Australian Information
Industry Association

Australian Information Industry Association

Submission on

Australian Government Gateway Security Standard Consultation Paper

Introduction

The Australian Information Industry Association (AIIA) welcomes the opportunity to provide input to the Department of Home Affairs on the Australian Government Gateway Security Standard consultation paper. The increasing adoption of cloud-based security services and Zero Trust principles presents both opportunities and challenges, particularly in the areas of procurement, regulatory compliance, and interoperability across agencies. We recognise the importance of the proposed Gateway Security Standard within the broader Resilient Digital Infrastructure (RDI) framework and commend the Government's engagement with industry stakeholders. Given the evolving cyber threat landscape and the increasing reliance on cloud-based security services, it is critical that policies remain technology-neutral, outcomes-focused, and risk-based to maximise security while maintaining flexibility and innovation.

Procurement Improvements for Stronger Security Outcomes

A well-structured procurement process is essential for ensuring government agencies can access secure and reliable cloud-based security solutions without unnecessary complexity or delays. The procurement process should incorporate pre-approved security templates for SSE adoption, ensuring that agencies can select from validated security configurations that align with government cyber security requirements. Standardised security configurations would streamline secure cloud adoption, reduce the complexity and cost of procurement, and ensure agencies implement proven security architectures. This approach would also help agencies with limited in-house cyber security expertise by reducing the burden of designing and validating security models individually. By centralising the development of vetted security patterns, the Government can minimise redundant security assessments, accelerate SSE adoption, and enhance the resilience of government IT infrastructure. Strengthening procurement frameworks in this manner will enable agencies to scale cyber security capabilities more effectively.

Two-Year Reauthorisation Policy for Gateways

A two-year Authority to Operate (ATO) reauthorisation cycle may be too rigid given the fast-evolving cyber threat landscape. High-risk gateways require more frequent reviews, while lower-risk systems do not need the same level of scrutiny. Additionally, threat intelligence updates occur far more frequently than the two-year cycle, meaning agencies may not reassess security risks in a timely manner.

To address this, a risk-based reauthorisation framework should be introduced:

- High-risk systems should undergo annual security reviews to ensure critical infrastructure is continuously reassessed.
- Lower-risk systems should remain on a two-year cycle, reducing administrative burdens while maintaining oversight.

Additionally, ATO reauthorisation should align with real-time threat intelligence updates from the Australian Cyber Security Centre (ACSC) rather than being tied to a fixed timeframe. Reviews should be triggered by emerging cyber threats, major security incidents, or regulatory changes, ensuring security assessments remain relevant. This risk-based and intelligence-driven approach will prioritise resources efficiently and ensure gateway security reviews remain proactive.

Gateway Hosting

Section 7.1.2 of the draft Standard mandates that cloud Secure Service Edge (SSE) solutions must be hosted within Hosting Certification Framework (HCF)-certified facilities and/or provided by HCF-certified Cloud Service Providers (CSPs). A requirement that could significantly impact SSE performance, security, and flexibility. Given the potential operational and cost burdens associated with this prescriptive localisation requirement, we recommend that the government adopt an outcomes-based approach—one that ensures security objectives are met while allowing government agencies to leverage globally competitive, cutting-edge SSE solutions.

We acknowledge that the HCF plays a critical role in safeguarding sensitive Australian Government data by ensuring it is stored in secure, locally based facilities to mitigate the risks posed by malicious foreign actors. However, SSE solutions operate differently from traditional cloud services. Unlike traditional CSPs that allow users to deploy and run workloads in specific regions, SSE providers do not “host” applications or store data in the same way. Instead, SSE providers offer cloud-based security services which inspect and secure traffic at distributed Points of Presence (PoPs), strategically positioned to mitigate threats in real time. These PoPs utilise anycast routing and load-balancing methods to optimise both security checks.

Given this distinct architecture, Section 7.1.2 should differentiate between the three distinct states of data in SSE solutions:

1. **Data Inspection**: The point at which SSE technology decrypts data to inspect for threats and vulnerabilities. This is the only stage where plaintext data exists and, therefore, presents a potential security risk. However, SSE solutions decrypt data only momentarily, discarding plaintext buffers from memory immediately after security scans.

2. **Data at Rest**: SSE log data (e.g., data for threat detection). This can be stored by the SSE provider or within an Australian Government entity's HCF-certified CSP. Encryption can be managed by the vendor, the government agency, or both.
3. **Data in Transit**: Data transiting networks (e.g., between a government employee's device and an SSE server). This data remains encrypted at all times by default.

If the HCF's objective is to protect government data from compromise from malicious foreign actors, then the only relevant SSE-specific security risk lies in the data inspection point. Therefore, we recommend that the draft Standard:

- Only require SSE data inspection tools to be housed within HCF-certified facilities.
- Exempt data in transit from the HCF requirement as is not static, and any concerns associated with data in transit should be minimal given its continual state of encryption by default. Forcing data in transit to traverse a limited number of facilities will significantly curtail the ability of SSE technologies to mitigate cyber security attacks, given that SSE technology mitigates threats at their source (which could be anywhere in the world), as noted above.
- Acknowledge that Australian Government entities are able to use HCF-certified CSPs to store SSE logging data.

If Section 7.1.2 remains unchanged—requiring that all three SSE data states 'must' be hosted within HCF-certified facilities—the following negative outcomes are likely:

- Reduced flexibility in cloud security strategies;
- Performance degradation with possible latency;
- Operational inefficiencies and increased costs;
- Challenges in maintaining zero-trust principles in a cloud-base environment; and,
- Increased risk of single point of failure.

This is particularly pertinent in the context of SSE data. By encrypting data across multiple stages and retaining direct control over cryptographic keys—through methods such as Bring Your Own Key (BYOK), Hold Your Own Key (HYOK), or external Key Management Service (KMS) setups—the Australian Government can prevent unauthorised access, even if SSE data physically resides in another jurisdiction or uncertified data centres. This approach transforms raw data into unreadable ciphertext outside the trusted boundary, thereby ensuring that agencies can uphold national security while still leveraging the key advantages of SSE's distributed, cloud-based framework.

Conclusion

The Gateway Security Standard plays a pivotal role in securing government IT infrastructure, and it is essential that policies reflect real-world security challenges without imposing unnecessary constraints on agencies or industry providers. A risk-based, outcomes-driven approach will allow agencies to adopt modern security solutions while

ensuring compliance with national security objectives. The AIIA welcomes continued dialogue with the Department of Home Affairs to support the effective implementation of the Gateway Security Standard.

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.