Cisco Systems Australia Pty Ltd

Level 14, 101 Collins Street
Melbourne Victoria Australia 3000

CISCO AUSTRALIA RESPONSE: SOCI Act Draft Risk Management Program Rules and other guidance

Cisco welcomes the opportunity to provide feedback on the Draft Risk Management Program rules and other guidance.

Draft Risk Management Program Rules

The draft legislative instrument and explanatory statement are consistent with the collaborative engagement and discussions led by the Department of Home Affairs to date and hence much of our previous input is already addressed.

We do recommend a change to the definition of "high risk vendor" to improve alignment with that term as understood under the TSSR and supply chain security advice from the ACSC.

The draft legislative instrument Part 1.3 defines

high risk vendor *means any vendor that by nature of the product or service they offer, has a significant influence over the security of an entity's system.*

The explanatory statement Section 10 states

A high risk vendor is any vendor that by nature of the product or service they offer, has a significant influence over the security of an entity's system. For example, the vendor may be subject to adverse extrajudicial direction, the vendor's poor cyber security posture may mean they are subject to adverse external interference, or the vendor may in some other way transfer unreasonable risk to an entity's system; and

Logically, critical infrastructure asset owners identify their critical vendors (who have a significant influence over the security of a system) and then assess the risk of that vendor across multiple criteria (refer to ACSC) to determine if they are a high risk vendor, or some lower risk.

Cisco Systems Australia Pty Ltd

Level 14, 101 Collins Street
Melbourne Victoria Australia 3000

Separate definitions of "critical vendor" and "high risk vendor" - as expanded upon in the explanatory statement - would better align with Australian telecommunications sector guidance especially related to 5G, ACSC supply chain guidance, and that from peers such as the NCSC[1].

Draft Risk Management Program Guidance for Industry

Supply Chain Hazards - point 68 also defines high risk vendor. This would need aligning with any critical vendor vs high risk vendor clarification changes as per the above.

[1] NCSC advice on high risk vendors in UK telecoms - NCSC.GOV.UK