intensify after an acquisition has occurred. This reflects industry reality. Security risk is not static at the point of investment approval; it can change through board appointments, commercial restructuring, changes in foreign law, vendor substitution, or evolving cyber tradecraft.

The proposed safeguards are also appropriate. Requiring tailored ASIO advice, ministerial consideration of less intrusive options, consultation with entities and relevant ministers, review within 12 months and then at least every 24 months, and the ability for entities to notify material change all help ensure the power remains targeted, reviewable and proportionate over time.

Measure 3

Anchoram strongly supports the proposed power to restrict the use of high-risk vendors, products or services. The consultation paper correctly identifies that the existing section 32 power is not a practical mechanism for addressing systemic vendor or technology risk across multiple entities or an entire sector. In operational technology and enterprise environments alike, systemic dependencies on high-risk vendors can create hidden concentrations of risk that cannot be effectively managed through entity-by-entity engagement alone.

The proposed vendor-risk direction power is welcomed because it would enable coordinated and orderly action where a vendor, product, service or technology presents a material national security risk. Anchoram supports the ability to direct removal, restriction, segmentation, remediation, future procurement bans, and compensating controls where immediate replacement is not feasible. This is consistent with how mature risk treatment should operate in critical infrastructure environments, where transition pathways often need to balance urgency, resilience, interoperability, safety and service continuity.

The Trustee for Anchoram Consulting
ABN 85 197 062 817
Level 1, Suite 3, 16 Napier Close
Deakin, ACT 2600
Tel: +61 1300 042 833
www.anchoramconsulting.com.au

The consultation paper's emphasis on reasonable transition timeframes and consideration of economic, social, reliability and market implications is particularly important and strongly supported.

In sectors such as energy, transport, communications and data services, sudden technology substitution is not always viable due to asset lifecycles, testing demands, safety constraints, outage windows, contractual commitments and limited alternative supply. A framework that enables decisive action while accommodating phased transition and compensating controls is therefore both realistic and necessary.

Measure 4

Anchoram supports the intent of the proposed delayed disclosure reform for high-risk cyber incidents. The consultation paper appropriately recognises that immediate public disclosure in rare cases may undermine coordinated incident response, alert threat actors, expose shared vulnerabilities, or increase systemic risk across interconnected sectors. For critical infrastructure and the supporting digital ecosystem, this is a credible and increasingly relevant problem set.

Anchoram supports a limited, tightly governed, time-bound mechanism that can defer disclosure where public disclosure would threaten national security or public safety. Any such power should remain exceptional, subject to clear thresholds, strong inter-agency coordination, defined expiry periods, and disciplined governance so that it is used only where delay materially supports containment, remediation, and coordinated cross-sector risk reduction.

The options presented in the paper both warrant consideration, but the core policy intent is sound. From a critical infrastructure resilience perspective, the availability of an enforceable mechanism may be necessary in some scenarios to avoid premature disclosure that could compromise defensive operations, especially where incidents involve shared service providers, identity infrastructure, or cascading dependencies across multiple sectors.

Measure 5

Anchoram supports the proposal to increase the maximum civil penalty for non-compliance with a Ministerial direction under Part 3 from 250 penalty units to 2,000 penalty units. The current penalty level does not adequately reflect the seriousness of failing to comply with a direction issued to manage a material national security risk, particularly where non-compliance could have consequences across essential services, economic stability, or public safety.

Alignment with the stronger enforcement settings already operating in Part 2D of the SOCI Act is sensible and promotes consistency across the broader framework. Anchoram agrees that an effective and balanced deterrence regime is necessary, while preserving court discretion and the existing availability of proportionate enforcement tools such as civil penalty proceedings, enforceable undertakings and injunctions.

Implementation observations

While Anchoram supports the reforms, effective implementation will be critical to industry confidence and practical success.

The consultation paper itself recognises the importance of clear legislative design, robust safeguards, and a framework that is easily understood by industry and government alike. That objective should remain central as the reforms progress.

The Trustee for Anchoram Consulting
ABN 85 197 062 817
Level 1, Suite 3, 16 Napier Close
Deakin, ACT 2600
Tel: +61 1300 042 833
www.anchoramconsulting.com.au

In particular, industry would benefit from:

- clear guidance on likely use cases, thresholds and decision factors for each power, especially where material risk, proportionality and reasonable necessity are being assessed.
- practical guidance on consultation expectations, evidentiary standards, and how good-faith negotiation will be demonstrated in urgent and non-urgent contexts.
- implementation guidance, templates and assurance expectations for conditions directions and vendor-related transition planning, including treatment of legacy operational technology and complex outsourced environments.
- clear articulation of how these powers will interact with CIRMP obligations, existing sector regulation, FATA conditions, privacy obligations, corporate governance requirements, and other concurrent reforms referenced in the paper.

Providing this guidance will help ensure that strengthened powers also deliver predictability, consistency and defensibility in application.

Anchoram Consulting welcomes the proposed amendments to the Ministerial Directions powers and supports the reform package as a necessary evolution of the SOCI framework.

Collectively, the five measures improve clarity, agility and precision in the management of serious national security risks, while retaining important safeguards including consultation, proportionality, review mechanisms and judicial oversight.

From Anchoram's experience supporting the critical infrastructure industry, these changes are both appropriate and timely. They better reflect the realities of contemporary critical infrastructure risk, including governance compromise, hostile state-linked influence, systemic vendor dependency, cyber pre-positioning, and the need for calibrated intervention before those risks escalate into serious national harm.

Anchoram would welcome continued engagement as these reforms progress and supports the development of associated guidance to help responsible entities, operators and boards implement the framework in a practical, proportionate and security-focused manner.