Zscaler Submission to the Consultation on the Exposure Draft of the Critical Infrastructure Risk Management Program Rules under the Security of Critical Infrastructure (SOCI) Act 2018

1 May 2026

Zscaler welcomes the Australian Government's continued leadership in strengthening the security and resilience of Australia's critical infrastructure through the proposed enhancements to the Critical Infrastructure Risk Management Program Rules (CIRMP) of the SOCI Act 2018.

Zscaler supports the Government's continued commitment to a risk-based and all-hazards approach to critical infrastructure security. The proposed amendments build on existing CIRMP obligations, remain principles-based and continue to apply the "as far as reasonably practicable" standard. This is an important foundation, particularly given the diversity of critical infrastructure assets, operating models, legacy systems and risk profiles across the sectors in scope.

However, Zscaler considers that the exposure draft should more directly align the CIRMP with the Australian Government's stated policy objective of transitioning its own systems away from outdated, perimeter-based network security models and toward modern Zero Trust architectures.

ln Zscaler's context, Zero Trust means enforcing identity and policy-based access for each user, workload, and increasingly each Artificial Intelligence (AI) agent, verifying explicitly and continuously rather than trusting a network location or perimeter. This approach is in line with internationally recognised guidance, including the Zero Trust Architecture described in the National Institute of Standards and Technology Special Publication 800-207.[1]

Zero Trust is a security model supported by empirical evidence showing both a measurable security dividend and measurable transformation benefits.

- Security dividend: The *IBM/Ponemon Cost of a Data Breach Report* (2022)[2] found organisations with a mature Zero Trust architecture experienced approximately USD 1-1.7 million lower average breach costs per incident than organisations without Zero Trust architecture in place.

- Transformation benefit: Independent economic analyses, including Forrester Total Economic Impact (TEI) studies of Zero Trust access, commonly quantify rapid payback and high return on investment when Zero Trust is used to replace broad network access models such as VPN-centric access and reduce operational overhead.

[1] *Zero Trust Architecture (NIST SP 800-207)* – https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

[2] *Cost of a Data Breach Report 2022* – https://newsroom.ibm.com/2022-07-27-IBM-Report-Consumers-Pay-the-Price-as-Data-Breach-Costs-Reach-All-Time-High

- For example, *Forrester's TEI for Zscaler Private Access*[3] reported 289% return on investment over three years for a composite organisation.

This is important in the context of the perceived regulatory burden associated with SOCI compliance. Ensuring entities in scope understand the benefits of modernising their cyber security infrastructure is therefore essential.

Achieving strategic alignment on Zero Trust

The 2023-2030 Australian Cyber Security Strategy[4] states that the Government will draw on internationally recognised approaches to Zero Trust, aiming to develop a whole-of-government Zero Trust culture. To achieve this objective, since the release of the Strategy, the Government has updated the Information Security Manual and the Protective Security Policy Framework (PSPF) to execute this shift. Additionally, important steps were taken with the release of the Guiding Principles to embed a Zero Trust Culture[5] and the Foundations for Modern Defensible Architecture (MDA)[6]. Together, they provide clear policy intent and practical implementation direction for departments and agencies to move away from implicit trust and perimeter-based controls and toward identity-centric, least-privilege, continuously verified access and inspection across users, devices, applications and data.

Despite this, the exposure draft employs terminology that may be interpreted as reflecting traditional, perimeter-centric network assumptions - such as trusted internal networks, perimeter-based access, network segregation and legacy remote access models. This creates a risk of misalignment between the Government's stated strategic direction toward Zero Trust and the way critical infrastructure entities may interpret and implement the CIRMP requirements in practice.

In particular, the Rules should avoid unintentionally reinforcing, implicitly or explicitly, legacy architectures such as virtual private networks, flat networks, implicit trust zones and perimeter-dependent security controls. These architectures have proven insufficient in the face of modern cyber threats, including credential compromise, lateral movement, ransomware and supply chain compromise.

This is becoming increasingly critical because developments in frontier AI (including generative AI and autonomous agents) are rapidly amplifying cyber threats. Attacks driven or automated by advanced AI can quickly overwhelm legacy perimeter defences. In this context, adopting Zero Trust (continuous identity-based verification) becomes even more critical: every user and AI agent accessing systems must be authenticated and authorised, and lateral trust must be eliminated.

---

[3] *The Total Economic Impact™ of Zscaler Private Access* – https://tei.forrester.com/go/Zscaler/PrivateAccess/?lang=en-us

[4] *2023-2030 Australian Cyber Security Strategy - https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf*

[5] *Guiding Principles to Embed Zero Trust Culture - https://www.homeaffairs.gov.au/cyber-security-subsite/files/consultation-paper-guiding-principles-to-embed-zero-trust-culture.pd*

[6] Foundations for Modern Defensible Architecture - https://www.cyber.gov.au/sites/default/files/2025-10/foundations-for-modern-defensible-architecture.pdf

The Department should ensure the enhanced rules are written, interpreted and implemented in a manner consistent with Australia's Zero Trust policy direction as outlined in the 2023-2030 Strategy, the shift underway within the Federal Government, and established best practice.

Targeted Amendments to Embed Zero Trust within the CIRMP

To achieve greater alignment between the Government's stated objectives for cyber uplift through Zero Trust, Zscaler recommends several amendments to the draft rules.

There is a need to explicitly draw the link to better security outcomes through Zero Trust under the frameworks section of the draft. Zscaler recommends this amendment, adding the bold text below at Section 8A(4):

A responsible entity for a CI asset specified in subsection 4A(1) may otherwise comply with subsection (3) of this section by establishing and maintaining a process or system in their CIRMP to comply with a framework that is equivalent to a framework in a document mentioned in subsection (3), including any [relevant] conditions. ***This may include modern Zero Trust approaches (for example, identity- and context-based access decisions, least privilege, continuous verification and monitoring), provided the responsible entity achieves equivalent or stronger security outcome****s.*

This reduces the risk of inadvertently entrenching VPN-centric or perimeter-centric approaches, while preserving flexibility for diverse environments and operating models.

Update "remote access" framing from "access to networks" to "access to applications/systems/services"

References to remote access "to networks" may unintentionally signal that broad network tunnels are an expected pattern, whereas modern best practice is to grant access at the application/system/service level with continuous verification.

Where relevant, Zscaler recommends replacing "remote access to networks" with "remote access to applications, systems or services", to ensure controls are framed as outcomes (least privilege, session controls, monitoring, rapid revocation). Consistent with CISA's Zero Trust Maturity Model, this framing ensures that security is applied at the resource level to explicitly prevent lateral movement across the network. This approach adopts the NIST SP 800-207 principle that access should be granted on a per-session basis, moving away from "implicit trust" based on a user's presence on a network segment.

Broaden "network segregation" to "segmentation by any means" (Section 8A(8)–(9))

Mandating "network segregation" and controls "between critical systems and all other networks" can be read as privileging perimeter/VLAN-based segmentation over identity/application-based segmentation and cloud-native controls.

Recommended amendment: Replace “network segregation” with “segmentation”, and clarify that it may be achieved via network-based and/or non-network-based means (e.g., identity controls, host-based controls, application-layer controls, software-defined micro-segmentation, cloud-native controls).

Zscaler suggests replacing “network segregation” with *“segmentation of critical systems from other systems and services, by network-based and/or non-network-based means, to limit unauthorised access and lateral movement.”*

This preserves the security objective (limit blast radius; prevent lateral movement) without embedding legacy assumptions about internal trusted networks or requiring a specific segmentation technique.

Refine MFA scope to remain risk-based

MFA phrased around “internet-facing networks” and “remote access to networks” can create an “inside vs outside” security distinction. Separately, exceptions that are too narrow can lead to either non-compliance or “tick-box” compensating controls, especially in safety/operationally constrained environments.

Proposed amendment to text at Section 8A(5)(a):

(a) authenticate:

> *(i) users to applications, systems or services used to access or administer critical systems;*
>
> *(ii) privileged and unprivileged users of critical systems;*
>
> *(iii) remote access to critical systems (including remote access via any intermediary system or service).*

This keeps the Rules risk-based and enforceable in complex environments, encourages modernisation where feasible, and avoids inadvertent encouragement of “internal equals safe” assumptions.

Remove implicit endorsement of “trusted internal networks”

Phrases implying networks are ordinarily “trusted” (e.g., “no longer trusted networks”) can embed outdated security assumptions into the compliance model.

Zscaler recommends replacing “no longer trusted” style language with an assurance-based formulation tied to compromise, integrity, or loss of confidence in access pathways and communications.

This aligns legislative language with a Zero Trust posture (assume breach; verify explicitly) without mandating any particular control.

Suggest change at Section 8A(8)(c)(i):

CI asset networks are compromised or there is a loss of integrity

Additional amendment requested: explicitly address AI agent / non-human user identities (Section 8A)

There is a need to ensure "users" includes AI agents and other non-human actors; require attributable, controllable identities.

"User" is commonly interpreted as a human. In modern environments, non-human actors (AI agents, automated accounts, service accounts, workloads) can initiate actions that materially affect critical systems. If the Rules do not clearly capture non-human actors, a compliance gap may emerge where strong controls apply to human logins but not to agent/service identities, tokens, and delegated access.

Recommended amendment (Section 8A): Insert a new subsection near access control/MFA requirements or in the SOCI definitions:

For the purposes of this section, references to a user accessing a critical system include a human user and any non-human actor acting on behalf of a human or process, including an automated account, workload, service account, or Artificial Intelligence (AI) agent. A responsible entity must ensure such access is attributable to a unique identity and is subject to appropriate authentication, authorisation, monitoring and timely revocation commensurate with risk.

This future-proofs the Rules as AI-enabled operations mature, aligns with the risk-based intent under the CIRMP, and ensures the same "verify explicitly" discipline applies to non-human access paths that may otherwise bypass user-centric controls.

Conclusion

Zscaler supports the intent of the enhanced CIRMP and thanks the Department for engaging with industry. The proposed measures will enhance Australia's critical infrastructure resilience. By incorporating the above amendments, particularly those embedding Zero Trust outcomes, preserving architectural flexibility, and explicitly capturing AI agent identities and access, the Rules will better align with government policy and current security best practices. This alignment will help Australia not only mitigate today's threats, but also transition to a more secure, modern cyber posture for the long term. Zscaler looks forward to being a partner in the continued uplift of the security of Australia's critical infrastructure.

[redacted]