Australian Government

Department of Home Affairs

Protective Security Policy Framework

Australian Government Gateway Security Standard

Release 2025

Contents

1. Purpose 2
2. Applicability 2
   - 2.1. Language in Policy Statements 3
   - 2.2. Exemptions to Policy Statements 3
3. Gateway Concepts and Definitions 3
   - 3.1. Security Domains 3
   - 3.2. Gateway Definition 3
   - 3.3. Gateway Architecture 4
4. Gateway Governance and Procurement 5
   - 4.1. Insourced Gateways 5
   - 4.2. Gateway Providers 5
   - 4.3. Shared Services Agreements 6
   - 4.4. Cloud Native Gateway Services 6
   - 4.5. Shared Responsibility Model 6
   - 4.6. Reporting of Gateway Procurement Arrangements to Home Affairs 6
5. Gateway Assessment and Authorisation 6
   - 5.1. Authority to Operate 6
   - 5.2. Infosec Registered Assessors Program 7
   - 5.3. Continuous Assurance 8
6. Gateway Hosting 8
   - 6.1. Security of On-Premise Gateways 8
   - 6.2. Security of Cloud Hosted or Outsourced Gateways 8
   - 6.3. International Gateway Infrastructure 8
7. Gateway Operations and Monitoring 9
   - 7.1. Log Collection 9
   - 7.2. Traffic Inspection 9
   - 7.3. Cyber Threat Intelligence 10
   - 7.4. BGP Route Security 10
8. Gateway Services 11
   - 8.1. Domain Name System 11
   - 8.2. Mail Relays 11
   - 8.3. Web Proxies 13
   - 8.4. Reverse Web Proxies 14
   - 8.5. Remote Access 16
   - 8.6. Key Management 17

1. Purpose

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

Gateway 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 gateway solutions 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 (RDI) strategy. This Standard was developed with extensive collaboration with the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) and should be read alongside the technical guidance published in the Gateway Security Guidance Package and where relevant, the related Cross Domain Solutions publications. The broader application of the Protective Security Policy Framework (PSPF) and the Information Security Manual (ISM) should also be applied when considering gateway security.

Requirement 0214 | TECH | All entities | 01 July 2025

Digital Infrastructure that processes, stores or communicates Australian Government security classified information is protected by a Gateway or Security Service Edge in accordance with the Australian Government Gateway Security Standard.

Requirement 0114 | TECH | All entities | 01 July 2025

Gateways or Secure Service Edges that have completed an IRAP assessment (or ASD assessment for TOP SECRET gateways) against the latest version of ASD's Information Security Manual within the previous 24 months are used.

2. Applicability

The Australian Government Gateway Security Standard has been developed as part of the Resilient Digital Infrastructure strategy. 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 PSPF, it is a mandatory element of the framework for non-Corporate Commonwealth Entities. The PSPF also represents better practice for Corporate Commonwealth Entities and wholly-owned Commonwealth Companies.

This Standard is applicable to gateway solutions that interact with the internet. This standard does not apply when connecting systems between different security domains where at least one security domain is classified SECRET or TOP SECRET. Refer to ASD's Information Security Manual and Cross Domain Solution resources when gateway solutions contain at least one security domain classified SECRET or TOP SECRET. The use of Cross Domain Solutions may be appropriate at classifications at PROTECTED and below where a high assurance solution is required to manage identified risks.

2.1. Language in Policy Statements

To assist in the application of this Standard, policy statements are dispersed throughout it to highlight where Home Affairs is setting a minimum standard or strategic direction for gateway solutions 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 0214.
- **Should:** This is a recommendation and reflective of the strategic direction for gateway solutions. Implementation of these is encouraged unless there are significant organisational or architectural barriers.
- **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 0214.

2.2. Exemptions to Policy Statements

Where Australian Government entities are not able to adhere to a mandatory policy statement, entities **must** request an exemption to the standard from Home Affairs. Requests for exemption to this standard can be submitted to the Resilient Digital Infrastructure mailbox at rdi@homeaffairs.gov.au.

3. Gateway Concepts and Definitions

This section of the Standard details a number of key concepts and definitions required to understand the requirements of the Standard. These include security domains, gateways, Security Service Edges, and Policy Enforcement Points.

Australian Government entities **must** have a comprehensive understanding of the security domain/s they manage and interact with. Entities **must** ensure all data entering or leaving a security domain passes through a Gateway or Security Service Edge.

3.1. Security Domains

A security domain is a set of systems operating under a consistent set of security polices and standards[1]. This includes systems that are operated by different organisations, or systems that handle information of a different classification.

3.2. Gateway Definition

A gateway is a set of capabilities responsible for securely managing data flows between connected networks from different security domains. This position in the network means that gateway solutions are critical implementation points for a broad range of security capabilities used to enforce an organisation's security policies prior to allowing access between different security domains.

Common examples of a gateway solutions include a Secure Internet Gateway (SIG) that is used to manage traffic between an organisation's internal network and the internet, and a Security Service Edge (SSE) that utilise cloud-based services to enforce security policies.

[1] The ISM defines a security domain as: *"A system or collection of systems operating under a consistent security policy that defines the classification, releasability and special handling caveats for data processed with the domain.*

3.2.1. Security Service Edge Definition

A Security Service Edge (SSE) is a set of cloud-based gateway capabilities and provide a central mechanism 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 included within SSE solutions typically include:

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

Additionally, SSE capabilities can be integrated with a Software Defined Wide Area Network (SD-WAN) solutions 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.

3.2.2. Cross Domain Solution

A CDS is a system capable of implementing comprehensive data flow security policies with a high level of trust between two or more differing security domains, and can be used as part of an internet gateway solution. CDS are implemented between SECRET or TOP SECRET networks and any other networks belonging to different security domains. A CDS can be implemented for networks that operate at or below PROTECTED and the internet, where high assurance security policy enforcement is needed to manage risk.

3.2.3. Policy Enforcement Points

A Policy Enforcement Point (PEP) may be a hardware or software component, security device, integrated appliance, tool, function or application. PEPs perform a combination of blocking, inspecting, filtering and validating actions on incoming and outgoing data to mitigate IT risks in accordance with an organisations security policy.

The types of PEP used vary based on the design of the Gateway 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.

3.3. 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, and
- Hybrid**:** provides all required gateway services through a mixture of central and disaggregated service offerings and control planes.

Australian Government Entities can refer to ASD's ACSC's Gateway Security Guidance Package and Cross Domain Solutions in determining the most appropriate gateway architecture for their IT environment.

4. Gateway Governance and Procurement

Australian Government entities are no longer required to adhere to the Lead Gateway Agency model established under the Australian Government Internet Gateway Reduction Program.

Australian Government entities **should** procure gateway solutions through appropriate DTA Procurement Panels. The procurement approach ought to consider the size of the entity, composition of the IT 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.

4.1. Insourced Gateways

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

The internal development and operation of an insourced gateway is resource intensive. Australian Government entities that operate an insourced gateway **must** ensure ongoing adherence to this Standard and their broader organisational security requirements.

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.

4.2. Gateway Providers

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

When procuring a gateway service from the private-sector, entities **must** ensure that the service is suitable to meet their security requirements, operational needs and adheres to this Standard. To assist in with this, vendors intending to sell gateway services to the Australian Government **should** ensure that their products meet the technical requirements of this Standard with minimal additional hardening or configuration changes.

Australian Government entities **must** request vendor hardening guidance. Where available, entities **must** implement vendor hardening guidance to meet the technical requirements of this Standard.

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

4.2.1. Third Party Risk Management of Gateway Services

Australian Government entities procuring gateway services from a provider **must** assess and manage third-party security risk that arises from the use of this outsourced arrangement. This includes identifying and managing the risk of the provider's Foreign Ownership, Control and Influence (FOCI) potential, as well as 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 PSPF Release 2025 (s 6 and 7) as well as Home Affairs' FOCI Risk Assessment Guidance, the Guidelines for Procurement and Outsourcing within the ISM, and ASD's Choosing Secure and Verifiable Technologies publications.

4.3. Shared Services Agreements

Australian Government entities with a minimal IT footprint, or entities with similar IT requirements can establish a Shared Services Agreement with an entity that either manages an insourced gateway environment or has a contract with a gateway service 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 IT environment.

Where a Shared Services Agreement is established, the entity providing the gateway is a Shared Service Provider Entity (SSPE) in accordance with PSPF Release 2025 (Section 1.4). In accordance with PSPF Requirement 0004, SSPEs are required to supply security services that help to achieve 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.

4.4. Cloud Native Gateway Services

Australian Government entities using cloud based IT services may wish to use cloud-native security boundary services as part of their gateway solution. When using these services, entities **must** ensure that it can meet the requirements of this Standard, or be confident that they can layer additional PEPs to build the capabilities to meet it.

4.5. Shared Responsibility Model

In the provision of gateway 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** document their shared responsibility model with their gateway provider to delineate shared responsibilities.

4.6. Reporting of Gateway Procurement Arrangements to Home Affairs

Part of the objectives of the Resilient Digital Infrastructure strategy is to enhance information sharing abilities 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 services procurement arrangements through the Resilient Digital Infrastructure mailbox at rdi@homeaffairs.gov.au. Events that should be reported include moving to an insourced gateway, the classification of the connected systems to the gateway, establishing or extending a contract with a gateway service provider, or establishing a Shared Services Agreement.

In addition, Entities **must** provide a point of contact that can address gateway enquires from Home Affairs. These should be provided to the Resilient Digital Infrastructure mailbox at rdi@homeaffairs.gov.au.

5. Gateway Assessment and Authorisation

5.1. Authority to Operate

Gateway 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 **must** reauthorise their gateway systems when they undergo significant architectural changes or there is a significant change in the threat landscape.

5.2. 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 solution that has been IRAP assessed against the latest version of the ISM within the last 24 months.

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

- phase one assessment that focuses on the provider's implementation of ISM controls; and
- phase two assessment that focuses on the ISM 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 an 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.

5.2.1. 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 service 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 **should** share the phase one IRAP Assessments for their Gateway solution with ASD upon request.

5.2.2. 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 government entity 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 IT environment, entities may consider developing these gateways to a standard architectural pattern.

5.3. Continuous Assurance

With the move toward disaggregated gateway architecture and the increased deployment of PEPs, entities **should** consider integrating their gateway environments into a continuous assurance program to ensure that security controls remain in place and effective. Threat modelling can be used to help entities develop a suite of continuous validation tests.

The ASD's ACSC produced the ISM in Open Security Controls Assessment Language (OSCAL) to assist with this process. Entities should consider using OSCAL-based tooling to automate control validation and support continuous assurance. Australian Government entities can refer to the Gateway Security Guidance Package: Gateway Operations and Management for guidance on implementing Continuous Assurance in gateway environments.

6. Gateway Hosting

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

6.1. Security of On-Premise Gateways

Gateway solutions are expected to handle and provide protections to the level of the highest security domain that it manages data flow into or out of, even if this is restricted to preventing classified information leaving the security domain. As such, gateway infrastructure **must** be physically 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 PSPF Release 2025 (Section 13.8.1) to determine the appropriate Security Zone.

6.2. Security of Cloud Hosted or Outsourced Gateways

For gateway capabilities or PEPs that are hosted by Cloud Service Providers, or are hosted by a Managed Service Provider, entities **must** ensure that they are within a data centre or cloud service provider that has been certified in accordance with the Hosting Certification Framework (HCF), with the exemption of internationally hosted gateway infrastructure.

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

6.3. International Gateway Infrastructure

Certain gateway capabilities, such as Content Delivery Networks (CDNs) require an international point of presence to operate. Data processing and storage services at the network edge, outside the control of entity managed gateway or SSE services (like CDNs) **must** be separately risk assessed.

7. 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 IT environment.

Australian Government entities **must** ensure that their gateway solution 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, as well as ACSC's SIEM guidance package, and the ISM's Guidelines for Systems Management, Guidelines for System Monitoring and, Guidelines for Gateways for technical guidance on operating and monitors gateway environments.

7.1. Log Collection

A gateway environment **must** generate adequate logs and telemetry to allow for the identification of and response to cyber security incidents. Logs are generated from a broad range of sources and in the case of disaggregated or hybrid gateway, multiple ingress and 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 relevant gateway logs into their centralised logging solution.

Australian Government entities can refer to the ISM's Guidelines for System Monitoring and the Gateway Security Guidance Package, Best Practices for Event Logging and Threat Detection, Priority logs for SIEM ingestion: Practitioner guidance and Implementing SIEM and SOAR platforms publications for technical advice on Gateway logging.

7.2. 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 environment and an enabler of a broad range of security measures such as content filtering and Data Loss Prevention (DLP).

Australian Government entities **must** ensure that they can either decrypt or have other arrangements, such as host-based measures on entity managed devices, 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.

7.2.1. 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. Entities **should** take a risk-based approach in their use of DPI.

7.3. Cyber Threat Intelligence

Gateway 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, PSPF Requirement 0216 requires entities connect to ASD's Cyber Threat Intelligence Sharing (CTIS) platform. 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 act 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.

7.4. BGP Route Security

Border Gateway Protocol (BGP) is a mechanism to exchange routing information among autonomous systems on the internet. BGP is susceptible to a range of attacks, including BGP route hijacks 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 the public IP addresses controlled by, or used by, the entity are signed by valid ROA records.

Australian Government entities **should** configure routers that exchange routes via BGP, to reject or deprioritise routes for RPKI-registered IP addressed that are advertised from invalid Autonomous Systems.

8. Gateway Services

8.1. Domain Name System

The DNS translates domain names to IP addresses (and vice versa), and provides other information through queries for resource records (e.g. CNAME, SPF and DMARC).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.

8.1.1. 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.

8.1.2. 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 a sinkhole address (or alternatively a "no such domain" response) 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 methods, are 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 select Australian Government entities. 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 it has been made available to them.

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

8.1.3. DNS Security Extensions

DNS Security Extensions (DNSSEC) provides a mechanism to verify the integrity of DNS records by utilising Public Key Cryptography. This allows name servers to prove that they are the authoritative server for the zone, and that their responses have not been tampered with.

Australian Government entities **should** implement measures to implement measures to verify the integrity of DNS responses originating outside of their security domain. Entities **should** also implement measures to allow external parties to verify the integrity of Authoritative DNS responses provided by the entity.

8.1.4. 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. Where supported, and where this visibility can be retained, entities **should** implement DNS encryption.

8.2. 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 is 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.

8.2.1. 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** ensure emails are appropriately encrypted and implement measures to prevent the downgrading or removal of email encryption. Entities **should** configure outbound email encryption to only make use of ASD Approved Cryptographic Algorithms (AACAs).

For technical guidance on implementing email encryption, entities can refer to ACSC's Implementing certificates, TLS, HTTPS and opportunistic TLS publication.

8.2.2. Email Authentication Protocols

Malicious actors commonly manipulate 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, and 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.

8.2.2.1. 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.

8.2.2.2. DomainKeys Identified Mail (DKIM)

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

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

Entities **must** publish a DMARC policy for all domains and subdomains they manage. Entities with existing domains **must** publish a policy of 'quarantine' or 'reject' in their DMARC record within 3 months of first enabling DMARC for an existing domain. Entities registering new domains **must** immediately publish a DMARC record with a policy of 'quarantine' or 'reject'.

8.2.3. Email Protective Markings

Emails sent from Australian Government entities **must** be marked in accordance with PSPF Requirement 0067, and the Australian Government Email Protective Marking Standard.

Security policy enforcement capabilities **should** be implemented to ensure that outbound emails (including attachments) containing sensitive or classified information are only sent to recipient systems authorised to receive the appropriate classification of data.

8.2.4. GovLINK

Australian Government entities **must** make use of either GovLINK, or a GovLINK TLS solution when sending PROTECTED emails between Australian Government entities. GovLINK uses ASD Approved Cryptographic Algorithms (AACAs). For further guidance, refer to the GovLINK webpage on the Department of Finance website.

8.2.5. Email Content Filtering

Emails are routinely used as a vector for transporting malicious code into an organisation's IT environment. To address this, entities **should** remove active content (such as JavaScript and tracking content) from incoming email content and perform reputation checks on Uniform Resource Locators (URLs) within email body and attachments.

Australian Government entities **must** 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, or otherwise deleted.

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

8.3. 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 the 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.

8.3.1. Web Security Policy

Australian Government entities **must** ensure that web proxies, or other methods, are used to enforce security policies. 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.

8.3.2. 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 service to transfer, store or process Australian Government data.

8.3.3. 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.

Web proxies, or other methods, **must** be used to control 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.

8.3.4. 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)

8.3.4.1. TLS Decryption and Payload Inspection

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

8.3.5. 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.

8.3.6. Identity Awareness

Web proxies **should** be identity aware and support user authentication and authorisation. This allows for the implementation of access controls 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 from a security domain. In addition, they **should** be configured to block web resources by privileged user accounts or from privileged environments, unless explicitly authorised.

8.4. 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.

8.4.1. Traffic Forwarding

Internet facing reverse web proxies **must** only be able to forward web traffic to internet facing websites and web application. Reverse web proxies should be configured to prevent protocol tunnelling, or access to unapproved internal web resources. Likewise, entities **must** ensure that their public websites and web applications are only accessible through a reverse web proxy.

8.4.2. Restricting Unauthorised Access to Cloud Services

Controlling access to an entity's 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. If not properly managed there is a significant risk of unauthorised users accessing Australian Government cloud services.

Australian Government entities **must** ensure that unauthorised users are not able to access an entity's cloud services.

8.4.3. Malware Detection and Prevention

Australian Government entities **should** 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)

8.4.3.1. TLS Termination

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

8.4.4. 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 block web traffic as part of incident prevention and response activities.

8.4.5. HTTP Header Inspection, Filtering and Manipulation

Reverse 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.

8.4.6. Denial of Service (DoS) protection

Service availability is critical for business operations and organisational reputation. Determining what functionality and quality of service is acceptable for legitimate users of services, how to maintain that functionality, and what functionality is not required during DoS attacks, can help organisations decide which measures to implement to help prepare for, and respond to DoS attacks.

Entities may unintentionally contribute to DoS attacks that could impact others. This can be mitigated by avoiding exposing unnecessary services to the internet, and by securely configuring, maintaining and monitoring services that are exposed.

Australian Government Entities can refer to ASD's Preparing for and responding to denial-of-service attacks, publication for detailed guidance.

8.5. Remote Access

Australian Government entities **must** 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, PSPF Release 2025 (Section 9.3), and ASD's Risk Management of Enterprise Mobility (Including Bring Your Own Device), Remote access to operational technology environments, and other related publications on cyber.gov.au for technical guidance on Remote Access.

8.5.1. Authentication

PSPF Requirement 0101 requires that Australian Government entities implement multi-factor authentication (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, and ASD's Implementing multi-factor authentication publication for guidance on implementing MFA.

8.5.2. Remote Access to Cloud Services

Remote users accessing cloud services pose a challenge in enforcing security policy as users can typically access a cloud resource without transiting through an entity's gateway environment. If inadequate consideration is placed in designing cloud solutions, entities can inadvertently place sensitive data into a cloud platform that can be accessed without having a mechanism to enforce the entity's security policy. Alternative architectural patterns may be used to mitigate risk (for example a browse-down CDS may also be used to browse-across to systems with a similar trust level).

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 cloud services used by that entity.

8.5.3. 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). Public Key Infrastructure (PKI) certificates **should** 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.

8.5.3.1. 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 identified business requirements. Entities **must** implement other policy enforcement mechanisms on traffic split from a VPN connection to ensure that it adheres to the entity's security policy and the requirements of this Standard.

8.5.4. 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 solution that meets this Standard.

Australian Government entities **should** implement measures for entity managed devices to assess and validate endpoint health, patching, Endpoint Detection and Response status, and machine authentication before allowing endpoints to connect through the gateway solution.

8.6. Key Management

Australian Government entities **must** document their use of entity managed and externally managed PKI cryptographic keys including the following information: usage, storage location, access, permissions, and expiry.

Where practical, Australian Government entities **should** ensure any private key of a root certificate they control is kept in an isolated secure offline storage mechanism when not in use.

8.6.1. Key Management Plan

Australian Government entities **should** develop and maintain a Key Management Plan (KMP) for all PKI cryptographic keys and secrets used within their gateway. Entities **should** ensure the following key items are covered in their Key Management Plan (KMP): generation, storage and access, exchange, rollover (including key lifetimes), chains of trust, and positions of trust.

For gateways or PEPs that are hosted by a Cloud Service Provider or are hosted by a Managed Service Provider (MSP), entities **must** ensure that their provider has a KMP. If the provider supports bring your own key capabilities entities **must** ensure that their own KMP and the KMP of their provider have a clearly documented shared responsibilities model.

8.6.2. Key Revocation

Australian Government entities **should** ensure revocation checks are exercised against all PKI cryptographic digital certificates used in their gateway, that are not a root certificate, each time the key is utilised.

8.6.3. Key Rollover

Australian Government entities **must** rollover keys or secrets in the following situations:

- they have reached end of life as defined in their KMP.
- their digital certificate has expired or been revoked.
- an indication of compromise has been identified.

When performing a key rollover entities **must** use new keys when re-issuing a digital certificate.