T +61 2 23 5744 **F** +61 2 9232 7174
E info@governanceinstitute.com.au
Level 7, 60 Carrington Street,
Sydney NSW 2000
GPO Box 1594, Sydney NSW 2001
W governanceinstitute.com.au

06 May 2026

Department of Home Affairs
4 National Circuit,
Barton ACT 2600

By email: ci.reforms@homeaffairs.gov.au

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

Who we are

Governance Institute of Australia is the only fully independent professional association dedicated to the advancement of governance and risk practice in Australia. Our internationally recognised qualifications equip a diverse professional network of business leaders to make good decisions for the benefit of Australia's economy and society. With a history dating over 100 years, Governance Institute is Australia's leading and trusted voice of governance. Our fully accredited education and training is tailored to meet the needs of governance professionals across public listed, unlisted, and private companies, as well as the public sector and not-for-profit organisations.

Governance Institute is committed to independent, evidence-based advocacy that is focused on strengthening the governance capability of Australian organisations. We believe that good governance is the foundation of organisational resilience, productivity, and public trust.

Introduction

Governance Institute supports the policy intent of the *Security of Critical Infrastructure Act 2018* (SOCI Act). The SOCI Act has laid the foundation for safeguarding Australia's most important infrastructure assets and driven positive changes across Australia's governance community by *'increasing executive and board-level awareness of infrastructure vulnerabilities, established baseline governance and accountability structures, improved asset visibility and incident reporting mechanisms and created a common language for discussing critical infrastructure across sectors'*.[1]

The importance of the SOCI Act cannot be understated. ASIO's current threat assessment provides sobering advice about the extent of state-sponsored actors actively mapping Australian critical infrastructure networks to pre-position malware for potential future disruption, recruitment of employees, executives and leaders within Australian businesses to steal IP and sensitive data and use of platforms, to approach employees with fake consulting opportunities to gain insights into foreign policy, trade and infrastructure risks.[2]

Given the context of a fast-paced, dynamic and highly evolved threat landscape, the effectiveness of the SOCI Act as a means of effectively managing Australia's national security interests has come under greater scrutiny. Since the commencement of the SOCI Act in 2018, the regime has undergone several significant changes within a relatively short period of time, adding layers of compliance, duplication and complexity. This has acted to diminish adherence and effectiveness. The Independent Review of the

[1] https://www.homeaffairs.gov.au/cyber-security-subsite/files/independent-review-soci-act-final-report.pdf
[2] ASIO Annual Threat Assessment 2025 | Office of National Intelligence

SOCI Act in assessing whether it was achieving its intended objectives made an overall finding that the SOCI Act *'requires major legislative change to remove complexity and confusion while becoming more agile and responsive'*.

The proposed amendments to the Ministerial Directions Powers should aim to further reduce ambiguity and uncertainty regarding directors', officers' and senior executives' lines of responsibility before, during and after a Ministerial direction has been issued. Simple, targeted and proportionate powers will drive stronger adherence and mitigate additional costs on regulated entities. We recommend that immediate efforts are made to simplify and clarify the effectiveness of the SOCI Act to remove the overall ambiguity, confusion and duplication identified by the Independent Review to strengthen adherence and increase awareness of obligations under the SOCI Act.

The Independent Review of SOCI Act

Prioritise regulatory simplification
As noted above the SOCI Act is complex and has undergone several changes over recent years. The Independent Review made clear that a priority for effective implementation is to remove all possible Commonwealth regulatory duplication from the SOCI Act to produce harmonisation and reduce administrative burden. The reforms must be designed in a way which delivers clear authorities, robust safeguards and a framework that is understood by all affected stakeholders. Graduated options that assist in the management of security threats should be prioritised with clear statutory guardrails embedded so that Ministerial powers are proportionate, targeted and necessary under the circumstances. Directions' powers must equally consider broader economic and social impacts and the commercial realities of the day. Mandatory consultation with relevant State and Territory Ministers should continue to ensure cross-government consultation is subject to necessary scrutiny.

Recommendation 1: Simplify and strengthen adherence to the SOCI Act by removing all possible Commonwealth regulatory duplication to produce harmonisation and reduce administrative burden and costs.

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

Existing policy rationale
The current formulation of section 32 imposes procedural and legal requirements on the Minister that were included to avoid duplication or conflict and preserve comity with state and territory schemes and to provide reassurance that the SOCI directions powers would be used as a 'last resort' rather than a first-instance intervention. This underlying policy rationale should endure unless exceptional circumstances justify the Minister taking alternative more immediate actions that may be necessary in instances of cyber warfare or imminent threats targeting critical assets.

Reasonable steps and good faith provisions
The Minister should only issue a direction if they are satisfied that such action is necessary to manage the significance of the risk. Prior to issuing the direction, it must be demonstrated that reasonable efforts have been made to negotiate with the entity in good faith to achieve the intended outcome of eliminating or reducing the risk without resorting to a direction. Furthermore, the Minister must determine that the risk has not been sufficiently eliminated or mitigated in the course of prior engagement with the regulated entity, to the extent that they lack the appropriate assurance that the threat no longer constitutes a nationally significant security concern.

Limited carve-out for extraordinary circumstances
A limited carve-out from the administrative action framework should be used by the Minister only under exceptional circumstances. For example, if ASIO's threat-level advice has escalated or inaction could

result in catastrophic consequences for critical asset infrastructure, the Minister may need to intervene quickly and decisively. The Minister must be able to demonstrate when an extraordinary circumstance exists including that the risk is a 'significant material risk', that the risk is 'immediate or imminent' and that the Ministerial direction is 'necessary and proportionate' as to 'reduce or eliminate the risk' under the given circumstances. The Minister must be satisfied that the given threat as advised by ASIO risks 'significant harm' to economic, social and national security interests, that undue delay would create unnecessary and disproportionate risks to Australia's national security interests and that the risk carries substantial specificity and detail as to provide the critical asset owner with sufficient transparency of the risk.

Recommendation 2: Implement a restricted exception to the administrative action framework for extraordinary circumstances that necessitate timely action. The Minister must demonstrate that their actions were taken under exceptional conditions when there was a significant material risk to critical infrastructure capable of causing significant or catastrophic harm.

Measure 2 – Conditions Power

The proposed amendments enabling the Minister to impose targeted conditions on reporting entities where existing ownership, control, or governance arrangements may create a material risk to national security may create excessive regulatory burden and do not appear to be in keeping with the good faith objectives of the SOCI Act.

Company directors' duties
Existing legal and regulatory frameworks, such as directors' duties under the *Corporations Act 2001* that place the onus of responsibility on company directors to exercise a duty of care and diligence and the good faith and proper purpose duties are designed to ensure directors act in the company's best interests, and not in their own self-interest. Directors' also have duties in relation to insolvent trading and to appropriately manage conflict of interests. These duties are enforced through civil and pecuniary penalties. Director duties have enduring qualities that incentivise risk management by requiring careful oversight of company operations and strategic decision-making, which in turn supports the long-term viability of a corporation.

The SOCI Act is an important legislative instrument, but it is primarily aimed at facilitating cooperation and collaboration between government, regulators and owners and operators of critical infrastructure, requiring critical asset operators to identify and manage risks in a commercially responsible manner.

Limited conditions power under extraordinary circumstances
The Ministerial conditions direction may operate well where existing or known threats have been significantly revised such as would be the case during a rapid escalation of cyber warfare, evoking extraordinary circumstances where there are 'significant, immediate, material risks at play' creating the potential to threaten the availability, operational integrity and security of the asset as assessed by ASIO. Following this imminent threat level change the Minister is satisfied that the risk presents an 'immediate and significant threat to national security' that outweighs other regulatory approaches and necessitates a timely and proportionate response through a conditions power requiring steps, actions or responses from the regulated entity to appropriately eliminate and reduce the risk.

The limited conditions power should articulate specific terms including the legitimacy and the immediacy of the risk, the steps or actions required, how those steps or actions aim to reasonably and proportionately address the immediacy and urgency of the risk under the exceptional circumstances, why the Minister is satisfied an ASA is not required, an opportunity for the asset owner to raise practical implementation difficulties and present alternative steps or actions within a reasonable time that can

ameliorate the risk, the duration and currency of the direction, the duration of time the asset owner has to respond, and under what conditions the direction may be revoked or expire such as if the threat level changes.

Some of the conditions powers described are not suitable for immediate, high-level threat mitigation such as board, governance and decision-making safeguards. Proposed requirements relating to board composition, such as a minimum number of independent, Australian security-cleared directors are practically problematic. Eligibility for Australian Government Security Vetting Agency (AGSVA) issued security clearances require Australian citizenship which unreasonably limits a corporations' ability to tap global talent pools for directors. Large-listed corporations often seek directors from the European, Asian or US markets with relevant jurisdictional experience or multi-jurisdictional experience such as directors having worked in both Australia and New Zealand. Restrictions on director citizenship may drive corporations to seek jurisdictional expertise from external consultants which may unintentionally increase rather than reduce risks.

Governance education, training and the development of industry standards
Many of the conditions described within the conditions powers are better suited as 'industry standards' such as the Essential Eight, cyber security mitigation strategies and best practice security measures. Companies could be nudged into best practices such as cyber security baselines and uplift, board and governance decision-making safeguards, personnel security controls and access to sensitive information.

The DHA and portfolio Minister should continue to work with regulated entities, industry bodies and professional associations to lift executives' and non-executive directors' education and training on governance, cyber security and risk management practices so that critical asset operators are sufficiently informed over how to identify, manage and responsibly act on risk, hazards and harms, understand the cyber warfare ecosystem and its potential impacts on critical infrastructure. Working with industry to develop National Security Standards for Critical Infrastructure Asset Owners will enable industry participants to contribute to the overall uplift of national security standards in a commercially responsible and viable manner.

Focus on long-term and sustainable uplift in security
This has the effect of improving the long-term security and viability of critical infrastructure assets. Crisis-driven activities may be more costly and complex to administer driving overall regulatory costs higher. The Minister should continue to have regard to the sensitivity of the asset in question, and the likely consequences if it were compromised, the period of time it would be compromised and the compounding effect that may have, whether less intrusive measures are available that would more effectively reduce or remove the risk, as well as the views and evidence provided by the entity in response to regulatory or threat level advice, and whether an existing Commonwealth, State or Territory regime could more effectively address the identified risk.

Recommendation 3: A limited conditions power should only be evoked under extraordinary circumstances where there is 'significant, immediate, material risks at play', where the material risk has changed quickly or decisively. The limited conditions power should articulate specific terms including the legitimacy and immediacy of the risk, steps and actions required and how those steps and actions are reasonably proportionate to mitigate the risk, why the Minister is exempt from an ASA, duration and currency of the limited conditions power.

Recommendation 4: Work with industry to develop National Security Standards for Critical infrastructure asset owners to enable industry participants to contribute to the overall uplift of national security standards in a commercially responsible and viable manner.

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

The proposed 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 may create practical risks in real world settings. Government should consider learnings from the UK's Telecommunications (Security) Act 2021 which contains a similar vendor directions power as to assess its effectiveness.

Litigation risk and conflict of laws
The proposed directions may be a cause of significant litigation risk where contractual obligations, cost outlays may have been predetermined or partially executed. The proposed power requires further specification and protections so that it is clear for all parties involved to understand whether there is overriding state and federal legislation such as workplace laws, corporations' law and competition law that may interfere or have enduring application. For the proposed restriction to effectively work in practice the SOCI Act would need to more clearly articulate the effect of existing legal duties or responsibilities.

Recommendation 5: Vendor risk-direction power requires further specifications and protections, particularly as to the enduring effect of other laws such as workplace laws, corporations' law and competition law and how this may impact contractual obligations and the procurement of infrastructure and services.

Measure 4 – Delay continuous disclosure requirements

Continuous disclosures critical to financial market integrity
Continuous disclosure obligations promote transparency and well-functioning markets and play a vital role in the integrity and stability of Australia's financial markets. Continuous disclosure enhances investor confidence and ensures fair trading by requiring listed entities to immediately release material, price-sensitive information to the market. Ultimately, the aim is to reduce information asymmetry between insiders and investors, ensuring that all market participants have equal, timely access to vital information. Continuous disclosure is an enduring and necessary means of promoting financial system integrity.

Iron-clad and enduring protections required
Where the Minister considers immediate disclosure in rare, high-risk cyber incidents may inadvertently undermine coordinated responses, reveal a vulnerability or heighten systemic risks, then proportionate, iron-clad and enduring protections must be provided to companies, directors and officers of regulated entities to mitigate against any real or perceived litigation risks before, during and after a direction to delay continuous disclosure requirements.

Option 2 – Ministerial directions power
Where the public disclosure of a cyber security incident would materially threaten Australia's national security or public safety, a new directions power allowing the Minister for Home Affairs to direct an entity to not publicly disclose the existence of the cyber incident for a prescribed period (option 2) would be more effective than granting powers to ASIC to exempt entities from disclosure obligations under section 111AT of the Corporations Act. The Ministerial directive would have a decisive effect on continuous disclosure obligations under the ASX Listing Rules on the basis that it would be a breach of law to disclose the information. The power should be limited to entities captured under the SOCI Act.

Conflict of laws

Other issues that are not adequately captured by the proposed direction to delay continuous disclosures include the effect of other communication tools that may be used by the affected entity during a crisis such as an email to notify consumers of an impact, temporarily or otherwise affecting the delivery of product or services, such as what has occurred in the past during a banking service outage. There may also be existing obligations under the *Privacy Act 1988*, as well as advice provided by OAIC on appropriate steps of disclosure and mitigation in the event of stolen or misappropriated sensitive or personal information that may conflict with the Minister's directions. Distinguishing between a service message and a branding message, that aims to keep consumers calm and informed during a significant incident requires further specification as to how it would be dealt with under the proposed provisions.

Recommendation 6: A ministerial direction to delay continuous disclosure obligations requires further detail in relation to how other laws may impact the affected entity, whether other types of disclosures are permissible during an impacted period, and what protections apply to directors before, during and after a direction.

Measure 5 – Increased civil penalty provisions

The current penalties do not provide a credible compliance incentive in circumstances where a failure to comply could have serious national security consequences. However, we consider that increased civil penalties should only be legislated when commensurate efforts to eliminate risk of confusion between overlapping or duplicative regulatory duties and obligations are in place. Parts of the proposed reforms do not sufficiently clarify board-level accountability such as how director duties apply when a Ministerial direction is executed or where conflicting instructions from multiple regulatory agencies apply, who emerges as the lead regulator under the given circumstances. Clarification of the law is a necessary precondition before increasing civil penalty provisions.

Recommendation 7: Increase penalties when and if regulatory duplication and complexity is addressed to avoid confusion over roles, duties and responsibilities of directors and executives of regulated entities.