TELSTRA GROUP LIMITED

Submission to the Department of Home Affairs consultation on proposed amendments to the Ministerial Directions Powers in Part 3 of the Security of Critical Infrastructure Act 2018

Public Submission

1 May 2026

Summary

We welcome the opportunity to provide our views to the Department of Home Affair's consultation on proposed amendments to the Ministerial Directions Powers in Part 3 of the Security of Critical Infrastructure Act 2018 (**SOCI Act**). Telstra is committed to strengthening the resilience of Australia's critical infrastructure in response to expanding external or domestic threats and vulnerabilities.

Broadly we are supportive of the enhanced clarity that these amendments are seeking to make to the Ministerial Directions framework, as it provides Government with the appropriate tools and levers to manage national security risks.

We support in principle Measures 1 and 3 and propose that the Minister also consider the technical feasibility and reasonable timeframes unique to each sector when using these powers. For Measures 2 and 4, we consider that the existing mechanisms could be more effectively utilised.

We support the Department's intent to ensure the national security framework relating to critical infrastructure remains cohesive and supports effective implementation in practice.

Measure 1: Amendments to existing Directions Power in section 32

We support the proposal to amend the current guardrails relating to adverse security assessments and regulatory exhaustion requirements. We agree with the Department's assessment that these targeted amendments to section 32 will improve clarity, operability and timeliness, while maintaining existing safeguards.

The Minister has existing obligations to consult with the relevant entity prior to issuing a direction and have regard to the costs incurred by the entity and consequences on competition and customers. We propose that the Minister must also ensure that technical feasibility based on the unique circumstances of the entity are taken into consideration and there is a corresponding reasonable time frame applied for compliance.

Measure 2: New Conditions power

We support in principle the ability for Government to impose tailored governance controls to address a specific vulnerability relating to an individual director of a SOCI entity. However, imposing these types of governance conditions more broadly would be onerous, impractical to implement and would ultimately have the effect of hindering rather than enhancing the governance arrangements of SOCI entities. We propose clear guardrails to ensure this last resort power is only available in discrete use cases and where existing mechanisms have proven to be ineffective and does not conflict with existing regulations, such as director's duties under the Corporations Act.

We do not support a new power for Government to impose tailored operational controls on a SOCI entity. For example, access, information-handling, and personnel security controls or baseline security standards. This is overreach into the operations of a SOCI entity and would become untenable where an entity received multiple conditions from Government. It is contrary to the long-standing SOCI principle that a responsible entity is best placed to identify material risks and controls based on their unique critical infrastructure asset and operating environment.

We propose that the Government continue using the existing general directions power in section 32 of the SOCI Act and lean into other levers to address specific concerns. This includes two way threat information sharing, risk management program rules under Part 2A and notification obligations under Part 2D, as applicable to the telco sector. In many cases, there are also existing operational controls imposed on entities under relevant industry standards. We consider the ongoing partnership between government and industry where national security threats are identified and materialised, may continue to be effectively managed through these existing mechanisms.

Measure 3: New power for restrictions on the use of high risk vendors, products or services

We support the Government's intention, through a vendor-risk direction, to identify circumstances in which a vendor or its products, equipment, services or technologies may pose a material risk to national security. It would enable us to deliver more cohesive, Government-endorsed advice and guidance to our Telstra operational teams to inform decision-making and risk management.

In addition to the considerations the Minister must make, we also propose that the Minister must consult with the impacted relevant entity and sector, to ensure the technical feasibility for the unique circumstances for each sector are taken into consideration, with a reasonable time frame applied for compliance. In circumstances where there is high reliance on the vendor, creating concentration risk, adequate transition times will be necessary to identify and implement suitable replacements.

Additionally, we welcome the proposed coordinated mitigation measures and directions across an asset class, sector or supply chain. These measures could help address commercial inequities where organisations have differing levels of awareness of, or appetite to manage, high-risk vendor risk.

Measure 4: New power for temporarily delaying continuous disclosure requirements

We welcome the additional certainty this measure would bring to entities responding to a cyber incident, provided it included appropriate liability protections. We consider the *Corporations Act 2001*

(**Corporations Act**) to be the most effective mechanism for ensuring national security and public safety implications are adequately considered by all relevant parties when assessing continuous disclosure requirements during a cyber incident. The Corporations Act applies to all listed entities in a consistent manner, rather than just SOCI regulated entities. ASIC also has a comprehensive library of guidance materials, including Guidance Note 8 relating to continuous disclosure requirements.

The continuous disclosure requirements under the Corporations Act are critical to the integrity and efficiency of Australia's equity capital markets. The requirements are set out in ASX Listing Rules 3.1-3.1B and apply to all listed entities. ASIC has published Guidance Note 8 to assist listed entities to understand and comply with their continuous disclosure obligations. This is a comprehensive and helpful document that spans over 100 pages and includes a detailed worked example for a cyber incident.

To be effective, the measure should provide immunity to listed entities where they would not have otherwise delayed their disclosure, and certainty about scope, thresholds, duration and engagement requirements with the Government and ASIC. When matters of continuous disclosure are prosecuted, the issues that are tested typically include whether disclosure was made in a timely manner as required by the ASX Listing Rules (or at all) and whether the disclosure that was made was accurate and not misleading and deceptive (including by omissions).

There are some practical limitations to delaying continuous disclosure requirements. For example, where an incident becomes public, is notifiable under another regulation or could cause harm (such as a major service outage), it would be ineffective to attempt to restrict a listed entity from disclosing the incident to the market. However, ASIC could restrict the entity from disclosing certain details that were assessed as having national security and public safety implications (on advice from the relevant security agencies) and would otherwise be disclosable as being material to the incident.