Australian Institute of Company Directors

Level 12, Tower 3, Darling Park,
201 Sussex Street,
Sydney NSW 2000

1300 739 119
contact@aicd.com.au
aicd.com.au

ABN 11 008 484 197

1 May 2026

Department of Home Affairs
Langton Cres
Parkes ACT 2600

Via online form

Dear Home Affairs

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

Thank you for the opportunity to provide a submission to the consultation paper on proposed amendments to Ministerial Directions Powers in Part 3 of the *Security of Critical Infrastructure Act 2018* (**SOCI Act**).

The Australian Institute of Company Directors' (**AICD**) mission is to be the independent and trusted voice of governance, building the capability of a community of leaders for the benefit of society. The AICD's membership of more than 53,000 reflects the diversity of Australia's director community, comprised of directors and leaders of not-for-profits (**NFPs**), large and small and medium enterprises (**SMEs**) and the government sector.

The AICD has in recent years engaged extensively on Government consultations and proposed reforms in the cyber security and data management policy areas, including submissions on the independent review of the SOCI Act, the *Cyber Security Act 2024*, the development of the 2023-2030 Australian Cyber Security Strategy, previous rounds of SOCI Act reform and amendments *Privacy Act 1988*.[1]

We have supported directors to improve their knowledge of cyber security and data governance best practice through extensive guidance materials, including the *Cyber Security Governance Principles*, *Governing Through a Cyber Crisis*, *Data Governance Foundations for Boards* and a joint publication with the Australian Signals Directorate (**ASD**) in October 2025 on cyber security priorities for boards in 2025/26. The AICD also offers the Cyber Security for Directors short course and regularly features cyber security and data governance in director webinars and events to support director cyber skills.

1. Executive Summary

The SOCI Act is an important legislative framework in promoting critical asset entities, and their boards, to take proactive steps to address material risks and hazards. The regime has contributed to a strengthening of the operational resilience of critical asset entities to the benefit of the Australian economy and society.

The AICD accepts that in certain exceptional national security circumstances, a Ministerial direction is an appropriate last resort mechanism to address significant risk control weaknesses at an entity and to manage the immediate response period during a significant incident. However, the consultation paper does not clearly set out the policy case for such an expansion of unfettered Ministerial powers. Further, we are concerned that the proposed directions powers do not sufficiently reflect the associated legal complexity and challenges, including potential conflict with directors' duties under the *Corporations Act 2001* (**Corporations Act**).

[1] AICD submission, Independent Review of the SOCI Act, January 2026, available here.

Our key points are as follows:

- **Measure 2 – Conditions Power**. The AICD recognises that in certain exceptional circumstances there may be a necessity for a Minister to direct a SOCI entity to change governance arrangements, information flows and security settings. We are concerned though that what is proposed is far broader than the conditions regime under the *Foreign Acquisitions and Takeovers Act 1975*. We are particularly concerned with the potential conflict with directors' duties under the Corporations Act where an entity is directed to exclude a director from certain decisions, information flows and oversight functions.
- **Measure 3 – Restrictions on the use of high-risk vendors, products or services**. The AICD in-principle supports a formal legislative mechanism by which the Government can prescribe or list high risk products, service or vendors which pose a heightened national security risk and that SOCI Act entities are prohibited from using. However, we are not satisfied that this mechanism should reside as a Ministerial direction power given the limited transparency on the process and the inability of impacted parties to engage on the cost and complexity of any direction. Our view is that such a mechanism should be a formalised administrative process within the SOCI Act and the supporting SOCI Act Rules with a comprehensive consultation process that allows due consideration of the complexities of prescribing a particular vendor.
- **Measure 4 – Delay continuous disclosure requirements**. Whilst we support the underlying policy intent, we consider there are very significant legal complexities with the draft proposals and a risk of unintended consequences. Before progressing this proposal, it is imperative that further consultation with relevant legal experts is undertaken, as well as the Australian Securities Exchange (**ASX**), to ensure that entities and directors are adequately protected and not exposed to serious consequences (including potential shareholder class actions) for breaching continuous disclosure rules. At a minimum, we strongly recommend that the model that Home Affairs pursues includes an explicit statutory safe harbour in the Corporations Act as essential to protect directors who act in good faith to comply with a Ministerial direction not to disclose information.

2. General comments: Policy case and legal complexity

The AICD recognises the importance of effective Ministerial mechanisms under the SOCI Act in exceptional national security circumstances. We note that what is proposed in the consultation paper is a significant expansion of the existing Ministerial powers in Part 3 of the SOCI Act. In the AICD's view, the consultation paper does not present a strong policy case or clearly articulate the policy problem these proposals are intended to address and why such a significant expansion is justified. Importantly, it does not sufficiently reflect the legal complexity of the proposals in the context of Corporations Act duties and obligations.

We understand that the existing Ministerial directions powers have not been utilised to date. The consultation paper does not provide a clear assessment across proposed new directions powers two to four of how the existing powers are considered inadequate, or the circumstances in which existing drafting has materially constrained necessary action. For example, a preliminary view is that the scope of the existing 'action' direction power under Section 35AQ is so broad as to allow the Secretary of Home Affairs to address many of the issues that are the focus of the conditions proposal. In the absence of this analysis, it is difficult to assess whether the proposed reforms are proportionate or whether they risk expanding executive discretion beyond what is necessary to achieve the stated policy objectives.

The Independent Review of the SOCI Act by Dr Jill Slay AM does not cover the effectiveness of existing Ministerial powers. To the extent the strength of the powers is noted in Dr Slay's report, it is as an issue to examine.[2] We would encourage Home Affairs to prioritise consultation on the review's findings and to develop a clear evidence base for proposed expansion.

We are also concerned that the legal complexity that arises with the proposed directions powers, particularly the conditions and disclosure proposals, has not been fully assessed. As highlighted in our responses to the conditions

[2] Dr Jill Slay, Independent Review of the Critical Infrastructure Act 2018, February 2026, page 11.

and disclosures proposals, there is a real risk that any direction would, at a minimum, create tension with other legislative obligations and, at worst, be in direct conflict, including with directors' duties under the Corporations Act.

3. Measure 2 – Conditions Power

The AICD recognises the broad policy objective underlying the proposed conditions power. National security risks at an entity may emerge outside of, or after, the *Foreign Acquisitions and Takeovers Act 1975* (**FATA**) regime and Foreign Investment Review Board (**FIRB**) review. The proposed power would allow conditions to be imposed where ownership, control or governance risks emerge, persist or intensify after the acquisition, or arise outside the foreign investment approval process altogether. Further, we understand that the global geopolitical environment is increasingly volatile, heightening national security risks.

However, we are concerned with the broad scope of the proposed condition power in the context of the governance of an entity and the resulting tension with directors' duties.

We also note that the Minister and the Secretary of Home Affairs have existing broad directions powers in the SOCI Act, including an action direction under Section 35AQ. These powers were introduced to the legislation in 2024 with the express objective of allowing the Government to intervene when it observed risk management program deficiencies that an entity had failed to remediate. The new proposed power appears to be in part addressing similar concerns (e.g. information controls, cyber security baseline settings). We would welcome information on how existing powers have proved deficient in practice, rather than adding further complexity to an already complex SOCI regime.

Governance scope is broader than FATA

It is challenging, in the absence of legislative drafting, to assess whether the proposed power would complement and be consistent with the FATA regime. However, from the list of examples shared in the consultation paper what is being contemplated does appear to facilitate directions or conditions that are far broader than currently under FATA.

The Treasurer's conditions power in FATA is broad, however Treasury guidance on conditions notes that in respect of governance they are typically limited to 'a certain number or proportion of directors who are Australian citizens, characteristics of the Chair and/or requirements for a quorum.'[3] In contrast, what is contemplated under the proposal goes beyond board composition and the nationality/residence of directors to cover:

- targeted voting exclusions or restrictions for decisions that materially affect the security posture of the asset;
- establishment of an independent security risk committee responsible for oversight of cyber, operational technology, physical-security and supply-chain risks; and
- requirements to notify the regulator of Board resolutions or organisational changes that materially affect the entity's security posture.

From engagement with Australian legal experts, we understand that FIRB does not currently propose governance conditions that are this intrusive and that fundamentally undermine the role of the board as the accountable body for the organisation. For example, to require targeted board exclusions and/or the board to notify Home Affairs of specific board resolutions is, in the AICD's view, excessive. It risks directly influencing the decision making of the board and placing the Government, via Home Affairs, in a quasi-governance role. As outlined below, we consider there is a strong risk of direct conflict with directors' duties.

Our strong view is that in respect of governance settings, the proposed power should be limited to board composition and director appointment (i.e. consistent with the approach of FIRB). If Home Affairs is satisfied with the composition of the board and the fitness and propriety of individual directors, then it follows that the board as a governance body should be left with the accountability to oversee the operation of the organisation. This oversight

[3] The Treasury, Guidance Note 11 Protecting the National Interest – Guiding principles for developing conditions, page 7, available here.

role would continue to be subject to a wide range of governance obligations and duties, including overseeing the entity's obligations under the SOCI Act and signing off on the critical infrastructure risk management program.

Conflict with directors' duties

We consider there is a real risk that the proposed power will result in directions that will conflict with a director's duties under the Corporations Act.

As described in the consultation paper, the power could extend to highly intrusive governance conditions, including excluding a director from voting on, or participating in, specified board matters, or requiring the board to provide heightened or ongoing reporting of board resolutions to Home Affairs. Directors are required under legislation and common law to exercise independent judgment and act in good faith in the best interests of the company as a whole, informed by collective deliberation at the board table. Measures that curtail a director's ability to participate in governance decisions, or that mandate reporting of board resolutions and decisions outside well established governance and accountability frameworks, risk undermining these principles and fragmenting collective board responsibility.

It is difficult to envisage how a director who is subject to a Ministerial direction (via a direction on the entity) excluding participation in certain decisions or receiving certain information related to a critical asset due to national security considerations would be able to continue in their role. For instance, at most SOCI entities, and particularly with Systems of National Significance, it is the critical asset(s) that is central to the operations of an entity. For a director to be excluded from such oversight and decision making would be fundamentally inconsistent with their duties. The consultation paper does not address how directors are expected to reconcile compliance with such conditions where they may reasonably consider that exclusion from decision-making or compelled reporting is inconsistent with their statutory and fiduciary duties.

Given the significant implications of being subject to a direction we strongly support appropriate safeguards to ensure that any information that a direction is based on is fair, reasonable and can be examined by the impacted entity and/or individual. We appreciate that it may not be possible to share specific sources or methods, however it should not be the case that a direction can simply be explained to the impacted parties as being solely on 'national security grounds'.

The AICD strongly recommends that Home Affairs undertake further detailed consultation with corporate law experts on this proposal.

As above, at a minimum we consider the directions power should be limited to the composition of the board and the fitness and propriety of individual directors, including nationality where appropriate, consistent with FATA and subject to appropriate safeguards. For a Minister to direct who participates in board decisions is not only overreach but risks fundamentally restricting the functioning of the board and its governance role.

Risk of regulatory complexity and overlap

There is a risk that rather than complementing FATA, the SOCI directions regime becomes a new source of regulatory complexity, cost and uncertainty for entities.

We understand that the FIRB process is already complex and costly, particularly where conditions are imposed that require ongoing compliance and monitoring. Given the scope of the proposed conditions power we can envisage scenarios where there are FIRB conditions and then separately Ministerial directions under the SOCI Act. This will exacerbate the complexity and cost for entities and may ultimately serve to undermine effective governance. For instance, FIRB imposes a board composition condition and then at a certain point the Minister under the SOCI Act directs the establishment of a board security committee. To the greatest extent possible, such scenarios should be avoided.

For this proposal to work in practice we strongly recommend close coordination between Treasury and Home Affairs on further policy design and drafting of this proposal. Were the conditions power to be legislated it should be

supported by clear guidance from Home Affairs and Treasury on the interaction between the two regimes and how the respective regulators will work together, including ongoing oversight of any conditions or directions.

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

The AICD in-principle supports a formal legislative mechanism by which the Government can prescribe or list high risk products, services or vendors which pose a heightened national security risk and that SOCI Act entities are prohibited from using. We are however not satisfied that this mechanism should reside as a Ministerial direction power. Our view is that such a mechanism should be a formalised administrative process within the SOCI Act and the supporting Rules that allows due consideration of the complexities of prescribing a particular vendor.

As the consultation paper notes, the supply chains of critical infrastructure entities are highly complex, particularly in respect of digital services and products. Elements or components provided by key vendors can be so intertwined with an entity's systems and operations that it can be impractical to quickly cease using a particular product or service and switch to an alternative. SOCI entities have noted to us that it is common in some markets for there to be no alternative suppliers or products with this dynamic particularly prevalent in technology infrastructure markets. Further, given how particular equipment or infrastructure connects with partners or customers a direction to cease using a particular product may cascade into reliability or integrity issues through a supply chain. Finally, an entity will often not have full visibility or control over the multiple layers of the digital supply chain where a key vendor will in turn have multiple subcontractors in its own supply chain.

We are concerned that a largely unfettered Ministerial direction power will result in scenarios where SOCI entities will receive a direction with limited or no warning and face considerable costs and complexity in complying with the direction by an arbitrary timeframe set under the direction. We also consider there is a high risk that a Minister may make a direction based on incomplete information, including limited visibility of the economic implications of the direction and the impact of such a direction on the reliability of the critical infrastructure assets.

To address these risks there should be legislative settings for an appropriate public consultation process with impacted vendor(s), entities and broader stakeholders. The paper notes that 'affected entities would be consulted wherever reasonably practicable'.[4] This is not sufficient comfort. Impacted entities should be allowed to publicly present to Government on the impact of such a direction, the associated costs and the complexity of meeting the direction in the proposed timeframe. The consultation paper provides a hypothetical scenario of network switches and routers in telecommunications infrastructure. This example is instructive as it is difficult to envisage how the Government would understand the complexities and costs of a direction in such a technically complex area without the benefit of a comprehensive and genuine consultation process with all affected parties.

A direction of this nature will also have ramifications beyond the SOCI Act population. Notably, it is highly likely that demand for the vendor's product and services will be impacted in the broader Australian business environment and given globalised supply chains also internationally. Organisations outside the SOCI Act population should be afforded the opportunity to provide submissions. Further, it is unclear from the consultation paper whether the impacted vendor will be consulted on the proposed direction and have an opportunity to remediate or address the Government's concerns. Given the very significant impact on the business operations of the vendor in Australia from a direction, we do consider it should be afforded due process through a formal administrative process.

A formal process under which the Government can propose to prescribe a vendor, product or services through a delegated instrument under the SOCI Act Rules should be subject to comprehensive consultation. This at a minimum will allow consideration of the potential impact in a more rigorous manner than the opaque and unclear process that is outlined in the consultation paper. It also provides time for impacted entities to start planning to transition off a vendor or product/service.

We highlight the Home Affairs consultation in December 2025 of reform to the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006*, including a proposed power for the AUSTRAC CEO to prohibit a product,

[4] Consultation Paper, page 15.

service or delivery channel.[5] That proposal includes a mandatory minimum 30 day public consultation period and for the direction to be a legislative instrument subject to parliamentary oversight.

We appreciate that given national security considerations it may not be possible for the Government to provide the full detail for a proposed prohibition in a public process. Nonetheless, a formal process under the SOCI Act and the accompanying Rules will provide more rigour and greater confidence that any prohibition is grounded in a genuine balance between national security considerations and the cost and economic impact of the prohibition.

5. Measure 4 – Delay continuous disclosure requirements

The AICD recognises that in certain exceptional national security circumstances it may be appropriate for a listed entity to not disclose a cyber incident for a very limited period. However, we consider there are very significant legal complexities with the draft proposals and a risk of unintended consequences that need to be examined before finalising any policy position.

Although in certain exceptional circumstances it may be appropriate for a listed entity to not disclose a cyber incident for a very limited period of time, we are unconvinced on the basis of the consultation paper, that the two options will achieve the stated policy objective without material unintended consequences.

We urge careful consideration of the complexity and significant legal risks for both listed entities and directors that are associated with a listed entity not meeting its continuous disclosure obligations.

If Home Affairs believes that it is critical to enable the delay of an entity's continuous disclosure obligations for a limited time in exceptional circumstances, it is imperative that significant consultation with legal experts is undertaken, as well as the ASX, investors and companies, to ensure that entities and directors are adequately protected from legal risks.

Option 1

We do not support Option 1. It relies on case-by-case exemption mechanisms by ASIC that are not designed to operate in fast-moving, high-risk national security incidents. Our understanding of the operation of section 111AT is that it rests on an entity making an application to ASIC for an exemption rather than ASIC unilaterally granting an exemption to an entity due to particular circumstance, such as national security considerations. Further, as noted in the consultation paper, the exemption itself does not place an obligation on the entity to not disclose information.

Further, ASIC currently has a legal obligation under the Corporations Act to cause a copy of an exemption to be published in the ASIC Gazette. This would appear to defeat the intent of the policy objective.

Option 2

Whilst Option 2 has some merit, the consultation paper does not demonstrate sufficient appreciation of the implementation challenges, including legal complexities.

As Home Affairs would be aware, listed entities have very clear disclosure obligations under the ASX Listing Rules, which are given the force of law under the Corporations Act. A listed entity must immediately disclose to the market any information that is not generally available and that a reasonable person would expect to have a material effect on the price or value of the company's securities. This obligation applies once the entity becomes aware of the information and is subject to limited exceptions under Listing Rule 3.1A. Under the current legal framework, directors can be liable if an entity breaches this obligation.

A failure to appropriately disclose to the market risks both regulatory action and shareholder class actions against the entity and the board. Boards of listed entities take disclosure obligations very seriously, in supporting a properly informed market and effective engagement with shareholders and stakeholders. Breaches of disclosure obligations also carry substantial legal and reputational risks, for corporations, boards and executives. The consultation paper

[5] Department of Home Affairs, *Consultation Paper – 2026 Reforms to the AML/CTF Act*, December 2025.

notes that a direction by the Minister under the SOCI Act would 'enliven an exemption from the continuous disclosure obligations under the ASX Listing Rules'. We are not satisfied that provisions alone in the SOCI Act will achieve this result, particularly noting that each of the limbs in Listing Rule 3.1A will need to be satisfied for an exception to apply.[6] Critically, it also fails to address the duties and obligations on directors under the Corporations Act, including prohibitions on false or misleading conduct and statements.

In circumstances where a direction is given, we are particularly concerned that an entity and its board will need to navigate the tension between complying with the direction (particularly one that extends over a number of days) and complying with existing laws in relation to market disclosure and directors' duties. Unless this tension can be addressed, compliance with a direction could risk a concurrent breach of disclosure laws, directors' duties and/or other provisions of the Corporations Act (e.g. relating to false and misleading conduct, insider trading and making financial reports) with serious legal and reputational consequences for both the entity and directors (including the potential for shareholder class actions) and ramifications for investor confidence in the market.

Confidentiality

It is inconceivable that a board can allow its securities to continue to trade for an extended period (i.e. up to 30 days) while in the background a cyber security incident has occurred of such severity that absent a direction it would have been considered material (i.e. price sensitive) and would have been disclosed to the market. As time goes on, more individuals and organisations will become aware of the cyber incident due to the involvement of technical experts and required notification to other parties (e.g. notifying another regulator such as APRA). Further, customers, clients and suppliers may observe issues with the reliability and integrity of the asset. This would quickly void the confidentiality arm of the ASX exceptions under Listing Rule 3.1A.

Inevitably, an outcome of broad awareness of the incident will undermine the integrity of the listed market and the objective of investors having equal access to all material, price-sensitive information, enabling them to make informed investment decisions. This would enliven risks that arise from asymmetrical information, including risks of insider trading and loss of market confidence.

Ultimately, a board may consider it necessary to apply to the ASX to place the entity in a voluntary suspension or trading halt to manage its continuous disclosure obligations given the significant risk of an entity's securities continuing to trade when a material event has occurred. A voluntary suspension or trading halt would naturally result in questions from the market (assuming the ASX had already been confidentially advised of the direction) on the reasoning, which in turn is likely to undermine the rationale for the direction.

There is no indication in the consultation paper on whether the ASX has provided input to the design of this proposal. We strongly recommend that no proposal should proceed without close engagement with, and the support of, the ASX. Further engagement with corporate law experts is also essential. Close consideration must be given to the interaction of the proposal with all other relevant regulatory and legal requirements.

Duration of delay

The consultation paper and the Home Affairs Town Hall indicated that a direction to delay disclosure could be time-bound up to 30 days. We are concerned that this proposed length is impractical and inappropriate.

As noted above, it is highly likely that in a short period of time, knowledge of the cyber security event will spread due to the need for a technical response and the entity making other notifications to other regulators and stakeholders (e.g. notifying key customers that it cannot fulfil a contractual obligation). As Home Affairs and ASD are aware, the immediate period of a cyber incident can be difficult to manage with a high number of stakeholders, government and non-government, seeking information and attempting to provide a targeted response and understanding the implications of the incident. As events progress, more people and parties are brought into the response phase, for example providing technical support. Over a period of 30 days, the pool of people aware of the

[6] For example, it may be a breach of law to disclose the information, but for an exception to apply it is also essential that the information is confidential (and ASX has not formed the view that it has ceased to be confidential) and that a reasonable person would not expect the information to be disclosed.

incident will have grown exponentially despite the entity having made no disclosure. As we have stressed above, such a scenario runs the real risk of materially undermining the integrity of listed markets and creating legal risk for entities and directors.

Our initial view is that any direction to delay disclosure should be no longer than **48 hours – 72 hours**. This length may provide sufficient time for the ASD and Home Affairs to address any vulnerabilities that may exist, undertake immediate mitigation efforts and for the impacted entity to understand the incident in greater detail to provide a more fulsome disclosure to the market at the end of the period. A delay of 48 hours also aligns with ASX's position in Guidance Note 8 that it may grant a trading halt or suspension for 2 days to allow an entity to make a more fulsome disclosure.[7]

Safe Harbour essential

The AICD considers that were Home Affairs to pursue Option 2, then an explicit statutory safe harbour in the Corporations Act is essential to protect directors who act in good faith to comply with a Ministerial direction not to disclose information, where that direction is given for national security reasons under the SOCI Act.

Absent such protection, we have serious concerns that directors may be exposed to civil liability and subject to regulatory enforcement or private actions connected to an entity's breach of continuous disclosure obligations under the Corporations Act, notwithstanding that non-disclosure was compelled by law. This places directors in an untenable position, as they may be required to choose between compliance with a Ministerial direction (noting the proposed increased penalties for failure to comply) and disclosure obligations to the market, particularly in circumstances where the materiality of the information is clear but disclosure is prohibited.

A carefully framed safe harbour is essential to provide legal certainty by confirming that directors of an entity that complies with a lawful non-disclosure direction, acting honestly and reasonably, will be protected from liability. This protection is critical to ensure that directions can be implemented swiftly and effectively without creating unacceptable personal legal risk for directors or undermining confidence in board decision-making.

Assess alternative options

We recommend that Home Affairs also consider alternative options to achieve the outlined policy objective.

The ASX in May 2024 updated Guidance Note 8 to introduce a new worked example to help illustrate when, in the context of a cyber incident, relevant information would, or would not, be expected to be disclosed to the ASX.[8] The example suggests that disclosure will generally not be required where the company cannot yet ascertain the materiality of the cyber incident to the price or value of its securities due to limited information.

Home Affairs may find that the policy objective can be mostly achieved through working with the ASX to understand how national security considerations could be reflected in the ASX's regulatory processes and guidance in respect of cyber security incidents, including factors to be considered by the ASX in a trading halt or voluntary suspension and the existing exceptions under Listing Rule 3.1A (e.g. it would be a breach of law to make the disclosure).

This approach would also have the benefit of being applicable to the broader population of listed entities, rather than just SOCI Act entities.

This is a complex area of corporation law and governance practice, thereby necessitating further consultation with legal experts, the ASX and market participants more broadly.

[7] ASX, ASX Listing Rules - Guidance Note 8, available here.

[8] ASX, ASX Listing Rules - Guidance Note 8, available here.

6. Next Steps

We hope our submission will be of assistance. We welcome further engagement with Home Affairs as it works through the complexity of further reform of the SOCI Act.

If you would like to discuss any aspects of our submission further, please contact [redacted]

Yours sincerely,

[redacted]

[redacted]