6 May 2026

BSA RESPONSE TO PROPOSED SECURITY OF CRITICAL INFRASTRUCTURE ACT AMENDMENTS (MINISTERIAL DIRECTIONS POWERS)

Submitted Electronically to the Department of Home Affairs (DHA)

The Business Software Alliance (**BSA**)[1] welcomes the opportunity to respond to DHA's Consultation Paper on proposed amendments to the Ministerial Directions Powers in Part 3 of the *Security of Critical Infrastructure Act 2018* (**Consultation Paper** and **SOCI Act** respectively), which put forth a package of five proposed measures.[2]

BSA is the leading advocate for the global software industry. BSA members create technology solutions that power other businesses, including cloud storage services, customer relationship management software, human resources management programs, identity management services, network infrastructure services, cybersecurity solutions, and collaboration systems. Our members have made significant investments in Australia, and we are proud that many Australian companies and organisations continue to rely on our members' products and services to do business and support Australia's economy.

BSA supports the Australian Government's efforts to ensure that the SOCI Act remains fit-for-purpose in an evolving threat environment and capable of addressing serious risks to critical infrastructure. At the same time, any expansion of Ministerial powers requires careful calibration. DHA should ensure that any amendments are necessary, proportionate, and consistent with broader efforts to simplify and harmonise Australia's security regulatory framework.

Guiding Principles and Recommendations

At the outset, we have witnessed the impact of the advancement of AI model capabilities that has fundamentally transformed the cyber threat landscape and lowered the entry barrier for sophisticated and automated attacks, and the consequential need to improve and streamline the capability to effectively respond. As such, BSA urges DHA to consider the following guiding principles in the context of the proposed amendments. These principles reflect BSA's

[1] BSA's members include: Adobe, Alteryx, Amadeus, Amazon Web Services, Asana, Atlassian, Autodesk, Avalara, Bentley Systems, Box, Cisco, Cloudflare, Cohere, Cohesity, Dassault Systemes, Databricks, Datadog, Docusign, Dropbox, Elastic, EY, Graphisoft, HubSpot, IBM, Kyndryl, MathWorks, Microsoft, Notion, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, PTC, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Trend Micro, TriNet, Veeam, Workday, Zendesk, and Zoom Communications Inc.

[2] Consultation Paper: Proposed amendments to the Ministerial Directions Powers in Part 3 of the Security of Critical Infrastructure Act 2018, March 2025, https://www.homeaffairs.gov.au/how-to-engage-us-subsite/files/consultation-on-proposed-amendments-to-ministerial-directions-powers-cirmp/public-consultation-paper-soci-act-ministerial-directions-reforms.pdf. The five proposed measures are: 1) amendments to the existing directions power in section 32; 2) a new conditions power; 3) a new power to address high-risk vendors, products, or services; 4) a mechanism to delay public disclosure of certain cyber incidents; and 5) an increase in civil penalties for non-compliance with Ministerial directions.

longstanding positions and are generally applicable across all proposed measures set out in the Consultation Paper.[3]

- First, efforts to improve regulatory coherence and harmonisation should be prioritised. As highlighted in the recently published Independent Review of the SOCI Act 2018 (**Independent Review**)[4], the SOCI Act operates within a broader regulatory environment that is already complex and, in some cases, duplicative. Introducing new powers without first addressing this underlying fragmentation risks compounding uncertainty, particularly where entities must navigate overlapping obligations with differing triggers and timelines. Greater alignment across frameworks is essential to ensure that entities can identify and comply with their obligations with confidence. And most importantly, harmonizing regulations can improve national security by strengthening governments' ability to track, monitor, compare, and share information about cyber incidents and malicious campaigns within and across sectors and borders.
- Second, any expansion of Ministerial powers should be clearly justified by a demonstrated policy need. The Consultation Paper identifies a number of potential risks and challenges but, in several cases, does not provide sufficient evidence that existing powers are inadequate in practice. New or expanded powers, particularly those that are coercive or interventionist in nature, should only be introduced where there is a clearly defined gap that cannot be addressed through existing mechanisms. In general, governments should avoid introducing multiple or overlapping regulatory tools that will, in effect, collect more information or generate more compliance activity than authorities can realistically process or translate into meaningful security outcomes.
- Third, the exceptional nature of these powers must be preserved. Powers such as section 32 of the SOCI Act[5] are designed as measures of last resort, with deliberately high thresholds and a clear, narrow criteria for when the power may be activated. This ensures they are used only in limited and necessary circumstances. Proposals that lower these thresholds or introduce parallel intervention tools risk diluting this discipline and blurring the distinction between ordinary regulatory mechanisms and exceptional Government intervention.
- Fourth, any new or expanded powers should be supported by robust safeguards to ensure proportionality and predictability. Such safeguards should include access to a merits review or an appeal mechanism to provide a structured avenue for entities to challenge or seek reconsideration of directions where there are legitimate grounds for disagreement.[6]

---

[3] For examples, see:

a) BSA Response to Cyber Security Strategy "Horizon 2" Policy Discussion Paper, August 2025, https://www.bsa.org/policy-filings/australia-bsa-response-to-cyber-security-strategy-horizon-2-policy-discussion-paper.

b) BSA Comments on Cyber Security Legislative Package 2024, October 2024, https://www.bsa.org/policy-filings/australia-bsa-comments-on-cyber-security-legislative-package-2024.

[4] Independent Review of the SOCI Act 2018, February 2026, https://oia.pmc.gov.au/sites/default/files/posts/2026/04/Independent%20Review%20of%20the%20SOCI%20Act%20-%20Final%20Report%20%282026%29.pdf.

[5] Section 32 of the SOCI Act allows the Government to issue a direction to a reporting entity for, or an operator of, a critical infrastructure 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.

[6] One possible check is the implementation of a mandatory review process whenever such a power is exercised, during which a panel of independent technical experts assess the security, feasibility, and reasonableness of exercising the power.

There should also be a clear preference for the least intrusive means of addressing identified risks.

- Fifth, the operational realities of cross-border cloud and software services that support Australia's critical infrastructure must be considered. Global cloud service providers typically operate multi-tenant environments, leverage globally distributed infrastructure, and support customers across multiple jurisdictions. As such, directions that require the removal, restriction or modification of specific components or service configurations can have a direct impact on system stability and service availability across different jurisdictions. Any new or expanded Ministerial powers should be designed and implemented in a way that provides sufficient lead times and technical flexibility to accommodate these models. This is essential to avoid unintended disruption to essential services or fragmentation of global security architectures that are also central to Australia's own cyber resilience.

Specifically, on each of the measures, our recommendations are as follows:

- **On Measure 1:**
  - DHA should retain the existing Adverse Security Assessment (**ASA**) regulatory exhaustion requirements to ensure that section 32 is only invoked where necessary and remains a genuine measure of last resort.
  - A detailed examination of measures to streamline the ASA process should be conducted before the ASA requirement is replaced. Should DHA proceeds with replacing the ASA requirement with "tailored" advice from the Australian Security Intelligence Organisation (**ASIO**), DHA should: 1) ensure that such advice remains specific to the relevant entity and threat; and 2) clearly set out what the "tailored" advice should contain (e.g., likely impact of risk, rationale for why a direction is necessary, timelines).
  - Any adjustments to the existing section 32 requirements should only be made after broader work on regulatory simplification and harmonisation has been undertaken, in line with the recommendation in the Independent Review.
- **On Measure 2:**
  - If DHA considers that a new conditions power is necessary to address persistent governance-related risks, it should first clearly demonstrate the specific gap in the existing framework, including evidence that section 32 has been insufficient in practice and clear explanations on how the new power would not overlap with section 32.
  - In this regard, the proposal would benefit from a structured research study into the specific situations the conditions proposal is designed to address. Such a study should demonstrate clearly and empirically where a conditions power would be helpful and should include the opportunity for consultation with affected entities.
- **On Measure 3:**
  - Establish a clear and transparent framework, in partnership with industry, for identifying high-risk vendors, products, or services (including defined criteria, thresholds, and evidentiary standards), as well as guidance on how key concepts such as "material risk", "prejudicial to national security", and "adequately mitigated" will be applied in practice.

  - This should be complemented by feasibility studies to assess the technical risks involved with removing complex, layered technology stacks, especially where components are deeply embedded or used across multiple offerings.
  - The proposed measure should also be supported by robust safeguards, including access to merits review and appeal processes. Relatedly, DHA should address liability implications, including how entities will be protected from contractual and operational risks arising from compliance with a direction.
  - DHA should also clearly demonstrate why existing powers, including section 32, are insufficient (in line with broader efforts to support regulatory harmonisation and simplification).
- **Measure 4:**
  - DHA should proceed with an assessment of whether existing powers under Section 111AT of the *Corporations Act 2011* (**Corporations Act**)[7] can be effectively leveraged or refined to exempt entities from disclosure obligations in the event of a high-risk cyber incident.
  - If DHA determines that a delay mechanism is necessary, it should be narrowly scoped and designed to operate coherently with existing domestic disclosure obligations, contractual notification requirements, and applicable foreign reporting regimes. DHA should also clarify how entities are expected to manage potential conflicts between these obligations.
  - In addition, DHA should consider adopting a model that allows for both entity-requested and Government-directed delay in clearly defined circumstances, to better reflect operational realities and support effective incident response.
- **Measure 5:**
  - DHA should proceed with caution in increasing civil penalties and ensure that any changes are implemented alongside clearer definitions, thresholds, and safeguards governing the exercise of Ministerial powers.
  - Overly expansive liability frameworks, especially where obligations are not clearly defined, can also have unintended consequences for the cybersecurity workforce, including deterring qualified (and much needed) individuals from taking on senior roles.

General Observations on Regulatory Coherence and Simplification

The proposed measures form part of a wider effort to reform the SOCI Act. A core finding of the Independent Review is that the SOCI Act is overly complex, duplicative, and creates substantial administrative burden. In fact, the Independent Review's very first recommendation is to "*[r]emove all possible Commonwealth regulatory duplication from the SOCI Act to produce harmonisation and reduce administrative burden*".[8]

This context is critical. As it stands, the proposed measures will significantly expand Ministerial powers within a framework that lacks regulatory coherence. Without first addressing this

[7] Section 111AT of the Corporations Act grants the Australian Securities and Investments Commission (**ASIC**) the power to exempt entities from disclosure obligations under the Corporations Act. It was noted that 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.

[8] Independent Review (2026), p. 11.

underlying issue, implementing these powers will only further increase uncertainty around how different overlapping regulations interact, which obligations take priority, and how entities should manage risk in practice. This runs counter to the Independent Review's call for greater regulatory coherence and simplification.

DHA should therefore prioritise efforts to simplify and harmonise existing regulations before assessing if new or expanded Ministerial powers are necessary. This includes identifying and resolving overlaps with existing frameworks, clarifying definitions and thresholds, and improving the usability of current obligations. Only after these foundational issues are addressed should DHA assess whether there remains a clear and demonstrated need for further Ministerial powers. Introducing new powers ahead of this work may compound complexity rather than address the underlying challenges identified in the Independent Review.

On Measure 1 – Amending Existing Directions Power in Section 32

Measure 1 would amend the existing SOCI Act section 32 power to make it easier for the Government to issue directions where national security risks arise.[9] The Consultation Paper notes that "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", as it requires: 1) an ASA from the ASIO; and 2) that the Minister be satisfied no other existing regulatory levers can be used to eliminate or reduce the risk.[10]

BSA recognises that a statutory power should be capable of practical use where genuinely necessary. However, the fact that the power is difficult to invoke does not mean that the safeguards are defective and have "inhibit[ed] the power's effective use".[11] Indeed, the nature of the section 32 power as a measure of last resort requires that the thresholds for its activation to be appropriately high. The Consultation Paper itself acknowledges that these guardrails were deliberately designed "to ensure restraint, legitimacy and coherence" and to provide assurance that the power would be used "as a last resort rather than a first-instance intervention".[12] In this context, a degree of procedural rigour and constraint is not only expected, but necessary to preserve the integrity and credibility of the power.

Specifically on the proposed shift from an ASA requirement to a requirement for the Minister to have regard to "tailored" ASIO advice, BSA notes that the requirement for a Minister to obtain an ASA is an important step to ensuring that any directions issued under section 32 are necessary and remain a power of last resort. However, we acknowledge the Consultation Paper's observation that decisions under section 32 require the Minister to "balanc[e] [security] risks against broader regulatory, economic, commercial and policy considerations".[13] In the circumstances, we urge DHA to first conduct a detailed examination of how the existing ASA process can be further streamlined. To the extent that DHA proceeds with replacing the ASA

[9] Section 32 allows the Government to issue a direction to a reporting entity for, or an operator of, a critical infrastructure 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.

[10] Consultation Paper (2026), p. 5.

[11] Consultation Paper (2026), p. 5.

[12] Consultation Paper (2026), p. 5.

[13] Consultation Paper (2026), p. 5.

requirement, it should ensure that such advice remains specific to the relevant entity and threat, rather than generalised at a sectoral level, so as to preserve a sufficiently robust evidentiary basis for intervention. Relatedly, DHA should clearly stipulate what such advice should contain/address, including what is the specific risk, assessed likelihood and impact of said risk, and rationale for why a direction is necessary and proportionate. The advice should also contain clear timelines and provide opportunities for affected entities to seek clarification, recognising that they may need to coordinate complex technical and operational responses while maintaining service continuity.

Separately, BSA is concerned about the proposed amendment to recalibrate the regulatory exhaustion requirement. As proposed, the Minister would only need to *consider* whether other regulatory mechanisms could address the risk, rather than be satisfied that no other mechanism is capable of doing so. This represents a substantive shift in the function of section 32 from a last resort power to one that may be exercised in parallel with, or in preference to, existing regulatory tools. This change risks undermining an important safeguard built into the current provision. Furthermore, the difficulty in satisfying the "regulatory exhaustion" requirement likely stems not only from the design of section 32, but from the overlap and duplication of security regulations. In practice, this makes it harder to determine which mechanism is best placed to address a given risk. Lowering the threshold for invoking section 32 will address the symptom but not the underlying issue. A more effective approach would be to focus on harmonising security regulations and reducing regulatory duplication, so that the appropriate regulatory pathway can be identified and applied with greater certainty. In other words, it is the current confusing and fragmented regulations that make it difficult for the Minister to find satisfaction that no other existing regulatory levers can be used to eliminate or reduce the risk, and if simplified (as the Independent Review called for), this burden would be appropriately lightened.

Recommendation:

- DHA should retain the existing ASA regulatory exhaustion requirements to ensure that section 32 is only invoked where necessary and remains a genuine measure of last resort.
- A detailed examination of measures to streamline the ASA process should be conducted before the ASA requirement is replaced. Should DHA proceeds with replacing the ASA requirement with "tailored" advice from the ASIO, DHA should: 1) ensure that such advice remains specific to the relevant entity and threat; and 2) clearly set out what the "tailored" advice should contain (e.g., likely impact of risk, rationale for why a direction is necessary, timelines).
- Any adjustments to the existing section 32 requirements should only be made after broader work on regulatory simplification and harmonisation has been undertaken, in line with the recommendation in the Independent Review.

On Measure 2 – Introducing a Conditions Power

Measure 2 would introduce a new "conditions power" enabling the Minister to impose ongoing, tailored requirements on entities where "ownership, control, or governance arrangements create a material risk to national security that cannot be sufficiently mitigated through existing regulatory

obligations or voluntary measures".[14] The Consultation Paper notes that this power "offers clearer legislative intent and a more proportionate mechanism for managing serious governance-related risks", in contrast to the section 32 power, which "lacks specificity and the flexibility to impose tailored, ongoing governance controls".[15] Importantly, this proposed conditions power would operate "only where other levers are insufficient to address the identified concern",[16] which suggests that this is another measure of last resort.

We would appreciate further details on how this new power will operate alongside section 32. Section 32 is designed to operate where existing regulatory levers are insufficient and is subject to deliberately high thresholds and safeguards to ensure they are used only in exceptional circumstances. The proposed conditions power appears to be triggered by a similar threshold but is framed as a more flexible alternative. This may create ambiguity as to how the two powers are intended to operate in practice, as it is not clear when the Government would rely on the existing section 32 power as opposed to the new proposed conditions power. Furthermore, without clearly defined boundaries, there is a risk that the distinction between exceptional (i.e., measures of last resort) and ordinary intervention tools becomes blurred. This further reduces predictability for industry. Ultimately, it is unclear how the introduction of a second "last resort" mechanism improves the overall functioning of the regime.

There is also no clear data on why this power is needed. Beyond assertions that the section 32 power lacks specificity and flexibility, the Consultation Paper did not provide details or evidence showing that section 32, with its broad scope of coverage, is insufficient for managing governance-related risks. Absent such evidence, the case for introducing a new and arguably broader intervention power remains incomplete.

BSA is also concerned by the wide range of conditions that may be imposed under this proposed measure, which include governance and structural interventions, such as requirements relating to board composition and access to information.[17] These measures extend beyond technical risk mitigation and introduce uncertainty as to how far Government may interfere with internal governance arrangements and operational structures within private entities. In particular, the absence of clearly defined limits or thresholds makes it difficult for entities to anticipate the scope of potential intervention and to plan their operations accordingly. Moreover, the proposed timeframe (being 12 months and thereafter every 24 months) within which a direction would be required to be reviewed by the Minister for continuing reasonableness is overly long.

Recommendation:

- If DHA considers that a new conditions power is necessary to address persistent governance-related risks, it should first clearly demonstrate the specific gap in the existing framework, including evidence that section 32 has been insufficient in practice and clear explanations on how the new power would not overlap with section 32.

[14] Consultation Paper (2026), p. 9-10.

[15] Consultation Paper (2026), p. 9.

[16] Consultations Paper (2026), p. 10.

[17] Consultation Paper (2026), p. 10

- In this regard, the proposal would benefit from a structured research study into the specific situations the conditions proposal is designed to address. Such a study should demonstrate clearly and empirically where a conditions power would be helpful and should include the opportunity for consultation with affected entities.

On Measure 3 – Restrictions on Use of High-Risk Vendors, Products or Services

Measure 3 would introduce a new power enabling the Minister to issue directions in relation to "high-risk vendors, products, or services". The Consultation Paper explained that vendors, products or services can create a material national security risk due to factors such as being subject to foreign laws that allow extrajudicial direction, opaque ownership structures, or exposure to foreign coercion/interference.[18] In these circumstances, the existing section 32 power is "not a practical mechanism for addressing systemic vendor or technology-related risks that affect multiple entities or an entire sector", and that a new power is required to enable "coordinated action" across critical infrastructure entities.[19]

BSA supports the objective of addressing supply chain and vendor-related risks, particularly where vulnerabilities are common and widely shared across critical infrastructure. However, the Consultation Paper does not provide details as to how a vendor, product, or service would be determined to be high-risk, which is a foundational issue for the operation of this power. Notably, there is no explanation of the criteria or thresholds that might apply, how different forms of risk (e.g., technical vulnerabilities, governance concerns, or jurisdictional exposure) would be distinguished, and the evidentiary basis required to support a finding that a vendor, product, or service is high-risk. Relatedly, while the Consultation Paper states that 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", it is not clear how the Minister will reach that determination, as the Consultation Paper did not specify the meaning of key terms such as "prejudicial" and "adequately mitigated". Greater specificity is necessary to ensure that the power can be applied predictably and proportionally, while mitigating the risk of it being exercised in a way that is broader or more intrusive than necessary (and which has the potential to affect sectors of the economy that are not directly regulated by the SOCI Act).

This uncertainty is compounded by the breadth of the proposed power and the limited articulation of safeguards governing its use. The Consultation Paper contemplates a wide range of possible directions that can be issued under this power, including removal and procurement restrictions. Many BSA members operate cross-border cloud and software services that rely on globally sourced components, services, and infrastructure, integrated into complex and interdependent technology stacks. Directions requiring the removal or restriction of particular vendors, specific products or even parts of the supply chain will have wide-ranging effects on interoperability, system stability, and the availability of the service or other offerings in Australia. In some cases, replacing deeply embedded technologies may be technically complex and itself

[18] Consultation Paper (2026), p. 14.

[19] Consultation Paper (2026), p. 14.

introduce operational and business continuity risks. Consequently, robust safeguards are essential. In this regard, DHA should implement a merits review and a formal appeal process to allow affected entities to challenge or seek reconsideration of directions where there are legitimate grounds for disagreement. DHA should also address potential liability implications, including providing clarity on how entities will be protected from vendor claims for breach of contract and customer claims arising from service degradation or reduced availability, where such impacts result from compliance with a direction.

Finally, while the Consultation Paper states that section 32 is not a practical mechanism for addressing systemic vendor risks, it does not provide examples or evidence showing where existing powers and obligations have proven insufficient in practice. In the absence of a clear explanation of its limitations, the introduction of a separate vendor-specific power risks duplicating existing capabilities rather than addressing a demonstrable gap.

Recommendation:

- Establish a clear and transparent framework, in partnership with industry, for identifying high-risk vendors, products, or services (including defined criteria, thresholds, and evidentiary standards), as well as guidance on how key concepts such as "material risk", "prejudicial to national security", and "adequately mitigated" will be applied in practice.
- This should be complemented by feasibility studies to assess the technical risks involved with removing complex, layered technology stacks, especially where components are deeply embedded or used across multiple offerings.
- The proposed measure should also be supported by robust safeguards, including access to merits review and appeal processes. Relatedly, DHA should address liability implications, including how entities will be protected from contractual and operational risks arising from compliance with a direction.
- DHA should also clearly demonstrate why existing powers, including section 32, are insufficient (in line with broader efforts to support regulatory harmonisation and simplification).

On Measure 4 – Delay of Continuous Disclosure Requirements

Measure 4 would introduce a mechanism to delay public disclosure of certain cyber incidents where immediate disclosure may create or exacerbate national security risks. The Consultation Paper observed that "immediate disclosure in rare, high-risk cyber incidents may inadvertently undermine coordinated responses, reveal vulnerabilities, or heighten systemic risks".[20] The Consultation Paper proposes either leveraging existing powers under Section 111AT of the *Corporations Act 2011* (**Corporations Act**)[21] or introducing a new SOCI-based directions power to temporarily prevent disclosure.

BSA supports delaying disclosure of cyber incidents when disclosure may negatively impact the cybersecurity of businesses or government agencies, which may occur for a number of reasons,

[20] Consultation Paper (2026), p. 17

[21] Section 111AT of the Corporations Act grants the Australian Securities and Investments Commission (**ASIC**) the power to exempt entities from disclosure obligations under the Corporations Act. It was noted that 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.

including alerting threat actors to ongoing investigations, accelerating malicious activity, undermining remediation efforts, and disrupting law enforcement or national security operations. As such, there may be narrow scenarios where a temporary delay is justified to support an effective and coordinated response.

Any delay mechanism must be clearly scoped and supported by well-defined thresholds. Most importantly, the mechanism should not lead to further fragmentation or create conflicting obligations in an already complex regulatory environment. In fact, the mechanism must be designed to operate coherently within an already complex disclosure environment. Entities already navigate multiple disclosure and reporting obligations with differing triggers, timelines, and legal consequences, and introducing a new delay mechanism without first addressing this issue may increase the existing complexity.

Should DHA proceed with implementing this mechanism, BSA urges DHA to consider how to allow an affected entity to similarly seek a delay in reporting obligations. A model that relies solely on unilateral Ministerial direction would not adequately reflect the practical reality that the affected entity is often best placed, in the first instance, to assess whether premature disclosure would prejudice ongoing response and remediation efforts.

Separately, the Consultation Paper did not address how a government direction to delay reporting would interact with contractual disclosure obligations and cross-border reporting requirements. Many entities are subject to contractual requirements to notify customers, partners and other stakeholders of security incidents within defined timeframes. In practice, incidents involving cross-border cloud and software services frequently trigger multiple, overlapping disclosure requirements across jurisdictions. Entities may be caught in a position of conflicting requirements, potentially exposing them to contractual liability. Delayed or constrained communication may also hinder effective incident response and coordination. Thus, any delay mechanism should be designed with clear guidance on how such conflicts are to be managed, including how it interacts with contractual obligations and international reporting regimes, to ensure that entities can comply without introducing additional legal or operational risk.

Recommendation:

- DHA should proceed with an assessment of whether existing powers under Section 111AT of the *Corporations Act 2011* (**Corporations Act**)[22] can be effectively leveraged or refined to exempt entities from disclosure obligations in the event of a high-risk cyber incident.
- If DHA determines that a delay mechanism is necessary, it should be narrowly scoped and designed to operate coherently with existing domestic disclosure obligations, contractual notification requirements, and applicable foreign reporting regimes. DHA should also clarify how entities are expected to manage potential conflicts between these obligations.
- In addition, DHA should consider adopting a model that allows for both entity-requested and Government-directed delay in clearly defined circumstances, to better reflect operational realities and support effective incident response.

[22] Section 111AT of the Corporations Act grants the Australian Securities and Investments Commission (**ASIC**) the power to exempt entities from disclosure obligations under the Corporations Act. It was noted that 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.

On Measure 5 – Increased Civil Penalties

Measure 5 proposes to increase the maximum civil penalty for non-compliance with a Ministerial direction under Part 3 of the SOCI Act from 250 penalty units to 2,000 penalty units, aligning it with equivalent obligations under Part 2D of the SOCI Act.[23] The Consultation Paper states that the current penalty does not provide a "credible compliance incentive in circumstances where a failure to comply could have serious national security consequences".[24]

BSA recognises that stronger civil penalty provisions can promote effective enforcement. However, the increase in civil penalties, when viewed in conjunction with the other four proposed measures, constitutes grounds for concern. The other proposed measures significantly expand the ability of the Government to issue directions – increasing penalties in parallel with broader and, in some respects, less clearly defined powers, will disproportionately increase compliance risk for entities. Higher penalties may also discourage open engagement between industry and government as entities become more defensive and legalistic. This is further exacerbated by the complex regulatory environment, where entities must straddle overlapping obligations and may face practical challenges in reconciling competing requirements. In such circumstances, increasing penalties without first improving regulatory coherence risks placing undue burden on entities acting in good faith.

The Consultation Paper also states that the reason for increasing penalties is to align with the enforcement framework already operating under Part 2D of the SOCI Act. However, this comparison warrants closer examination. Part 2D applies to a narrower category of assets, specifically critical telecommunications infrastructure, and is appropriately accompanied by enhanced and more targeted regulatory obligations. In addition, the directions power under section 30EF of Part 2D is also subject to the critical safeguard of requiring an ASA before a direction can be issued. In contrast, the scope of assets covered by Part 3 is larger, and the proposed amendments seek to remove the ASA requirement. In summary, the circumstances under Part 2D are not directly comparable to those under Part 3 to warrant an alignment of penalties.

There are also broader workforce implications. Security executives are responsible for making real-time decisions and responding to Government requests/directions in complex risk scenarios. Where liability exposure increases at the same time as the underlying powers become broader or less clearly bounded, the effect is to shift more risk onto those individuals without giving them corresponding certainty as to what compliance requires. This matters because cybersecurity leadership already operates in a constrained talent market, with roles such as a Chief Information Security Officer requiring highly specialised expertise. If those roles also carry heightened exposure to penalties in circumstances where the scope of obligations remains unclear, organisations may find it harder to recruit and retain qualified personnel.

Recommendation:

[23] Consultation Paper (2026), p. 19.

[24] Consultation Paper (2026), p. 19.

- DHA should proceed with caution in increasing civil penalties and ensure that any changes are implemented alongside clearer definitions, thresholds, and safeguards governing the exercise of Ministerial powers.
- Overly expansive liability frameworks, especially where obligations are not clearly defined, can also have unintended consequences for the cybersecurity workforce, including deterring qualified (and much needed) individuals from taking on senior roles.

Conclusion

We thank DHA for the opportunity to provide our recommendations in response to the Consultation Paper. We hope our comments are useful as you continue to refine the SOCI Act and the broader security regulatory landscape. We welcome DHA's consistent commitment to engaging with industry stakeholders, including BSA and our members and we look forward to continued dialogue in support of your important mission to protect Australian citizens and assets.

Yours sincerely,