Australian Information
Industry Association

Australian Information Industry Association

Submission on

Guiding Principles to Embed Zero Trust Culture

28 February 2025

Introduction

The Australian Information Industry Association (AIIA) welcomes the opportunity to provide feedback to the Department of Home Affairs on the *Guiding Principles to Embed Zero Trust Culture* Consultation Paper. We note that a separate consultation is underway regarding the *Government Gateway Security Standard*, which also has implications for Zero Trust (ZT) implementation.[1] While this submission primarily focuses on the *Guiding Principles to Embed Zero Trust Culture*, we provide high-level commentary on the *Gateway Security Standard* here and will address that separate consultation in more detail in a later submission.

AIIA has long supported the adoption of Zero Trust (ZT) principles as part of a modern, risk-based approach to cyber security across government agencies. With cyber threats becoming more sophisticated and persistent, traditional perimeter-based security models are no longer sufficient. As set out in our 2025–2026 Pre-Budget Submission[2], we believe well-resourced and risk-driven cyber security investments are central to enhancing national resilience. Similarly, our response to the *2023–2030 Cyber Security Strategy Discussion Paper*[3] emphasised the need for integrated frameworks that break down silos. In the context of Zero Trust, that means ensuring alignment across various policies—from protective security frameworks through to digital identity and user-centric design, as we highlighted in our *myGov User Audit* submission[4].

The AIIA therefore welcomes these Guiding Principles as an important step forward in embedding Zero Trust culture more deeply across government. We look forward to working collaboratively with the Department of Home Affairs and other stakeholders on refining these principles, ensuring compatibility with broader digital transformation initiatives, including future policy settings on the Government Gateway Security Standard.

Q6. Education, Training, and Leadership Engagement

Question:
What requirements and policies are most effective to ensure that all areas within an organisation (technical and non-technical) develop a necessary baseline understanding of cyber security concepts applicable to their role?

Successfully embedding a Zero Trust culture within government agencies requires more than just technical and policy-based changes; it necessitates a fundamental shift in workforce understanding, behaviour, and accountability. This shift must be reinforced through ongoing education, structured training programmes, and direct engagement with

[1] Department of Home Affairs, Commonwealth Cyber Security Policy Consultation Package, 2025.
[2] Australian Information Industry Association, 2025-2026 Pre-Budget Submission, 31 January 2025, p. 5.
[3] Australian Information Industry Association, Response to the Cyber Security Strategy 2023-2030 Discussion Paper, 20 April 2023, p. 16.
[4] Australian Information Industry Association, myGov user audit – AIIA Response, 30 November 2022, p. 6.

leadership to ensure ZT principles are actively implemented across all levels of government.

A key aspect of this transformation is moving beyond traditional cyber security awareness to developing *cyber fluency*. The consultation paper highlights the importance of cyber fluency as the ability to apply cyber security knowledge proactively in everyday work environments, rather than relying on compliance-based checklists. This means that ZT education should not only introduce security concepts but also empower employees to identify and mitigate risks autonomously.

Furthermore, leadership plays a crucial role in embedding these principles across government agencies. Senior officials and decision-makers must not only endorse the framework but also actively engage with it. ZT education should be integrated into government leadership development programmes, ensuring that executives and agency heads are equipped to make informed decisions regarding security investments, policy design, and risk management. Without a top-down commitment, ZT adoption risks being seen as an IT-driven initiative rather than a whole-of-government transformation.

A successful ZT culture is not achieved through policy mandates alone but requires ongoing education, continuous engagement, and strategic leadership involvement. By embedding cyber security into workforce training and executive decision-making, government agencies can move beyond compliance and foster a culture of proactive cyber resilience.

Recommendations

1. **Establish Structured Cyber Fluency Programmes**
   Move beyond compliance-based checklists by incorporating regular, scenario-based training for all staff. These programmes should emphasise autonomous risk identification, enabling employees to recognise and mitigate threats in their daily work.

2. **Embed ZT Education in Leadership Development**
   Integrate Zero Trust awareness into executive and leadership training. Senior leaders and agency heads should actively endorse and sponsor ZT adoption, ensuring it remains a priority for governance and budgetary decisions.

3. **Ensure Continuous Engagement and Accountability**
   Create pathways for regular feedback, refresher training, and performance reviews tied to cyber risk management. This helps cultivate a sustained culture of security, rather than one-off compliance exercises.

Q7. Modified Requirements for the PSPF and HCF

Question:
What modified or new requirements would you recommend for the PSPF, HCF or the Whole of Government Gateway policy to embed zero trust culture?

The Australian Signals Directorate's (ASD) *Foundations for Modern Defensible Architecture* (The Foundations) defines Zero Trust's core principles as *"never trust, always verify"*, *"assume breach"*, and *"verify explicitly."* These principles draw on global standards (e.g. NIST, CISA) and emphasise a risk-based approach rather than rigid compliance checklists.

Zero Trust principles do not equate greater security outcomes with a specific geolocation for data or technology. Instead, they allow organisations to maintain flexibility over how and where data is stored, provided the appropriate controls are in place. By contrast, the Protective Security Policy Framework (PSPF) and Hosting Certification Framework (HCF) can be highly prescriptive, limiting the government's ability to engage with providers offering robust, yet differently architected, solutions.

Australia's Information Security Manual (ISM) offers a more flexible model, where the *intent* of controls is prioritised. Entities may deploy alternate controls if they achieve equivalent security outcomes. Aligning the PSPF and HCF more closely with such Zero Trust-style, outcome-based approaches would foster innovation while maintaining strong security.

Recommendations

1. **Focus PSPF and HCF using a Risk-Based Approach**
   Move away from prescriptive mandates, allowing alternate controls that meet or exceed security objectives.
2. **Use the ISM as a Model for Flexibility**
   Adopt the ISM's practice of allowing "alternate controls" for non-standard architectures that still achieve strong Zero Trust outcomes (e.g. micro-segmentation, robust identity management, continuous verification).
3. **Enable Access to World-Class Solutions**
   Remove overly rigid constraints so the government can access leading-edge technologies—particularly modern cloud-based and distributed solutions—without sacrificing compliance.
4. **Prioritise Outcomes**
   Recognise that Zero Trust focuses on identity-based security rather than just location-based security. Data sovereignty can be achieved through measures like encryption and auditing.

Q9. Alignment Between Broader Cyber Strategy and Individual Uplift Plans

Question:
What requirements or policy change would you recommend to ensure alignment between your broader cyber strategy and individual uplift plans? What governance or oversight mechanisms are in place to coordinate these efforts?

Zero Trust as an Enabler of Agility and Operational Efficiency

Beyond its role in strengthening cyber security, Zero Trust also presents a significant opportunity to enhance operational agility, streamline access management, and improve the user experience across government agencies—an approach that resonates with the AIIA's broader calls for user-centric design in government digital services.[5].

Traditional cyber security models have historically created friction in government operations, requiring cumbersome authentication steps, restrictive network access policies, and complex compliance-driven security controls. These barriers often slow productivity and create inefficiencies, particularly in hybrid work environments where employees require secure access across multiple locations and devices. By shifting to a Zero Trust model, agencies can simultaneously improve security and reduce operational complexity.

One of the key advantages of Zero Trust is its ability to eliminate reliance on legacy access methods, such as virtual private networks (VPNs) and static password-based authentication. With identity-based access controls, adaptive authentication, and password-less security mechanisms, government employees can experience faster, more seamless access to the resources they need, regardless of their location. This not only strengthens cyber security but also creates a more efficient and user-friendly work environment. Zero Trust can also improve the consistency of hybrid work experiences, ensuring that employees, contractors, and third-party vendors receive the same level of secure access whether working from a government office, remotely, or across multiple devices. By applying continuous verification and conditional access policies, agencies can remove unnecessary authentication barriers while still ensuring strong security controls.

Given these benefits, it is important that Zero Trust is not only viewed as a security measure but as a tool for improving government agility and service delivery. Agencies should actively identify opportunities where security can enhance, rather than hinder, operational efficiency.

[5] Australian Information Industry Association, myGov user audit – AIIA Response, 30 November 2022, p. 6.

Recommendations

1. **Prioritise Tech Modernisation and Frictionless Zero Trust Solutions**
   Focus on VPN-less access, adaptive authentication, and password-less mechanisms that raise security posture while improving user experience.
2. **Enhance the Hybrid Work Environment**
   Adopt Zero Trust policies enabling the same secure experience for employees, contractors, and partners, whether on-site or remote, across various devices and networks.
3. **Align ZT with Broader Digital Transformation**
   Integrate Zero Trust into government innovation and service delivery initiatives, ensuring cyber security supports rather than hinders ongoing reforms (e.g. digital identity projects, cloud procurement).

Additional Feedback: Aligning Guiding Principles with ACSC Guidance and the Government Gateway Security Standard

With multiple consultations—including both the *Zero Trust Guiding Principles* and the *Government Gateway Security Standard*—currently under review, there is a growing risk of duplicative or inconsistent requirements. We also note that various government initiatives address Zero Trust concepts (e.g. changes to the *Security of Critical Infrastructure Act*, new cyber security obligations) yet appear to be developed in isolation. For example, many of the *Guiding Principles to Embed Zero Trust Culture* overlap with the Australian Signals Directorate's *Foundations for Modern Defensible Architecture*, demonstrating that there is still a need for more explicit cross-referencing. The AIIA recommends a coordinated approach to ensure each policy instrument complements the others, creating a clear, unified framework for agencies to follow.

Additionally, in the AIIA's *2023–2030 Cyber Security Strategy* response, we highlighted that smaller agencies would benefit from practical, hands-on guidance—beyond high-level principles. A standardised set of Zero Trust solution "templates" would help these agencies avoid repeatedly solving the same technical challenges.

Recommendations

1. **Clarify Alignment with ACSC Guidance**
   Explicitly map each proposed Zero Trust Guiding Principle to ASD Framework to prevent duplicative or conflicting advice.[6]

[6] Australian Cyber Security Centre, Foundations for Modern Defensible Architecture, 10 February 2025.

2. **Suggest Reference Architectures and Repeatable Patterns**
   Publish example *"blueprints"* or reference architectures (tailored for varying agency sizes/risk profiles) demonstrating how Zero Trust can integrate with existing controls like the Essential Eight (E8).

3. **Coordinate Multiple Consultations**
   a. Form a single coherent approach to oversee Zero Trust policy alignment with gateway standards, the PSPF/HCF, and future cyber initiatives, ensuring agencies can adopt holistic, risk-based approaches rather than a patchwork of compliance measures.
   b. *Enable* longer implementation lead times where mandated Zero Trust elements overlap with other reforms, so that organisations—particularly smaller ones—could handle compliance costs and planning in stages.

Conclusion

Successfully embedding Zero Trust culture within government agencies requires a fundamental shift in how cyber security is approached. Rather than relying on rigid, prescriptive controls, the government should embrace a flexible, risk-based security model that enables continuous verification, assumes potential breaches, and proactively mitigates threats. By positioning Zero Trust as an operational mindset—rather than merely a technical framework—the government can bolster cyber resilience, build public trust, and strengthen Australia's standing as a global leader in cyber security best practices.

This vision aligns with the AIIA's broader policy recommendations set out in our *2025–2026 Pre-Budget Submission*, *2023–2030 Cyber Security Strategy Response*, and *myGov User Audit Submission*—all of which underscore the importance of user-centric, risk-based, and forward-thinking approaches to digital government.

The AIIA appreciates the opportunity to contribute to this important initiative and looks forward to continued collaboration to support the implementation of a robust, adaptive, and effective Zero Trust culture across government agencies.

Should you require further information, please contact Ms Siew Lee Seow, General Manager, Policy and Media, at siewlee@aiia.com.au or 0435 620 406, or Mr David Makaryan, Advisor, Policy and Media, at david@aiia.com.au.

Thank you for considering our submission.

Yours sincerely
Simon Bush
CEO, AIIA

***

About the AIIA

The AIIA is Australia's peak representative body and advocacy group for those in the digital ecosystem. Since 1978, the AIIA has pursued activities to stimulate and grow the digital ecosystem, to create a favourable business environment for our members and to contribute to Australia's economic prosperity. We are a not-for-profit organisation to benefit members, which represents around 90% of the over one million employed in the technology sector in Australia. We are unique in that we represent the diversity of the technology ecosystem from small and medium businesses, start-ups, universities, and digital incubators through to large Australian companies, multinational software and hardware companies, data centres, telecommunications companies and technology consulting companies