**Cisco Systems Australia Pty Ltd**

Level 14, 101 Collins Street
Melbourne Victoria Australia 3000

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

Cisco welcomes the opportunity to respond to the Proposed Amendments to the Ministerial Directions Powers in Part 3 of the SOCI Act. We commend the Act for successfully raising awareness and driving action across Australia's diverse critical infrastructure sectors through its principles-based approach. We believe the Act has largely achieved its intended objectives, particularly in fostering a proactive stance towards risk management.

The security task for cyber defenders continues to evolve with rapid advances in technologies, such as AI, expanding and reshaping the threat landscape, transforming cyber defence, and reshaping workforce requirements. The principles-based approach is a key attribute of SOCI to remain agile to these changes. Cisco recognises the necessity for government processes to also be similarly agile. However, care is needed that this is not to the detriment of the checks and balances already present in SOCI that ensure appropriate consultation with affected entities and the application of "last report" powers are indeed those of last resort.

Cisco remains committed to supporting the objectives of the SOCI Act and ensuring the resilience of Australia's critical infrastructure. We welcome further industry consultation on the proposed amendments as they are developed.

Regards

[redacted]

[redacted]

Cisco Australia

**Cisco Systems Australia Pty Ltd**

Level 14, 101 Collins Street
Melbourne Victoria Australia 3000

## Detailed response

### Measure 1: Amendments to the existing directions power in section 32

Cisco recognises the need for government agility to react to a rapidly changing threat environment. We support the optimisation and streamlining of government process and decision making with agility as the goal. However, the robustness and rigour of the analysis that precedes any decision should not be weakened. As a point in case, the example scenario for Measure 1 in issuing directions to a data storage/processing provider to onshore certain capabilities would be very specific to the unique operational and technical architecture not only of that provider, but also in how that provider's cloud service or capability is integrated within each of the critical infrastructure entities own systems. Given the diversity of cloud service types and delivery models, any Ministerial direction should only apply to the specific provider and not the sector as a whole – even if the MSP in this scenario was also used by other providers. That the risk could not be mitigated by other controls might be very specific to that provider and not reflective of the wider sector.

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

As the first mitigation for high-risk vendors, products, or services, Cisco supports rigorous, standardised supply chain security and risk management frameworks – operationalised by both critical infrastructure asset owners through their CIRMP and the vendors and providers within their supply chain. As identified in the public consultation paper there are a range of compensating controls that not only could mitigate the risk during transition but also as an ongoing mitigation. Prior to any direction, expert advice such as that provided by A SD in the case of high-risk vendors in 5G networks and from the affected industries themselves should be sought. We request further consultation on the definition of high-risk noting that the IT supply chain is complex, and high-risk vendors might also supply low-risk componentry used in the supply chain of other vendors and services. Any declaration of high-risk vendor would likely need to be at least a declaration of vendor+products or vendor+services, potentially even extending to vendor+product+purpose of use / deployment. Lack of clarity and transparency on the specific concern or threat that cannot be otherwise treated may lead to confusion in CI sectors and industry on exactly what the priority to remediate is.

**Cisco Systems Australia Pty Ltd**

Level 14, 101 Collins Street
Melbourne Victoria Australia 3000

## Measure 4: Delay continuous disclosure requirements

A delayed disclosure power can be a necessary tool in specific, high-risk scenarios where immediate public disclosure might alert advanced threat actors, disrupt ongoing remediation efforts, or trigger cascading attacks on interconnected infrastructure. The practice of delayed public disclosure is already common where industry and government security agencies coordinate notification to relevant stakeholders. Providing some legal protection from disclosure obligation penalties would be beneficial. Of the two proposed options, option 1 is preferable where the agency requiring disclosure reporting (such as ASIC) is the agency providing the exemption. Where security incidents and threat actor campaigns span multiple countries and jurisdictions, option 2 would place companies at risk of violating other jurisdiction's obligations. For these types of incidents, coordination and collaboration between the security agencies of the various countries is required – option 1 would also support that coordination in Australia.

Cisco also recommends that the department develop a formal process whereby critical infrastructure entities themselves can formally request delayed disclosure. Whilst this might occur unofficially as part of incident support engagement with the CISC or ASD, a formal process to request the Minister issue a disclosure delay notification to relevant agencies such as ASIC will provide improved legal certainty for organisations.