Australian Government
Department of Home Affairs

CRITICAL
INFRASTRUCTURE SECURITY
CENTRE

Consultation Paper

Proposed amendments to the Ministerial Directions Powers in Part 3 of the *Security of Critical Infrastructure Act 2018*

Contact us
Enquiries regarding the licence and any use of this document are welcome at:

Critical Infrastructure Security Policy Branch
Department of Home Affairs
PO Box 25
BELCONNEN ACT 2616

Table of Contents

Executive Summary **3**

Proposed Amendments to the Ministerial Directions Powers in Part 3 of the SOCI Act **5**

Measure 1 – Amendments to the existing directions power in section 32 5
Measure 2 – Conditions Power 9
Measure 3 – Restrictions on the use of high-risk vendors, products or services 14
Measure 4 – Delay continuous disclosure requirements 17
Measure 5 – Increased civil penalty provisions 19

Executive Summary

The *Security of Critical Infrastructure Act 2018* (SOCI Act) has laid a strong foundation for safeguarding Australia's most important infrastructure assets. It has significantly strengthened national security and resilience, established a risk-based regulatory framework, and improved partnerships between Government and industry. However, the Government seeks to further strengthen the resilience of our critical infrastructure to external or domestic threats and vulnerabilities as the threat environment is becoming more dynamic, diverse, and degraded. Actors are increasingly willing and able to target, disrupt or destroy critical infrastructure through a range of means, especially cyber.

Foreign ownership, control or influence (FOCI) can create profound systemic vulnerabilities in critical infrastructure when entities or individuals may be compelled to act against Australian interests, including through extrajudicial direction under foreign laws. These risks may enable hostile state actors to leverage access for espionage, sabotage and interference. However, governance weaknesses and coercion risks are not confined to foreign actors. Domestic boards, executives, or service providers can also become compromised through corruption, insider threats, or failure to comply with mandatory security obligations, creating similar pathways for exploitation. Where governance frameworks are insufficient to prevent such coercion or non-cooperation, existing security controls cannot fully mitigate the threat.

These governance risks are compounded by technical and supply chain exposures embedded in the products and services that underpin critical infrastructure. Vendor supply chains often involve opaque ownership structures, vertically integrated operations, and remote management practices that concentrate control in jurisdictions where state direction is legal and routine. These arrangements can embed hidden dependencies and single points of failure, enabling covert access or sabotage through software updates or maintenance functions. These vulnerabilities are not hypothetical; they have been actively exploited by hostile states to gain strategic leverage.

In this environment, reactive measures are not enough. Government must have the tools to act early and decisively to anticipate, prevent, and neutralise threats before they materialise. The Ministerial directions framework in Part 3 of the SOCI Act is a vital component of this toolkit. Since the framework commenced, however, practical experience has demonstrated that while the legislative intent is strong, aspects of the current provisions are difficult to apply in practice. Certain provisions lack clarity, resulting in unintended legal uncertainty, and are cumbersome to enact, potentially delaying the resolution of national security risks. Targeted refinements to the SOCI directions framework are essential to ensure it remains agile and fit-for-purpose in managing serious and cascading risks to national security.

The Government is seeking industry views on a potential package of five targeted measures to enhance the Ministerial directions powers under Part 3 of the SOCI Act. These measures aim to provide greater flexibility and precision in managing serious national security risks to critical infrastructure, while maintaining clear safeguards and accountability. They also respond to previous feedback from industry, including through submissions received on both *Developing Horizon 2 of the 2023–2030 Australian Cyber Security Strategy* and the Independent Review of the SOCI Act, calling for greater clarity on how and when a direction may be used, and what procedural safeguards will apply.

The proposed reforms could:

- Introduce graduated options to more effectively manage serious national security threats to critical infrastructure, including those arising from FOCI risks, malicious cyber pre-positioning, and vendor supply chain risks, before they escalate.
- Embed clear statutory guardrails requiring the Minister to consider a broader range of relevant factors before issuing a direction, including economic, commercial and social impacts, and continue to take reasonable steps to negotiate in good faith with affected entities prior to exercising a direction. These safeguards ensure decisions are proportionate, legally robust, and commercially workable.

- Strengthen cross-government consultation mechanisms to ensure decisions are subject to increased scrutiny, while retaining judicial oversight. Consultation with relevant State and Territory Ministers would continue to be mandatory and consultation with relevant Commonwealth Ministers would be expanded. This approach ensures that powers will only be exercised after exhaustive engagement and careful consideration of all relevant interests, while maintaining a clear focus on robust, defensible decision-making in the national interest.

These refinements aim to ensure Government can intervene decisively when required, while providing clearer expectations for responsible entities and maintaining a framework that is legally robust, operationally practical, and aligned with Australia's national security interests. They reflect the need to act on credible intelligence to address extreme and persistent risks that cannot be delivered through regulatory mechanisms alone. These reforms would ensure Australia's critical infrastructure remains resilient in an era of accelerating geostrategic competition.

To support clarity, coherence and effective implementation, the Government will work closely with the Office of Parliamentary Counsel (OPC) on the most appropriate legislative design for these reforms. Our intent is to ensure that each measure's policy objectives can be achieved, whether through targeted amendments to the existing section 32 directions power or through the creation of new, specific heads of power. We do not hold a fixed preference on the drafting pathway, provided the final design delivers clear authorities, robust safeguards, and a framework that is easily understood by industry and government alike.

For the purposes of consultation, Measures are described separately to draw out the distinct issues they address and to invite specific, granular feedback. This structure does not pre-judge how the powers will ultimately be drafted. Instead, it reflects our commitment to ensuring that the legislative framework supports transparent, proportionate and defensible decision-making, with powers that are appropriately calibrated to the different types of risks they are intended to manage.

Broader Government work to uplift the security of Australia's critical infrastructure will continue alongside this consultation process. This includes consideration of the recommendations made through the Independent Review into the operation of the SOCI Act, amendments to the *Critical Infrastructure Risk Management Program Rules*, amendments to the *Aviation Transport Security Act 2004* (ATSA) and the *Maritime Transport and Offshore Facilities Security Act 2003* (MTOFSA) legislative frameworks, the development of Horizon 2 of the *2023-2030 Australian Cyber Security Strategy*, and considerations to streamlining and strengthening the foreign investment framework (led by Treasury). These processes are out of scope for this paper but will remain aligned to ensure a coherent and consistent national security framework.

Proposed Amendments to the Ministerial Directions Powers in Part 3 of the SOCI Act

Measure 1 – Amendments to the existing directions power in section 32

The issue

Section 32 of the SOCI Act is intended to enable Government to manage national security risks by issuing a direction to a reporting entity for, or an operator of, a critical infrastructure asset to do or refrain from doing an act or thing, if satisfied that there is a risk of an act or omission that would be prejudicial to 'security' (as defined in the *Australian Security Intelligence Organisation Act 1979* (ASIO Act)).

In practice, the current formulation of section 32 imposes procedural and legal requirements that can make the power difficult to use, particularly in response to time-sensitive threats. Relevantly, two of the current pre-conditions to the exercise of the general directions power are that:

- the Minister for Home Affairs must have received an Adverse Security Assessment (ASA) in respect of the relevant entity from the Australian Security Intelligence Organisation (ASIO), and
- the Minister must be satisfied that no existing regulatory system of the Commonwealth, a State or a Territory could instead be used to eliminate or reduce the security risk.

These two guardrails were designed to ensure restraint, legitimacy and coherence across the SOCI framework. The ASA was intended to anchor the ability to direct an entity to a single, well-understood security threshold that provided an independent, high-bar assessment of prejudicial risk, and ensured sensitive intelligence would be handled within established processes. The regulatory exhaustion pre-condition was included to avoid duplication or conflict and preserve comity with state and territory schemes, and to provide reassurance to industry that the SOCI powers would be used as a last resort rather than a first-instance intervention.

In practice, however, these guardrails in their current form have led to a range of challenges that inhibit the power's effective use:

- For a security assessment to constitute an 'ASA', it must contain both advice on a security issue and a recommendation that a specific action be taken on security grounds. While the Director-General of Security is best placed to provide advice on threats to security, determining what action should be taken in the SOCI context often requires balancing those risks against broader regulatory, economic, commercial and policy considerations. In these circumstances, it may be more appropriate for this decision to be made at the ministerial level, informed by broader departmental advice. The ASA framework can also limit flexibility by requiring a definitive adverse finding before advice and recommendations can be issued, which may frustrate timely intervention.
- Similarly, the existing requirement for the Minister to be satisfied that no existing regulatory systems of the Commonwealth, a State or a Territory could instead be used to eliminate or reduce the risk before issuing a direction as a legal bar creates unnecessary delay when action is required to manage a material risk to security. In practice, this test invites legal and procedural argument about process rather than outcomes, particularly where multiple regulators are involved, and creates a crutch for bad faith actors to lean on through protracted litigation.

What we propose

The Government is considering targeted amendments to section 32 of the SOCI Act to improve clarity, operability and timeliness, while maintaining existing safeguards. The proposed amendments would:

- **Replace the existing ASA requirement**: Repeal the existing requirement for the Minister to have been given an ASA in respect of the relevant entity and replace with a requirement for the Minister to

obtain, and have regard to, advice from ASIO for the purposes of exercising the relevant directions power.

  - The proposed shift from an ASA requirement to tailored ASIO threat advice reflects practical experience that the current Part IV security assessment framework can delay action in time-sensitive circumstances. The intent is not to reduce the role of intelligence advice but to ensure the Minister receives timely, fit-for-purpose threat assessments that support proportionate and defensible decision-making. The Minister would continue to rely on strong intelligence inputs, and decisions would continue to be subject to judicial review and statutory safeguards.
  - While the measure introduces greater flexibility in the form of intelligence advice the Minister may rely upon, it does not lower the standard the Minister must meet. The Minister would remain required to be satisfied that a material risk exists and that a direction is reasonably necessary and proportionate. These statutory tests continue to provide a high threshold and maintain strong accountability for the use of the power.

- **Introduce a limited carve-out from the prescribed administrative action framework**: Insert a new subsection 35(1B) in the ASIO Act to provide that any decision made under Part 3 of the SOCI Act – inclusive of those proposed in Measures 1–3 – that is directed at a legal person[1] is not prescribed administrative action.
  - This would allow ASIO to provide tailored advice outside the Part IV security assessment framework (i.e. ASAs and qualified security assessments (QSAs)) and aligns with existing carve-outs for decisions made under the *Foreign Acquisitions and Takeovers Act 1975* (Cth) (FATA) or regulations under that Act.
  - Where a proposed direction is issued to a natural person, ASIO advice would be provided in the form of an ASA or QSA to preserve notice and review rights under the ASIO Act. This safeguard is intended to apply to decisions directly affecting an individual's legal rights or obligations, including where a direction imposes requirements on a specific natural person. Impacts that flow indirectly from business or commercial decisions would not typically enliven this safeguard. Procedural fairness obligations will also apply to these security assessments.
  - Advice from ASIO would form a central component of the Minister's overall national-interest assessment alongside other relevant inputs from across government.
- **Recalibrate the 'regulatory exhaustion' requirement**: the Minister must consider whether other regulatory mechanisms could more effectively address the identified risk before issuing a direction, rather than being required to be satisfied that no existing regulatory systems could instead be used to eliminate or reduce the risk.

The Minister would continue to only be able to issue a direction if satisfied the direction is reasonably necessary for the purposes of managing the risk, and that reasonable steps have been taken to negotiate with the entity in good faith to achieve the outcome of eliminating or reducing the risk without a direction being given. The additional considerations set out in subsection 32(4) of the SOCI Act and requirements to consult with the affected entity set out in section 33 would remain unchanged beyond any necessary consequential amendments.

The proposed measure would also expand consultation requirements to ensure that relevant Commonwealth Ministers and agencies for an affected industry sector must be consulted before any Part 3 power is used. Existing State and Territory consultation requirements would also be retained.

The desired result is a directions power that is legally durable and operationally robust, while ensuring decisions are informed by security advice but not limited to it. The amendments would allow the Minister to

[1] For the purposes of this paper, 'legal person' means a body corporate (whether or not formed or carrying on business in Australia), a body politic (whether or not an Australian body politic), a partnership (whether or not formed in Australia), a trust (whether or not created in Australia), or an unincorporated foreign company.

weigh all relevant factors, including economic, commercial, social and regulatory considerations, alongside national security risks, so that responses are proportionate, defensible and aligned with whole-of-government objectives.

The Minister's decision to issue a direction would be subject to judicial review.

Directions issued under Part 3 would not be legislative instruments and would not be published. This reflects the sensitive nature of the risks being managed and is intended to avoid exacerbating national security or commercial impacts. Where entities choose to make disclosures required under other laws, they may reference a direction where legally necessary and consistent with protected information-handling obligations under the SOCI Act.

Consultation Questions – Regulatory Impact and Policy Design

Scenario:[2]

A major data storage/processing provider that services multiple critical infrastructure assets utilises an offshore managed service provider with links to a foreign state-owned enterprise. The Government has worked with the entity to improve and increase security around access controls and personnel hazards, but engagement stalls and privileged access pathways remain exposed. Based on whole-of-government advice, the Minister has determined the residual national security risk remains unacceptable. The Minister directs the provider to migrate privileged access functions back to Australia within a defined period and implement independent assurance of identity and access management. The direction follows extensive unsuccessful attempts to negotiate voluntary mitigation steps.

What this could look like for your organisation:

A Ministerial direction could require you to relocate high-risk system access functions to a secure Australian-based operating environment, strengthen identity and access management controls, and increase transparency over subcontracting arrangements and personnel security assurance measures. The direction would set outcomes and milestones, but allow flexibility in how you meet them, maintaining continuity of operations while reducing national security risk.

Questions:

Please answer as many questions as are relevant to your organisation. Provide short, factual responses, noting assumptions and any data limitations. It is noted that may be challenging to quantify the impact of these proposed changes without specific details of what may be directed in future under these proposed changes. Therefore, you may choose to identify several potential hypothetical directions that you consider may be issued under this proposed change to answer realistically.

How this compares to what you do now

1. How closely does the scenario align with how similar risks or dependencies are managed within your organisation? If not, what key differences would apply?

Options and feasibility

2. Relative to maintaining the status quo, what non-regulatory or lighter-touch approaches (e.g., guidance, independent assurance, contractual undertakings) could reasonably achieve a similar outcome in your context? Briefly rate feasibility and expected effectiveness.

Implementation steps and timeframes

3. What internal steps and approvals would be needed to implement a direction of this kind (e.g., architectural changes, data/operational technology (OT) segregation, replacement of physical components, supplier re-papering, governance)?

[2] The scenarios described in this paper are illustrative only and are intended to demonstrate how the proposed powers could operate in practice. They do not represent the full range of potential use cases, threat types, or risk profiles that may warrant the imposition of a direction, nor do they limit the circumstances in which such a power could be exercised.

4. What is a realistic implementation timeline by milestone (e.g., design, procurement, migration, cut-over) while maintaining service continuity? Identify the top three schedule drivers (e.g., change windows, supplier lead times).

Benefits and risk-reduction

5. What operational or risk-reduction benefits would you expect from implementing the direction (e.g., reduced likelihood of privileged compromise, improved mean time to detect/contain, fewer exception pathways)? Please indicate any available internal metrics (even if approximate).

Costs and constraints

6. What one-off activities would drive effort/cost (e.g., migration, tooling uplift, legal re-papering)? What ongoing activities would persist (e.g., monitoring, periodic assurance)? (You may provide numbers separately if you prefer.)
7. Are there operational, contractual or technical impediments that would materially affect how you could comply (e.g., vendor lock-in clauses, specialised OT equipment, data residency constraints)?

Board, governance and legal interfaces

8. What board-level processes or approvals would you expect to trigger (e.g., risk acceptance thresholds, major capex approval, change of risk appetite)?
9. For corporate entities: Are there any legal or compliance interfaces under the Corporations Act that would need to be managed to comply with a direction (such as continuous disclosure, related-party approvals, conflicts management, or director duty considerations)? What guidance from Government would assist your board/company secretary to document compliance?

Market, customers and cumulative effects

10. Would compliance have any material impacts on customers, prices, or service quality during transition? Are there cumulative burden issues when combined with other obligations (e.g., CIRMP, privacy, sectoral rules)?

Evaluation and support

11. What success indicators (e.g., control maturity, reduction in privileged access exceptions, incident metrics) would show the direction achieved its objective in your context? What support or guidance from Government would help (e.g., reference architectures, assurance templates)?

Measure 2 – Conditions Power

The issue

Board and executive governance arrangements in critical infrastructure, whether foreign or domestic, can create pathways for coercion, interference, or compromise that elevate national security risk. These vulnerabilities arise when individuals in positions of trust, such as directors or senior officers, are compromised or subject to undue influence through coercion, extrajudicial direction, conflicts of interest, or other relationships. With privileged access to sensitive systems, information, and decision-making processes, such individuals can obstruct compliance with security obligations, weaken controls, or influence strategic procurement and operational decisions in ways that materially degrade the security and resilience of essential assets. If left unmanaged, these risks can escalate into serious harm to Australia's national security.

While section 32 provides a general directions power, it lacks legal specificity and the flexibility to impose tailored, ongoing governance controls. Using section 32 to manage persistent governance risks could require repeated or open-ended directions, creating uncertainty for industry and operational inefficiency for Government. By contrast, a dedicated conditions power offers clearer legislative intent and a more proportionate mechanism for managing serious governance-related risks. It enables conditions to be precisely scoped to the identified threat, supported by statutory safeguards such as mandatory consultation and a defined list of factors the Minister must consider before acting. This approach provides greater predictability for industry, ensures decisions are legally defensible, and avoids the blunt application of a general power where a more targeted tool is appropriate.

The power is intended to operate as part of a graduated escalation pathway, beginning with regulatory compliance through the Critical Infrastructure Risk Management Program (CIRMP) obligations and voluntary engagement, then moving to tailored conditions where risks persist.

Interactions between this measure and the FATA

This measure is not limited to managing foreign ownership risks. It applies to governance and control risks regardless of origin, including circumstances where domestic actors are compromised or where boards fail to cooperate with mandatory security obligations. It is not intended to override or duplicate the existing FATA approval and conditions framework for foreign investment. The powers under FATA to manage foreign ownership, control or influence risks are limited to specific circumstances. The Treasurer can apply conditions at the time of certain 'actions' covered by the legislation, which can assist in mitigating risks from high-risk ownership. However, practical experience shows that some risks emerge or intensify post-acquisition – for example, changes in foreign law, appointment of new directors, or evolving cyber tradecraft – which may not be adequately addressed by these existing frameworks alone.

This reform does not change the operation of FATA but is designed to complement it. Under the FATA, the Treasurer will continue to assess the need for conditions at the point of approving an acquisition, while this measure will address governance risks that arise after a transaction has occurred. The Minister would consult across government to ensure responses are coordinated, consistent, and operationally viable, and to avoid duplication or conflict. This would include where a SOCI-related risk intersects with existing FATA conditions. For entities regulated under both SOCI and FATA, arrangements would be established to determine which legislative action should be taken, noting that some circumstances may enliven action under both frameworks.

This measure will also be developed with consideration to proposed FATA reforms also under development to ensure alignment and clarity for industry.[3]

What we propose

The proposed amendment would enable the Minister to impose targeted, fit-for-purpose conditions on reporting entities where ownership, control, or governance arrangements create a material risk to national

[3] Foreign investment framework reforms – discussion paper | Treasury.

security that cannot be sufficiently mitigated through existing regulatory obligations or voluntary measures. This power is intended to operate in a proportionate and risk-specific manner, and only where other levers are insufficient to address the identified concern. Conditions imposed under this mechanism would depend on the nature of the risk and the operational context of the asset. Illustrative examples include:

Access, information-handling, and personnel security controls

- Role-based controls limiting access to sensitive systems, data, or operational technologies.
- Security vetting requirements for defined roles.
- Information-handling controls with access to sensitive operational security-related information restricted to specified roles or personnel with demonstrated need-to-know.

Board, governance and decision-making safeguards

- Targeted voting exclusions or restrictions for decisions that materially affect the security posture of the asset (e.g., procurement, network architecture, operational arrangements, or high-impact financial decisions linked to resilience of the asset).
- Requirements relating to board composition, such as a minimum number of independent, Australian security-cleared directors.
- Establishment of an independent security risk committee responsible for oversight of cyber, operational technology, physical-security and supply-chain risks.

Cyber security baselines and uplift

- Requirements to implement specified cyber-security baseline controls, such as privileged-access management, continuous monitoring and logging, network segmentation, and secure remote-access arrangements.
- Mandatory incident-response planning and exercising, including vulnerability assessments and cyber-security drills.
- Mandated segregation of critical systems, networks, logs, or sensitive data from parent-company or shareholder environments, including prohibitions on offshore access, support, or administration for critical systems.

Transparency, oversight and audit

- Requirements to notify the regulator of Board resolutions or organisational changes that materially affect the entity's security posture.
- Periodic independent audit and reporting obligations designed to provide transparency and accountability over compliance with imposed conditions, CIRMP implementation, information handling practices, and insider risk controls.

Conditions would be tailored, time-bound, and constrained to the minimum necessary to mitigate the identified risk. The Department of Home Affairs would be responsible for monitoring and evaluating adherence to any imposed conditions. Non-compliance with an imposed condition would be managed through the existing enforcement framework in Part 5 of the SOCI Act. These provisions enliven monitoring, investigation and civil penalty provisions under the *Regulatory Powers (Standard Provisions) Act 2014*, enabling the Government to seek civil penalty orders and take other proportionate enforcement action where required.

In determining whether a material risk exists that could justify issuing a condition direction, the Minister would need to obtain and have regard to tailored, entity-specific security-threat advice from ASIO (as per Measure 1). This advice would be considered together with other relevant inputs from across government to inform the Minister's overall national-interest assessment. A condition direction would only be available where a material risk that threatens the operation, availability, integrity or security of the asset has been identified, and the Minister is satisfied the risk presents a threat to national security.

To ensure confidence and avoid regulatory duplication, the Minister would be required to have regard to a range of factors as safeguards before giving a direction, including:

- How sensitive the asset is and the likely consequences if it were compromised.
- Whether less intrusive measures are available and would effectively reduce or remove the risk.
- The views and evidence provided by the entity and consultation with any relevant Ministers and agencies.
- Whether an existing Commonwealth, State, or Territory regime could more effectively address the identified risk.

The Minister must be satisfied that issuing a conditions direction is reasonably necessary to mitigate or eliminate the risk, and that good-faith efforts have been made to negotiate a voluntary solution with the affected entity or individual before a direction is given.

Where conditions relate to governance or board-level processes, the Minister would consider the interaction with directors' duties under the Corporations Act to avoid unnecessary duplication or inconsistency. Entities would also be able to provide representations on governance impacts as part of the consultation process.

It is proposed that the Minister would be required to cause the direction to be reviewed within 12 months after it is given, and thereafter at least every 24 months, to consider whether the direction remains reasonably necessary to mitigate or eliminate the risk. Following each review the Minister could revoke, vary or continue the direction, or cause it to lapse if a decision is not made within a reasonable period of initiating the review. A reporting entity could also notify the Minister of any material change relevant to the risk that is mitigated by the direction. On receiving a notice of material change from the entity, the Minister would need to cause a review of the direction to be undertaken.

The Minister's decision to issue a direction would be subject to judicial review.

Directions issued under Part 3 would not be legislative instruments and would not be published. This reflects the sensitive nature of the risks being managed and is intended to avoid exacerbating national security or commercial impacts. Where entities choose to make disclosures required under other laws, they may reference a direction where legally necessary and consistent with protected information-handling obligations under the SOCI Act.

Consultation Questions – Regulatory Impact and Policy Design

Scenario:

A major cloud services provider that is a critical infrastructure entity under the SOCI Act enters a commercial arrangement with a foreign venture capital fund. Under the agreement, the fund receives a board observer right with access to relevant committee papers. In accordance with SOCI Act Part 2A, the Board is required to approve the entity's Critical Infrastructure Risk Management Program (CIRMP), which contains detailed cross-domain vulnerabilities (physical, cyber, personnel, and supply chain), security architecture diagrams, incident response dependencies, and prioritised remediation plans.

The fund is linked to a foreign state-owned enterprise that is subject to extrajudicial direction under foreign intelligence or national security laws. Government engagement seeks to limit access to security-sensitive materials, but the provider declines, citing investor rights and contractual undertakings. The national security risk remains unresolved.

The foreign-affiliated observer obtains access to the full CIRMP documentation and exfiltrates content. Because foreign compulsion laws can require individuals to cooperate with foreign intelligence agencies, the sensitive material (an aggregated, high-value map of the entity's weaknesses) is at real risk of use for espionage, sabotage, coercion, or targeting (including impacts that could degrade grid reliability, cloud availability, or national security functions). The risk persists even where there is no compromise of IT systems, as the access is legitimate from a corporate governance perspective.

What this could look like for your organisation:

If a board observer or investor representative continued to access sensitive strategic or cyber security information despite unresolved FOCI concerns, the Minister could impose governance-related conditions requiring:

- limited access to defined categories of material (e.g., classified CIRMP annexes only on a need-to-know basis)
- restructured committee participation, including a security-cleared Security Risk Committee independent of foreign-affiliated directors/observers
- independent oversight, including external assurance of CIRMP handling and insider-risk controls, and/or
- ring-fencing of critical systems and data, including prohibitions on offshore access, support, or administration.

Questions:

Please answer as many questions as are relevant to your organisation. Provide short, factual responses, noting assumptions and any data limitations.

How this compares to what you do now

1. How closely does the scenario align with how similar governance or control risks would manifest in your organisation? If not, what key differences would apply?

Options and feasibility

2. Relative to maintaining the status quo, what non-regulatory or lighter-touch approaches could reasonably achieve a similar outcome in your context (e.g., revised observer protocols, targeted NDAs, committee charter changes, information segregation, independent assurance)? Briefly rate feasibility and expected effectiveness.

Implementation steps and timeframes

3. What internal steps and approvals would be needed to implement governance-focused conditions (e.g., board/committee resolutions, constitution or shareholder agreement changes, access control changes, security vetting for defined roles, independent audit engagement)?
4. What is a realistic timeline by milestone (e.g., design of safeguards, approvals, contracting, rollout) while maintaining continuity of operations? Identify the top three schedule drivers (e.g., shareholder approvals, meeting cycles, vetting lead times).

Benefits and risk-reduction

5. What governance or risk-reduction benefits would you expect from implementing the conditions (e.g., reduced likelihood of undue influence over security-sensitive decisions, lower exposure of sensitive materials, improved audit findings)? Please indicate any available internal metrics (even if approximate).

Costs and constraints

6. What one-off activities would drive effort/cost (e.g., legal re-papering, charter/constitution changes, access model redesign, onboarding independent directors/committee members, vetting)? What ongoing activities would persist (e.g., additional committee oversight, periodic independent assurance, access monitoring)? (You may provide numbers separately if you prefer.)
7. Are there operational, contractual or technical impediments that would materially affect how you could comply (e.g., investor rights clauses, listing rule obligations for committees, identity/access tooling limits)?

Board, governance and legal interfaces

8. What board-level processes or approvals would you expect to trigger (e.g., committee restructuring, conflicts management protocols, risk appetite changes)?
9. For corporate entities: Are there any legal or compliance interfaces under the Corporations Act and related frameworks that would need to be managed to comply with conditions (such as director duties, related-party considerations, changes to constitutions, or disclosure obligations)? What guidance from Government would assist your board/company secretary to document compliance?

Market, customers and cumulative effects

10. Would compliance have any material impacts on customers, prices, service quality or investor relations during transition? Are there cumulative burden issues when combined with other obligations (e.g., existing FATA conditions, CIRMP, Protective Security Policy Framework (PSPF), sectoral rules)?

Evaluation and support

11. What success indicators (e.g., reduction in access to sensitive materials by observer roles, improved independence in security-sensitive decisions, audit outcomes) would show the conditions achieved their objective in your context? What support or guidance from Government would help (e.g., template conditions, model committee charters, sample access matrices, assurance templates)?

Measure 3 – Restrictions on the use of high-risk vendors, products or services

The issue

Critical infrastructure increasingly depends on complex, globally integrated supply chains. Vendors, whether foreign or domestic, often provide cloud services, operational technology, communications hardware, and managed services with privileged access to sensitive systems. Where vendors operate under or are subject to foreign laws that allow extrajudicial direction, have opaque ownership or governance structures, or are based in jurisdictions assessed as high-risk for coercion or interference, they can introduce persistent and potentially systemic national security risks to critical infrastructure.

These concerns underpinned previous decisions to apply the Protective Security Policy Framework (PSPF) to direct Commonwealth entities to not utilise certain products and web services in their networks, and to identify indicators of FOCI risk as they relate to procurement and maintenance of technology assets and appropriately manage and report those risks.

The existing directions power in section 32 is designed to manage risk at the level of an individual entity. It is not a practical mechanism for addressing systemic vendor or technology-related risks that affect multiple entities or an entire sector. Where coordinated mitigation is required across an asset class, sector, or supply chain, the current framework is too narrow and operationally inefficient to provide a timely or consistent response to multiple entities at once.

What we propose

The Government is considering a vendor-risk direction power to enable coordinated action where a specific vendor or its products, equipment, services or technologies, presents a material risk to national security. This power would ensure systemic supply chain vulnerabilities can be managed consistently across affected critical infrastructure entities and sectors. The new power would:

- Allow the Minister to issue targeted, risk-based directions to responsible entities, either individually or by class, where a vendor or technology dependency creates a material national security risk.
- Enable coordinated and orderly removal, remediation or restriction of products, equipment, services or technologies, or the implementation of compensating security controls where immediate removal is not feasible.
- Include a requirement to consider reasonable transition timeframes to minimise operational and contractual impacts.

The power would permit analogous types of directions against a vendor, product, equipment, technology or service as enabled under the PSPF or the comparable vendor directions power within the United Kingdom's *Telecommunications (Security) Act 2021*.

Examples of directions that could be issued include:

- Cease using a specified product or service by a defined date.
- Isolate, segment, remove or remediate identified technologies.
- Refrain from procuring identified equipment in the future.
- Implement compensating controls (e.g. architecture segregation, enhanced logging and monitoring, code-integrity assurance, software bill-of-materials and supplier assurance, uplifted access controls, and independent verification and audit).

A direction would only be considered where the Minister has determined that the vendor, product, service or technology poses a material risk that is prejudicial to national security and cannot be adequately mitigated through other measures. Before issuing a direction, the Minister must be satisfied that issuing a direction is necessary to mitigate or eliminate the risk.

In determining whether and how to issue a direction, the Minister must also consider:

- Any material economic or social implications of the direction (this could include, but would not be limited to, reasonably foreseeable impacts on markets, supply chains and end users, and competition impacts, including whether it would confer an unfair commercial advantage, or disproportionately burden one or more entities).
- Any material implications for the availability or reliability of the asset, or for connected assets or systems, including circumstances where replacement technologies or services may not provide like-for-like functionality
- Representations from affected entities and consultation with any relevant Minister and agency.

Affected entities would be consulted wherever reasonably practicable. Where a direction applies to a large class of entities, consultation processes may be tailored to ensure timely and efficient engagement.

Consultation Questions – Regulatory Impact and Policy Design

Scenario:

It is identified within a specific sector that a widely deployed brand of network switches and routers includes an undocumented remote access capability that routes traffic through infrastructure located in a foreign jurisdiction subject to national security laws that are hostile towards Australia's interests. The vendor refuses to allow independent verification of the firmware and does not provide a credible technical explanation for the remote function. Government issues security guidance and engages with the sector to encourage transitioning away from the equipment, but uptake remains inconsistent due to vendor lock-in, limited alternative supply, and commercial upgrade cycles. Security advice concludes that entity-level risk management cannot reliably mitigate the exposure, and the risk is systemic across the sector.

What this could look like for your organisation:

If specified high-risk equipment posed a persistent access risk that could not be mitigated by individual entities, a Ministerial direction could restrict further procurement or deployment of the equipment across the sector, with a phased transition plan and reasonable timeframes to avoid service disruption.

Where immediate removal is not possible, compensating controls (e.g., segmentation, enhanced logging/monitoring, code-integrity assurance, SBOM/supplier assurance, uplifted access controls, independent verification and audit) may be required during transition.

Questions:

Please answer as many questions as are relevant to your organisation. Provide short, factual responses, noting assumptions and any data limitations. It is noted that may be challenging to quantify the impact of these proposed changes without specific details of what may be directed in future under these proposed changes. Therefore, you may choose to identify several potential hypothetical directions that you consider may be issued under this proposed change to answer realistically.

How this compares to what you do now

1. How would a vendor-specific restriction of this kind interact with your current technology stack, procurement cycles, network/OT architecture, and operational processes? Are there key differences from the scenario that would affect implementation?

Options and feasibility

2. Relative to maintaining the status quo, what non-regulatory or lighter-touch approaches could reasonably achieve a similar outcome in your context (e.g., strengthened sector guidance, an industry code with independent audit, Government procurement restrictions only, enhanced vendor due-diligence/assurance)? Briefly rate feasibility and expected effectiveness.

Implementation steps and timeframes

3. What internal steps and approvals would be required to comply (e.g., asset inventory and criticality mapping, replacement program planning, network redesign/segmentation, firmware validation, contract variations or re-tenders, outage/change windows, customer communications)?
4. What is a realistic timeline by milestone (e.g., design/validation, procurement, lab and integration testing, staged deployment, decommissioning) that maintains service availability and resilience? Identify the top three schedule drivers (e.g., supply constraints, interoperability testing, regulatory dependencies).

Benefits and risk-reduction

5. What security or resilience benefits would you expect (e.g., reduction in privileged/remote access pathways, lower probability of systemic compromise, improved detectability/forensics, reduced attack surface across interdependent assets, reduced mean-time-to-detect anomalies due to standardised telemetry)? Please indicate any available internal metrics (even if approximate).

Costs and constraints

6. What one-off activities would drive effort/cost (e.g., equipment replacement or remediation, redesign and testing, contract modifications, data migration, workforce upskilling)? What ongoing activities would persist (e.g., compensating controls, enhanced monitoring/telemetry, periodic independent assurance)? (You may provide numbers separately if you prefer.)
7. Are there operational, contractual, supply-chain or technical impediments that could materially affect your ability to comply (e.g., vendor lock-in, limited comparable technologies, third-party dependencies, integration with legacy OT)?

Board, governance and legal interfaces

8. What board-level processes or approvals would you expect to trigger (e.g., major capex approvals, risk appetite changes, write-down decisions, customer notification strategies)?
9. For corporate entities: Are there any legal or compliance interfaces under the Corporations Act and related frameworks that would need to be managed to comply with a vendor-restriction direction—such as continuous disclosure, asset impairment disclosures, or directors' duty considerations in balancing transition risk and service continuity? What guidance from Government would assist your board/company secretary to document compliance?

Market, customers and cumulative effects

10. What are the likely market and competition implications (e.g., near-term vendor concentration, price effects, supply constraints, interoperability impacts) during transition? Would compliance have material impacts on customers, prices or service quality? Are there cumulative burden issues alongside other obligations (e.g., CIRMP, privacy, sectoral rules)?

Evaluation and support

11. What success indicators would demonstrate the direction achieved its objective in your context (e.g., % removal or remediation by milestone, reduction in high-risk remote access paths, incident/near-miss trends, independent verification results)? What support or guidance from Government would help (e.g., reference architectures, interoperability/segmentation patterns, minimum telemetry/assurance requirements, SBOM formats, model contract clauses)?

Measure 4 – Delay continuous disclosure requirements

The issue

Cyber security incidents affecting Australian businesses are becoming more sophisticated and may have national-security or public-safety implications. While continuous disclosure obligations promote transparency and well-functioning markets, immediate disclosure in rare, high-risk cyber incidents may inadvertently undermine coordinated responses, reveal vulnerabilities, or heighten systemic risks.

Currently, there is no mechanism used by the Australian Securities and Investments Commission (ASIC) or available to the Government to temporarily delay disclosure solely to prevent broader harm. The Government is considering a limited, time-bound power to delay an entity's disclosure obligations under the *Corporations Act 2001*.

The intent is not to shield entities from commercial impacts, but to prevent disclosure from compromising national security including significant flow-on impacts across the economy. Similar powers exist internationally, including in the United States.[4] The Government seeks stakeholder input on the need, scope, safeguards, and impact of this proposed reform.

What we propose

The Government is considering two options.

Under both options the threshold for using the power would be the same – whether the public disclosure of a cyber security incident would threaten Australia's national security or public safety. A number of safeguards are being considered including strict time limitations; delays in relation to all or part of the information to be disclosed; notification requirements by the entity to government while a delay is in progress; consultation requirements; the ability to revoke a delay previously provided to an entity prior to its expiration; and consideration of interactions with any other regulatory regimes the entity may be subject to, including the notifiable data breaches scheme in the *Privacy Act 1988* (which has its own regime related to exemption from reporting notifiable data breaches where appropriate).

Option 1

Section 111AT of the Corporations Act grants ASIC the power to exempt entities from disclosure obligations under the Corporations Act. This exemption can be used either unconditionally or subject to specified conditions, such as being subject to specific timeframes. This existing power allows ASIC to manage unforeseen or special circumstances on a case-by-case basis. Currently, exemptions must be published in the ASIC Gazette.

Section 111AT of the Corporations Act applies to all disclosing entities. Therefore, this power would apply to a broad cohort of entities but would not place a positive, enforceable obligation on the entity to not disclose the information.

ASIC and the Government would establish guidance with industry that outlines how section 111AT could be used to delay an entity's disclosure obligations if the threshold for use of the power was met, and processes to support ASIC to discharge its power in these circumstances.

Option 2

Insert a new directions power into the SOCI Act to allow the Minister for Home Affairs to direct an entity to not publicly disclose the existence of the cyber incident for a prescribed period.

If a direction is made, an entity would be legally required to comply with it. The existence of the direction would enliven an exemption from continuous disclosure obligations under the ASX Listing Rules on the basis it would be a breach of law to disclose the information.

The power would be limited to entities that are captured under the SOCI Act.

---

[4] United States Department of Justice, Material Cybersecurity Incident Delay Determinations

Consultation Questions – Regulatory Impact and Policy Design

Scenario:

A publicly listed operator and SOCI Act-captured entity that hosts cloud and colocation services for government agencies, financial institutions, and large corporates, detects a potential cyber intrusion within its privileged access management systems. The affected environment supports identity and access functions for numerous tenants, including several operators of critical infrastructure assets.

The company investigates the potential compromise which reveals that the intrusion bears hallmarks of a highly capable state-backed threat actor, including advanced tradecraft designed to move laterally across client environments without immediate detection. It engages the Australian Signals Directorate's (ASD) Australian Cyber Security Centre (ACSC) for technical advice and support.

While the entity has contained the attacker's initial foothold, evidence is identified suggesting that the malicious actor has attempted to harvest authentication tokens used by several interconnected tenants, including operators in the aviation, banking, and energy sectors. Preliminary advice indicates a real possibility that premature public disclosure such as through the entity's continuous disclosure obligations could, among other things:

- Alert the threat actor their activities are known, thereby accelerating their activities before remediation can be completed.
- Encourage opportunistic attackers to exploit similar identity related vulnerabilities shared across other Australian data storage and processing assets, including those used by the Government and critical infrastructure.
- Disrupt migration efforts underway with ASD and making detection of the actor's activities against other entities more difficult.

Following the initial period of analysis, the entity determines it would need to make a public disclosure in accordance with the Corporations Act and ASX Listing Rules. Government advises that a premature public announcement could create material national security and systemic economic risks, including potential unauthorised access to sensitive government workloads and cascading disruptions across multiple industries relying on hosted systems.

Under the proposed options, ASIC or the Minister for Home Affairs could delay the entity's disclosure obligations for a limited period, for example, 30 days. This temporary delay would enable:

- Completion of cross-tenant remediation and token revocation.
- Hardening of identity infrastructure across other data centre operators facing related vulnerabilities.
- Coordination with impacted aviation, banking and energy operators to ensure continuity of essential services.
- Preparation of a controlled, accurate public communication once systemic risks were mitigated.

Questions:

Answer as many questions as are relevant to your organisation. Provide short, factual responses, noting assumptions and any data limitations. In your response, please indicate whether you are a Listed company or other disclosing entity captured under Chapter 6CA of the *Corporations Act 2001* and must comply with continuous disclosure requirements.

1. Is a delayed disclosure power necessary in high-risk cyber incidents, and what types of disclosure obligations (under the Corporations Act or otherwise) should it cover?
2. In the above scenario, would section 111AT (Option 1) be sufficient to prevent an entity disclosing the cyber incident or would the entity require a direction under SOCI (Option 2) to prevent disclosure? Why?

3. Are there any non-legislative disclosure obligations (e.g., contractual requirements during capital raisings or major transactions) that could prevent or undermine a delayed Corporations Act disclosure?
4. Who should hold the power to delay disclosure (ASIC, the Minister for Home Affairs, or both)?
5. What criteria should govern when a delay can be issued?
6. What safeguards, time limits, and oversight mechanisms are needed while still enabling effective risk management?
7. What operational or compliance impacts might arise during a delay?
8. What guidance, tools, or support would entities need to meet their obligations under this power, and how should the market be informed once a delay is lifted?
9. Are there relevant international practices that should inform the model, and what unintended consequences should be considered?

Measure 5 – Increased civil penalty provisions

The issue

Under Part 3 of the current SOCI Act, failure to comply with a Ministerial direction carries a maximum civil penalty of 250 penalty units. This penalty level does not reflect the significance of a direction issued to manage a material risk to national security. It also creates inconsistency between equivalent obligations under Part 2D of the SOCI Act, which attract substantially higher penalty settings. The current penalty does not provide a credible compliance incentive in circumstances where a failure to comply could have serious national security consequences.

What we propose

The Government is seeking views on increasing the maximum civil penalty for non-compliance with a Ministerial direction under Part 3 to 2,000 penalty units, aligning it with the enforcement framework already operating in Part 2D of the SOCI Act for carriers and carriage service providers.

Restoring an effective and balanced deterrence regime across asset classes ensures that all entities are sufficiently motivated to comply. Importantly, the courts' discretion to calibrate penalties to the misconduct's magnitude and circumstances is preserved. This change would be accompanied by guidance to industry on expectations for compliance with directions and would apply prospectively. Existing enforcement tools (civil penalty proceedings, enforceable undertakings, and injunctions) would remain available, ensuring proportionate and graduated responses to non-compliance.

Consultation Questions – Policy Design

1. Does the proposed increase in the maximum civil penalty (from 250 to 2,000 penalty units) provide an effective deterrent to non-compliance with Ministerial directions under Part 3 of the SOCI Act? Why or why not?
2. What level of penalty would you consider proportionate to the seriousness of failing to comply with a direction issued to manage a material national security risk?
3. Are there alternative mechanisms, in addition to or instead of increased penalties, that could more effectively encourage timely and complete compliance with Ministerial directions?
4. What guidance or support would assist your organisation to understand and meet compliance expectations under an updated penalty framework?
5. Do you foresee any unintended consequences of increasing the maximum penalty to 2,000 penalty units (e.g., operational, financial or implementation impacts)? If so, please describe.