Cisco Systems Australia Pty Ltd

Level 14, 101 Collins Street
Melbourne Victoria Australia 3000

Cisco response to the Proposed amendments to enhance the Critical Infrastructure Risk Management Program Rules

Cisco welcomes the opportunity to provide feedback to the Proposed amendments to enhance the Critical Infrastructure Risk Management Program Rules. Cisco remains committed to supporting the objectives of the SOCI Act and ensuring the resilience of Australia's critical infrastructure. We provide the following comments to the questions relevant to our expertise.

All-hazard 1 – Consideration of specified risk advice

Are there any controls on the scope of this measure that your organisation would suggest to assist with compliance and implementation?

The proposal to issue Specified Risk Advice under the All Hazards would be beneficial to ensure awareness of emerging threats.

If the department were to issue Specified Risk Advice, we suggest that guidance clearly explaining the underlying threat also be provided. The PSPF Direction 001-2025 (DeepSeek) is an example where some Critical Infrastructure (CI) entities voluntarily adopted this advice and then subsequently extended the requirement to their supply chain. In this instance that did not prove problematic, as many private organisations had already made the same decision to prevent use of DeepSeek. However, the wording of that directive itself does not provide any context to the nature of the threat. It is foreseeable, that Specified Risk Advice relevant to one sector is not relevant to other supporting sectors or all parts of the supply chain. Whilst that may be the expected thinking, our own experience is that organisations from other CI sectors sometimes request “compliance” with their sector specific standards or frameworks. However, many of those requirements are operational responsibilities of the entity itself not transferable to other sectors or to the supply chain. This is an area where cross-sector maturity needs to improve such that cross sector compliance requirements are presented in a manner that industry can either directly address or jointly with the CI entity itself in a “shared-responsibility model” approach.

Key to assisting with implementation of specified risk advice is ensuring CI entities consider the material risk to the CI asset and whether that risk extends to all or some of their supply chain.

Cisco Systems Australia Pty Ltd

Level 14, 101 Collins Street
Melbourne Victoria Australia 3000

Could existing engagement mechanisms be adapted or improved to deliver more value, and support this obligation?

Like the CISC Factsheet on the Subsection 12F(3) Obligation to notify data storage or processing providers, the department could develop similar material including case studies on how Specified Risk Advice should be considered and communicated cross-sector and to their supply chain.

Cyber 1 – Cyber security framework uplift

Where applicable, what maturity/profile does your organisation seek to achieve?

Due to its international recognition and widespread country adoption including Australia, ISO/IEC 27001 is the baseline security framework Cisco certifies itself and cloud services against. Given, many of our services delivered to other CI Sectors are cloud-based, we also adopt and certify to ISO 27017 Code of practice for information security controls based on ISO/IEC 27002 for cloud services and ISO 27018 Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.

As a global provider, Cisco then seeks to meet the requirements of many country specific security frameworks some of which are specific to different parts of our organisation or offers. These include the ASD ISM via IRAP, US FedRAMP, Japan ISMAP, Germany C5, Spain ENS and others.
In conjunction with AICPA SOC2 audits, ISO 27001 is the certifiable foundation of Cisco's ISMS.

The department has proposed that where a framework does not contain maturity levels (as is the case with AS ISO/IEC 27001 which focuses on continuous improvement rather than explicit levels), an organisation must also in effect adopt an additional framework seemingly purely to achieve a maturity level 2 rating. We recommend further additional discussion of the suggested cybersecurity frameworks and understand how organisations using them achieve uplift in the absence of a maturity levels within the framework itself.

Cisco Systems Australia Pty Ltd

Level 14, 101 Collins Street
Melbourne Victoria Australia 3000

Cyber 2 – Critical systems network segregation

What current measures does your organisation implement to segregate their critical systems from all other internet facing and less secure systems?

Cisco uses a variety of, and layered approach, to separate or segment systems including physical segmentation, network segmentation, administrative and management interface segmentation, identity segmentation, and other approaches.

The paper suggests there two segmentation approaches: segmentation by design and (ad hoc or dynamic) segmentation as a means of incident containment. The former is generally well covered in cybersecurity frameworks and advice from ASD. The later, requires planning and design such that the capability for dynamic segmentation exists should the need for incident response and containment arise. Some approaches to segmentation (which should be multilayered) may not provide the dynamic capability desired. Without being prescriptive on the technological means of achieving segmentation, we do agree with the value of promoting both approaches.

Cyber 3 – Multi-factor authentication (MFA)

What type of systems in your organisation are currently protected by MFA?

The requirement is for all access to be protected by MFA. Cisco implements phishing resistant MFA broadly across its systems, including production environments, VPN access, cloud applications, privileged account access, root access, and management consoles.

Cisco supports the proposal that only where a cyber security framework does not already in effect already require MFA that organisations demonstrate or attest to MFA as a separate requirement. For example, ISO 27001 requires secure authentication – where MFA is typically a core component of demonstrating compliance.

The department may consider also adopting “secure authentication” or similar wording rather than MFA explicitly. MFA is generally a requirement of human to machine interfaces whereas machine to machine (e.g. API), or agentic AI might use certificate-based authentication. A requirement for secure authentication (if not already in the framework) may have a broader uplift impact than that of specifically MFA.

Cisco Systems Australia Pty Ltd

Level 14, 101 Collins Street
Melbourne Victoria Australia 3000

Personnel 1 – Personnel Security Hazards

How many AusCheck background checks do you anticipate undertaking each year?

As a global company, Cisco uses background check providers who can service many markets including Australia. Cisco recommends the current guidance of AusCheck *or equivalent* is retained including for Australia based critical workers. The criminal record and visa work entitlement checks for the CIRMP security-relevant offences are also met by commercial background checking services. We recommend the CIRMP should both continue to focus on the personnel hazard and also continue to allow organisational flexibility in treating that risk.