Australian Government

Australian Government Gateway Security Standard

Consultation Paper

February 2025

Purpose

The purpose of this consultation paper is to engage with interested stakeholders on the *"Australia Government Gateway Security Standard*" (the *Gateway Standard*). The *Gateway Standard* describes the strategic direction for the Commonwealth's use of Gateway services and sets the minimum security standard expected to be applied by entities in their use of gateway capabilities.

The success of the intended protections afforded by the *Gateway Standard* requires a collaborative approach across all relevant stakeholders. As the Department considers the application of the *Gateway Standard* through the Protective Security Policy Framework (PSPF) Release 2025, we are eager to ensure a common understanding of its agenda and an accurate assessment of potential impacts through closer engagement with industry as well as the broader Commonwealth entity cohort.

The *Gateway Standard* is a part of a broader coordinated Commonwealth Cyber Security Uplift consultation agenda facilitated by the Department of Home Affairs. As the Department continues to work to provide best practice policy guidance to protect the Commonwealth digital services from cyber-attacks, additional open consultation opportunities will be provided to ensure the success of the proposed policy changes. Other opportunities include the "*Guiding Principles to embed a Zero Trust Culture,"* consultation paper which is currently open for submissions, with upcoming opportunities including the Hosting Certification Framework revision to be released this year.

The Gateway Standard consultation paper has been developed in consideration of technical advice provided by the Australian Signal Directorate's Australian Cyber Security Centre (ASD's ACSC), including the *Gateway Security Guidance Package*.

Context

Shield 4 of 2023-2030 Australian Cyber Security Strategy, highlights the importance of uplifting Commonwealth Government cyber security. To achieve this, we are delivering a suite of policies for the Australia Government's cyber security capabilities to build resilient systems for the future. Commonwealth Cyber Security requires multiple lines of effort across business domains. Globally, we are seeing a growing focus for governments and industry to adopt zero trust practices, to provide a modern defensible architecture that offers a way to increase our systems cyber security resilience.

To support this critical agenda, the Department is consolidating a number Australian Government IT infrastructure policies under a cohesive Resilient Digital Infrastructure (RDI) framework. This includes replacing the existing *Australian Government Gateway Policy (Gateway Policy)* and the *Secure Cloud Strategy,* as well as integrating with reforms to the Hosting Certification Framework.

The RDI provides a set of core concepts and pillars, seeking to guide an extensible policy basis for the Department to promote the adoption of more contemporary technology and security practices to secure Australian Government's digital infrastructure at its foundations. The policies, strategies and standards developed under the RDI guidance will support the adoption of contemporary, essential cyber security resilience practices including Zero Trust, Secure-by-Design and Secure-by-Default concepts.

Submission Guidance

The Gateway Standard consultation paper calls out suggested consultation points throughout the document. These consultation points are not mandatory and have been provided to assist interested parties in providing targeted feedback. Responses to this paper will assist in the Department in its development of the final version of the Gateway Standard and may help to inform other artefacts developed under RDI framework.

Submissions can be submitted via email at consultCCSU@homeaffairs.gov.au.

RDI Framework

The RDI framework has two policy layers managed by Home Affairs and a technical layer managed by ASD's ACSC; These two policy layers are:

- **Pillars,** which provide overarching policy guidance for Australian Government digital infrastructure, and allows for a broad application to all forms of digital infrastructure.
- **Standards**, which outlines the policy direction and minimum-security standards for specific elements of the Australian Government's digital infrastructure.

The technical layer is the **Guidance** layer which provides technical guidance for the security of a specific element of digital infrastructure that is applicable to the Australian Government. ASD will be providing this guidance in line with their existing mission to provide the Australian public with threat informed and intelligence driven cyber security advice.

Pillars

The Resilient Digital Infrastructure (RDI) Pillars provide a consistent set of principles to govern both the development of policy under RDI and describe the characteristics that the framework is encouraging with the Australian Government's digital infrastructure. The pillars have broad applicability to all elements of IT infrastructure, regardless of whether a standard or guidance package has been published for it.

The RDI Pillars are intended to be published as a section within the PSPF Release 2025 as well as being incorporated across the other layers of the framework and within other applicable policy initiatives.

Secure

A resilient digital infrastructure is comprised of elements that are both intrinsically secure and secure in their context.

This pillar seeks to build up the resiliency of the Australian Government's digital infrastructure through uplifting the security of the infrastructure's individual elements. These elements include individually hardening assets as well as ensuring those assets are deployed in a secure environment.

Open

A resilient digital infrastructure is built on the open exchange of information and the active participation of all suitable participants.

This pillar seeks to uplift the resiliency of the Australian Government's digital infrastructure through an open approach in two areas. Firstly, the open exchange of information and good practice between commonwealth entities, vendors, and trusted partners. Secondly, through the open participation of a broader range of IT vendors.

Flexible

A resilient digital infrastructure is flexible and modular, able to support and secure the changing functional requirements of its users and their environments.

This pillar seeks to uplift the resiliency of the Australian Government's digital infrastructure by improving its flexibility in how infrastructure is developed, deployed, and used. This includes ensuring that the infrastructure is robust enough to support a broad range of use cases and organisational needs.

Adaptable

A resilient digital infrastructure provides a secure foundation that can readily adapt and respond to emergent threats.

This pillar seeks to uplift the resiliency of the Australian Government's digital infrastructure by ensuring that infrastructure is adaptable to new technologies and threats. This includes ensuring that both IT infrastructure, and the policy governing it, can be modified and adapt to new and emerging technology, new technical and security practice, and new threats.

Scalable

A resilient digital infrastructure is readily scalable to meet the requirements of an evolving risk landscape.

This pillar seeks to increase the resiliency of the Australian Government by making it easier to scale up and down to support Commonwealth entities' capacity requirements. This will allow Commonwealth entities to readily expand and contract in response to either planned or unplanned spikes and drops in demand.

Consultation Point 1:

What are the challenges and opportunities that Australian Government Entities might discover in aligning their digital infrastructure outcomes with the RDI Pillars?

Consultation Point 2:

What other policy measures could be considered to encourage the adoption of the RDI Pillars?

Standards

The standards layer of the framework provides the extensible element to the framework and allows Home Affairs to develop policy for specific components of the Australian Government's digital infrastructure. These standards provide the policy direction and minimum security standards specifically for Australian Government entities deploying certain IT infrastructure components.

Standards are developed by Home Affairs and will be published as a PSPF standard. Each standard will have a corresponding PSPF requirement that entities will need to address. PSPF Standards detail additional mandatory requirements on specific topics.

Gateways have been identified as the first component of digital infrastructure for an RDI standard and a consultation draft of the Gateway Standard has been included in this consultation draft. Home Affairs also has RDI standards planned for cloud computing over 2025.

Consultation Point 3:

What other components of IT infrastructure should be considered for a RDI Standard?

Guidance

As the Australian Government's technical authority on cyber security, the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) develops threat informed technical advice and guidance. The PSPF Standards will refer to ASD's ACSC technical advice where relevant to those standards.

The guidance layer of the framework provides technical advice and guidance to Australian Government entities on particular IT infrastructure components. This ensures that Australian Government entities have the necessary technical information to implement RDI Standards and manage their IT infrastructure in a secure manner.

Guidance will be developed by the ASD's ACSC as the Australian Government's technical authority on cyber security. Guidance packages will be published on cyber.gov.au as part of their existing mission to provide the Australian public with threat informed and intelligence driven cyber security advice.

For the Australian Government Gateway Security Standard, ASD's ACSC's Gateway Security Guidance Package contributes to the guidance layer of the Framework.

Australian Government Gateway Security Standard

The Gateway Standard is the first component of RDI that has been published for open consultation and will be the first PSPF Standard released under the framework.

Gateways was selected as the first component to be addressed under RDI due to the significant changes that have occurred in this space both technologically and architecturally since the current Gateway Policy was developed. Changes to gateway policy arrangements are also designed to support the government's adoption of Zero Trust. Additionally this will provide the gateway policy replacement intended for delivery as part of the Cyber Hubs program.

1. Purpose

The Australian Government Gateway Security Standard (the Standard) applies to all Non-Corporate Commonwealth Entities and provides them with guidance on the strategy direction and minimum standards for Gateway and Security Service Edge (SSE) solutions within the Australian Government. This standard also represents better practice for Corporate Commonwealth Entities in their deployment of Gateways and SSE solutions.

Gateways and SSE solutions provide Australian Government entities with a broad suite of cyber security functionality and capabilities at the boundary of their security domains. The Department of Home Affairs has developed this standard to assist Australian Government entities in the deployment of gateways to manage their own cyber security risk, as well as improving the of Whole of Government (WofG) cyber security risk posture.

The Australian Government Gateway Security Standard forms part of the Resilient Digital Infrastructure Framework (RDI) framework, alongside the technical guidance published by the Australian Signal Directorate's (ASD) Australian Cyber Security Centre (ACSC) in the Gateway Security Guidance Package. The broader application of the Protective Security Policy Framework (PSPF) and the Information Security Manual (ISM) should also be applied when considering the gateway security.

Requirement XXXX | TECH | All entities | XX Month 202X

Digital infrastruture that processes and stores Australian Government information is protected by a Gateway or Security Service Edge in accordance with the Australian Government Gateway Security Standard.

Consultation Point 4:
How do you interpret the newly proposed PSPF Requirement?

Requirement 0114 | TECH | All entities | 31 October 2024

Gateways that have completed an IRAP assessment against ASD's Information Security Manual with the previous 24 months are used.

2. Applicablility

The Australian Government Gateway Security Standard has been developed as part of the Resilient Digital Infrastructure Framework. It supersedes the Government Gateway Policy, previously developed by the Digital Transformation Agency as part of the Hardening Government IT program.

As a standard of the Protective Security Policy Framework, it is a mandatory element of the framework for Non-Corporate Commonwealth Entities.

This Standard is applicable to gateways that interact with the internet and not applicable to Cross Domain Solutions that handle highly classified material.

2.1.1. Language in Policy Statements

To assist in application of this standard, policy statements are dispersed throughout this standard to highlight where Home Affairs is setting a minimum standard or strategic direction for gateways operated by the Australian Government. Policy Statements can be identified in their use of one of the following key phases in bold. Description of the key terms are also included below:

- **Must:** This is a mandatory element of this standard. Entities who have not conducted the action within this policy statement, have not implemented this Standard in accordance with PSPF Requirement XXXX.

- **Should:** This is a strong recommendation and reflective of the strategic direction for gateways. Entities may only not implement this policy statement where they face significant organisational or architectural barriers in doing so, with their decision supported by a risk assessment.
- **May:** This is a permissive element of the standard, frequently used to clarify where entities might take certain actions where it is good practice, or another policy element could suggest prohibition.
- **Should not:** This is a strong recommendation against the described action as it is opposed to the o the strategic direction for gateway security practices. Entities may only implement what is articulated in the policy statement where there are existing contra-indicative organisational or architectural requirements. This decision must be supported by a risk assessment.
- **Must not:** This is a mandatory element of the standard prohibiting an action. Entities that perform the action referenced have not implemented this Standard in accordance with PSPF Requirement XXXX.

Consultation Point 5:
Is the use of the terms 'Must,' 'Should' and 'May' clear throughout the standard and does it contribute to understanding the policy objectives of this standard?

3. Gateway Concepts

3.1. Security Domains

A security domain is a set of systems operating under a consistent set of security polices and standards. This includes systems that are operated by different organisations, or systems that handle information of a different classification.

Australian Government entities **must** have a comprehensive understanding of the security domain/s they manage and interact with.

Consultation Point 6:
In your experience, to what extent do Australian Government entities understand their security domain/s. What actions could be undertaken to improve this understanding?

3.2. Gateway Definition

A gateway is a boundary system that is responsible for controlling data flow into and out of a security domain. This position in the network means that gateways are critical implementation points for a broad range of security capabilities used to enforce an organisation's security policies prior to allowing access into a security domain.

A common example of this is a Secure Internet Gateway (SIG) that is used to manage traffic between an organisation's internal network and the internet.

Australian Government entities **must** ensure all data entering or leaving a security domain passes through a Gateway or Security Service Edge.

Consultation Point 7:
Based on your understanding of section 3.2, do you consider cloud services in scope?

3.3. Security Service Edge Definition

A Security Service Edge (SSE) is a set of cloud security capabilities that are similar to those provided by a Gateway. However, instead of exclusively managing the access between two different domains, SSE solutions

provide a central platform to manage these security capabilities between an organisation's data and resources. This reduces the administrative burden associated with operating multiple security domains and acts as an enabler for Zero Trust through allowing for a greater degree and more streamlined application of network segmentation.

Capabilities typically included within a SSE include:

- Cloud Access Security Broker (CASB)
- Firewall-as-a-Service (FWaaS)
- Secure Web Gateway (SWG), and
- Zero Trust Network Access (ZTNA)

Additionally, SSE's are frequently integrated with a Software Defined Wide Area Networking (SD-WAN) solution to become a Secure Access Service Edge (SASE). This allows for the centralisation of both the security capabilities and traffic management aspects currently handled by traditional gateway environments.

Consultation Point 8:
What are the challenges that an Australian Government entity may experience in adopting an SSE or SASE solution? What are the benefits?

Consultation Point 9:
Are there other products/solutions that provide similar capabilities?

3.4. Policy Enforcement Points

A Policy Enforcement Point (PEP) is an individual component of a broader Gateway or SSE solution that provide the specific capability that allows for the enforcement of gateway policy. The form that PEP can vary based on the design of the Gateway or SSE solution but include specific hardware components, software components, network and endpoint firewalls and can be applied across all of the Open Systems Interconnection (OSI) layers. PEPs can also be layered to provide a full suite of capabilities or to provide additional defence in depth.

4. Gateway Architecture

Gateway solutions can be deployed in accordance with several different architectural approaches including:

- Monolithic provides all gateway security functions through one centrally managed system (for example a SIG)
- Disaggregated provides service-specific gateway functions through discrete but interoperable systems, which do not share a common control plane
- Hybrid provides all required gateway services through a mixture of central and disaggregated service offerings and control planes

Where monolithic gateways have previously provided significant benefits through centralising a large number of security functions, the increased adoption of cloud platforms and remote working has introduced significant challenges to this model. The shift to modern technologies and working arrangements increase the benefits for organisations who move to a disaggregated or hybrid architecture.

Australian Government Entities should refer to ASD's ACSC's Gateway Security Guidance Package in determining the most appropriate gateway architecture for their ICT environment.

Consultation Point 10:
What are some of the challenges Australian Government entities might face in moving to a Disaggregated or Hybrid Gateway architectures? What are some of the benefits?

Consultation Point 11:
What are some of the factors that may require an organisation to retain a Monolithic architecture?

5. Gateway Procurement

Australian Government entities are no longer required to adhere to the Lead Gateway Agency model established under the Gateway Reduction Program, once the Standard supersedes the previous Gateway Policy.

Australian Government entities **should** procure Gateways or Secure Service Edges through the DTA Cloud or Telco Panels. The procurement approach will considers the size of the entity, composition of the ICT environment, workforce skill profile and their operational requirements.

Australian Government entities are encouraged to familiarise themselves with the Digital Transformation Agency's (DTA) Digital Investment Oversight Framework and the Department of Finance's Commonwealth Procurement Rules.

Consultation Point 12:
How could current procurement arrangements for gateways be modified to achieve better security outcomes?

5.1. Insourced Gateways

Australian Government Entities with extensive ICT environments may find operating an insourced gateway or SSE capability to be the most suitable option for their operational and security needs.

The internal development and operation of an insourced gateway is resource intensive. Should an Australian Government Entity operate an insourced gateway, they **must** ensure ongoing adherence to this standard and their broader organisational security requirements.

Consultation Point 13:
What are the common challenges that organisations implementing an insourced gateway/SSE solution? What are some of the benefits?

Where appropriate, Australian Government entities with insourced gateway arrangements **may** extend these services to other entities through a Shared Services Agreement.

Australian Government entities deploying or operating an insourced gateway can refer to the Gateway Security Guidance Package.

5.2. Gateway Providers

Based on organisational functional and security requirements, some Australian Government Entities may determine that procuring a gateway or SSE capability directly from a private-sector provider is the most appropriate way to implement gateway capability.

When procuring a gateway or SSE service from the private-sector, Australian Government entities are responsible for ensuring that the service is suitable to meets the entities' security requirements, and

requirements and adheres to this standard. To assist in with this, vendors intending to sell gateway or SSE services to the Australian Government **should** ensure that their products meet the technical requirements of this standard with minimal hardening or configuration.

Where hardening is required to meet the technical requirements of this standard, Australian Government entities **should** request and vendors should be able to provide specific hardening guidance required to meet this standard with their product.

Where a Gateway or SSE service is unable to meet the requirements of this standard, Australian Government entities **should not** procure it unless they have adequately assessed the limitations and can layer other PEPs to build the capabilities needed to meet the standard

5.2.1. Third Party Risk Management of Gateways and SSE Solutions

Australian Government entities procuring gateway or SSE service from a provider **must** assess and manage third-party security risk that arises from use of this outsourced arrangement. This includes identifying and managing the risk of the provider's Foreign Ownership, Control and influence (FOCI) potential and establishing a shared responsibility model with providers to delineate the duties of both the vendor and customer.

Australian Government entities can refer to guidance on managing third party and FOCI risk available in Section 6 and 7 of the PSPF as well as the Guidelines for Procurement and Outsourcing within the ISM and ASD's Choosing Secure and Verifiable Technologies publications.

Consultation Point 14:
What additional tools or resources might assist Australian Government entities in the assessment and management of 3rd Party and FOCI risk?

5.3. Shared Services Agreements

Australian Government entities with a minimal ICT footprint, or entities with similar ICT requirements **may** wish to establish a Shared Services Agreement with an entity that either manages an insourced gateway environment or has a contract with a Gateway or SSE provider. This can be in the form of either a Shared Services Agreement for the gateway service alone, or through an overarching Shared Services Agreement to use an entity's broader ICT environment.

Where a Shared Services Agreement is established, the entity providing the gateway is a Shared Service Provider Entity (SSPE) in accordance with section 1.4 of the PSPF. In accordance with **PSPF Requirement 0004,** SSPEs are required to supply security services that help to achieve and maintain and maintain an acceptable level of security. to meet this requirement, entities providing gateway services **must** only provide gateway services that adhere to this standard.

Consultation Point 15:
What are some of the risks in Shared Service Gateway arrangements? What are the benefits?

5.4. Shared Responsibilities Model

In the provision of gateway and SSE solutions to other entities, there are shared responsibilities and risks between the provider and the consumer of the service. One party may be predominately responsible for certain aspects, or different aspects may be a joint responsibility. Entities **must** establish a shared responsibility model with their gateway provider to delineate shared responsibilities and risk.

5.5. Reporting of Gateway Procurement Arrangements to Home Affairs.

Part of the objectives of the Resilient Digital Infrastructure Framework is to enhance the information sharing to ensure entities looking to procure gateways are well informed of potential security concerns. To support this, Australian Government entities **must** inform the Department of Home Affairs of changes to their gateway/SSE procurement arrangements through the Resilient Digital Infrastructure Framework mailbox at rdif@homeaffairs.gov.au. Events that should be reported include moving to an insourced gateway, establishing or extending a contract with a gateway/SSE provider, or establishing a Shared Services Agreement.

Consultation Point 16:
How else can we improve the information sharing arrangements for entities looking for a new gateway arrangements?

6. Gateway Assessment and Authorisation

6.1. Authority to Operate

Gateway and SSE systems are subject to **PSPF Requirement 0086**, which determines that Australian Government entities **must** authorise IT systems to operate based on the acceptance of residual security risk. This is achieved through the endorsement of an Authority to Operate (ATO) by the delegated authorising officer. This ensures Australian Government entities are aware of the security risk present and the measures that have been implemented to address them.

Entities will need to repeat the ATO process in accordance with **PSPF Requirement 0090**. Specifically, entities will need to reauthorise when they undergo significant architectural changes or there is a significant changes in the threat landscape for the gateway/SSE environment. It is recommended that this occurs at least every two years to align with IRAP assessment requirements.

Australian Government entities **should** also identify which of their ICT systems include a gateway or SSE solution within their register of authorised systems required by **PSPF Requirement 0089**.

Consultation Point 17:
Should a two year ATO reauthorisation period be introduced as a policy requirement to better manage risk??

6.2. Infosec Registered Assessors Program

Through the Infosec Registered Assessors Program (IRAP), ASD endorses suitably qualified cyber security professionals to provide cyber security services to Australian Government entities and the broader Australian economy. This includes conducting independent cyber security assessments of systems against the ISM. **PSPF Requirement 0114** requires that Australian Government entities use a gateway or SSE solution that has been IRAP assessed against a version of the ISM that is not more than 24 months old. For example, if a gateway had been IRAP assessment against the September 2024 version of the ISM, it can continue to be used until September 2026, regardless of when the IRAP assessment itself was completed.

IRAP assessments of outsourced gateway services, require at least two assessments (a service that involves multiple outsourced providers will require additional assessments):

- a phase one assessment that focuses on the provider's implementation of controls; and
- a phase two assessment that focuses on the controls that the consumer is responsible for implementing and maintaining.

Together the assessments should cover all aspects of the service's shared responsibility model. This provides an accurate picture of residual risk to the authorising officer.

An Australian government entity making insourced gateway services available to other Australian government entities are considered gateway providers in the context of this document.

Information on preparing for and IRAP assessment, and how to interpret an IRAP assessment is available in the Gateway Security Guidance Package: Executive Guidance and the IRAP webpage on cyber.gov.au.

6.2.1. Phase One Assessments

A phase one assessment is focused on the provider of the gateway services and assesses their implementation of controls and ability to provide consumer configurable controls to a given classification. This allows government entities looking to procure gateway services to determine if the service meets their security requirements.

Gateway/SSE providers intending to provide gateway solutions to Australian Government entities **must** conduct an IRAP Assessment of their gateway product (phase one), and **must** share the IRAP assessment with Australian Government entities considering the service. Australian Government entities **must** review the phase one IRAP Assessment of gateway/solutions from providers, including other Australian Government entities, before committing to procuring that solution.

Australian Government entities **must** also share the phase one IRAP Assessments for their Gateway/SSE Solution with Home Affairs upon request.

Consultation Point 18:
Could the discrete sharing Phase One IRAP assessments for gateway/SSE providers through a secured centralised model improve security outcomes for the Australian Government? What other measures could be considered to streamline processes without compromising security posture?

6.2.2. Phase Two Assessments

A phase two assessment focuses on the integration of a gateway service into the government entity's environment; including any controls the consumer is responsible for implementing and maintaining. Australian Government entities' implementation of gateway services **must** undergo an IRAP assessment (phase two) to assess the implementation and effectiveness of security controls.

Where a disaggregated gateway architecture is utilised, or where an Australian Government entity intends to deploy several gateways across their ICT environment, entities **may** consider developing these gateways to a standard architectural pattern. Where this is the case, Australian Government entities are only required to conduct a Phase Two IRAP assessment against the pattern, and not each deployment of it.

Australian Government entities sharing their insourced gateway environment with other Australian Government entities, through a Shared Services Agreement, **may** make use of their Phase Two IRAP Assessment as a Phase One IRAP Assessment for the consuming entity. Entities will need to consider any sensitive material that might be shared.

6.3. Continuous Assurance

With the move toward disaggregated gateway architecture and of the increased deployment of PEPs, entities **should** consider integrating their gateway/SSE environments into a continuous assurance program to ensure that security controls remain in place and effective.

The ASD's ACSC produced the ISM in Open Security Controls Assessment Language (OSCAL) to assist with this process. Australian Government entities can also refer to the Gateway Security Guidance Package: Gateway Operations and Management for guidance on implementing Continuous Assurance in gateway environments.

Consultation Point 19:
What are the key policy considerations for implementing Continuous Assurance across a gateway environment?

7. Gateway Hosting

In addition to the direct handling of sensitive information, Gateways and SSE Solutions are responsible for the implementation of a broad range of security measures aimed at protecting sensitive and classified information. In addition, particularly where monolithic gateways are concerned, they can serve a central point for data transiting a security domains and are at risk of compromise. The location where gateways are hosted have the potential to cause detrimental impacts to network performance, particularly for entities who are geographically dispersed or have a large remote workforce.

7.1. Gateway Hosting Security

7.1.1. Security of On-Premise Gateways

Gateways and SSE solutions are expected to handle and provide protections to the level of the highest security domain that it manages data flow into, even if this is restricted to preventing classified information leaving the security domain. As such, Gateways **must** be hosted in the appropriate Security Zone for the classification of the highest security domain it interacts with in accordance with **PSPF Requirement 0094**. Australian Government entities **must** refer to Section 13.6 of the PSPF to determine the Appropriate Security Zone.

7.1.2. Security of Cloud Hosted or Outsourced Gateways

For gateways or PEPs that are hosted in the cloud, or are hosted by a Managed Service Provider, entities **must** ensure that they are within a datacentre or cloud service provider that has been certified in accordance with the Hosting Certification Framework (HCF).

More information on HCF is available on hostingcertification.gov.au.

8. Gateway Operations and Monitoring

It is not possible to protect data that you cannot see. Australian Government entities need to carefully balance security measures designed to protect data being transmitted between security domains, and those designed to protect the security domain itself. Malicious actors have been known to use encryption to bypass security measures to deliver malicious code into an ICT environment.

Australian Government entities **must** ensure that their Gateway/SSE environment provides them with adequate visibility over incoming and outgoing traffic to implement security measures it requires to manage its security risk, as well as what is required to implement this standard.

Entities can refer to the Gateway Security Guidance Package: Gateway Operations and Management and the ISM's Guidelines for Systems Management, Guidelines for System Monitoring and, Guidelines for Gateways for technical guidance on operating and monitors gateway/SSE environments.

8.1. Log Collection

A gateway/SSE environment **must** generate adequate logs and telemetry to allow for the identification of and response to cyber security incidents. Log are generated from a broad range of sources and in the case of disaggregated or hybrid gateway, multiple egress points. These logs are critical for the detection and investigation of incidents and hold sensitive data and are high value targets for adversaries.

Australian Government Entities **must** feed gateway logs into their centralised logging solution.

An entity's ability to ingest and monitor will vary based on entity size and the monitoring capabilities they hold, such as a Security Incident and Event Management (SIEM) solution, the availability of storage and a Security Operations Centre (SOC). It is rarely practical for an entity to monitor all logs generated by a gateway; therefore, entities **should** integrate gateway logs into their broader event logging and retention policies.

Australian Government entities can refer to the ISM's Guidelines for System Monitoring and the Gateway Security Guidance Package and ASD's Best Practices for Event Logging and Threat Detection publication for technical advice on Gateway logging.

8.2. Full Packet Capture

It is rarely practical for entities to implement continuous full packet capture for all network traffic processed by a Gateway/SSE environment. However, full packet capture is an important capability when determining an adversary's presence within a network during an incident.

8.3. Traffic Inspection

While encryption is a fundamental element of ensuring the security of data transmitted across the internet and other unsecured networks is kept secure, it can also pose a significant barrier to the enforcement of gateway policies by preventing the inspection of traffic. The ability to inspect network traffic is a core capability for a gateway or SSE environment and an enabler of a broad range of security measures such as content filtering and Data Loss Prevention (DLP).

Australian Government entities **should** ensure that they can either decrypt or have other arrangements, such as host-based measures, which to ensure they have adequate visibility over network traffic. Where network traffic cannot be inspected, Australian Government entities **should** block it or quarantine for later inspection.

Entities can refer to the ISM's Guidelines for Gateways and the Gateway Security Guidance Package for technical advice on traffic inspection.

8.3.1. Deep Packet Inspection

Deep Packet Inspection (DPI) allows for the inspection of packet payload information in addition to packet header information. This allows for the detection of malicious code or intercepted traffic that might be present within a packet's payload.

Australian Government entities **should** take a risk-based approach in their use of DPI.

Consultation Point 20:
What other technologies or practices are present that might reduce reliance on Full Packet Capture and Deep Packet Inspection?

8.4. Flow Telemetry

Flow Telemetry is the measurement of key metrics across the network traffic and devices that egresses through a point within a network. Flow telemetry allows for the rapid identification of anomalous connections that could indicate a denial of service (DoS) attack or the exfiltration of compromised data.

8.5. Cyber Threat Intelligence

Gateway and SSE solutions play a significant role in both the collection and actioning of Cyber Threat Intelligence (CTI). As the intermediary between the internet and internal networks, they are typically the first point where an entity can observe adversarial behaviour used to target them. As such, this behaviour can be observed and shared with other organisations.

To support the use and sharing of CTI, Home Affairs issued PSPF Direction 003-2024 requiring all Australian Government entities to enrol in the ASD managed Cyber Threat Intelligence Sharing (CTIS) Platform arrangement. The CTIS platform allows for the expedited bi-directional sharing of CTI amongst Australian Government and industry partners, ensuring threat intelligence is provided for recipients to take action as soon as possible. Provision of CTI via CTIS also supports ASD's broader visibility of threat activity targeting Australia and allows ASD to enrich CTI and provide enhanced threat intelligence for the improved security of CTIS community members.

8.6. BGP Route Security

Border Gateway Protocol (BGP) is a mechanism to exchange routing information among autonomous systems on the internet. BGP is suspect able to a range of attacks, including BGP route hijacking where actors can maliciously or accidently reroute internet traffic. To address this Resource Public Key Infrastructure (RPKI) provides a mechanism to cryptographically associate resource owners with IP address blocks and Autonomous System Numbers (ASN). To support this RPKI Route Origin Authorisation (ROA) records are configured to describe the route traffic is expected to originate from.

Australian Government entities **must** ensure that their public IP addresses have signed and valid ROAs.

9. Gateway Services

9.1. Domain Name System

The Domain Name System (DNS) is the internet protocol that is responsible for the resolution of human readable domain names (e.g. example.com) into machine readable Internet Protocol (IP) addresses (e.g. 203.0.113.1 or 2001:db8::1).

For technical guidance on securing DNS, entities can refer to the Gateway Security Guidance Package: Gateway Technology Guide and ASD's DNS Security for Domain Resolvers and DNS Security for Domain Owners publications.

9.1.1. Domain Names

The Department of Finance is the Registrar for the gov.au second-level domain. Australian Government entities **must** adhere to the Eligibility and Allocation Policy and Australian Government Domain Name Policy when creating new domain names or maintaining their existing domains.

9.1.2. Protective DNS

A Protective DNS (PDNS) service can be an effective way of blocking connections to known malicious endpoints by preventing the resolution of known malicious domain names. This is achieved through the use of a recursive resolver that will return either a sinkhole address when they receive a request to resolve a domain name known to be associated with malicious activity.

PSPF Requirement 0108 requires that a PDNS solution, or other method, is used by Australian Government entities to prevent connections to known malicious endpoints.

To support this, ASD provides access to its PDNS system AUPDNS free of charge to all Australian federal, state and local government organisations. AUPDNS also provides ASD with visibility to build up a picture of Australia's threat landscape, therefore Australian Government entities **should** make use of AUPDNS where possible.

Where it is not possible to implement a PDNS service, Australian Government entities **must** implement a different mechanism to prevent the establishment of connections with known malicious endpoints.

Consultation Point 21:
What are common situations were an organisation would be unable to implement a PDNS solution?

9.1.3. DNS Security Extensions

DNS Security Extensions (DNSSEC) provides a mechanism to verify the integrity of DNS records through the use of Public Key Cryptography. This allows name servers to verify that they are the authoritative name server for a particular DNS zone.

Australian Government entities **should** implement measures to verify the integrity of their DNS records.

9.1.4. DNS Encryption

While introducing increased confidentiality for individual users, the implementation of standards that encrypt DNS traffic, such as DNS over TLS (DoT), DNS over HTTPS (DoH) and DNS over QUIC (DoQ), can hinder gateway visibility and policy enforcement.

Entities **must** ensure they can retain adequate visibility over DNS Traffic to meet their own security requirements and the requirements of this standard.

Consultation Point 22:
To what extent does encrypted DNS hamper the enforcement of gateway policy and solutions are available to provide visibility over DoH, DoT and DoQ traffic?

9.2. Mail Relays

Mail relays, also referred to as email gateways, provide Australian Government entities with the ability to enforce security policy over email traffic entering and leaving a security domain. Email remains core to the daily operations of Australian Government but also a key avenue for exploitation by malicious actors. As such, the effective implementation of security measures by mail relays plays a key role in the protection of sensitive data the Australian Government manages.

9.2.1. Email Encryption

Opportunistic TLS (STARTTLS) provides email traffic with a base level of security by negotiating the highest level of encryption that can be supported when two mail servers establish a connection. This is susceptible to downgrade attacks.

Australian government entities **must** implement measures to prevent the downgrading of email encryption to make use of insecure algorithms or cipher suites.

9.2.2. SPF, DKIM and DMARC

Malicious actors commonly modify the sender addresses of phishing emails to make them appear more legitimate. Due to the profile of the government, malicious actors commonly seek to impersonate Australian Government entities. To address this, organisations can publish a number of DNS records to allow recipients to authenticate the source of an email as legitimate or inform them how to handle suspect emails. These are Sender Policy Framework (SPF), DomainKeys Identify Mail (DKIM) and Domain-based Message Authentication, Reporting and Conformance (DMARC).

Entities can refer to the Gateway Security Guidance Package: Gateway Technology Guide and ASD's How to Combat Fake Emails publication for guidance implementing SPF, DKIM and DMARC.

9.2.2.1. Sender Policy Framework (SPF)

Australian Government entities **must** publish an SPF record for all the domains and subdomains they manage. This includes publishing SPF reject all records for domains and subdomains that do not send emails.

9.2.2.2. DomainKeys Identify Mail (DKIM)

Entities **must** publish a DKIM record and sign outgoing emails with a DKIM signature.

9.2.2.3. Domain-based Message Authentication, Reporting and Conformance (DMARC)

Entities **must** publish a DMARC record with a quarantine or reject policy.

Consultation Point 23:
Should a set transition period for the implementation of SPF, DKIM and DMARC that allows DMARC policy to be set to none be explicitly outlined? If so what would be a sufficient timeframe?

9.2.3. Email Protective Markings

Mail relays **should** be configured to support the implementation of Data Loss Prevention (DLP) capabilities. As such, emails sent from Australian Government entities **must** be marked in accordance with **PSPF Requirement 0067** and the Australian Government Email Protective Marking Standard. Australian Government entities **must** configure mail relays to prevent emails that are not appropriately marked from leaving the security domain. In addition entities **should** configure mail relays to block emails that are classified higher than what sending or recipient security domain can handle.

When implementing mail relay policy, Australian Government entities **should** ensure that email attachments are also inspected to determine if the attachments are classified and to detect under classification.

9.2.4. GovLINK

Australian Government entities **must** make use of either GovLINK, or GovLINK TLS solution when sending PROTECTED emails between Australian Government entities. For further guidance, refer to the GovLINK webpage on the Department of Finance website.

9.2.5. Email Content Filtering

Emails are routinely used as a vector for transporting malicious code into an organisations ICT environment. To address this, entities should consider removing active content (such as JavaScript and tracking content) from incoming emails and preforming reputation checks on URLs.

Australian Government entities **must** also have a mechanism for scanning emails, including attachments, for possible malicious content. Emails with content that cannot be scanned in the gateway environment **should** be quarantined until the content is confirmed safe.

Entities can refer to ASD's Malicious Email Mitigation Strategies publication, for technical guidance on countering malicious content in emails.

9.3. Web Proxies

Web proxies (also referred to as Forward Web Proxies) are typically deployed between users/clients and the internet. They facilitate gateway security capabilities that can be used to enforce an organisations web security policy. These capabilities include content filtering, DLP, malware scanning and generation of logs and telemetry.

Entities can refer to the ISM's Guidelines for Gateways and the Gateway Security Guidance Package: Gateway Technology Guide for further advice on the deployment of Web proxies.

9.3.1. Web Security Policy

Australian Government entities **must** enforce their web security policy through the use of web proxies by default. Entities **may** wish to consider layering this with other security capabilities such as endpoint security agents however web proxies are still required to ensure all internet traffic has web security policy applied to it.

9.3.2. Restricting Access to Unauthorised Cloud Services

Controlling user access to cloud systems is critical for limiting the deployment of Shadow IT that can then be used to bypass an entity's security policies and potentially lead to data spills. Australian Government entities **must** ensure that its users, regardless of location, are not able to access unauthorised cloud services.

9.3.3. Web Content Filtering

Web proxies, alongside endpoint-based solutions, provide an opportunity for implementing a "defence in depth" approach for preventing the execution of malicious code within Australian Government systems.

PSPF Requirement 0103 requires that Australian Government entities implement Application Control which achieves Maturity Level Two of the Essential Eight Maturity Model. Entities **must** make use of their web proxies to prevent the processing of un-authorised executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets into a security domain.

Web proxies **should** also be used to restrict access to websites based on website categorisation in line with the entity's Web usage policy. Given that many malicious websites have a short life span, entities **should** block access to websites that do not have a category or are categorised as new. Entities **should** also block web browsing to IP addresses.

9.3.4. Malware Detection and Prevention

Australian Government entities **must** have a malware detection or prevention capability for traffic processed by their web proxies.

This malware detection capability can consist of one or multiple of the following:

- Detection based on heuristics, reputation or signature.
- Malicious link detection
- Obfuscated code detection
- Sandbox detonation
- Threat intelligence-based detection
- Content Disarm and Reconstruction (CDR)

9.3.4.1. TLS Decryption and Payload Inspection

Australian Government entities **should** take a risk-based approach when determining where TLS decryption and payload inspection is performed

Consultation Point 24:
What are some of the gaps in the current information available on TLS keys and certificates across PEPs? Are there other related areas that should to be considered?

9.3.5. Deny Listing

Web proxies **must** allow Australian Government entities to configure their own approach to block access to certain domains or IP address ranges. This is to allow entities to action CTI or block web traffic as part of their incident prevention and response activities.

9.3.6. HTTP Header Inspection, Filtering and Manipulation

Web proxies **must** have the capability to log Hypertext Transfer Protocol (HTTP) headers and filter and manipulate them to address security concerns surrounding them. This includes the ability to remove header data that poses security risks or adding header data that allows the implementation of security functionality.

9.3.7. Identity Awareness

Web proxies **should** be identity aware and support user authentication and authorisation. This allows for the implementation of access control to restrict access to resources and assist in incident investigation.

Where web proxies are identity aware, they **must** be configured to restrict access for non-person entities (NPE), such as service accounts, to the explicit list of websites required for functionality. This limits an adversary's ability to leverage compromised service account credentials to exfiltrate data out of a security domain. In addition, they **should** be configured to block web resources from privileged user accounts or from privileged environments.

Consultation Point 25:
Would there be benefit in providing further information regarding the relationship between these policy statements and the requirements of the Essential Eight Maturity Model?

9.4. Reverse Web Proxies

A reverse web proxy sits between an organisation's websites and web applications and the internet to provide gateway security capabilities before forwarding web traffic onto the destination site or application.

Entities can refer to the ISM's Guidelines for Gateways and the Gateway Security Guidance Package: Gateway Technology Guide for technical advice on the deployment of reverse web proxies.

9.4.1. Traffic Forwarding

Reverse web proxies **must** only be able to forward web traffic to web resources. Likewise, entities **must** ensure that their websites and web applications are only accessible through a reserve web proxy.

9.4.2. Restricting Unauthorised Access to Cloud Services

Controlling access to entities' cloud systems (particularly SaaS systems) is critical given the limited ability that entities have over the infrastructure that is deployed to implement its security policy. Australian Government entities **must** ensure that unauthorised users, are not able to access an entities cloud services.

9.4.3. Web Content Filtering

PSPF Requirement 0103 requires that Australian Government entities implement Application Control to Maturity Level Two of the Maturity Level Two of the Essential Eight Maturity Model. To provide defence in depth, entities **must** make use of their reverse web proxies to prevent the unauthorised execution of code in addition to measures hosted on web servers themselves.

9.4.4. Malware Detection and Prevention

Australian Government entities **must** have a malware detection or prevention capability for traffic processed by their reverse web proxies.

This malware detection capability can consist of one or multiple of the following

- Detection based on heuristics, reputation or signature.
- Malicious code and link detection
- Obfuscated code detection

- Sandbox detonation
- Threat intelligence-based detection
- Content Disarm and Reconstruction (CDR)

9.4.4.1. TLS Termination

To enable malware detection and policy enforcement, reverse web proxies **must** terminate TLS session and then re-encrypt TLS traffic before forwarding it onto web servers.

9.4.5. Deny Listing

Reverse web proxies **must** allow Australian Government entities to configure their own approach to prevent web traffic accessing specified domains or IP address ranges. This is to allow entities to action CTI or block web traffic as part of detection and prevention and incident response activities.

9.4.6. HTTP Header Inspection, Filtering and Manipulation

Reserve web proxies **must** have the capability to log HTTP headers and filter and manipulate them to address security concerns surrounding them. This includes the ability to remove header data that poses security risks, or adding header data that allows the implementation of security functionality.

Consultation Point 27:
Are there additional gateway based capabilities that could assist in addressing other security concerns such as vulnerability management that could be considered?

9.5. Remote Access

Australian Government entities **should** actively risk manage their current remote access solutions, ensuring existing capability provides adequate mitigation of their threat and vulnerability landscape.

Australian Government entities can refer to the ISM's Guidelines for Enterprise Mobility, Section 9.3 of the PSPF, and ASD's Risk Management of Enterprise Mobility (Including Bring Your Own Device) publication for technical guidance on Remote Access.

9.5.1. Authentication

PSPF Requirement 0101 requires that Australian Government entities implement MFA to Maturity Level Two of the Essential Eight Maturity Model.

Australian Government entities **must** implement MFA for users using a remote access solution and one of the authentication factors used **must** be phishing resistant. Entities can refer to the Authentication Hardening section of the ISM's Guidelines for System Hardening, for guidance on implementing MFA

9.5.2. Remote Access to Cloud Services

Remote users accessing cloud services pose a challenge in enforcing security policy as network access as users can typically access a cloud resource without transiting through an organisations gateway environment. If inadequate consideration is placed in designing cloud solutions, organisations can inadvertently place sensitive data into a cloud platform that can be accessed without having a mechanism to enforce the organisations security policy.

Australian Government entities, when designing and deploying cloud systems, **must** document the security domains that cloud services belongs to and how security policy is going to be applied to remote users accessing that cloud service. Entities **must** ensure they have adequate mechanisms in place to enforce their security policy and this standard for remote users accessing their cloud services.

9.5.3. Virtual Private Networks

Virtual private networks (VPNs) are a common approach to enabling secure remote access to an organisation network through the use of TLS or IPsec encryption. Entities **must** configure VPN connections to only make use of ASD Approved Cryptographic Algorithms (AACAs). PKI certificates **should** also be used to facilitate VPN connections and VPN solutions **should** support the revocation of these certificates.

Australian Government entities can refer to the ISM's Guidelines for Cryptography for the implementation of either TLS or IPsec based VPNs.

9.5.3.1. VPN Split-tunnelling

Entities **should** avoid the use of VPN split-tunnelling where possible as this introduces new attack vectors into an entity. Where split tunnelling is used it **must** be threat modelled and limited to what is required to support the remote access solution. Additionally, entities **must** implement other policy enforcement mechanisms on traffic split from a VPN connection adheres to the entities security policy and the requirements of this standard.

Consultation Point 28:
How might the Australian Government's position on VPN split tunnelling, as reflected in publication like the ISM need to adapt to support the adoption of capabilities such as Zero Trust?

9.5.4. Remote Endpoints

Australian Government entities **should** issue entity-owned devices or provide a virtual desktop interface (VDI) for users accessing sensitive or classified material. Where access is allowed from personal owned devices, these devices **must not** be considered as part of the same security domain, and their traffic **must** go through a gateway or SSE environment.

Australian Government entities **should** also implement measures to assess and validate endpoint health, patching, Endpoint Detection and Response, and machine authentication to before allowing endpoints to connect through the Gateway/SSE environment.

Acronyms and Abbreviations

Abbreviation	Meaning
AACA	ASD Approved Cryptographic Algorithms
ACSC	Australian Cyber Security Centre
ASD	Australian Signals Directorate
ASN	Autonomous System Numbers
ATO	Authority to Operate
CASB	Cloud Access Security Broker
CTI	Cyber Threat Intelligence
DKIM	DomainKeys Identify Mail
DLP	Data Loss Prevention
DMARC	Domain-based Message Authentication, Reporting and Conformance
DNS	Domain Name System
DNSSEC	DNS Security Extensions
DoH	DNS over HTTPS
DoQ	DNS over QUIC
DoS	Denial of Service
DoT	DNS over TLS
DPI	Deep Packet Inspection
DTA	Digital Transformation Agency
FOCI	Foreign Ownership, Control and Influence
FWaaS	Firewall-as-a-Service
HCF	Hosting Certification Framework
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
IP	Internet Protocol
IRAP	InfoSec Registered Assessors Program
ISM	Information Security Manual
MFA	Multifactor Authentication
NPE	Non-person Entities
OSCAL	Open Security Controls Assessment Language

OSI	Open Systems Interconnection
OWASP	Open Worldwide Application Security Project
PDNS	Protective DNS
PEP	Policy Enforcement Point
PKI	Public Key Infrastructure
PSPF	Protective Security Policy Framework
RDI	Resilient Digital Infrastructure
ROA	Route Origin Authorisation
RPKI	Resource Public Key Infrastructure
SaaS	Software-as-a-Service
SASE	Secure Access Service Edge
SD-WAN	Software Defined Wide Area Networking
SIEM	Security Incident and Event Management
SIG	Secure Internet Gateway
STARTTLS	Opportunistic TLS
SPF	Sender Policy Framework
SSE	Security Service Edge
SWG	Secure Web Gateway
TLS	Transport Layer Security
VDI	Virtual Desktop Interface
VPN	Virtual Private Networks
WofG	Whole of Government
ZTNA	Zero Trust Network Access