Australian Government

Department of Home Affairs

Protective Security Policy Framework

Australian Government Protective Security Policy Framework

Release 2025

protectivesecurity.gov.au

pspf@homeaffairs.gov.au

Foreword

Directive on the Security of Government Business

The Australian Government is committed to ensuring the secure delivery of government business and continuing to build trust and confidence in our ability to engage with and manage security risks.

As the Minister responsible for protective security policy for the Australian Government, I direct Accountable Authorities of non-corporate Commonwealth entities that are subject to the *Public Governance, Performance and Accountability Act 2013* (PGPA Act) to comply with the Protective Security Policy Framework (PSPF).

The PSPF sets the Australian Government's minimum protective security standards to achieve effective and efficient secure delivery of government business, both domestically and internationally.

Entities must implement the PSPF requirements within their unique security risk environments.

Security is everyone's responsibility. I expect all Australian Government personnel to support a positive, embedded security culture.

The Australian Government, led by the Department of Home Affairs, will continue to assess emerging security risks and develop and refine protective security policy that reflects the current threat environment in which entities conduct their business.

Hon Tony Burke MP

Minister for Home Affairs, Minister for Immigration and Citizenship, Minister for Cyber Security, Minister for the Arts, and Leader of the House of Representatives

Executive Summary

The PSPF sets out Australian Government policy across six security domains and prescribes what Australian Government entities must do to protect their people, information and resources, both domestically and internationally. Application of the PSPF assures government that entities are implementing sound and responsible protective security practices, and identifying and mitigating security risks and vulnerabilities.

Every entity has an important role to play in the security of Australian Government business. The Australian public expects that government services are secure with effective systems in place to protect the data and information they manage. We face unique challenges in our environment; threats are escalating with frequency and complexity. More than 350,000 public servants are employed in the Australian Government, providing services to Australians domestically and internationally. Protection of our people, information and resources is at the heart of our operations and is paramount. We will continue to invest in measures to uplift the security maturity of Australian government entities.

We look forward to working with all Australian government partners, industry and the wider community to transform our collective protective security.

Stephanie Foster PSM

Secretary, Department of Home Affairs

Contents

About the PSPF

Purpose

The Protective Security Policy Framework (PSPF) sets out Australian Government policy across six security domains and prescribes what Australian Government entities must do to protect their people, information and resources, both domestically and internationally.

The PSPF provides direction and guidance for:

- The Accountable Authorities of Australian Government entities, per the *Public Governance, Performance and Accountability Act 2013* (PGPA Act).
- Entity Chief Security Officers, Chief Information Security Officers, security advisers and other named security officials.
- Service providers that provide services to Australian Government entities, or are required to implement the PSPF according to relevant deeds or agreements.
- Those responsible for communicating security information to Australian Public Service (APS) employees, third-party service providers delivering services to Australian Government entities, and visitors to government facilities.
- Those working within, and for, the Australian Government, including APS employees, third-party service providers and contracted staff.

Applicability

The *Directive on the Security of Government Business* establishes the PSPF as Australian Government policy.

Non-corporate Commonwealth entities (entities) must apply the PSPF in accordance with section 21 of the PGPA Act.

The PSPF represents better practice for Corporate Commonwealth Entities and wholly-owned Commonwealth Companies.

State and territory government agencies that hold or access Australian Government security classified information are required to apply the PSPF to regulate access to that information, in accordance with arrangements agreed between the Commonwealth, states and territories.

Non-government organisations and third-party service providers may be required to implement aspects or parts of the PSPF. This will be detailed in relevant deeds or agreements between the Australian Government and the non-government organisations or third-party service providers.

Non-government organisations may implement the PSPF as a security framework.

Accountability

Accountable Authorities are responsible for implementing the PSPF within their entities and are accountable to their minister for the security of their entity.

Implementation of the PSPF does not absolve Accountable Authorities of their obligations to comply with other legislation or regulatory requirements.

Delegation

Roles mandated in the PSPF have specific responsibilities and powers.

Responsibilities and powers can only be delegated where explicitly stated in the PSPF.

Reporting

Accountable Authorities must annually report compliance against the PSPF to both their minister and the Department of Home Affairs.

These reports assure government that entities are implementing sound and responsible protective security practices, and identifying and mitigating security risks and vulnerabilities.

The Department of Home Affairs will undertake quality assurance of submitted reports. Information about this activity can be found in Protective Security Reporting Quality Assurance.

Structure

The PSPF comprises five tiers:

- Principles – apply to all aspects of protective security.
- Protective security domains – define interconnected subject areas.
- Policy – detail requirements that entities must apply.
- Standards and Technical Manuals – detail additional mandatory requirements for specific areas of the PSPF. These include manuals maintained by Technical Authority Entities.
- Guidelines – provide advice and examples to assist entities in implementing the requirements and standards.

Figure 1 details the structure of the PSPF.

Principles

The principles apply to all aspects of protective security, and must be integrated into the thinking, practice and decision making of entities at all levels. This enables entities to effectively manage security risks in a pragmatic way. Figure 2 details the principles of the PSPF.

Domains

The principles are applied through compliance with the mandatory requirements and standards in the following domains:

- Governance Part One.
- Risk Part Two.
- Information Part Three.
- Technology Part Four.
- Personnel Part Five.
- Physical Part Six.

These domains are not mutually exclusive – each connects with, and impacts, the other. Entities must manage security within a framework of coordinated planning across these domains.

Policy

The PSPF policy suite includes mandatory requirements in each domain that entities must implement to achieve minimum protective security standards.

Requirements

Requirements are presented as follows:

Component	Description
Number	Unique number for each requirement (retained indefinitely)
Domain	The domain under which the requirement sits
Applicability	All entities – entity, organisation or provider required to apply the PSPF
	TAE – Technical Authority Entity
	DOS – Department of State
	AVA – Authorised Vetting Agency
	SSPE – Shared Services Provider Entity
	SOGS – Entities operating a System of Government Significance
Date	Date requirement last updated

Standards

PSPF Standards detail additional mandatory requirements on specific PSPF topics. They are more granular and prescriptive in nature.

Technical Manuals

Technical Manuals are authorised by the PSPF. They take a variety of forms (e.g. single manual, framework) and are maintained by the relevant Technical Authority Entity.

A list of Technical Manuals authorised by the PSPF can be found in the PSPF Guidelines.

Guidelines

The PSPF Guidelines provide best practice implementation advice. They cover a wide range of topics and reference the various PSPF Standards and Technical Manuals.

Annual Releases

The Department of Home Affairs is responsible for the Australian Government's protective security policy, and administration of the PSPF.

The PSPF is reviewed annually to ensure it reflects the current threat environment. Entities are consulted on proposed updates via the Government Security Committee. Updates culminate in an annual release.

Technical Authority Entities remain responsible for updates to the Technical Manuals they maintain and will consult entities on updates as appropriate.

Oversight

Australian Government protective security is overseen by two governance bodies.

Protective Security Board

The Protective Security Board provides agency-head oversight of strategic protective security policy issues and challenges.

Its purpose is to:

- provide strategic direction to, and oversight of, whole of government protective security policy
- provide assurance to the Secretaries Board on relevant protective security matters
- empower and support the Government Security Committee, and
- support the Chief Security Officer network.

The Secretary of the Department of Home Affairs chairs the board. The board endorses policy updates to the PSPF Standards and Technical Manuals authorised by the PSPF.

Government Security Committee

The Government Security Committee provides Deputy Secretary-level strategic direction setting for whole of government protective security policy issues and challenges.

It is supported by topic-specific subcommittees.

Its purpose is to:

- provide Senior Executive Service Band 3 level direction to whole of government protective security policy
- coordinate policy and operational response to emerging protective security policy threats and issues
- inform the Protective Security Board on significant security policy matters, and
- provide direction to continuous improvement on the protective security maturity of entities.

The Head of National Security within the Department of Home Affairs chairs the committee.

It meets three times a year and, at a minimum, endorses new requirements in the PSPF.

It reports to the Protective Security Board.

Contact Us

The Department of Home Affairs produces and maintains the PSPF.

Contact:

- Email: PSPF@homeaffairs.gov.au
- PSPF Hotline: (02) 5127 9999
- PSPF GovTEAMS community

Figure 1: PSPF Structure

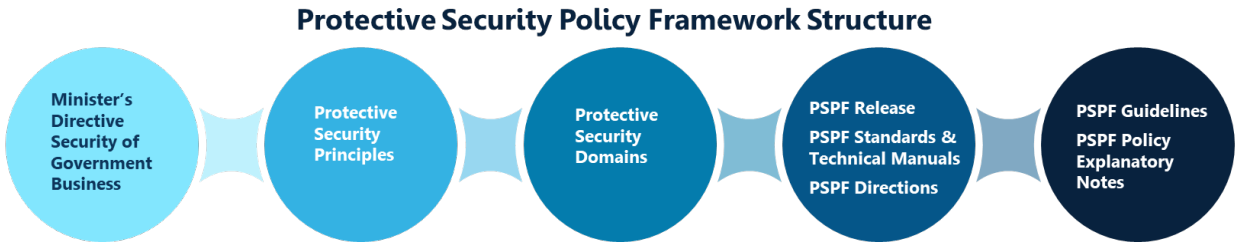
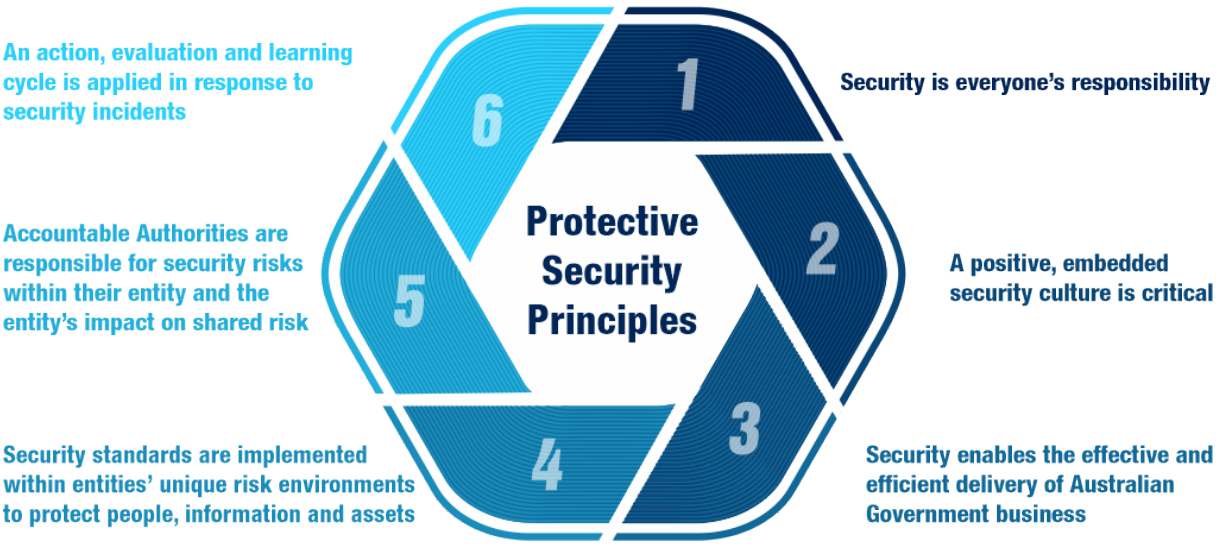


Figure 2: Protective Security Principles



Part One

Governance

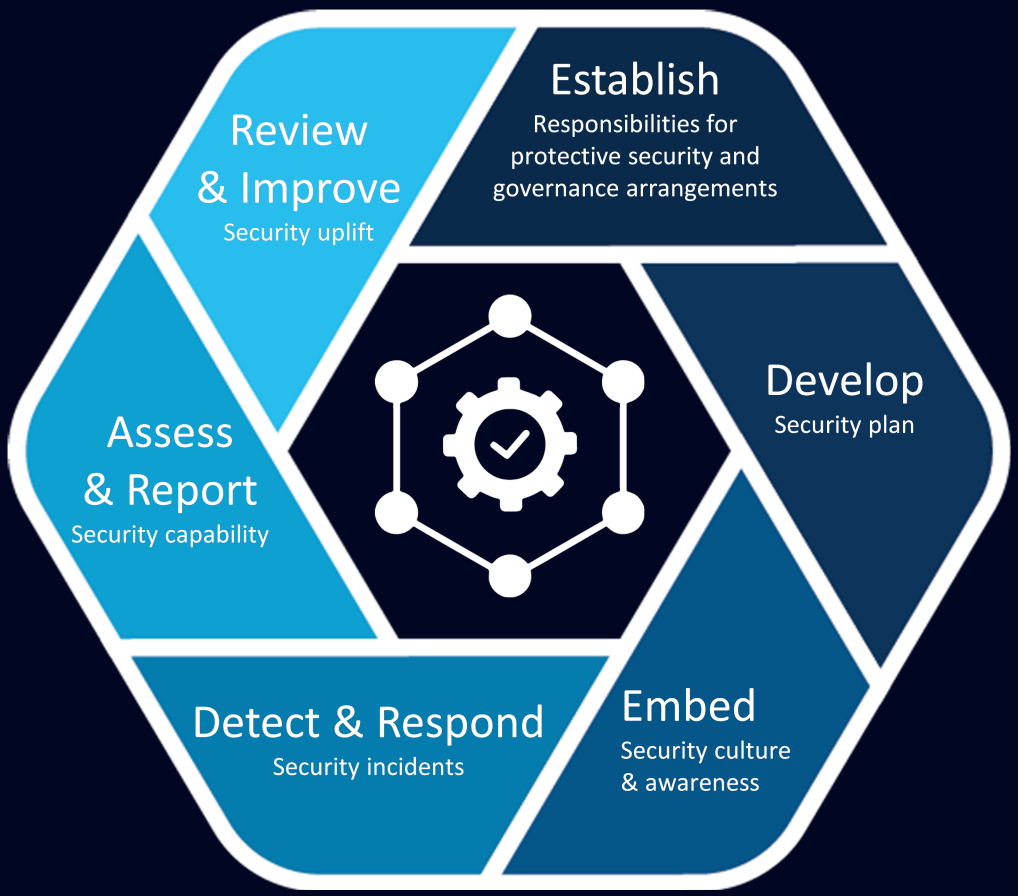
Whole of Government Protective Security Roles

Entity Protective Security Roles and Responsibilities

Security Planning, Incidents and Training

Protective Security Reporting

Governance Lifecycle



1 Whole of Government Protective Security Roles

1.1 Departments of State

Departments of State (DOS) are established by the Governor-General to conduct the core aspects of government operations. Departments of State encompass the lead entity in each portfolio, as detailed in the Department of Finance's Flipchart of Commonwealth entities and companies. These entities are denoted as DOS in the requirement ribbon.

Requirement 0001 | GOV | DOS | 31 October 2024

The Department of State supports portfolio entities to achieve and maintain an acceptable level of protective security through advice and guidance on government security.

1.2 Department of Home Affairs

In accordance with the Administrative Orders, the Department of Home Affairs is responsible for the administration of the PSPF. This includes responsibility for managing and coordinating policy responses to systemic security risks to government.

1.2.1 Protective Security Directions

The PSPF provides that, having considered advice from key Technical Authority Entities, the Secretary of the Department of Home Affairs may issue a Direction to Accountable Authorities to manage an unacceptable protective security risk to the Australian Government.

Accountable Authorities of entities that are subject to the PGPA Act must adhere to any Protective Security Directions issued by the Secretary of the Department of Home Affairs.

Accountable Authorities are responsible for ensuring that non-government organisations and third-party service providers who are subject to PSPF requirements under relevant deeds or agreements adhere to Protective Security Directions.

Protective Security Directions are made available on the PSPF website (unless security classified). Entity Chief Security Officers and Chief Information Security Officers are notified when Protective Security Directions are issued.

Requirement 0002 | GOV | All entities | 31 October 2024

The Accountable Authority complies with all Protective Security Directions.

1.3 Technical Authority Entities

Technical Authority Entities are entities that have additional accountabilities to provide domain-specific security advice, technical standards or intelligence services in support of Australian Government protective security outcomes. These entities are denoted as TAE in the requirement ribbon.

See PSPF Guidelines for the current list of Technical Authority Entities.

Requirement 0003 | GOV | TAE | 31 October 2024

The Technical Authority Entity provides technical advice and guidance to support entities to achieve and maintain an acceptable level of protective security.

1.4 Shared Service Provider Entities

Shared Service Provider Entities (SSPE) are non-corporate Commonwealth entities that provide corporate or technical services to other entities under an agreement or arrangement. These entities are denoted as SSPE in the requirement ribbon.

Existing partnership and shared-service arrangements must have clearly defined accountability, responsibilities and agreed processes for responding to change and incident management. These should be periodically reviewed to ensure accountabilities and responsibilities remain suitable and appropriate.

Supported entities may outsource responsibility for specific functions under shared-services or partnership arrangements, provided the Accountable Authority of the shared service provider entity agrees. The Accountable Authority of the supported entity remains responsible for the overall security of their entity.

Requirement 0004 | GOV | SSPE | 31 October 2024

The Shared Service Provider Entity supplies security services that help relevant entities achieve and maintain an acceptable level of security.

Requirement 0005 | GOV | SSPE | 31 October 2024

The Shared Service Provider Entity develops, implements and maintains documented responsibilities and accountabilities for partnerships or security service arrangements with other entities.

1.5 Authorised Vetting Agencies

Security vetting is conducted to ensure personnel are eligible and suitable to access security classified government information and resources. These functions may only be performed by vetting agencies authorised to assess, process and grant security clearances (Baseline up to and including Positive Vetting security clearances) for Australian Government entities. Authorised Vetting Agencies (AVA) entities are denoted as AVA in the requirement ribbon.

See PSPF Guidelines for the list of Authorised Vetting Agencies.

1.5.1 TOP SECRET-Privileged Access Authority

Only the TOP SECRET-Privileged Access (TS-PA) Authority is authorised to implement requirements of the TS-PA Standard, issue TS-PA security clearances and manage the ongoing suitability of TS-PA security clearance holders.

This includes, but is not limited to, assessing information provided by sponsoring entities and other sources (including changes of circumstances), and conducting annual clearance reviews of all TS-PA security clearances, reviews for cause, and revalidation of TS-PA security clearances.

1.6 Sponsoring Entities

Australian Government entities are authorised to sponsor Australian Government security clearances. Entities that sponsor security clearances are known as 'Sponsoring Entities' and have additional responsibilities in the vetting process and the ongoing management of security cleared personnel.

The Australian Government may also authorise non-government organisations to sponsor security clearances. See Sponsoring Security Clearances and PSPF Guidelines for details.

State and territory government agencies are also authorised to sponsor security clearances.

Related Standards – Whole of Government Protective Security Roles

- Legislation: Commonwealth of Australia Constitution Act
- Government policy: List of Commonwealth Entities

2 Entity Protective Security Roles and Responsibilities

2.1 Accountable Authority

The Accountable Authority of a Commonwealth entity is defined under section 12 of the PGPA Act as the person or group of persons responsible for, and with control over, the entity's operations.

The Accountable Authority has overall responsibility for the protective security of their entity's people, information and resources, both domestically and internationally.

- People – employees and contractors, including secondees and any service provider that an entity engages. It also includes anyone who is given access to Australian Government resources in Australia or internationally held by the entity as part of entity sharing initiatives.
- Information – physical documents/papers, electronic/digital data or intellectual information (knowledge) that is owned, managed or maintained by the entity. It includes details of methodologies, classified military/intelligence activities or operations, diplomatic discussions and negotiations.
- Resources – including applications/technology systems/mobile devices that process, store or communicate official and security classified information/data, tangible assets, equipment, facilities, buildings and other spaces/places, elements of infrastructure and intangible assets such as data centres.

To achieve this they are responsible for implementing the PSPF mandatory requirements and standards and having effective protective security arrangements in place. The Accountable Authority is also responsible for implementing any Protective Security Directions issued by the Secretary of the Department of Home Affairs. See Protective Security Directions.

With support from their Chief Security Officer and Chief Information Security Officer, the Accountable Authority has overall responsibility for managing the entity's security risks including determining their entity's tolerance to security risks and how to identify, assess and prioritise risks to people, information and resources. They must also consider how these decisions will impact other entities and whole of government security.

It is critical that the Accountable Authority establishes arrangements to ensure the Chief Security Officer and the Chief Information Security Officer work together to ensure a consistent approach to protective security across the entity and to achieve the entity's security objectives.

Other mandatory requirements for the Accountable Authority are denoted through this policy.

Requirement 0006 | GOV | All entities | 31 October 2024

The Accountable Authority is answerable to their minister for the entity's protective security.

Requirement 0007 | GOV | All entities | 31 October 2024

The Accountable Authority is responsible for managing the security risks of their entity.

2.2 Chief Security Officer

The Chief Security Officer (CSO) is a Senior Executive Service (SES) officer responsible for oversight of the entity's protective security arrangements, with support from the Chief Information Security Officer on cyber security arrangements. Where an entity has fewer than 100 employees, the Accountable Authority may appoint their CSO at the Executive Level 2 (EL2), providing the EL2 reports directly to the Accountable Authority on security matters, and has sufficient authority and capability to perform the responsibilities of the CSO role.

The CSO answers to the Accountable Authority and supports them by providing strategic oversight of protective security matters to assist with the continuous delivery of business operations.

The CSO establishes and maintains security arrangements that are tailored to the scale, complexity and risk profile of the entity and its people, information and resources. The intention is that as a single senior officer with central oversight and responsibility for security arrangements in the entity, they have the flexibility to delegate the day-to-day activities of protective security where required. The CSO is also responsible for fostering a culture where personnel have a high degree of security awareness, reinforced through practices that embed security into entity operations.

Requirement 0008 | GOV | All entities | 31 October 2024

A Chief Security Officer is appointed and empowered to oversee the entity's protective security arrangements.

Requirement 0009 | GOV | All entities | 31 October 2024

The Chief Security Officer is a Senior Executive Service officer[1] and holds a minimum security clearance of Negative Vetting 1.

Requirement 0010 | GOV | All entities | 31 October 2024

The Chief Security Officer is accountable to the Accountable Authority for protective security matters.

2.3 Chief Information Security Officer

The Chief Information Security Officer (CISO) is accountable to the Accountability Authority and supports the CSO by providing cyber security leadership for the entity and the entity's most critical technology resources, incorporating information technology and operational technology. This includes responsibility for the entity's cyber security strategy and uplift plan and implementing the Australian Signals Directorate's Information Security Manual and Strategies to Mitigate Cyber Security Incidents and cyber security risks.

If the CISO does not report directly to the CSO, they should work closely with the CSO and keep them informed, to ensure a holistic approach to security is maintained and cyber security does not become siloed from other security arrangements. This approach allows the CSO to retain a complete view of protective security across the entity.

The CISO may be located in another entity where the entity's cyber security services are wholly provided through a shared services arrangement with another entity. In such cases, the supported entity's Accountable Authority and CSO is required to establish suitable arrangements to retain visibility of cyber security matters.

[1] Where an entity has fewer than 100 employees the Accountable Authority may appoint their CSO at the Executive Level 2 (EL2), providing the EL2 reports directly to the Accountable Authority on security matters, and has the sufficient authority and capability to perform the responsibilities of the CSO role.

The CISO needs to possess the appropriate capability, leadership experience and technical skills to perform the role and make informed cyber security decisions for the entity.

Under the Public Governance, Performance and Accountability Rule 2014, entities are required to have an audit committee to review systems of risk oversight and management. Refer to Section 0 for the CISO's reporting obligations and to the entity's Audit Committee.

Requirement 0011 | GOV | All entities | 01 July 2025

A Chief Information Security Officer is appointed to oversee the entity's cyber security program and the cyber security for the entity's most critical technology resources.

Requirement 0012 | GOV | All entities | 31 October 2024

The Chief Information Security Officer has the appropriate capability and experience and holds a minimum security clearance of Negative Vetting 1.

Requirement 0013 | GOV | All entities | 01 July 2025

The Chief Information Security Officer is accountable to the Accountable Authority for cyber security risks and how the entity's cyber security program is managing these risks.

2.4 Security Practitioners

Security practitioners perform security functions or specialist services to support the CSO and CISO in the day-to-day functions of protective security.

While not mandated, the CSO and CISO have the flexibility to delegate the day-to-day activities of protective security to security practitioners and to perform specialist services.

Requirement 0014 | GOV | All entities | 31 October 2024

Where appointed, security practitioners are appropriately skilled, empowered and resourced to perform their designated functions.

Requirement 0015 | GOV | All entities | 31 October 2024

Where appointed, security practitioners have access to training across government to maintain and upskill on new and emerging security issues.

2.5 Security Governance

Under the Public Governance, Performance and Accountability Rule 2014, entities are required to have an audit committee to review systems of risk oversight and management. Audit committees perform an important role in oversight of risk management, including security risks.

The Accountable Authority determines the entity's governance arrangements and ensures they are commensurate with the entity's size, complexity and risk environment.

Requirement 0016 | GOV | All entities | 31 October 2024

The Accountable Authority approves security governance arrangements that are tailored to the entity's size, complexity and risk environment.

2.5.1 Security Email Address

Each entity must establish, maintain and monitor a dedicated security email address and provide this address to the Department of Home Affairs (PSPF@homeaffairs.gov.au). The Department will use this

address to provide entities with security-related policy advice, notifications and information and will blind copy the CSO, and where relevant the CISO.

Entities are to ensure this information is distributed to the relevant people and functions across the entity, including the CSO, CISO, Departmental Security Unit, Personnel Security team, Physical Security Teams, personnel involved in security reporting or incident management, and any other relevant security-related personnel or teams.

Requirement 0017 | GOV | All entities | 31 October 2024

A dedicated security email address is established and monitored as the central conduit for distribution of protective security-related information across the entity.

Related Standards – Entity Protective Security Roles and Responsibilities

- Legislation: Public Government, Performance and Accountability Act 2013
- Legislation: Public Governance, Performance and Accountability Rule 2014
- Guidance: Protective Security Guide for Chief Security Officers
- Guidance: ASD's Guidelines for Cyber Security Roles

3 Security Planning, Incidents and Training

3.1 Security Planning

Security planning is unified and holistic, as part of a security life cycle approach. Entity security plans address all domains of protective security.

Security planning establishes the strategic direction and sets out the expectations for the efficient and effective security management practices in the entity. The plan also articulates how security risks will be managed effectively and consistently across the entity to adapt to change, minimise damage and disruption, and build resilience.

A security plan is used to identify and manage risks and assist decision-making by:

- consistently applying controls that are both appropriate and effective in managing the entity's security risks
- adapting to change while safeguarding the delivery of core business and services
- improving resilience to threats, vulnerabilities and emerging challenges, and
- driving protective security performance improvements.

Each entity's security plan will be unique but must include the mandatory elements listed in Table 1.

Where a single security plan is not practicable due to the entity's size or complexity of business, entities may develop an overarching security plan that is approved by the Accountable Authority, supported by more detailed plans (referred to as supporting security plans), approved by the CSO or CISO (for cyber security plans), or their delegate.

Table 1: Security Plan Mandatory Elements

Plan component	Mandatory elements
Security goals and objectives	The security plan must detail the entity's security goals and strategic objectives, including how security risk management intersects with and supports broader business objectives and priorities.
Security risk environment	The security plan must detail the environment in which the entity operates; the threats, risks and vulnerabilities that impact the protection of the entity's people, information and resources. This includes that the Accountable Authority has overall responsibility for managing: • what the entity needs to protect (via a risk assessment) being the people, information and resources assessed as critical to its ongoing operation and to the national interest • what it needs to protect against (via threat assessment) • how security risks will be managed within the entity.
Risk tolerance	The security plan must detail the entity's tolerance to security risks, agreed by the Accountable Authority (see 5.1). Each entity's level of tolerance for risk will vary depending on the level of potential damage to the Australian Government or to the entity.
Security capability	The security plan must detail the maturity of the entity's capability to manage security risks.

Plan component	Mandatory elements
Security risk management strategies	The security plan must detail the entity's mitigation strategies appropriate to the levels of threat, risks to its resources and risk tolerances, and strategies to implement security risk management and maintain a positive risk culture. The entity's approach to managing security risks, including identifying how it will apply proportional and sufficient controls to deter, detect, delay and respond to threats (internal or external) that affect the security of its people, information or resources. This includes: • establishing risk stewards and managers • instigating steps that minimise risks (according to risk environment and tolerances) • managing residual risks to ensure the protection of people, information and resources.
Implications of risk decisions	The security plan must detail how information on the entity's risk management decisions will be shared with other entities that are, or may be, impacted by those decisions (see 5.2 Security Risk Management Process)
PSPF implementation	The security plan must detail the entity's strategies to deliver against the PSPF requirements and standards.
PSPF Directions	The security plan must detail the entity's arrangements for implementing any direction issued by the Secretary of the Department of Home Affairs under the PSPF. This includes the entity's approach to implementing the requirements specified in any directions, as well as to ensure any timeframes or additional reporting obligations specified in the direction are met. If the direction allows, this may include the entity's arrangements to implement alternative mitigations.
Critical people and resources	The security plan must identify people and resources that are critical to the ongoing operation of the entity and the national interest. It must detail the protections applied to safeguard these resources to support the continuity of the entity's core business. Resources covers information, systems, assets and facilities.
Threat levels	The security plan must be calibrated to the security environment in which the entity operates, including the National Terrorism Threat Level and relevant ASIO reporting related to espionage, foreign interference or sabotage threats. The plan should promote flexibility and scalable security controls which can be calibrated to changes in the security environment.
Incident management plan	The security plan must detail entity's security incident management plan covering the procedures to ensure security incidents are identified, managed and responded to.
Monitoring and improvement	The security plan must detail the entity's monitoring arrangements and plans to uplift protective security improvement in areas of insufficient implementation.
Review	The security plan must include how the entity will consider the security plan annually and review the security plan at least every two years, assessing the: • adequacy of existing measures and mitigation controls, and • arrangements to respond to and manage significant shifts in the entity's risk, threat and operating environment.

Requirement 0018 | GOV | All entities | 31 October 2024

A security plan is developed, implemented and maintained to address the mandatory elements of the plan.

3.1.1 Security Plan Responsibilities

The Accountable Authority has overall responsibility for managing the entity's security risks, with support from their CSO, CISO and where established, the security governance committee.

This obligation extends to determining their entity's tolerance to security risks and ensuring appropriate measures are in place to identify, assess and prioritise risks to people, information and resources. The Accountable Authority must also consider how these decisions will impact other entities and whole of government security.

The Accountable Authority must approve the entity's annual review of the security plan.

The CSO defines the strategic direction and allocation of resources to deliver the strategy, strengthen operations and improve the entity's security maturity in order to make sound decisions about security planning.

Requirement 0019 | GOV | All entities | 31 October 2024

The Accountable Authority approves the entity's security plan.

3.1.2 Security Plan Review

Entities must consider their security plan (and any supporting plans) annually to decide whether updates are required. Entities must also undertake a formal review of the plan at least every two years to ensure the plan is sufficient to manage the entity's security risks, and is able to adapt to changes in the entity's risk or operating environment, a change in the National Terrorism Threat Level or an emerging threat that alters the entity's business impact level.

A security plan is a 'living' document and requires review and adjustment to ensure the goals and management of security risks keep pace with changes in the entity and with emerging threats. Security plans are best developed by a person who also has an understanding of the entity's strategic goals and objectives and the appropriate level of security risk management knowledge and expertise.

Entities determine how the review of the security plan (and supporting security plans) is conducted, that is the process used to review the plan. The security plan must be approved by the Accountable Authority and may be reviewed by the CSO, CISO, or appointed security practitioner, an external security consultant or through a security governance oversight committee for larger or more complex business operations.

Requirement 0020 | GOV | All entities | 31 October 2024

The security plan is considered annually and reviewed at least every two years to confirm its adequacy and ability to adapt to shifts in the entity's risk, threat or operating environment.

3.2 Security Practices and Procedures

Protective security practices and procedures reflect the entity's implementation of, and compliance with, the PSPF requirements and standards. Entities must develop practices and procedures to cover all elements of protective security consistent with the PSPF requirements and standards.

Protective security practices detail the entity's general approach to security tasks and activities. Protective security procedures set clear guidelines for entity personnel to follow and perform work functions safely, in accordance with the PSPF requirements and standards, and any additional entity requirements.

The CSO is responsible for the protective security practices and procedures, other than for cyber security, which are the responsibility of the CISO.

Requirement 0021 | GOV | All entities | 31 October 2024

Procedures are developed, implemented and maintained to ensure all elements of the entity's security plan are achieved.

3.3 Continuous Monitoring and Improvement

Monitoring security maturity is an ongoing process and involves routine assessment of the entity's security capability, performance against a set of indicators and compliance with the PSPF requirements and standards.

Achieving and maintain compliance with the PSPF requirements and standards requires effective monitoring of the entity's security posture and a continuous cycle of improvement. These arrangements also assist the entity to respond to changes in its threat environment and respond to emerging security risks.

The entity security plan must detail the entity's monitoring arrangements and plans to uplift protective security improvement in areas of insufficient implementation.

Requirement 0022 | GOV | All entities | 31 October 2024

Develop, establish and implement security monitoring arrangements to identify the effectiveness of the entity's security plan and establish a continuous cycle of improvement.

3.4 Positive Security Culture

A positive security culture is vital to effectively and securely delivering Australian Government business and safeguarding information for which the entity is the trusted custodian. It is an effective method of reducing the threat to the entity, its people, information and resources. In addition to keeping an entity and its personnel safe, a strong and healthy security culture helps to increase internal and external trust, embed consistent positive behaviour, and support personnel to engage productively with risk.

The Accountable Authority and Chief Security Officer are ultimately responsible for fostering a positive security culture. They are supported by the Chief Information Security Officer and security practitioners to promote a culture where personnel value, use and protect entity information and resources appropriately.

Requirement 0023 | GOV | All entities | 31 October 2024

The Accountable Authority and Chief Security Officer develop, implement and maintain a program to foster a positive security culture in the entity and support the secure delivery of government business.

3.5 Security Awareness Training

Security awareness training is a vital element of fostering a positive security culture and ensuring personnel understand their protective security responsibilities and any entity-specific security obligations. It also embeds good security processes and supports the consistent application of protective security practices and procedures across the entity.

Security awareness training is most effective when it:

- is championed and practiced by senior leadership
- delivers an ongoing security awareness program to inform and regularly remind individuals of security responsibilities, issues and concerns
- briefs personnel on the access privileges and prohibitions attached to their security clearance level prior to being given access, or when required in the security clearance renewal cycle

- ensures that personnel who have specific security duties receive appropriate and up-to-date training
- fulfils security clearance renewal briefing requirements for all personnel and contracted service providers who hold a security clearance of Negative Vetting 1 or higher
- fulfils security clearance requirements and training obligations detailed in the TS-PA Standard
- clearly communicates to all personnel, including contractors, the entity's protective security practices and procedures, and
- provides all personnel including contractors with a clear understanding of the security environment in which the entity operates and the security threats relevant to their roles and responsibilities.

Requirement 0024 | GOV | All entities | 31 October 2024

Security awareness training is provided to personnel, including contractors, at engagement and annually thereafter.

Requirement 0025 | GOV | All entities | 31 October 2024

Targeted security training is provided to personnel, including contractors, in specialist or high-risk positions.

3.6 Security Incidents

Security incident management is the process of identifying, managing, recording and analysing any irregular or adverse activities or events, threats and behaviours in a timely manner. Effective monitoring of security incidents is fundamental to good security management. In turn, good security management contains the effects of a security incident and enables recovery as quickly as possible.

A security incident is defined as an:

- action, whether deliberate, reckless, negligent or accidental, that fails to meet protective security requirements or entity–specific protective security practices and procedures that results in, or may result in, the loss, damage, corruption or disclosure of official information or resources
- attempt to gain unauthorised access to official information or resources
- approach from anybody seeking unauthorised access to official resources, or
- event that harms, or may harm the security of Australian Government people, information or resources.

A security incident becomes reportable where it is a:

- specified significant security incident that due to its nature is considered to be significant or it meets external incident reporting or referral obligations, or
- significant business impact level security incident that due to the assessed severity of the potential or actual consequences or damage to Australian Government security classified people, information or resources, the national interest, an organisation or individuals, is considered to be significant. A significant security incident is generally serious or complex and is likely to have wide ranging and critical consequences for the entity and/or the Australian Government.

3.6.1 Security Incident Management and Exercises

A security incident management plan can increase the likelihood of successfully planning for, detecting and responding to malicious activity, insider threat and security incidents. The CSO, with support from the CISO for cyber security incidents, is responsible for establishing a security incident management plan, including consequence management, and incorporating this into the entity's business continuity arrangements to ensure that business-critical people, operations, systems and services are supported appropriately in the event of an incident or disaster.

Establishing security exercises as part of security planning can increase the success of the entity's procedures for detecting and responding to security incidents, including cyber security incidents and incidents caused by trusted insiders.

A security exercise tests the entity's preparedness to detect, respond to and recover from all types of security incidents. It also tests whether the entity's security incident management plans and procedures are appropriate and effective.

See Externally Reportable Security Incidents and Referral Obligations.

Responsibility for investigating, responding to and reporting on security incidents sits with the CSO, with support from the CISO for cyber security incidents. The CSO develops, implements and maintains procedures to ensure security incidents are responded to and, where required appropriately investigated. The CSO also undertakes regular exercises of these arrangements.

Information gathered on security incidents and investigations assists the CSO, or CISO (for cyber incidents), to determine the adequacy of protective security practices, measure security culture, highlight vulnerabilities in security awareness training and inform security improvement activities.

The CSO and CISO are accountable to the Accountable Authority for the management of security incidents, exercises and investigations, in accordance with the PSPF and any other regulatory requirements.

Requirement 0026 | GOV | All entities | 31 October 2024

Procedures are developed, implemented and maintained to ensure security incidents are responded to and managed.

Requirement 0027 | GOV | All entities | 31 October 2024

Security incident management and response plans are incorporated into the entity's business continuity arrangements.

3.6.2 Coordination of Cyber Security Incidents

The National Cyber Security Coordinator coordinates responses to major cyber incidents, whole of government incident preparedness efforts, and strengthens Australian Government cyber security response capability, in accordance with Australian Government Crisis Management Framework (AGCMF).

The National Cyber Security Committee (NCSC) is the mechanism for inter-jurisdictional coordination for cyber security incident response. If a national cyber security incident escalates in impact and severity, the response may require escalation in accordance with existing national crisis management arrangements. This occurs in collaboration with the National Cyber Security Coordinator and the National Emergency Management Agency, to ensure that consequence management is activated as appropriate.

3.6.3 Externally Reportable Security Incidents and Referral Obligations

Entities must report any significant or reportable security incidents to the relevant authority. Relevant authorities fall broadly into three categories:

- authorities able to assist with advice, containment or remediation
- authorities with policy or legislative responsibility, and
- others who may be impacted by the security incident.

The purpose of this reporting obligation is to ensure the entity receives assistance with containment and/or remediation, regardless of whether the incident is considered 'significant' or not, or to comply with obligations to report to specific authorities. It further ensures the relevant authority is aware of the types and numbers of security incidents occurring with their area of responsibility.

The mandatory externally reportable security incidents and referral obligations are listed in Table 2. This is not an exhaustive list and there may be other legislative requirements or Government policy obligations for reporting security incidents. Some security incidents have more than one line of reporting and may require the entity to report to multiple relevant authorities.

Entities must report to the relevant authority within the set specific timeframes for reporting. If no timeframe is specified, then entities must report once they become aware that the security incident is occurring or has occurred.

Requirement 0028 | GOV | All entities | 31 October 2024

Significant or externally reportable security incidents and referral obligations are reported to the relevant authority (or authorities) within the applicable timeframe.

Table 2: Externally reportable security incidents and referral obligations

Reportable incident	Relevant authority	Reporting obligation	Timing of reporting	Notes	Method of reporting
Significant security incidents	Department of Home Affairs	• Significant security incidents. • Lessons learnt from any incidents, investigations, reports or reviews relating to the incident. • Potential or identified foreign ownership, control or influence risks identified during the procurement process.	As soon as possible (ASAP) after incident occurs/detected and annual PSPF reporting	Lessons learnt can be shared via the PSPF reporting portal, or by email PSPF@homeaffairs.gov.au. Entities will be required to also report on incidents and lessons learnt in their annual report on security.	• OFFICIAL to PROTECTED) – PSPF Reporting Portal: https://portal.protectivesecurity.gov.au/ • (SECRET and above) – contact PSPF@homeaffairs.gov.au or PSPF Hotline (02) 5127 9999 for advice
National security incidents	Australian Security Intelligence Organisation	Security incidents or situations that have, or could have, an impact on national security, as defined in the *Australian Security Intelligence Organisation Act 1979*, including suspected: • espionage and foreign interference • sabotage • politically motivated violence • promotion of communal violence • attacks on Australia's defence system, and • serious threats to Australia's territorial and border integrity.	ASAP after incident occurs/detected	ASIO and the reporting entity will conduct an initial assessment of the potential harm. Dependent on the assessment, ASIO will either: • recommend the entity continue with its own investigation and advise ASIO of the outcome, or • conduct the investigation, in close consultation with the entity, and possibly the Australian Federal Police. The need-to-know principle applies in relation to the details of a major security incident and its occurrence within an entity, until ASIO advises otherwise.	Notifiable Incidents, Threats or Reportable Observations (NITRO) secure online portal: nitro.asio.gov.au
Cyber security incidents	Australian Signals Directorate's Australian Cyber Security Centre (ACSC)	Cyber security incidents relating to system and network activities: • suspicious privileged account lockouts • suspicious remote access authentication events • service accounts suspiciously communicating with internet-based infrastructure • compromise of sensitive or classified data • unauthorised access or attempts to access a system • emails with suspicious attachments or links • denial-of-service attacks • ransomware attacks, and • suspected tampering of electronic devices.	ASAP after incident occurs/detected	If ASD is requested to assist with the entity's investigation, no actions which could affect the integrity of evidence should be carried out before ASD becomes involved. Refer to Information Security Manual.	Email: asd.assist@defence.gov.au Reporting form: https://www.cyber.gov.au/report-and-recover/report Cyber Security Hotline: 1300 CYBER 1 (1300 292 371)
Cabinet material	Department of the Prime Minister and Cabinet	Security incidents (or suspected incidents) involving Cabinet material.	ASAP after incident occurs/detected	Refer to the Cabinet Handbook for information on handling of Cabinet documents.	Cabinet Division, Department of the Prime Minister and Cabinet via entity Cabinet Liaison Officers.
Contact reporting	Australian Security Intelligence Organisation	Government personnel are required to report contact, either official or social, with a foreign national seems suspicious, persistent or unusual in any respect, or becomes ongoing. Such contact should be reported irrespective of whether it occurs within or outside Australia. Personnel should report where a person or group, regardless of nationality, seeks to obtain information they do not need-to-know in order to do their job.	ASAP after contact occurs/detected	Foreign nationals may include, but are not limited to, embassy or foreign government officials, including trade or business representatives. Contact as part of official meetings does not need to be reported provided a formal corporate record is produced detailing the topics discussed. However, employees should complete a contact report where a foreign national seeks to establish social contact outside official meetings, and/or where the contact seems suspicious, persistent or unusual.	Australian Government Contact Reporting Scheme Email: cr@asio.gov.au
Incidents involving security clearance subjects	Authorised Vetting Agency	Report security incidents caused by, or directly affecting a security clearance holder or clearance subject including incidents that point to a person's suitability to hold a security clearance	Appropriate time	The appropriate time will depend on the significance of the incident, whether it is subject to investigation and an assessment of the related personnel security risks.	Authorised Vetting Agency point of contact. For clearances issued by the Australian Government Security Vetting Agency (AGSVA), report via: https://www.agsva.gov.au/about/myclearance Email: securityclearances@defence.gov.au Phone 1800 640 450
Correspondence of security concern	Entity CSO, CISO (or security practitioner) to determine	Correspondence received that may be of a security concern, including but not limited to: • threat to use violence to achieve a political objective, and • warning of imminent threats to specific individuals, groups, property or buildings.	ASAP	The CSO, CISO (or delegate) will assess and determine the appropriate law enforcement or national security entity to externally report the incident.	Entity significant security incident channels.

Reportable incident	Relevant authority	Reporting obligation	Timing of reporting	Notes	Method of reporting
Incident affecting another entity	Accountable Authority (or delegate) of the impacted entity	Security incidents or unmitigated security risks that affect another entity's people, information or resources.	ASAP after incident occurs/detected	Particular consideration should be given to sharing information with entities that are co-located or are providing services to another entity.	Refer to the Australian Government Directory
Classified courier services	Security Construction and Equipment Committee (SCEC)	Security incidents involving SCEC-endorsed safe hand courier services.	ASAP after incident occurs/detected		Email: SCEC@SCEC.gov.au Report via: https://www.scec.gov.au/scec-endorsed-courier-incidents
Classified equipment and services	Security Construction and Equipment Committee (SCEC)	Security incidents involving SCEC Security Zone Consultants and SCEC approved locksmiths, including: • SCEC-approved products faults or failure, and • destruction services - National Association for Information Destruction (NAID) AAA Certification with PSPF endorsement.	ASAP after incident occurs/detected		Email: SCEC@SCEC.gov.au
Unauthorised foreign entity access to classified Australian information or assets	Entity CSO, CISO (or security practitioner) to determine	Occurrences of Australian security classified information and assets being shared with a foreign national or international entity without the protection of an appropriate agreement or arrangement.	ASAP after incident occurs/detected	International agreements or international arrangements may impose additional reporting and security violation handling requirements beyond those detailed in the PSPF. The CSO, CISO (or delegate) will assess and determine the appropriate law enforcement or national security entity to externally report the incident along with reporting under another category in this table.	Entity significant security incident channels.
Compromise of foreign entity information or assets	Originating foreign government (or entity that provided the information)	Where a suspected security incident involves the compromise of information, or other resources, that originate from a foreign government or governments, entities must comply with the arrangements outlined in the agreement or arrangement under which the information was obtained.	ASAP in accordance with the overarching agreement or arrangement	Where the foreign government information has been provided by another entity, inform the providing entity of the security incident as soon as possible. The providing entity may have obligations it needs to apply under an agreement or arrangement.	Entity significant security incident channels.
Eligible data breaches	Australian Information Commissioner	Report eligible data breaches, in accordance with the Notifiable Data Breaches scheme under Part IIIC of the *Privacy Act 1988*, to the OAIC. When an entity is aware of reasonable grounds to believe an eligible data breach has occurred, notify any individual at likely risk of serious harm.	Commissioner: as soon as practicable. Individuals at likely risk of serious harm: ASAP	The scheme only applies to data breaches involving personal information that are likely to result in serious harm to any individual affected. These are referred to as 'eligible data breaches'.	Report through a statement about the eligible data breach using form: https://www.oaic.gov.au/NDBform
Potential criminal/serious incidents	Australian Federal Police or Local Police	Incidents that may constitute a criminal offence. • Commonwealth crimes – as detailed on AFP website, and • State or territory crimes – threats, cybercrime, online fraud, internet scams, stalking etc.	ASAP after incident occurs/detected	Examples of Commonwealth crimes (report to AFP): • theft from the Commonwealth Government • assault on a Commonwealth official • threats against a Commonwealth official.	Commonwealth crimes: https://www.afp.gov.au or 02 6131 3000 State or territory crimes: 13 14 44 Crime Stoppers: 1800 333 000 to anonymously provide information about a crime
Critical incidents involving public safety	National Situation Room (NSR)	Critical incidents that may affect public safety or require a coordinated response in support of the Australian Government and/or state and territory governments relating to: • assault, including armed or military style assault • arson, including suspected arson • assassination, including suspected assassination • bombing, including suspected use of explosive ordnance or improvised explosive devices • chemical, biological or radiological attack, including suspected attacks • attack on the National Information Infrastructure or critical infrastructure • violent demonstration involving serious disruption of public order • hijacking, including suspected hijacking • hostage situation, including suspected hostage situation • kidnapping, including suspected kidnapping • mail bomb, including suspected mail bomb, or • white powder incident, including real or significant hoax incidents.	ASAP after incident occurs/detected	For critical incidents requiring immediate response, in particular where lives are at risk, call emergency services on triple zero (000).	Report suspicious behaviour (nationalsecurity.gov.au) Email: hotline@nationalsecurity.gov.au National Security Hotline: 1800 123 400 SMS: 0429 771 822 The NSR will advise the AFP, ASIO, local police and/or other entities as appropriate.

16

3.7 Security Investigations

A security investigation is a formal process of examining the cause and extent of a security incident that has, or could have, caused harm to individuals, the entity, another entity or the national interest.

The Australian Government Investigations Standards were developed to ensure quality investigative practices and outcomes in entities.

Responsibility for investigating security incidents sits with the CSO, with support from the CISO for investigations into cyber security incidents.

Where a suspected security incident involves the compromise of security classified information or other resources that originate from, or are the responsibility of another entity, it is important to seek advice from the originating entity prior to instigating any investigation. The originating entity may have operational security requirements that need to be applied to the investigation. In some cases, it may be more appropriate that the originating or responsible entity carries out the investigation. This requirement should not prevent or delay any immediate action required to prevent further compromise of classified information.

See PSPF Guidelines for the security investigation process.

Requirement 0029 | GOV | All entities | 31 October 2024

Procedures are developed, implemented and maintained to investigate security incidents in accordance with the principles of the Australian Government Investigations Standards.

3.7.1 Procedural Fairness

The principles of procedural fairness apply to all investigations. These principles require that individuals whose rights, interests or expectations are adversely affected, be informed of the case against them, that they be given an opportunity to be heard by an unbiased decision-maker, and to respond. This should be done in a manner that gives regard to national security considerations to the greatest extent practicable. Procedural fairness also applies to actions taken as the result of an investigation. Procedural fairness gives regard to ensuring the security integrity of any current or future investigation of the entity or of another entity.

Requirement 0030 | GOV | All entities | 31 October 2024

The principles of procedural fairness are applied to all security investigations, with due regard to national security considerations

See Security Incidents.

Related Standards – Security Planning, Incidents and Training

- Standard: Australian Government Investigations Standard
- Standard: Department of the Prime Minister and Cabinet's Cabinet Handbook
- Guidance: Office of the Australian Information Commissioner's Data breach preparation and response
- Guidance: ASIO's Countering the Insider Threat (on GovTEAMS)
- Guidance: ASIO's Contact Reporting (on GovTEAMS)
- Guidance: ASIO's Working from Home (on GovTEAMS)

4 Protective Security Reporting

4.1 Security Reporting to Government

The Department of Home Affairs prepares two annual reports using the annual PSPF reporting data:

- PSPF Assessment Report – consolidated report on the aggregated annual reporting data for the Minister for Home Affairs, Minister for Immigration and Citizenship, Minister for Cyber Security, Minister for the Arts and Leader of the House of Representatives. This consolidated report is provided to entities and published on the PSPF website for public transparency.
- PSPF Classified Assessment Report – provides the Government with entity-specific results and identifies entities not meeting the requirements and standards of the PSPF. This report also provides a heat map of protective security issues and vulnerabilities. This classified report is not made publicly available or provided to entities.

4.2 Annual Protective Security Report

Annual protective security reporting provides assurance to the Government that entities are complying with their security obligations, implementing sound and responsible protective security practices and identifying and mitigating security risks and vulnerabilities.

4.2.1 Reporting to Ministers

The Accountable Authority is responsible to their Minister for the protective security of their entity's people and resources, and must provide their Minister with an annual protective security report by December. If the entity reports to multiple Ministers, then each Minister is to receive a copy of the protective security report (or relevant extracts if that is more appropriate).

This report provides the Minister with assurance that entity is implementing sound and responsible protective security practices and demonstrating ongoing efforts to address security capability and posture.

Requirement 0031 | GOV | All entities | 31 October 2024

The annual protective security report is provided to the entity's Minister.

4.2.2 Reporting to the Department of Home Affairs

The Department of Home Affairs administers the PSPF on behalf of the Minister for Home Affairs, Minister for Immigration and Citizenship, Minister for Cyber Security, Minister for the Arts and Leader of the House of Representatives.

Entities must participate in the PSPF annual reporting process by completing and submitting an annual protective security report through:

- PSPF Reporting Portal – for reports classified up to and including PROTECTED, and
- Offline Reporting Template (submitted on the commensurate system) – for reports classified SECRET or TOP SECRET.

The Department uses the annual reporting data to prepare two reports each year for Government. See Security Reporting to Government.

Requirement 0032 | GOV | All entities | 31 October 2024

The annual protective security report is submitted to the Department of Home Affairs.

Requirement 0033 | GOV | All entities | 31 October 2024

The Accountable Authority approves the entity's annual protective security report and confirms that they have verified the report's content.

4.2.2.1. Protective Security Reporting Process

Compliance with PSPF requirements is a fundamental element of effective and accountable governance. Compliance reporting is designed to provide reasonable assurance to the Government that entities have achieved their objective by implementing the mandatory elements of the PSPF to protect their people and resources.

The PSPF requirements equate to the questions asked in the entity's annual protective security report. Additional seasonal questions that are not tied to a PSPF requirement may also be asked. Entities are provided with a list of the questions ahead of each reporting period.

Each question has been assigned one of the following reporting types:

- Performance
- Yes/No, or
- Yes/No/Not Applicable

See PSPF Release 2025 – List of Requirements for details of the reporting type assigned to each question.

See PSPF Guidelines for further information on reporting.

4.2.2.2. Protective Security Reporting Portal

The PSPF Reporting Portal allows Commonwealth entities to complete and submit their annual protective security report online, access benchmarking reports at the conclusion of the reporting period, and access reports from the previous reporting period. The PSPF Reporting Portal is accredited to process, store and communicate information up to PROTECTED.

The entity's CSO is responsible for ensuring the entity meets the annual protective security reporting obligations. The role of the 'Submitter' in the PSPF reporting portal is automatically assigned to the CSO, however this role can be delegated to another suitable officer. The Submitter is the key contact for the entity's annual protective security report and is responsible for commencing and submitting the assessment.

4.2.2.3. Protective Security Reporting Quality Assurance

The 2023–2030 Australian Cyber Security Strategy initiative to strengthen the security maturity of government entities includes a security assurance function to review the security maturity of Commonwealth entities.

Under this initiative, the Department of Home Affairs may undertake additional quality assurance of annual protective security reports submitted by entities. Where this occurs, the Department of Home Affairs will contact the CSO (or their delegate).

Annual PSPF reporting data and Cyber Security Survey data will be used to inform these reviews. These reviews will inform further evolution of our security frameworks and help government entities meet changes in the evolving threat landscape.

Requirement 0034 | GOV | All entities | 31 October 2024

Entities cooperate with the Department of Home Affairs' assurance activities to review annual protective security reports.

4.2.2.4. Sharing of Annual Security Reports

The annual PSPF reporting data is shared with:

- Australian Signals Directorate to support its cyber uplift programs, development of technical guidance on areas of targeted improvement and to support the Annual Commonwealth Cyber Security Posture Report to Parliament.
- Australian Security Intelligence Organisation to support its efforts to uplift government security capability.
- Australian National Audit Office when requested to support an audit and in line with its responsibilities under the *Auditor-General Act 1997*.

4.3 Reporting to the Australian Signals Directorate

The Australian Signals Directorate's Australian Cyber Security Centre is the Australian Government's lead agency on national cyber security operational matters, including technical cyber security incident response and advice. Entities must report on cyber security matters by completing the Australian Signals Directorate's annual Cyber Security Survey.

The Australian Signals Directorate uses this reporting data to prepare the Commonwealth Cyber Security Posture Report to inform the Australian Parliament on the implementation of cyber security measures across the Australian Government.

Requirement 0035 | GOV | All entities | 31 October 2024

The annual Cyber Security Survey is submitted to the Australian Signals Directorate.

Related Standards – Protective Security Reporting

- Reference: 2023–2030 Australian Cyber Security Strategy
- Reference: Commonwealth Cyber Security Posture Report

Part Two

Risk

Security Risk Management

Third Party Risk Management

Countering Foreign Interference and Espionage

Contingency Planning

Risk Lifecycle

5 Security Risk Management

Overall accountability for security risk management rests with the Accountable Authority. Security risks form part of the entity's enterprise risk management framework, which is the set of components and arrangements in place to appropriately manage the entity's risks.

Under the Public Governance, Performance and Accountability Rule 2014, entities are required to have an audit committee to review systems of risk oversight and management. Audit committees perform an important role in oversight of risk management, including security risks.

The Department of Finance's Commonwealth Risk Management Policy sets out the principles and mandatory requirements for managing risk in undertaking the activities of government. The Commonwealth Risk Management Policy supports section 16 of the PGPA Act which states that the Accountable Authority of a Commonwealth entity must establish and maintain appropriate system of risk oversight, management and internal control for the entity.

5.1 Security Risk Tolerance

Risk tolerance is an informed decision by the Accountable Authority to accept a certain level of risk. Risk tolerance describes the level of acceptable risk, after treatments are in place, to achieve an objective or manage a category of risk. It is highly dependent on the entity's unique context and the Accountable Authority's judgement.

Risk tolerance is the practical application of risk appetite, which is the amount of risk the entity is willing to accept or retain within the tolerance levels established by the Accountable Authority and the scope of the PSPF standards to achieve its objectives.

Risk tolerance includes:

- expectations for mitigating, accepting and pursuing specific types of risk
- boundaries and thresholds of acceptable risk taking, and
- actions to be taken or consequences for acting beyond approved tolerance levels.

Requirement 0036 | RISK | All entities | 31 October 2024

The Accountable Authority determines their entity's tolerance for security risks and documents in the security plan.

5.2 Security Risk Management Process

A security risk management process manages the entity's risks across all areas of security to determine the sources of threat and risk that could affect entity operations or the government. Security risk management is logical, systematic and transparent and forms part of the enterprise risk management process.

The key elements of the security risk management process are:

- Security risk assessment – the structured and comprehensive process to identify, analyse and evaluate security risks and determine practical steps to minimise those risks.
- Security risk treatment – the considered, coordinated and efficient actions and resources required to mitigate or lessen the likelihood of negative consequences of risk.

Security risk assessment is closely related to other entity risk assessment processes and should not be considered in isolation from other areas of risk.

Requirement 0037 | RISK | All entities | 31 October 2024

A risk steward (or manager) is identified for each security risk or category of security risk, including shared risks.

Requirement 0038 | RISK | All entities | 31 October 2024

The Accountable Authority considers the impact that their security risk management decisions could potentially have on other entities, and shares information on risks where appropriate.

5.2.1 Security Risk

A security risk is something that could result in the compromise, loss, unavailability or damage to information or assets, or cause harm to people.

Security risk is the effect of uncertainty on objectives and is often measured in terms of its likelihood and consequences, where:

- effect is a deviation from the expected and may be positive or negative, and
- an objective has different aspects such as financial, health, safety and environmental goals, and can apply at multiple levels such as strategic, organisation-wide, project, product and process levels.

The causes of security risks are generally people, systems, processes, procedures, crime, attacks or natural events.

5.2.2 Shared Security Risks

Shared security risks are those that extend across entities, premises, the community, industry, international partners or other jurisdictions. They require high levels of cooperation between stakeholders to effectively understand and manage those risks.

Where shared risks are identified, it is important to develop clear roles and responsibilities,

Related Standards – Security Risk Management

- Legislation: Public Governance, Performance and Accountability Act 2013
- Legislation: Public Governance, Performance and Accountability Rule 2014
- Government policy: Commonwealth Risk Management Policy

6 Third Party Risk Management

6.1 Procurement, Outsourcing and Contract Management

The Commonwealth Procurement Rules govern how entities procure goods and services and are designed to ensure the Government and taxpayers get value for money. Section 30 of the Public Governance, Performance and Accountability Rule 2014 states that non-corporate Commonwealth entities must comply with the Commonwealth Procurement Rules when performing duties related to procurement.

The procurement of goods or services does not transfer the operational risk from the Commonwealth. When an entity outsources the provision of goods or services, accountability for the goods or service and associated delivery outcomes (including managing security risks) remains with the entity.

Procurement and outsourcing arrangements can offer benefits (e.g. scalability, performance, resilience and cost efficiency), however these arrangements come with additional security risks. The Commonwealth Procurement Rules state that entities must establish processes to assess and treat risks when conducting a procurement to reduce the likelihood of additional financial and non-financial costs to government.

An unacceptable level of risk is when the identified security risks cannot be mitigated to a reasonable or acceptable level, or the security risks to the Australian Government or its people, information or resources, are too great. This includes where the security risks cannot be quantified or are too complex to be calculated. In these circumstances, entities must seek alternative procurement arrangements and maintain a record of such decisions.

The CSO is responsible for the security risks arising from the entity's procurement, outsourcing and contract management arrangements, other than for cyber security which is the responsibility of the CISO. The CSO is also responsible for determining where identified security risks pose an unacceptable level of risk.

Requirement 0039 | RISK | All entities | 31 October 2024

The entity is accountable for the management of security risks arising from procuring goods and services and ensures procurement and contract decisions do not expose the entity or the Australian Government to an unacceptable level of risk.

Requirement 0040 | RISK | All entities | 31 October 2024

Procurement, contracts and third-party outsourced arrangements contain proportionate security terms and conditions to ensure service providers, contractors and subcontractors comply with relevant PSPF Requirements and avoid exposing the entity or the Australian Government to an unacceptable level of risk.

Requirement 0041 | RISK | All entities | 31 October 2024

Entity ensures service providers, contractors and subcontractors comply with relevant PSPF Requirements as detailed by the entity.

Requirement 0042 | RISK | All entities | 31 October 2024

Contractual security terms and conditions require service providers to report any actual or suspected security incidents to the entity, and follow reasonable direction from the entity arising from incident investigations.

6.1.1 Outsourced Services provided by Government Entities

Government entities that perform the role of an outsourced managed service or cloud service provider must make any Infosec Registered Assessors Program (IRAP) assessment reports available to the government entities looking to consume their services. This allows consuming entities to meet their PSPF obligations while also managing any potential risk to their own security classified information and data when consuming such services.

Requirement 0043 | RISK | All entities | 31 October 2024

Government entities providing outsourced services provide IRAP assessment reports to the government entities consuming, or looking to consume, their services.

6.1.2 Ongoing Management of Security in Contracts

Security environments and risks constantly change. Sound contract management provides ongoing oversight and management, and helps adherence to essential security requirements of contracts.

Requirement 0044 | RISK | All entities | 31 October 2024

Contract security terms and conditions are monitored and reviewed to ensure the specified security controls, terms and conditions are implemented, operated and maintained by the contracted provider, including any subcontractors, over the life of a contract.

Requirement 0045 | RISK | All entities | 31 October 2024

Contractual terms and conditions include appropriate security arrangements for the completion or termination of the contract.

6.1.3 Foreign Ownership, Control or Influence in Procurement

As a result of the unprecedented levels of foreign interference targeting Australia, Australian Government entities that enter into commercial arrangements with organisations operating under Foreign Ownership, Control or Influence (FOCI) are at increased risk of foreign interference and espionage and must consider this risk as part of their obligations to mitigate security risks.

A contracted provider (organisation) may be operating under FOCI when a foreign interest has the power, direct or indirect, whether or not exercised, through the ownership of the organisation. This may occur under the scope of its National Security Authority/Designated Security Authority, by contractual arrangements or other means, to direct or decide matters affecting the management or operations. This may affect the organisation in a manner which may result in unauthorised access to classified information or adversely affect the performance of classified contracts or may otherwise be contrary to the interests of national security. In such cases, organisations may have to comply with directions that conflict with Australia's laws or interests, often granting a foreign government control over that business or access to its data holdings, and subsequently, entity data holdings. Not all instances of FOCI will create unacceptable security risks but security risks must be considered as part of all procurement and contract decisions involving providers operating under FOCI.

Robust due diligence must be undertaken when determining FOCI-related security risk. See ASIO's Due Diligence Integrity Tool for guidance on determining FOCI-related security risk.

The Department of Home Affairs has produced guidance on identifying FOCI risks in procurement. This includes a list of resources and templates to support contract managers to assess a vendor's exposure to

FOCI and correlating security risks. See Foreign Ownership, Control, or Influence (FOCI) Risk Assessment Guidance for details.

The Commonwealth Procurement Rules state that all potential suppliers to government must be treated equitably and not discriminated against due to their size, degree of foreign ownership or affiliation, location, or origin of their goods and services. However, there are exceptions to this rule, particularly where jurisdictional security risks are introduced or the provider or service is subject to a foreign government's lawful or covert data collection without their customers' knowledge. Other exceptions may also include the provider or service facilitating foreign government access to customer systems, or a foreign government gaining an ability to influence decisions or activities to their benefit at the expense of Australia's national interest. It is also important to note foreign countries' laws could change with little warning, potentially presenting FOCI risks during the contract period.

Contact procurementagencyadvice@finance.gov.au for advice on applying the Commonwealth Procurement Rules in such circumstances.

See Countering Foreign Interference and Espionage.

Requirement 0046 | RISK | All entities | 31 October 2024

Procurement and contract decisions consider the security risks before engaging providers operating under foreign ownership, control or influence, and in response to any developments during the contract period that may give rise to foreign ownership, control or influence risks.

6.2 Third Party Risk Management Lifecycle

Third party risk management is the process of identifying and addressing the security risks associated with third parties and understanding the lifecycle of third party relationships. A third party is any partner, consultant, vendor, service provider or supplier that provides a product or service to an entity or assists with its operations.

Identifying and managing jurisdictional, governance, privacy and security risks associated with the use of certain third party partners is crucial, particularly for application developers, ICT equipment manufacturers, service providers and other organisations involved in distribution channels. For example, outsourced cloud services may be located offshore and subject to lawful and covert data collection without their customers' knowledge. Risk can be reduced by selecting third parties that have committed to implementing and following secure-by-design and secure-by-default practices. See Secure-by-Design | Cyber.gov.au

Additionally, the use of offshore services introduces jurisdictional risks as foreign countries' laws could change with little warning. Finally, foreign owned suppliers operating in Australia may be subject to a foreign government's lawful access to data belonging to their customers.

See Foreign Ownership, Control or Influence in Procurement.

Requirement 0047 | RISK | All entities | 31 October 2024

Security risks arising from contractual arrangements for the provision of goods and services are managed, reassessed and adjusted over the life of a contract.

6.2.1 Vendor Risk Management

Vendor risk management is the process of identifying, analysing, monitoring and mitigating the risks that may arise if using individual vendors, service providers and partners. All vendors are third parties, but not all third parties are vendors.

It is a legitimate procurement activity for vendors to seek additional information from government panels, for example, clarification of requirements in an AusTender Approach to Market notice. However, some vendors may seek to use this process to elicit unique or sensitive insights into government processes, priorities and systems for commercial advantage over other vendors.

Vendor risk management forms part of the third party risk management lifecycle.

6.2.2 Supply Chain Risk Management

Supply chain risk management is the process of identifying, analysing, monitoring and mitigating supply chain-related risks. A supply chain is the flow of goods and services from internal or external suppliers through all stages of production and supply.

Supply chains can be large and complex, and may involve multiple layers of suppliers. They may expose the entity to unforeseen vulnerabilities and disruptions at any point in the supply chain.

Supply chain risk management forms part of the third party risk management lifecycle, and assessment of this is best conducted during the initial stages of procurement.

Entities must assess the source, reliability, and integrity of the suppliers and the supply chain of these strategic assets to ensure they comply with relevant laws and regulations, and the entity's security policies and standards. Diversifying the supply sources and reducing the dependency on single or dominant suppliers is advisable, as is enhancing the supply chain's resilience and redundancy in case of unexpected contingencies.

Supply chain risk management activities should be conducted during the earliest possible stage of procurement of applications, information technology (IT) equipment, operational technology (OT) equipment and services. Consider the security risks that may arise as systems, software and hardware are being designed, built, stored, delivered, installed, operated, maintained and decommissioned.

See Information Security Manual for guidance on cyber supply chain risk management.

Requirement 0048 | RISK | All entities | 31 October 2024

Secure and verifiable third-party vendors, providers, partners and associated services are used unless business operations require use, and the residual risks are managed and approved by the Chief Information Security Officer

Related Standards – Third Party Risk Management

- Standard: Commonwealth Procurement Rules
- Standard: ASD'S Information Security Manual – Procurement and Outsourcing
- Guidance: ASIO's Due Diligence Integrity Tool (available on GovTEAMs)
- Guidance: ASD's Choosing Secure and Verifiable Technologies
- Guidance: National Cyber Security Centre's Supply Chain Security Guidance
- Guidance: National Institute of Science and Technology's (NIST) IR 8276, Key Practices in Cyber Supply Chain Risk Management: Observations from Industry publication.
- Guidance: Department of Home Affairs Foreign Ownership, Control or Influence (FOCI) Risk Assessment Guidance

7 Countering Foreign Interference and Espionage

Left unchecked, foreign interference can have a corrosive effect on our national security. It can weaken our free and open system of government, our social cohesion and our economic prosperity. The best defence against foreign interference and espionage is to limit vulnerabilities that can be exploited by foreign actors, and to arm people who are possible targets with the information they need to recognise and report it.

Attempts at foreign interference are occurring at all levels of government, in all states and territories. Foreign powers may seek to undermine the integrity of our democratic institutions. They may also attempt to cultivate or recruit officials at any level of government, to gain a coercive or clandestine influence over government decision-makers and access to sensitive government information.

Appropriate due diligence is required to protect government people and resources from the risk of foreign interference, including:

- Understanding relationships - knowing the people the entity works with and possible associations those people might have with foreign powers, their position on sensitive policy matters and any history they might have in terms of sensitive legal and ethical issues.
- Being open and transparent in interactions and always acting with integrity – in accordance with the APS Values and Code of Conduct. Business decisions and relationships conducted in an open, lawful and transparent manner are less likely to present vulnerabilities for foreign actors to exploit.
- Understanding the potential warning signs of foreign interference and how to make informed decisions to mitigate risks.

7.1 Recognising Foreign Interference and Espionage

Foreign interference and espionage are the principal security concerns facing Australia.

Espionage is the theft of information or capabilities by someone acting on behalf of, or intending to provide information to, a foreign power or foreign political organisations that will prejudice Australia's national security, or advantage the national security of a foreign country. Espionage can target defence, political, industrial, foreign relations, commercial or other information or things that are usually otherwise unavailable to the foreign power.

Foreign interference are activities carried out by, or on behalf of, are directed or subsidised by, or are undertaken in active collaboration with, a foreign power. They either involve a threat to a person, or are clandestine or deceptive and detrimental to Australia's interests. Foreign interference involves covertly shaping decision-making to the advantage of a foreign power, and is hostile to our national interests. It is not the same as a foreign state taking open and transparent action to influence deliberations of importance to them.

Foreign interference is not the same as foreign influence. All governments, including the Australian Government, seek to influence issues of importance to them. Australia is not concerned with foreign influence activity that is open and transparent, and that respects our people, society and systems.

See ASIO's website for reporting on the domestic and international security environment.

Contact the Department of Foreign Affairs and Trade (security.training@dfat.gov.au) for advice on Foreign Intelligence Awareness Training for Australian Government personnel deployed or posted overseas.

See Foreign Ownership, Control or Influence in Procurement.

Requirement 0049 | RISK | All entities | 31 October 2024

Entities manage the security risks associated with engaging with foreign partners.

7.1.1 Foreign Delegations

Visits by foreign delegations should be more highly scrutinised than other visitors as malign foreign actors and intelligence services may use visiting foreign delegations to gain access to entity facilities, personnel, information, or assets that are of intelligence interest.

These individuals or groups may undertake espionage or foreign interference on behalf of a foreign state actor.

Visits by foreign delegations must be managed to ensure their exposure to information, technology, capabilities or personnel does not result in unacceptable security risks. Staff responsible for escorting and managing foreign delegations must have the knowledge, confidence and experience necessary to manage security risks.

See Security Zones and Visitor Access Control.

7.1.2 International Agreements

Australian Government security classified information and assets must not be shared with a foreign entity unless explicit legislative provisions, international agreements or arrangements for protection of classified information and assets are in place.

Vigilance is required when developing and entering into international agreements to avoid exposing Australian Government people, classified information or resources to foreign interference and espionage by a foreign entity or power.

See International Information Sharing.

7.1.3 Cultivation by a Foreign Actor

Foreign actors – whether Government officials, intelligence officers or their proxies – will seek to make contact and develop relationships with Australian individuals to enable them to exert influence and pursue their objectives. Foreign actors and those assisting them may not be readily identifiable, nor may their links to foreign powers.

Foreign actors may attempt to manufacture circumstances and situations to create a sense of personal connection with, and obligation from, an individual to cause them to make decisions, or act in certain ways that support the interests of a foreign power.

This is often done by engaging in activities to make targeted individuals feel a sense of reciprocity or indebtedness, such as providing:

- gifts
- donations
- paid travel expenses
- networking opportunities, and
- preferential access to senior officials or business people.

Gifts and benefits are often offered during official overseas trips or as part of foreign delegation visits to Australia. Accepting gifts or benefits may result in an actual or perceived conflict of interest, and at the extreme, can be construed as bribery.

Gifts may also present a security risk, particularly gifted chargers, removable media, wireless devices, internet connected devices, and radio frequency devices. There is the potential for malicious actors to plant malicious chips, software code or malware in order to collect data, compromise or gain unauthorised access to Australian Government information or systems. See www.cyber.gov.au for advice.

7.1.4 International Travel

International travel (both personal and official) carries heightened risks for government personnel due to the nature of their work and access to Australian Government information. Government personnel may be targeted by foreign actors during official and personal international travel to obtain information or as part of cultivation operations.

It is significantly easier for foreign actors to operate in their home country, but many foreign actors are also active in countries other than their own. Australian Government information of interest to foreign actors is not limited to security classified information. It can also extend to any non-publicly available information that may confer an advantage on another country. This can include diplomatic, economic, trade, financial, commercial, technical and scientific information. Even information that may seem innocuous in isolation may be aggregated with other information to fill intelligence gaps or identify individuals for possible future targeting.

Foreign actors use a variety of methods to gain influence and/or obtain information to use to their advantage. Many approaches or interactions with foreign actors are likely to be indistinguishable from normal networking opportunities, and may be designed to ingratiate the targeted individual or establish their complicity in benign activities. As such, it can be difficult for targeted individuals to know when they are engaging with foreign actors or their proxies.

Compromise of devices used to store or communicate official or classified Australian Government information pose the highest risk. Usage policies for these devices overseas should be calibrated to reduce this risk. Compromise of personal mobile devices can also provide foreign actors with access to sensitive information if they are used for business related communication, or access to personal information which may enable other targeting. For these reasons overseas travel policies and advice should include measures to reduce the risk that personal devices will be compromised.

To limit the risks of foreign interference and espionage during international travel, employees should always handle physical information appropriately, adopt good cyber hygiene practices, and only discuss classified matters in approved locations and via IT systems accredited to the classification level of the conversation.

See Minimum Protections and Handling Requirements, Security Classified Discussions, Working Remotely Outside of Australia (International), and Reportable Changes in Circumstances.

Contact DFAT (security.training@dfat.gov.au) for security advice related to international travel for Australian Government personnel deployed or posted overseas.

Contact ASIO (outreach@asio.gov.au) for advice on reporting suspicious contact, foreign interference or threats to Australia's security while travelling overseas.

For more information on cyber security while travelling, visit the Australian Cyber Security Centre website Travelling With Mobile Devices | Cyber.gov.au

7.1.5 Protecting Personal Information

Profiles on social media, recruitment and professional networking platforms can also be a vector for foreign actors to target individuals for potential cultivation and recruitment. Personal information online provides foreign actors with useful information to improve espionage and interference targeting.

Government employees who post details of clearance levels, position titles, projects and specialised systems on social media could make themselves a more attractive target for foreign actors. Entity personnel should consider what personal information they choose to share, and the privacy settings applied to this information. Public visibility of personal information, including to other entity personnel, provide opportunities for foreign actors to tailor a more effective approaches – often seemingly innocent. Likewise, membership of employment related networking groups on social media sites, provide information on professional contacts and group activities, either social or operational, which can also be used by foreign actors for malign purposes.

All government officials must exercise caution in relation to the personal information they share about themselves in the online domain, to help mitigate the risks of espionage and foreign interference.

Requirement 0050 | RISK | All entities | 31 October 2024

Personnel do not publicise their security clearance level on social media platforms, including employment-focused platforms such as LinkedIn.

See Social Media Applications.

7.2 Countering Foreign Interference and Espionage

Foreign interference can undermine the integrity of the Australian Government. Appropriate due diligence is required to protect the entity from the risk of foreign interference.

7.3 Insider Threat Programs

Insider threat is when an insider intentionally or unintentionally uses their access to conduct activities that could cause harm or negatively affect an entity or its operations.

An insider is a current or former personnel (including contractors) who has, or had, legitimate or indirect access to an entity's people, information, techniques, activities, technology, or resources. All APS employees are trusted to uphold the APS Values and comply with the APS Code of Conduct. They are therefore considered to be 'trusted insiders'. A trusted insider is commonly referred to as an insider.

A trusted insider may be acting on behalf of a foreign power, issue motivated group, organised crime groups or violent extremist groups etc. either intentionally or unintentionally to gain access to official, or security classified information.

Countering insider threat programs enable entities to identify and manage insider risk in a holistic and coordinated way. An effective insider threat program can protect critical assets, counter unintentional and malicious incidents, prevent loss of data and prevent reputational damage. To be effective, these programs should be both proactive and prevention focussed.

An effective insider threat program is multifaceted, covering:

- security governance and planning
- personnel security
- security culture and awareness training

- access controls
- physical and ICT security controls and audit, and
- review, reporting and response processes.

Requirement 0051 | RISK | All entities | 31 October 2024

An insider threat program is implemented by entities that manage Baseline to Positive Vetting security clearance subjects, to manage the risk of insider threat in the entity.

In addition, entities that manage TS-PA security clearance subjects are required to implement an insider threat program that meets the TOP SECRET-Privileged Access Standard (available from Quality Assurance Office).

Related Standards – Countering Foreign Interference and Espionage

- Standard: TOP SECRET-Privileged Access Standard (available from Quality Assurance Office)
- PEN: Countering Foreign Interference in Procurement
- Guidance: Countering the Insider Threat: A guide for Australian Government
- Guidance: Managing the Insider Threat – Security Manager's Guide (ASIO Outreach portal).

8 Contingency Planning

8.1 Exceptional Circumstances

Exceptional circumstances are situations beyond the entity's control that are not routine in nature, not enduring, and are unforeseen, unavoidable or unexpected. The exceptional circumstances provision allows the Accountable Authority, at their discretion, to adapt to arising circumstances that affect the entity's capability to implement or maintain a particular PSPF requirement or standard. Examples of exceptional circumstances include natural disasters, emergency situations. Entities are encouraged to consider alternative mitigation strategies during such periods to provide additional protection.

Section 19 of the PGPA Act requires that the Accountable Authority notifies the responsible minister of significant issues that affect, or may affect, the entity. This obligation includes advising the responsible minister, through the annual report on security, of any significant issues with implementing a PSPF requirement or standard or decisions to vary implementation.

Requirement 0052 | RISK | All entities | 31 October 2024

Where exceptional circumstances prevent or affect an entity's capability to implement a PSPF requirement or standard, the Accountable Authority may vary application, for a limited period of time, consistent with the entity's risk tolerance.

Requirement 0053 | RISK | All entities | 31 October 2024

Decisions to vary implementation of a PSPF requirement or standard due to exceptional circumstances are documented in the entity's security plan.

8.2 Alternative Mitigations

An alternative mitigation is a control or standard that differs from the PSPF requirement or standard but achieves the same intent. In the event that an entity is unable to implement a standard, a risk-based approach allows an alternative mitigation to be implemented where it achieves a level of protection that is the same as or exceeds that afforded by the PSPF requirement or standard. In such cases, the entity documents the decision in the entity's security plan, reports 'risk managed' for the corresponding standard and provides the required information as detailed in Protective Security Reporting.

Requirement 0054 | RISK | All entities | 31 October 2024

Decisions to implement an alternative mitigation measure that meets or exceeds a PSPF requirement or standard are reviewed and reported annually.

8.3 Business Continuity Planning

Business continuity management is a type of risk management designed to address the threat of disruptions to entity operations and support the prompt response to and recovery from these events.

The entity's business continuity plan documents the:

- set of planned procedures to continue or recover the entity's services to the Government and the public with minimal disruption over a given period, irrespective of the source of the disruption, and
- contingency post-event actions that can be implemented to prevent or limit losses and disruption.

The business continuity plan should also make provision for significant business disruptions to reduce the immediate impact on the entity and provide acceptable lower levels of service, or resumption plans to resume operations within acceptable timeframes

It is essential that the business continuity management plan complements the entity's security plan, other entity policies and procedures and is not prepared in isolation from these arrangements.

Requirement 0055 | RISK | All entities | 31 October 2024

A business continuity plan is developed, implemented and maintained to respond effectively and minimise the impacts of significant business disruptions to the entity's critical services and assets, and other services and assets when warranted by a threat and security risk assessment.

8.4 Emergency Management and Notifications

The Accountable Authority is responsible for the security of their entity's personnel. The preparedness of personnel and their ability to recognise and respond to a potential emergency is of paramount importance.

A key element of business continuity is planning for emergencies and the implications these events may have on the security of the entity's personnel, information and facilities. These arrangements must cover a broad range of emergencies, including:

- bombs and bomb threats
- potentially hazardous substances or hoaxes
- failure of essential services
- fire and explosions
- cyber-attacks and serious cyber security incidents (noting National Coordination requirements)
- major accidents
- natural disasters
- disruptive/dangerous visitors, including active shooter
- threatening telephone calls, emails and letters, and
- suspicious packages or deliveries.

Security awareness training, exercises and rehearsal of emergency counter-measures are vital to ensuring that the plans in place are effective and that entity personnel are ready and able to respond.

Requirement 0056 | RISK | All entities | 31 October 2024

Plans for managing a broad range of emergencies are integrated within the business continuity plan.

Requirement 0057 | RISK | All entities | 31 October 2024

Personnel who are likely to be impacted are notified if there is a heightened risk of an emergency.

8.5 Requesting Assistance/Sharing Information in Emergencies

Cyber security emergencies are complex and occur frequently. These events may also take place concurrently or consecutively. Entities experiencing security incidents have reporting obligations, including to share information with other entities that may be effected by the event (see Security Incidents) but may also require assistance to contain or remediate emergencies.

The National Emergency Management Agency develops, coordinates and supports effective management of national emergencies. The National Situation Room (NSR) is a 24/7 crisis management information and government coordination facility provided by the National Emergency Management Agency.

Related Standards – Contingency Planning

- Standard: ISO 22301 – International Business Continuity Standard details a framework to protect against, reduce the likelihood of, and ensure recover from disruptive events (available to purchase from International Organization for Standardization).
- Guidance: Business Continuity in a Box (Australian Cyber Security Centre)
- Guidance: ISO/TS 22318 – Guidelines for supply chain continuity management extends the principles of ISO 22301 to manage supply chain continuity (available to purchase from International Organization for Standardization).
- Guidance: The Business Continuity Institute's (BCI) Good Practice Guidelines

Part Three

Information

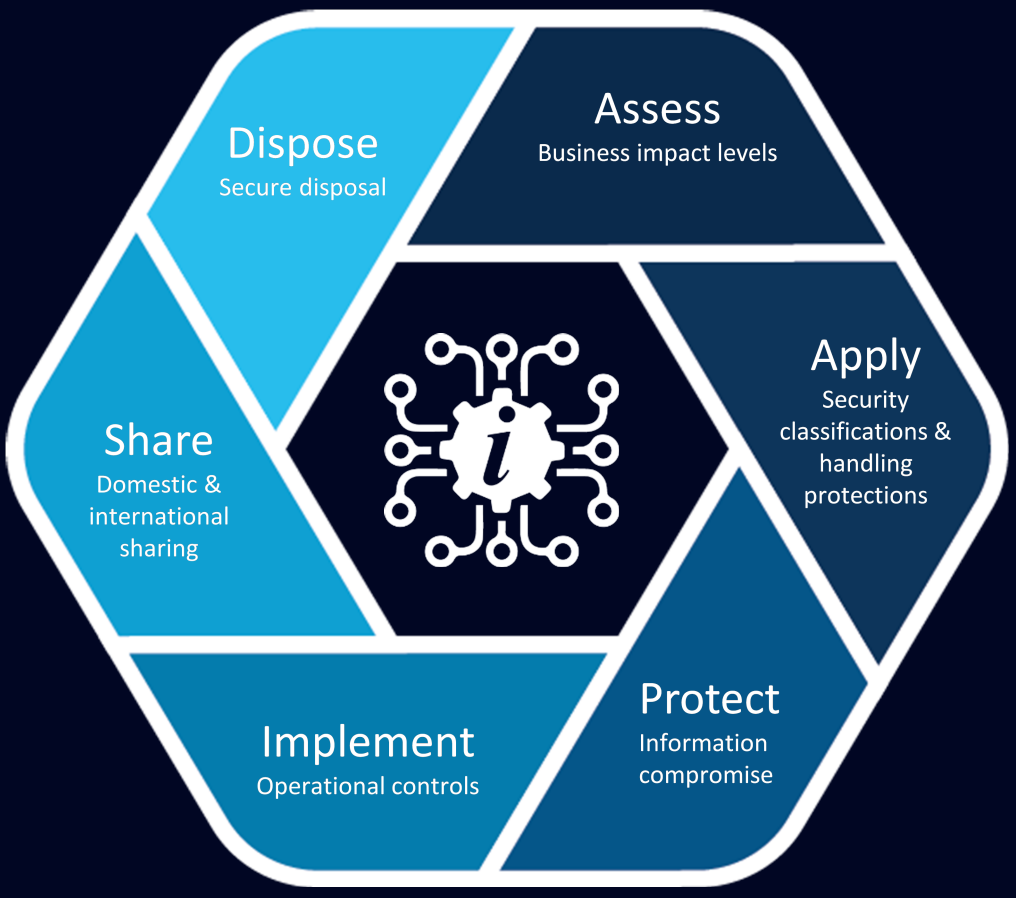
Classifications and Caveats

Information Holdings

Information Disposal

Information Sharing

Information Lifecycle



9 Classifications and Caveats

Information is a valuable resource and can be collected, used, stored and transmitted in many forms including electronically, physically and audibly.

Official information is all information created, sent or received as part of the work of the Australian Government. Official information is a record and provides evidence of what an entity has done and why. All official information requires an appropriate degree of protection as information (and assets holding information) are subject to both intentional and accidental threats.

Australian Government entities are required to maintain the confidentiality, integrity and availability of official information, including where the entity is the originator of the information.

9.1 Originator

The originator is the entity that initially generated the information, or first received the unmarked information (i.e. an Australian Government or third-party approved security classification has not been applied) from outside the Australian Government, and assessed the value, importance or sensitivity of the information by considering the potential damage that would arise if the information's confidentiality was compromised, and assigned the corresponding protective marking or security classification.

Requirement 0058 | INFO | All entities | 31 October 2024

The originator remains responsible for controlling the sanitisation, reclassification or declassification of official and security classified information, and approves any changes to the information's security classification.

9.2 Security Classifications

The Australian Government uses four security classifications: OFFICIAL: Sensitive, PROTECTED, SECRET and TOP SECRET. Security classified information includes OFFICIAL: Sensitive information unless otherwise stated.

All other information from business operations and services requires a routine level of protection and is treated as OFFICIAL. Information that does not form part of official duty is treated as UNOFFICIAL.

OFFICIAL and UNOFFICIAL are not security classifications and are not mandatory markings.

See_Email Protective Marking Standard and Recordkeeping Metadata Standard.

Requirement 0059 | INFO | All entities | 31 October 2024

The value, importance or sensitivity of official information (intended for use as an official record) is assessed by the originator by considering the potential damage to the government, the national interest, organisations or individuals that would arise if the information's confidentiality were compromised.

Requirement 0060 | INFO | All entities | 31 October 2024

The security classification is set at the lowest reasonable level.

Requirement 0061 | INFO | All entities | 31 October 2024

Security classified information is clearly marked with the applicable security classification, and when relevant, security caveat, by using text-based markings, unless impractical for operational reasons.

Table 3: Potential Damage of Compromise of Information's Confidentiality

	TOP SECRET	SECRET	PROTECTED	OFFICIAL: SENSITIVE	OFFICIAL	UNOFFICIAL
Business Impact level	5 – Catastrophic business impact	4 – Extreme business impact	3 – High business impact	2 – Low to medium business impact	1 – Low business impact	No business impact
Expected level of damage	Exceptionally grave damage to the national interest, organisations or individuals.	Serious damage to the national interest, organisations or individuals.	Damage to the national interest, organisations or individuals.	Limited damage to an individual, organisation or government generally if compromised.	No or insignificant damage. This is the majority of routine information.	No damage. This information does not form part of official duty.

9.3 Minimum Protections and Handling Requirements

The minimum protections and handling requirements establish the key operational controls for accessing, storing or communicating OFFICIAL and security classified information in a physical format, and on both government-issued and non-government issued mobile devices.

Entity facilities is defined as the physical premises or space that the entity occupies to perform its approved functions. Facilities can be a building, floor of a building or designated space. See Working Remotely in Australia for advice, including in co-location or hosting arrangements.

See Security Containers, Cabinets and Rooms for details of lockable containers.

See Information Security Manual for controls for non-mobile desktop equipment and servers.

Requirement 0062 | INFO | All entities | 31 October 2024

The minimum protections and handling requirements are applied to protect OFFICIAL and security classified information.

9.3.1 Protections and Handling Requirements for Physical information

Physical information means information that physically exists in hard copy, including printed copies of emails. Entities must apply the following minimum protections and handling requirements for all Australian Government physical information. Additional restrictions may apply for caveated information, refer to the Australian Government Security Caveat Standards for minimum handling requirements and protections for caveated information including codeword information.

Table 4: Physical Information – Inside Entity Facilities

	TOP SECRET	SECRET	PROTECTED	OFFICIAL: SENSITIVE	OFFICIAL
Text-based marking	Documents: Yes. Recommended application: Centre top and centre bottom of each page; capitals, bold text, large fonts, and distinctive colour (red preferred).	Documents: Yes. Recommended application: Centre top and centre bottom of each page; capitals, bold text, large fonts and distinctive colour (red preferred).	Documents: Yes Recommended application Centre top and centre bottom of each page; capitals, bold text, large fonts and distinctive colour (red preferred).	Documents: Yes. Recommended application: Centre top and centre bottom of each page; capitals, bold text, large fonts and distinctive colour (red preferred).	Documents: Optional. Recommended application: Centre top and centre bottom of each page; capitals, bold text, large fonts and distinctive colour (red preferred).
Alternative marking	Colour-based marking (red preferred) or apply entity's marking scheme.	Colour-based marking (salmon pink preferred) or apply entity's marking scheme.	Colour-based marking (blue preferred) or apply entity's marking scheme.	Colour-based marking (yellow preferred) or apply entity's marking scheme.	Colour-based marking (grey preferred) or apply entity's marking scheme.
Paragraph marking	Optional. (TOP SECRET) or abbreviated to (TS)	Optional. (SECRET) or abbreviated to (S).	Optional. (PROTECTED) or abbreviated to (P).	Optional. (OFFICIAL: Sensitive) or abbreviated to (O:S).	Optional. (OFFICIAL) or abbreviated to (O).
Access control	Need-to-know principle: Yes. Security clearance: NV2 (minimum). Temporary access: NV1 (minimum), supervised.	Need-to-know principle: Yes. Security clearance: NV1 (minimum). Temporary access: Supervised.	Need-to-know principle: Yes Security clearance: Baseline (minimum) Temporary access: Supervised	Need-to-know principle: Yes. Security clearance: Nil, employment screening only for entity personnel. Agreement or arrangement for non-government stakeholders[2].	Need-to-know principle: Recommended Security clearance: Nil, employment screening only for entity personnel. *Access controls N/A if information approved for public release.*
Use – Zone 1	No.	No.	Yes.	Yes.	Yes.
Use – Zone 2	No.	No.	Yes.	Yes.	Yes.
Use – Zone 3	Yes.	Yes.	Yes.	Yes.	Yes.
Use – Zone 4	Yes.	Yes.	Yes.	Yes.	Yes.
Use – Zone 5	Yes.	Yes.	Yes.	Yes.	Yes.
Leave unattended	No, store securely when unattended.	No, store securely when unattended.	Yes for brief absences in Zone 3 or higher Zone, otherwise store securely when unattended.	Yes, apply entity procedures.	Yes.
Store – Zone 1	No.	No.	No.	Yes, lockable container.	Yes, subject to entity procedures.
Store – Zone 2	No.	No.	Yes, Class C container.	Yes, lockable container.	Yes, subject to entity procedures.
Store – Zone 3	No. Exceptional circumstances – Class A container, max 5 days.	Yes, Class B container.	Yes, lockable container.	Yes, lockable container.	Yes, apply entity procedures.
Store – Zone 4	Yes, Class B container, max 5 days.	Yes, Class C container.	Yes, lockable container.	Yes, subject to entity procedures. Lockable container recommended.	Yes, apply entity procedures.
Store – Zone 5	Class B container.	Yes, Class C container.	Yes, lockable container.	Yes, subject to entity procedures. Lockable container recommended.	Yes, apply entity procedures.
Carry – Zone 1	Not recommended. If required, opaque envelope/folder that indicates Classification and place in security briefcase, pouch or satchel.	Yes, in opaque envelope/folder that indicates Classification place in security briefcase, pouch or satchel.	Yes, in opaque envelope/folder.	Yes, opaque envelope/folder recommended.	Yes, apply entity procedures.
Carry – Zone 2	Not recommended. If required, opaque envelope/folder that indicates Classification and place in security briefcase, pouch or satchel.	Yes, in opaque envelope/folder that indicates Classification.	Yes, in opaque envelope/folder.	Yes, opaque envelope/folder recommended.	Yes, apply entity procedures.
Carry – Zone 3	Yes, in opaque envelope/folder that indicates Classification.	Yes, in opaque envelope/folder that indicates Classification.	Yes, in opaque envelope/folder.	Yes, opaque envelope/folder recommended.	Yes, apply entity procedures.
Carry – Zone 4	Yes, in opaque envelope/folder that indicates Classification.	Yes, opaque envelope/folder recommended.	Yes, in opaque envelope/folder recommended.	Yes, opaque envelope/folder recommended.	Yes, apply entity procedures.
Carry – Zone 5	Yes, in opaque envelope/folder that indicates Classification.	Yes, opaque envelope/folder recommended.	Yes, in opaque envelope/folder recommended.	Yes, opaque envelope/folder recommended.	Yes, apply entity procedures.
Transfer - inside	Yes, transfer by hand or entity safe hand and apply 'carry' requirements. Can be uncovered if in close proximity and office environment presents low risk of unauthorised viewing. Written manager approval required for transfer in Zones 1-2. All transfers require a receipt.	Yes, transfer by hand or entity safe hand and apply 'carry' requirements. Can be uncovered if in close proximity and office environment presents low risk of unauthorised viewing. All transfers require a receipt.	Yes, transfer by hand or entity safe hand and apply 'carry' requirements. Can be uncovered if in close proximity and the office environment presents low risk of unauthorised viewing. All transfers require a receipt.	Yes, place in opaque envelope/folder and apply entity procedures to transfer by hand or internal mail.	Yes, apply entity procedures for transfer by hand or internal mail.

[2] Unless the entity is returning or responding to information provided by a non-government stakeholder, or their authorised representative, which the government entity would subsequently classify as OFFICIAL: Sensitive on receipt (as the government originator), in accordance with PSPF Requirement 0077.

	TOP SECRET	SECRET	PROTECTED	OFFICIAL: SENSITIVE	OFFICIAL
Dispose[3]	Class A shredder or ASIO-T4 approved destruction method, supervise and document.	Class A shredder or ASIO-T4 approved destruction method.	Class B shredder or ASIO-T4 approved destruction method.	Apply entity procedures for disposal.	Apply entity procedures for disposal.

Table 5: Physical Information – Working Remotely in Australia (including home-based work)

	TOP SECRET	SECRET	PROTECTED	OFFICIAL: SENSITIVE	OFFICIAL
Use – outside	No, do not use outside entity facilities.	No, do not use outside entity facilities.	Not recommended. If required, apply entity procedures and exercise judgement to assess environmental risk.	Yes, apply entity procedures and exercise judgement to assess environmental risk.	Yes.
Use – at home	No, do no use at home.	No, do not use for regular home-based work. Occasional: No, but if unavoidable, obtain manager approval, apply entity procedures on need for security risk assessment and exercise judgement to assess environmental risk.	Regular: Yes, apply entity procedures, which must include a security risk assessment of the proposed work environment. Occasional: Yes, apply entity procedures on need for security risk assessment and exercise judgement to assess environmental risk.	Yes, apply entity procedures on need for a security risk assessment and exercise judgement to assess environmental risk.	Yes.
Leave unattended	No.	No. If occasional home-based work approved, for brief absences, store in Class B (or higher) container that has been approved by the Accountable Authority or their delegate.	No, store security when unattended. For brief absences from home, apply entity procedures and exercise judgement to assess environmental risk.	Yes, can be left unattended for short periods subject to entity procedures and judgement to assess environmental risk.	Yes.
Store – outside	No, do not store outside entity facilities.	No. For brief absence from home, see 'leave unattended'.	Not recommended. If required, store in Class C (or higher) container. For brief absence from home, see 'leave unattended'.	Yes, opaque envelope/folder in lockable container recommended.	Yes, lockable container recommended.
Store – at home	No, do not store at home.	No. If unavoidable, refer to 'carry' outside entity requirement, retain in personal custody (strongly preferred), and return to entity facilities as soon as practicable.	Regular: Class C (or higher) container. Occasional: apply 'carry' outside entity requirements to store in security briefcase, pouch or satchel, with tamper-evident packaging recommended.	Yes, opaque envelope/folder recommended, and subject to environmental risk, store in lockable container.	Yes.
Carry – outside	Not recommended. If required, obtain written manager approval and place in tamper-evident packaging within security briefcase, pouch or satchel and retain in personal custody. . Do not 'Use' until in appropriate Zone at destination.	Yes, place in security briefcase, pouch or satchel and always retain in personal custody. Tamper-evident packaging recommended.	Yes, place in security briefcase, pouch or satchel. Tamper-evident packaging recommended if aggregate information increases risk.	Yes, recommend carry is opaque envelope/folder.	Yes, apply entity procedures.
Transfer – outside (includes transfer to an officer in a different government facility or entity)	Yes, written manager approval, apply 'carry' outside entity requirements and transfer by entity safe hand; or place in tamper-evident packaging and transfer by safe hand courier rated BIL 5 or DFAT courier. All transfers require a receipt.	Yes, apply 'carry' outside entity requirements and transfer by hand, entity safe hand, safe hand courier rated BIL 4 or DFAT courier. If transfer by courier, use tamper evident packaging. All transfers require a receipt.	Yes, apply 'carry' outside entity requirements and transfer by hand, entity safe hand, safe hand courier rated BIL 4 or DFAT courier. If transfer by courier, use tamper evident packaging. All transfers require a receipt.	Yes, place in opaque envelope/folder and apply entity procedures to minimise risk of unauthorised access (e.g. sealed envelope). Transfer by hand, mail or courier and exercise judgement to assess whether registered or other secure mail appropriate.	Yes, apply entity procedures for transfer by hand, external mail or courier.

Table 6: Physical Information – Working Remotely Internationally[4]

See Working Remotely Outside of Australia (International)

	TOP SECRET	SECRET	PROTECTED	OFFICIAL: SENSITIVE	OFFICIAL
Relocate	No.	No.	Not recommended. If required, entity must do a risk assessment of the proposed work environment and apply 'travel' outside Australia requirements.	Yes, apply entity procedures and exercise judgement to assess environmental risk.	Yes.
Use	No.	No.	Not recommended. If required, ensure overseas location meets all PSPF requirements for PROTECTED information.	Yes, apply entity procedures and exercise judgement to assess environmental risk.	Yes.
Leave unattended	No.	No.	No, store securely when unattended. For brief absences from approved remote location, apply entity procedures and exercise judgement to assess environmental risk.	Yes, apply entity procedures and exercise judgement to assess environmental risk.	Yes.

[3] See Section 11 – Information Disposal for details on disposal and destruction methods and equipment.
[4] Not in an Australian Government Facility or Post. See International Entity Facilities (including Missions and Posts) for information on Australian Government overseas posts and facilities.

	TOP SECRET	SECRET	PROTECTED	OFFICIAL: SENSITIVE	OFFICIAL
Store	No.	No.	Not recommended. If required, entity must risk assess international location and if approved, store in Class C (or higher) container.	Yes, if approved by entity risk assessment of location and stored in lockable container.	Yes.

Table 7: Physical Information – Travelling in Australia (domestic travel)

	TOP SECRET	SECRET	PROTECTED	OFFICIAL: SENSITIVE	OFFICIAL
Travel	Not recommended. If required, written manager approval, apply 'carry' outside entity requirements and any additional entity travel procedures. Do not 'use' until in appropriate Zone at destination.	Not recommended. If required, apply 'carry' outside entity requirements and any additional entity travel procedures. Do not 'use' until in appropriate Zone at destination.	Yes, apply 'carry' outside entity requirements and any additional entity travel procedures.	Yes, apply 'carry' outside entity requirements, any additional entity travel procedures and exercise judgement to assess environmental risk.	Yes, apply entity procedures and exercise judgement to assess environmental risk.
Air travel luggage	Not recommended. If unavoidable, retain in personal custody as carry-on luggage. If airline requires carry-on baggage to be checked at the gate, **do not travel.**	Not recommended. If unavoidable, retain as carry-on luggage. If airline requires baggage to be checked at the gate, place in tamper-evident packaging within a security briefcase, pouch or satchel, try to observe entering and exiting the cargo hold and reclaim as soon as possible. If tamper-evident packaging not available, **do not travel.**	Yes, retain as carry-on luggage. If airline requires carry-on luggage to be checked at the gate, try to observe it entering/exiting the cargo hold and reclaim it as soon as possible.	Yes, apply entity procedures.	Yes.
Leave unattended	No, do not leave unattended, retain in custody.	No, do not leave unattended, retain in custody.	No. If required for brief absences from hotel room, apply entity procedures and exercise judgement to assess environmental risk.	Yes, apply entity procedures and exercise judgement to assess environmental risk.	Yes, subject to entity procedures.
Store while travel	No, do not store, retain in custody.	No, do not store while travelling (e.g. in hotel room), retain in custody. If required, can be stored in Australian entity facility meeting 'store' inside entity requirements.	No, do not store will travelling. If required, can be stored in Australian entity facility meeting 'store' inside entity requirements. For brief absence from hotel room, see 'leave unattended'.	Yes, apply 'store' outside entity requirements.	Yes, lockable container recommended.

Table 8: Physical Information – Travelling Outside of Australia (international travel)

	TOP SECRET	SECRET	PROTECTED	OFFICIAL: SENSITIVE	OFFICIAL
Travel	No, do not travel with TS information. Seek DFAT advice on options to access information at international destination or see 'transfer' outside entity requirements.	Not recommended. Seek DFAT advice on options to access information at international destination. If required, apply 'carry' outside entity requirements and any additional entity travel procedures, and consider country-specific travel advice. Do not 'use' until in appropriate Zone at destination.	Not recommended. Seek DFAT advice on options to access information at international destination. If required, apply 'carry' outside entity requirements and any additional entity travel procedures, and consider country-specific travel advice. Do not 'use' until in appropriate Zone at destination.	Yes, apply 'carry' outside entity requirements, any additional entity travel procedures, and consider country-specific travel advice.	Yes, apply entity procedures.
Air travel luggage	No, do not travel with TS information.	Not recommended. If required, retain as carry-on luggage in a diplomatic bag and retain in the custody of a laissez-passer[5], Australian Diplomatic or Australian Official passport holder. If airline requires carry-on baggage to be checked at the gate, **do not travel**.	Not recommended. If required, retain as carry-on luggage. If airline requires carry-on baggage to be checked at the gate, **do not travel**.	Yes, apply 'carry' outside entity requirements, any additional entity procedures and exercise judgement to assess environmental risk.	Yes.
Leave unattended	No, do not travel with TS information.	No, do not leave unattended.	No, do not leave unattended.	Not recommended. If required, apply entity procedures and exercise judgement to assess environmental risk.	Yes, subject to entity procedures.
Store while travel	No, do not travel with TS information.	No, do not store while travelling (e.g. in hotel room). If required, can be stored in Australian entity facility meeting 'store' inside entity requirements.	No, do not store while travelling (e.g. in hotel room). If required, can be stored in Australian entity facility meeting 'store' inside entity requirements.	Yes, apply 'store' outside entity requirements and consider country-specific travel advice.	Yes, lockable container recommended.

[5] Laissez-Passer is a diplomatic travel document issued by a national government or international treaty organisation to allow a government employee to act as a temporary diplomatic courier. The Laissez-Passer and diplomatic pouch are issued to an individual and they are not transferable. The most common laissez-passer is the United Nations laissez-passer (UNLP) issued by the United Nations.

9.3.2 Protections and Handling Requirements for Government-issued Mobile Devices

A government-issued mobile device is a mobile or portable computing communications device that is owned and issued by an Australian Government entity to access the entity's systems and data and is approved by the relevant authority to process, store or communicate entity information of a specified protective marking or security classification. This includes mobile phones, handheld computers, tablets, laptops and personal digital assistants configured, encrypted and managed to Australian Signals Directorate's standards and guidance. If these requirements are met, then a government-issued mobile device is considered in a 'secured state'. Entities must apply the following minimum protections and handling requirements for all Australian Government-issued mobile devices.

The Australian Signals Directorate is the relevant authority for TOP SECRET and SECRET government-issued mobile devices and capabilities and may set additional restrictions or conditions for use. The may also approve alternative mitigation arrangements, including outside entity facilities, to support operational or ministerial briefing requirements. The entity is the relevant authority for other government-issued mobile devices.

Table 9: Government-Issued Mobile Devices – Inside Entity Facilities

	TOP SECRET	SECRET	PROTECTED	OFFICIAL: SENSITIVE	OFFICIAL
Access control	Need-to-know principle: Yes. Security clearance: NV2 (minimum).	Need-to-know principle: Yes Security clearance: NV1 (minimum).	Need-to-know principle: Yes. Security clearance: Baseline (minimum).	Need-to-know principle: Yes. Security clearance: Nil, employment screening only[6].	Need-to-know principle: Recommended Security clearance: Nil, employment screening only
Use – Zone 1	No.	No.	Yes.	Yes.	Yes.
Use – Zone 2	No.	No (unless exceptional circumstances).	Yes.	Yes.	Yes.
Use – Zone 3	Yes, subject to ASD approval[7] and conditions for use and entity CSO/CISO approval.	Yes, subject to ASD approval[7] and conditions for use. If TS information/device present[8] also subject to risk assessment and entity CSO/CISO approval.	Yes, but if TS or SECRET information/device present[8], subject to risk assessment and entity CSO/CISO approval.	Yes, but if TS or SECRET information/device present, subject to risk assessment and entity CSO/CISO approval.	Yes, but if TS or SECRET information/device present, subject to risk assessment and entity CSO/CISO approval.
Use – Zone 4	Yes, subject to ASD approval and conditions for use and entity CSO/CISO approval.	Yes, subject to entity CSO/CISO approval.	Yes, but if TS or SECRET information/device present, subject to risk assessment and entity CSO/CISO approval.	Yes, but if TS or SECRET information/device present, subject to risk assessment and entity CSO/CISO approval.	Yes, but if TS or SECRET information/device present, subject to risk assessment and entity CSO/CISO approval.
Use – Zone 5	Yes, subject to ASD approval and conditions for use and entity CSO/CISO approval.	No, unless ASD approve during Zone 5 certification and subject to ASD conditions for use.	No, unless ASD approve during Zone 5 certification and subject to ASD conditions for use.	No, unless ASD approve during Zone 5 certification and subject to ASD conditions for use.	No, unless ASD approve during Zone 5 certification and subject to ASD conditions for use.
Leave unattended	No, store securely when not in use.	No, store securely when not in use.	Yes, if locked or turned off.	Yes, if locked or turned off.	Yes, if locked or turned off.
Store – Zone 1	No.	No.	Secured: Yes, in lockable container. Unsecured: Yes, in Class C container.	Yes, if locked or turned off, lockable container recommended.	Yes, lockable container recommended.
Store – Zone 2	No.	No. Exceptional circumstances, store turned off in Class B container.	Yes, lockable container recommended.	Yes, lockable container recommended.	Yes, locked or turned off recommended.
Store – Zone 3	No. Exceptional circumstances – store turned off in Class A container, max 5 days.	Yes, store turned off in Class C container.	Yes, lockable container recommended.	Yes, lockable container recommended.	Yes, locked or turned off recommended.
Store – Zone 4	No. Exceptional circumstances – store turned off in Class B container, max 5 days.	Yes, store turned off in Class C container. Store away from irregular TOP SECRET discussions.	Yes, locked or turned off when not in use.	Yes, locked or turned off recommended.	Yes, locked or turned off recommended.
Store – Zone 5	Yes, stored turned off in Class B container.	Yes, store turned off in Class C container.	Yes if approved by ASD during Zone 5 certification. Store turned off and away from TOP SECRET or SECRET discussions.	Yes if approved by ASD during Zone 5 certification. Store turned off and away from TOP SECRET or SECRET discussions.	Yes if approved by ASD during Zone 5 certification. Store turned off and away from TOP SECRET or SECRET discussions.
Carry – inside entity	Yes, if locked or turned off and apply entity procedures and relevant Zone procedures.	Yes, if locked or turned off and apply entity procedures and relevant Zone procedures.	Yes, apply entity procedures and relevant Zone procedures, and carry locked or turned off recommended.	Yes, apply entity procedures and relevant Zone procedures, and carry locked or turned off recommended.	Yes, apply entity procedures and relevant Zone procedures, and carry locked or turned off recommended.
Transmit	TOP SECRET secure network, otherwise use ASD's High Assurance Cryptographic Equipment to encrypt TOP SECRET information.	SECRET (or higher) secure network, otherwise use ASD's High Assurance Cryptographic Equipment to encrypt SECRET information.	PROTECTED (or higher) network, otherwise encryption required.	OFFICIAL: Sensitive (or higher) network. Encrypt if transferred over public network infrastructure or through unsecured spaces (including Zone 1), unless residual risk of not doing so has been recognised and accepted by the CSO/CISO.	Encryption recommended, particularly for information communicated over public network infrastructure.
Dispose	Refer to Information Security Manual – ICT equipment sanitisation and destruction				

[6] Unless the entity is returning or responding to information provided by a non-government stakeholder, or their authorised representative, which the government entity would subsequently classify as OFFICIAL: Sensitive on receipt (as the government originator), in accordance with PSPF Requirement 0077.
[7] ASD is the relevant authority for TOP SECRET and SECRET government-issued mobile devices and capabilities and may set additional restrictions or conditions for use. ASD may also approve alternative mitigation arrangements, including outside entity facilities, to support operational or ministerial briefing requirements. The entity is the relevant authority for other government-issued mobile devices
[8] If classified devices owned/hosted by another entity are present then consultation required with the CSO or CISO of that entity to ensure they agree with the proposed arrangement.

Table 10: Government-Issued Mobile Devices – Working Remotely in Australia (including home-based work)

	TOP SECRET	SECRET	PROTECTED	OFFICIAL: SENSITIVE	OFFICIAL
Use – outside	No, do not use outside entity facilities.	No, do not use outside entity facilities.	Yes, apply entity procedures and exercise judgement to assess environmental risk.	Yes, apply entity procedures and exercise judgement to assess environmental risk.	Yes.
Use – at home	No, do not use at home.	Regular: No. Occasional: Not recommended, if required obtain manager approval, apply entity procedures on need for a security risk assessment and exercise judgement to assess environmental risk.	Regular: Yes, apply entity procedures, which must include a security risk assessment of the proposed work environment. Occasional: Yes, apply entity procedures on need for security risk assessment and exercise judgement to assess environmental risk.	Yes, apply entity procedures on need for security risk assessment and exercise judgement to assess environmental risk.	Yes.
Leave unattended	No, store securely when not in use.	No, store securely when unattended. For brief absences from home, exercise judgement to store in a Class C (or higher) container that has been approved as a proper place of custody by the Accountable Authority or their delegate.	Yes, if locked or turned off subject to entity procedures and exercise judgement to assess environmental risk.	Yes, locked or turned off.	Yes, locked or turned off recommended.
Store – outside	No, do not store outside entity facilities.	No, do not store outside entity facilities.	Yes, lockable container recommended.	Yes, lockable container recommended.	Yes, lockable container recommended.
Store – at home	No do not store at home.	Regular: No. Occasional: Not recommended. If required apply 'carry outside entity requirements and retain in personal custody. For brief absence from home, see 'leave unattended'.	Yes, apply entity procedures and exercise judgement to assess environmental risk.	Yes, apply entity procedures and exercise judgement to assess environmental risk.	Yes, apply entity procedures.
Carry – outside	Not recommended. If required, seek manager approval, and carry turned off and in tamper-evident packaging in security briefcase, pouch or satchel recommended.	Yes, if locked or turned off and apply entity procedures.	Yes, apply entity procedures.	Yes, apply entity procedures.	Yes, apply entity procedures.
Transmit	TOP SECRET secure network, otherwise use ASD's High Assurance Cryptographic Equipment to encrypt TOP SECRET information.	SECRET secure network, otherwise use ASD's High Assurance Cryptographic Equipment to encrypt SECRET information.	PROTECTED (or higher) network, otherwise encryption required.	OFFICIAL: Sensitive (or higher) network. Encrypt if transferred over public network infrastructure or through unsecured spaces (including Zone 1), unless residual risk of not doing so has been recognised and accepted by the CSO/CISO.	Encryption recommended for information communicated over public network infrastructure.

Table 11: Government-Issued Mobile Devices – Working Remotely Internationally[4]

	TOP SECRET	SECRET	PROTECTED	OFFICIAL: SENSITIVE	OFFICIAL
Relocate	No.	No.	Not recommended. If required, entity must do a risk assessment of the proposed work environment and apply 'travel' outside Australia requirements.	Yes, entity must do a risk assessment of the proposed work environment, apply entity procedures and exercise judgement to assess environmental risk.	Yes.
Use	No.	No.	Not recommended. If required, ensure international location meets all PSPF requirements for PROTECTED information.	Yes, apply entity procedures and exercise judgement to assess environmental risk. Use screen protectors where required, lock the screen when not in use and shut down device at end of each day.	Yes.
Leave unattended	No.	No.	No, store securely and locked or turned off when unattended. For brief absences from approved remote location, locked or turned off, apply entity procedures and exercise judgement to assess environmental risk.	Yes, if approved by entity risk assessment of location. Otherwise if required for brief absences, locked or turned off, apply entity procedures and exercise judgement to assess environmental risk.	Yes.
Store	No.	No.	Not recommended. If required, entity must risk assess international location and if approved, preferably store in Class C (or higher) container.	Yes, if approved by entity risk assessment of location and stored in lockable container.	Yes.

Table 12: Government-Issued Mobile Devices – Travel in Australia (domestic travel)

	TOP SECRET	SECRET	PROTECTED	OFFICIAL: SENSITIVE	OFFICIAL
Travel	Not recommended. If unavoidable, written manager approval, apply 'carry' outside entity requirements and any additional entity procedures. Do not 'use' until in appropriate Zone at destination.	Not recommended. If required, apply 'carry' outside entity requirements and any additional entity procedures. Do not 'use' until in appropriate Zone at destination.	Yes, apply 'carry' outside entity requirements and any additional entity procedures. If 'use' required while travelling, a privacy screen is recommended.	Yes, apply 'carry' outside entity requirements and any additional entity procedures, and exercise judgment to assess environmental risk.	Yes.

	TOP SECRET	SECRET	PROTECTED	OFFICIAL: SENSITIVE	OFFICIAL
Air travel luggage	Not recommended. If unavoidable, retain in personal custody in carry-on luggage and apply 'carry outside' requirements. If airline requires carry-on luggage to be checked-in, **do not travel.**	Not recommended. If unavoidable, retain as carry-on luggage. If airline requires baggage to be checked at the gate (e.g. premium luggage), place in tamper-evident packaging within a security briefcase, pouch or satchel and try to observe entering and exiting the cargo hold and reclaim as soon as possible. If tamper-evident packaging not available, **do not travel.**	Yes, retain as carry-on luggage. If airline requires carry-on luggage to be checked at the gate (e.g. premium luggage), try to observe entering/existing the cargo hold and reclaim as soon as possible.	Yes, retain as carry-on luggage recommended.	Yes.
Leave unattended	No, do not leave unattended, retain in custody.	No, do not leave unattended, retain in custody.	Not recommended. For brief absences from hotel room, apply entity procedures and exercise judgement to assess environmental risk.	Not recommended. For brief absences from hotel room, apply entity procedures and exercise judgement to assess environmental risk.	Yes, apply entity procedures and exercise judgement to assess environmental risk.
Store while travel	No, do not store while travelling, including in hotel. Storage in Australian entity facility accepted.	No, do not store while travelling (e.g. in hotel room). If required, can be stored in Australian entity facility meeting 'store' inside entity requirements.	Not recommended. For brief absence from hotel room, see 'leave unattended'.	Yes, apply 'store' outside entity requirements.	Yes, apply 'store' outside entity requirements.

Table 13: Government-Issued Mobile Devices – Travel Outside of Australia (international travel)

	TOP SECRET	SECRET	PROTECTED	OFFICIAL: SENSITIVE	OFFICIAL
Travel	No, do not travel with mobile device. Seek DFAT advice on options to access mobile device at international destination.	Not recommended. Seek DFAT advice on options to access mobile device at international destination.	Not recommended. Seek DFAT advice on options to access mobile device at international destination. If required, apply 'carry' outside entity requirements and any additional entity travel procedures, and consider country-specific travel advice.	Yes, apply 'carry' outside entity requirements, any additional entity travel procedures, and consider country-specific travel advice.	Yes, apply entity procedures and exercise judgement to assess environmental risk.
Air travel luggage	No, do not travel with mobile device.	Not recommended. If required, retain as carry-on luggage. If airline requires carry-on baggage to be checked at the gate, **do not travel**.	Not recommended. If required, retain as carry-on luggage. If airline requires carry-on baggage to be checked at the gate, **do not travel**.	Yes, apply 'carry' outside entity requirements, any additional entity procedures and exercise judgement to assess environmental risk.	Yes, apply 'carry' outside entity requirements.
Leave unattended	No, do not travel with mobile device.	No, do not leave unattended.	No, do not leave unattended.	Not recommended. If required, apply entity procedures, exercise judgement to assess environmental risk, and consider country-specific travel advice.	Yes, apply entity procedures.
Store while travel	No, do not travel with mobile device.	No, do not store while travelling (e.g. in hotel room). If required, can be stored in Australian entity facility meeting 'store' inside entity requirements.	No, do not store while travelling (e.g. in hotel room). If required, can be stored in Australian entity facility meeting 'store' inside entity requirements.	Yes, apply 'store' outside entity requirements and consider country-specific travel advice.	Yes, apply 'store' outside entity requirements.

Table 14: Government-Issued Mobile Devices – Provided at International Destination

	TOP SECRET	SECRET	PROTECTED	OFFICIAL: SENSITIVE	OFFICIAL
Use	Yes, in an appropriate Zone and apply 'use' in entity requirements.	Yes, in an appropriate Zone and apply 'use' in entity requirements.	Apply 'use' in entity requirements.	Apply 'use' in entity requirements.	Apply 'use' in entity requirements.
Store	Yes, in an appropriate Zone and apply 'store' in entity requirements.	Yes, in an appropriate Zone and apply 'store' in entity requirements.	Apply 'store' in entity requirements.	Apply 'store' in entity requirements.	Apply 'store' in entity requirements.
Carry	No, if unavoidable, apply 'carry' outside entity requirements and any additional entity procedures.	No, if unavoidable, apply 'carry' outside entity requirements and any additional entity procedures.	Apply 'carry' outside entity requirements and any additional entity travel procedures.	Apply 'carry' outside entity requirements and any additional entity travel procedures.	Apply 'carry' outside entity requirements.
Leave unattended	No, do not leave unattended.	No, do not leave unattended.	Retain in personal custody or store in Australian entity facility meeting 'store' inside entity requirements.	Yes, apply entity procedures, exercise judgement to assess environmental risk, and consider country-specific travel advice.	Yes, apply entity procedures.

9.3.3 Protections and Handing Requirements for Non-Government Mobile Devices

There are two types of non-government mobile devices and entities must apply the following minimum protections and handling requirements for both types of non-government mobile devices.

- **Authorised non-government device** – mobile or portable computing communications devices (including mobile phones, handheld computers, tablets, laptops and digital assistants) owned or issued by a non-government source (for example commercial organisation, non-government organisation, industry issued or privately-owned) that is managed, configured and encrypted in accordance with ASD standards and guidance, and the residual risk is accepted by the Commonwealth entity system risk owner to access, process, store or communicate OFFICIAL, OFFICIAL: Sensitive and PROTECTED Australian Government information. Non-government devices must not access, process, store or communicate SECRET or TOP SECRET information. If these requirements are fully met, then a non-government mobile device is considered in a 'secured state'. If these requirements are not fully met, refer to 'unsecured state' requirements.
- **All other mobile devices** – devices that are not owned, issued or authorised by the entity. These devices must not be authorised to access, process, store or communicate government OFFICIAL: Sensitive or above information, and must not enter Zones 4-5 or where SECRET or TOP SECRET information or devices are present. If use of these devices is required in a Zone 3, then use is subject to risk assessment and approval by the CSO or CISO. All other mobile devices also includes radio frequency and infrared devices such as private mobile phones, devices, wireless keyboards, Bluetooth devices, smart watches, cameras and any other infrared device that is capable of recording or transmitting audio or data. See the Information Security Manual for additional controls.
    - All other mobile devices includes radio frequency and infrared **medical devices** that connect to entity networks or the internet and may expose the entity to an increased cyber threat. Therefore, a risk assessment is required before allowing medical devices that rely on Wi-Fi, Bluetooth or are capable of recording or transmitting audio or data, into Zones 4 and 5 areas. See Table 20 in the PSPF Guidelines for the minimum recommended criteria to allow medical device use within Zones 4 and 5 areas.

Table 15: Non-Government Mobile Devices – Inside Entity Facilities

	Authorised non-government device - approved to access, process, store or communicate government information or data					**All other mobile devices**
	TOP SECRET	**SECRET**	**PROTECTED**	**OFFICIAL: SENSITIVE**	**OFFICIAL**	
Access control	Not applicable.	Not applicable.	Need-to-know principle: Yes. Security clearance: Baseline (minimum).	Need-to-know principle: Yes. Security clearance: Nil, employment screening only.	Need-to-know principle: Recommended. Security clearance: Nil, employment screening only.	Not applicable.
Use – Zone 1	Not applicable.	Not applicable.	Yes, subject to entity procedures.	Yes, subject to entity procedures.	Yes, subject to entity procedures.	Yes.
Use – Zone 2	Not applicable.	Not applicable.	Yes, subject to entity procedures.	Yes, subject to entity procedures.	Yes, subject to entity procedures.	Yes.
Use – Zone 3	Not applicable.	Not applicable.	If TS or SECRET information/device present: No. If unavoidable, then subject to risk assessment and entity CSO/CISO approval. Otherwise, Yes.	If TS or SECRET information/device present: No. If unavoidable, then subject to risk assessment and entity CSO/CISO approval. Otherwise, Yes.	If TS or SECRET information/device present: No. If unavoidable, then subject to risk assessment and entity CSO/CISO approval. Otherwise, Yes.	If TS or SECRET information/devices present: No. If unavoidable, then subject to risk assessment and entity CSO/CISO approval. Otherwise, Yes.
Use – Zone 4	Not applicable.	Not applicable.	If TS or SECRET information/device present: No. If unavoidable, then subject to risk assessment and entity CSO/CISO approval. Otherwise, Yes.	If TS or SECRET information/device present: No. If unavoidable, then subject to risk assessment and entity CSO/CISO approval. Otherwise, Yes.	If TS or SECRET information/device present: No. If unavoidable, then subject to risk assessment and entity CSO/CISO approval. Otherwise, Yes.	No, not permitted in Zone 4. Medical devices: requires risk assessment and entity CSO/CISO approval.
Use – Zone 5	Not applicable.	Not applicable.	No, unless ASD approved (and subject to ASD conditions of use) during Zone 5 certification and entity CSO/CISO approval.	No, unless ASD approved (and subject to ASD conditions of use) during Zone 5 certification and entity CSO/CISO approval.	No, unless ASD approved (and subject to ASD conditions of use) during Zone 5 certification and entity CSO/CISO approval.	No, not permitted in Zone 5. Medical devices: requires risk assessment and ASD approval.
Leave unattended	Not applicable.	Not applicable.	Yes, subject to entity procedures and locked or turned off.	Yes, subject to entity procedures and locked or turned off.	Yes, subject to entity procedures and locked or turned off.	Not applicable.
Store – Zone 1	Not applicable.	Not applicable.	No.	Secured: Yes, lockable container recommended. Unsecured: Yes, in lockable container.	Yes.	Yes, subject to entity procedures.
Store – Zone 2	Not applicable.	Not applicable.	Class C container.	Secured: Yes, lockable container recommended. Unsecured: Yes in lockable container.	Yes.	Yes, subject to entity procedures.
Store – Zone 3	Not applicable.	Not applicable.	If TS or SECRET information/device present: No. Otherwise, Yes in Class C container.	If TS or SECRET information/device present: No. Otherwise, Yes, and: Secured: lockable container recommended. Unsecured: lockable container.	If TS or SECRET information/device present: No. Otherwise, Yes.	If TS or SECRET information/devices present: No. Otherwise, Yes.
Store – Zone 4	Not applicable.	Not applicable.	If TS or SECRET information/devices present: No. Otherwise, Yes, locked or turned off when not in use, and	If TS or SECRET information/device present: No. Otherwise, Yes, locked or turned off recommended, and	If TS or SECRET information/device present: No. Otherwise, Yes, locked or turned off recommended, and	No, not permitted in Zone 4.

	Authorised non-government device - approved to access, process, store or communicate government information or data					All other mobile devices
	TOP SECRET	SECRET	PROTECTED	OFFICIAL: SENSITIVE	OFFICIAL	
			Secured: lockable container recommended Unsecured: No.	Secured: lockable container recommended Unsecured: lockable container.	Secured: lockable container recommended. Unsecured: lockable container.	
Store – Zone 5	Not applicable.	Not applicable.	No, unless ASD approved during Zone 5 certification and entity CSO/CISO approval.	No, unless ASD approved during Zone 5 certification and entity CSO/CISO approval.	No, unless ASD approved during Zone 5 certification and entity CSO/CISO approval.	No, not permitted in Zone 5.
Carry – Zones 1-2	Not applicable.	Not applicable.	Secured: Yes. Unsecured: Yes, apply entity procedures.	Secured: Yes. Unsecured: Yes, apply entity procedures.	Secured: Yes. Unsecured: Yes, apply entity procedures.	Yes, subject to entity procedures.
Carry – Zone 3	Not applicable.	Not applicable.	If TS or SECRET information/device present: No. Otherwise: Yes. If unsecured, apply entity procedures.	If TS or SECRET information/device present: No. Otherwise: Yes. If unsecured, apply entity procedures.	If TS or SECRET information/device present: No. Otherwise: Yes. If unsecured, apply entity procedures.	If TS or SECRET information/devices present: No. Otherwise: Yes, subject to entity procedures.
Carry – Zone 4	Not applicable.	Not applicable.	If TS or SECRET information/device present: No. Otherwise: Yes. If unsecured, apply entity procedures.	If TS or SECRET information/device present: No. Otherwise: Yes. If unsecured, apply entity procedures.	If TS or SECRET information/device present: No. Otherwise: Yes. If unsecured, apply entity procedures.	No, not permitted in Zone 4.
Carry – Zone 5	Not applicable.	Not applicable.	No.	No.	No.	No, not permitted in Zone 5.
Transmit	Not applicable.	Not applicable.	PROTECTED (or higher) network, otherwise encryption required.	OFFICIAL: Sensitive (or higher) network. Encrypt if transferred over public network infrastructure or through unsecured spaces (including Zone 1), unless residual risk of not doing so has been recognised and accepted by the CSO/CISO.	Encryption recommended for information communicated over public network infrastructure.	Not applicable.
Dispose	Not applicable.	Not applicable.	Refer to Australian Government Information Security Manual – ICT equipment sanitisation and destruction			Not applicable.

Table 16: Non-Government Mobile Devices – Working Remotely in Australia (including home-based work)

	Authorised non-government device - approved to access, process, store or communicate government information or data					All other mobile devices
	TOP SECRET	SECRET	PROTECTED	OFFICIAL: SENSITIVE	OFFICIAL	
Use – outside entity	Not applicable.	Not applicable.	Yes, apply entity procedures and exercise judgement to assess environmental risk.	Yes, apply entity procedures and exercise judgement to assess environmental risk.	Yes.	Yes
Use – at home	Not applicable.	Not applicable.	Regular: Yes, apply entity procedures, which must include a security risk assessment of the proposed work environment. Occasional: Yes, apply entity procedures on need for security risk assessment and exercise judgement to assess environmental risk.	Yes, apply entity procedures on need for security risk assessment and exercise judgement to assess environmental risk.	Yes.	Yes
Leave unattended	Not applicable.	Not applicable.	Yes, if locked or turned off, apply entity procedures and exercise judgement to assess environmental risk.	Secured: Yes. Unsecured: follow 'store' outside entity requirements.	Yes, locked or turned off recommended.	Yes
Store – outside entity	Not applicable.	Not applicable.	Secured: Yes, lockable container recommended. Unsecured: Yes, Class C (or higher) container.	Secured: Yes Unsecured: Yes in lockable container.	Yes, lockable container recommended.	Yes
Store – at home	Not applicable.	Not applicable.	Yes, apply entity procedures and exercise judgement to assess environmental risk.	Apply entity procedures and exercise judgement to assess environmental risk.	Yes, apply entity procedures.	Yes
Carry outside entity	Not applicable.	Not applicable.	Secured: Yes Unsecured: Yes, inside a security briefcase, pouch or satchel and consider tamper-evident packaging.	Secured: Yes. Unsecured: Yes, apply entity procedures.	Yes, apply entity procedures.	Yes

Table 17: Non-Government Mobile Devices – Working Remotely Internationally[4]

	Authorised non-government device - approved to access, process, store or communicate government information or data					All other mobile devices
	TOP SECRET	SECRET	PROTECTED	OFFICIAL: SENSITIVE	OFFICIAL	
Relocate	Not applicable.	Not applicable.	Not recommended. If required, entity must do a risk assessment of the proposed work environment and apply 'travel' outside Australia requirements.	Yes, apply entity procedures and exercise judgement to assess environmental risk.	Yes.	Yes, subject to entity procedures.
Use	Not applicable.	Not applicable.	Not recommended. If required, ensure international location meets all PSPF requirements for PROTECTED information.	Yes, apply entity procedures and exercise judgement to assess environmental risk. Use screen protectors where required, lock the screen when not in use and shut down device at end of each day.	Yes.	Yes, subject to entity procedures.
Leave unattended	Not applicable.	Not applicable.	No, store securely when unattended. For brief absences from approved remote location, apply entity procedures and exercise judgement to assess environmental risk.	Yes, apply entity procedures and exercise judgement to assess environmental risk.	Yes, locked or turned off recommended.	Yes, subject to entity procedures.
Store	Not applicable.	Not applicable.	Not recommended. If required, entity must risk assess international location and if approved, preferably store in Class C (or higher) container.	Yes, if approved by entity risk assessment of location and stored in lockable container.	Yes, lockable container recommended.	Yes, subject to entity procedures.

Table 18: Non-Government Mobile Devices – Travel in Australia (domestic travel)

	Authorised non-government device - approved to access, process, store or communicate government information or data					All other mobile devices
	TOP SECRET	SECRET	PROTECTED	OFFICIAL: SENSITIVE	OFFICIAL	
Travel	Not applicable.	Not applicable.	Yes, apply 'carry' outside entity requirements and any additional entity procedures.	Yes, apply 'carry' outside entity requirements and any additional entity travel procedures, and exercise judgment to assess environmental risk.	Yes.	Yes
Air travel luggage	Not applicable.	Not applicable.	Yes, retain as carry-on luggage. If airline requires carry-on luggage to be checked at the gate, try to observe entering/existing the cargo hold and reclaim as soon as possible.	Yes, retain as carry-on luggage recommended.	Yes.	Yes
Leave unattended	Not applicable.	Not applicable.	Not recommended. For brief absences from hotel room, apply entity procedures and exercise judgement to assess environmental risk.	Yes, apply entity procedures and exercise judgement to assess environmental risk.	Yes, apply entity procedures and exercise judgement to assess environmental risk.	Yes
Store while travel	Not applicable.	Not applicable.	Not recommended. For brief absence from hotel room, see 'leave unattended'.	Yes, apply 'store' outside entity requirements.	Yes, apply 'store' outside entity requirements.	Yes

Table 19: Non-Government Mobile Devices – Travel Outside of Australia (international travel)

	Authorised non-government device - approved to access, process, store or communicate government information or data					All other mobile devices
	TOP SECRET	SECRET	PROTECTED	OFFICIAL: SENSITIVE	OFFICIAL	
Travel	Not applicable.	Not applicable.	Not recommended. Seek DFAT advice on options to access mobile device at international destination. If required, apply 'carry' outside entity requirements and any additional entity travel procedures, and consider country-specific travel advice.	Yes, apply 'carry' outside entity requirements, any additional entity travel procedures, and consider country-specific travel advice.	Yes, apply entity procedures and exercise judgement to assess environmental risk.	Yes, subject to entity procedures.
Air travel luggage	Not applicable.	Not applicable.	Not recommended. If required, retain as carry-on luggage. If airline requires carry-on baggage to be checked at the gate, **do not travel**.	Yes, apply 'carry' outside entity requirements, any additional entity procedures and exercise judgement to assess environmental risk.	Yes, apply 'carry' outside entity requirements.	Yes, subject to entity procedures.

	Authorised non-government device - approved to access, process, store or communicate government information or data					All other mobile devices
	TOP SECRET	SECRET	PROTECTED	OFFICIAL: SENSITIVE	OFFICIAL	
Leave unattended	Not applicable.	Not applicable.	No, do not leave unattended.	Yes, apply entity procedures, exercise judgement to assess environmental risk, and consider country-specific travel advice.	Yes, apply entity procedures.	Yes, subject to entity procedures.
Store while travel	Not applicable.	Not applicable.	No, do not store while travelling (e.g. in hotel room). If required, can be stored in Australian entity facility meeting 'store' inside entity requirements.	Yes, apply 'store' outside entity requirements and consider country-specific travel advice.	Yes, apply 'store' outside entity requirements	Yes, subject to entity procedures.

9.4 Information Management Markers

Information management markers are an optional way for entities to identify information that is subject to non-security related restrictions on access and use. They are a subset of the controlled list of terms for the 'Rights Type' property in the National Archives of Australia's Australian Government Record Keeping Metadata Standard. Information management markers are not protective markers or security classifications.

See Recordkeeping Metadata Standard for requirements and PSPF Guidelines for description of optional information management markers.

9.5 Security Caveats and Accountable Material

9.5.1 Security Caveats

Security Caveats are a warning that the information has special protections in addition to those indicated by the security classification. Security Caveats are not classifications and must appear with a security classification.

There are four categories of security caveats:

- Codewords (sensitive compartment information that requires a compartmental briefing)
- Foreign Government Markings
- Special Handling Instructions, and
- Releasability Caveats.

Each security caveat is governed by a 'controlling authority', responsible for managing and administering the security caveat. See the Australian Government Security Caveat Standard for details.

Requirement 0063 | INFO | All entities | 31 October 2024

The Australian Government Security Caveat Standard and special handling requirements imposed by the controlling authority are applied to protect security caveated information.

Requirement 0064 | INFO | All entities | 01 July 2025

Security caveats are clearly marked as text and only appear in conjunction with a security classification.

9.5.2 Accountable Material

Accountable material is information that requires the strictest control over its access and movement. Accountable material includes:

- TOP SECRET information,
- all codeword information, see Australian Government Security Caveat Standard for details,
- select special handing instruction caveats, see Australian Government Security Caveat Standard for details, and
- any classified information designated as accountable material by the originator.

See Information Asset Registers for information on auditable records for accountable material.

Requirement 0065 | INFO | All entities | 31 October 2024

Accountable material has page and reference numbering.

Requirement 0066 | INFO | All entities | 31 October 2024

Accountable material is handled in accordance with any special handling requirements imposed by the originator and security caveat owner detailed in the Australian Government Security Caveat Standard.

9.6 Email Protective Marking Standard

The Australian Government Email Protective Marking Standard details the standardised format for protective markings, security classifications and, where relevant information management markers, on emails exchanged in and between Australian Government entities, and with other authorised parties. This includes authorised non-government entities and foreign partners where a formal agreement or arrangement has been established.

This standard supports processes and technology systems, such as an entity's email gateway, to control the flow of information into and out of the entity. For message recipients it also identifies what handling protections are needed to safeguard the information.

Requirement 0067 | INFO | All entities | 31 October 2024

The Australian Government Email Protective Marking Standard is applied to protect OFFICIAL and security classified information exchanged by email in and between Australian Government entities, including other authorised parties.

9.7 Recordkeeping Metadata Standard

Metadata is a term that means 'data about data'. Text-based protective markings on technology systems are supplemented by the use of metadata to describe, among other things, key security characteristics of information. For electronic records management systems, the National Archives of Australia produces the Australian Government Record Keeping Metadata Standard to provide standardised metadata terms and definitions for consistency across government. The minimum metadata set is a practical application of the standard that identifies the metadata properties essential for entity management and use of official information.

Requirement 0068 | INFO | All entities | 31 October 2024

The Australian Government Recordkeeping Metadata Standard's 'Security Classification' property (and where relevant, the 'Security Caveat' property) is applied to protectively mark information on technology systems that store, process or communicate security classified information.

Requirement 0069 | INFO | All entities | 31 October 2024

Apply the Australian Government Recordkeeping Metadata Standard's 'Rights' property where the entity wishes to categorise information content by the type of restrictions on access.

9.8 Security Classified Discussions

Security classified discussions includes any audible dissemination of information, including briefings, irregular discussions and meetings either in person or using a mobile device, phone or video conference platform. ASIO Technical Note 1/15 Physical Security of Zones defines 'irregular discussions' as those that are unpredictable, non-ongoing or unannounced.

Requirement 0070 | INFO | All entities | 31 October 2024

Security classified discussions and dissemination of security classified information are only conducted in approved locations.

9.8.1 Approved Locations for Security Classified Discussions

Table 20 details the approved locations for security classified discussions. This identifies when entities must 'exercise judgement', use discretion and to judge the suitability of the location, environment. Entities must also consider who else might be able to hear the security classified information.

The risk of deliberate or accidental overhearing can be minimised by controlling the environment where the discussion is taking place. This may be achieved by treating the room, area or entire facility acoustically, combined with other physical and procedural security measures. See Technical Surveillance Countermeasures and Table 48: Physical Security Measures and Controls – Technical surveillance counter-measures (TSCM) for mandatory elements.

To provide protection for security classified discussions, it is necessary for the sound created within the room to be unintelligible to a person or device located outside that room. Appropriate and effective sound insulation is critical to achieving the required level of security for security classified discussions as it is extremely difficult for an entity to ensure that only low-volume voice levels are used for security classified discussions or that background noise will always exist in the receiving area. See ASIO Technical Note 1/15 – Physical Security of Zones, Section 16: Audio Security and ASIO Technical Note 5/12 Physical Security Zones (TOP SECRET) areas.

Table 20: Approved Locations for Security Classified Discussions/Audible Dissemination of Information

Location of discussion	TOP SECRET	SECRET	PROTECTED	OFFICIAL: SENSITIVE
Zone 1	No	No	No	Yes, but exercise judgement
Zone 2	No	No	Yes, but exercise judgement	Yes
Zone 3	No	No, but ASIO Technical Notes permit irregular discussions[9]	Yes	Yes
Zone 4	No, but ASIO Technical Notes permit irregular discussions[9]	Yes	Yes	Yes
Zone 5	Yes	Yes	Yes	Yes
Outside entity – public spaces	No	No	No[10]	Yes, but exercise judgement
Outside entity – home based work	No[10]	No[10]	Yes, but exercise judgement	Yes, but exercise judgement
While travelling	No[10]	No[10]	No[10]	Yes, but exercise judgement

9.9 Historical Classifications

There are historical security classifications and other protective markings (e.g. UNCLASSIFIED, X-IN-CONFIDENCE, RESTRICTED, PROTECTED, CONFIDENTIAL and HIGHLY PROTECTED) that no longer reflect Australian Government policy. The historical security classifications and historical handling protections remain unless the originator reclassifies or declassifies the information and applies a current security classification.

See PSPF Guidelines for protections and handling requirements for historical classifications and markings.

[9] ASIO Technical Notes define 'irregular discussions' as those that are unpredictable, non-ongoing or unannounced.
[10] If required for operational or ministerial briefing purposes, then yes providing appropriate alternative mitigations are in place and, where required, agreed by the relevant authority or originator of the information.

Related Standards – Classifications and Caveats

- Standard: Australian Government Security Caveat Standard (on GovTEAMS)
- Standard: Australian Government Email Protective Marking Standard
- Standard: Australian Government Recordkeeping Metadata Standard
- Standard: ASIO Technical Note 1/15 – Physical Security of Zones: Audio Security (on GovTEAMS)
- Standard: ASIO Technical Note 1/15 Physical Security of Zones (on GovTEAMS)
- Standard: ASIO Technical Note 5/12 Physical Security Zones (TOP SECRET) areas (on GovTEAMS)

10 Information Holdings

Information is a valuable asset. Information is an all-encompassing term describing data, information and records in any format. All information entities create, use or receive as part of its business is subject to the *Archives Act 1983*, no matter what its format or location. All government personnel (including contractors) are responsible for creating and capturing information into systems that manage and support its use over time.

See the National Archives of Australia's Information Management Standard for guidance.

Requirement 0071 | INFO | All entities | 31 October 2024

Entity implements operational controls for its information holdings that are proportional to their value, importance and sensitivity.

10.1 Aggregated Information Holdings

Aggregated information is a compilation of information that may be assessed as requiring a higher security classification or additional security controls where the aggregated holding is significantly more valuable than its individual components. This is because the collated information reveals new or more sensitive information or intelligence than would be apparent from the individual source components, and would cause greater damage than individual components. When viewed separately, the components of the information holding retain their individual classifications. The entity that aggregates the information becomes the 'originator' and is therefore responsible for assessing the classification of the aggregated information.

Integrated information is information that is combined from different sources into a single, unified view. While the value of integrated data can be high, it is also generally de-identified, cleansed and transformed to the extent that it provides limited information outside of the insights for which it was created to provide. Considering this, integrated data is of a single value and should only be classified according to the value, importance and sensitivity of the fully integrated data set. The entity that integrates the data becomes the 'originator' and must therefore assess the classification of the integrated data.

10.2 Information Asset Registers

Monitoring and auditing the dissemination of information plays an important role in information protection. For highly classified or caveated information (such as TOP SECRET information and accountable material), it is critical to maintain an auditable register (such as a Classified Document Register or electronic document management repository) of all incoming and outgoing information and material, transfers or copying, along with regular spot check audits.

See Security Caveats and Accountable Material.

Requirement 0072 | INFO | All entities | 31 October 2024

An auditable register is maintained for TOP SECRET information and accountable material.

Related Standards – Information Holdings

- Standard: National Archives of Australia's Information Management Standard for Australian Government
- Legislation: *Archives Act 1983*

11 Information Disposal

All official information the Australian Government creates, sends and receives is considered a Commonwealth record. Not all official information is kept forever and disposing of it does not always mean itis destroyed.

Under the *Archives Act 1983*, disposal of Australian Government business information means either its destruction, the transfer of its custody or ownership, or damage or alteration. Destruction is the complete and irreversible process of erasing the business information so it cannot be reconstituted or reconstructed.

Business information is managed for as long as it has value; some information will have long-term historical and social value. The National Archives of Australia's Information Management Standard for Australian Government Principle 6 states *that business information is accountably destroyed or transferred* Records authorities set out the minimum periods for which business information should be retained. The Information Management Standard for the Australian Government states that entities must not destroy relevant business information until the disposal freeze or retention notice is no longer in place.

Destruction of Australian Government business information can occur if it is:

- approved by the National Archives through a records authority
- required by legislation, or
- covered under a normal administrative practice (NAP).

The careless disposal of security classified information is a serious source of leakage or compromise of information, and can undermine public confidence in the Australian Government.

ASIO-T4 provides advice on the destruction of physical security-classified information via several destruction methods. Refer to the ASIO-T4 Protective Security Circular 167— Destruction of Sensitive and Security Classified Information (available on a need-to-know basis on GovTEAMS) for details on approved destruction methods including:

- shredding using crosscut shredders (strip shredders are not approved for destruction of security classified information).
- pulping
- burning
- pulverising using hammermills, and
- disintegrating by cutting and reducing the waste particle size.

ASIO-T4 also approves for use destruction equipment for each destruction method. Refer to the ASIO-T4 Security Equipment Guides (on GovTEAMS) for guidance on testing and selecting equipment for the destruction of security classified information.

Requirement 0073 | INFO | All entities | 31 October 2024

OFFICIAL and security classified information is disposed of securely in accordance with the Minimum Protections and Handling Requirements, Information Security Manual, the Records Authorities, a Normal Administrative Practice and the *Archives Act 1983*.

Requirement 0074 | INFO | All entities | 31 October 2024

Security classified information is appropriately destroyed in accordance with the Minimum Protections and Handling Requirements when it has passed the minimum retention requirements or reaches authorised destruction dates.

Related Standards – Information Disposal

- Legislation: *Archives Act 1983*
- Legal instrument: Records Authorities
- Standard: Normal administrative practice (NAP)
- Standard: National Archives of Australia's Information Management Standard for Australian Government
- Standard: ASD's Information Security Manual
- Standard: ASIO-T4 Protective Security Circular 167— Destruction of Sensitive and Security Classified Information (on GovTEAMS)
- Guidance: Security Equipment Guides (on GovTEAMS)

12 Information Sharing

Australian Government security classified and caveated information requires protection if it is to be shared with other government entities, non-government stakeholders and international partners.

Entities must consider the information they share and disclose and ensure it is appropriately controlled, when sharing security classified information, or disclosing information outside of government.

Requirement 0075 | INFO | All entities | 31 October 2024

Access to security classified information or resources is only provided to people outside the entity with the appropriate security clearance (where required) and a need-to-know, and is transferred in accordance with the Minimum Protections and Handling Requirements

12.1 Need-to-Know Principle

The need-to-know principle reflects the need for personnel to only access information only where there is a requirement to do so to fulfil their official duties and applies to all security classified information.

Limiting access by personnel (including contractors) to information on a need-to-know basis guards against the risk of unauthorised access or misuse of information. Personnel are not entitled to access information merely because it would be convenient for them to know or because of their status, position, rank or level of authorised access.

12.2 Domestic Information Sharing

12.2.1 Sharing with Other Government Entities

All non-corporate Commonwealth entities are required to adhere to the PSPF. Entities may share information with other non-corporate Commonwealth entities provided the recipient holds the appropriate security clearance (where required), the need-to-know principle is applied, and the information is provided by means authorised in the PSPF.

The PSPF represents better practice for other Commonwealth entities (i.e. corporate Commonwealth entities and Commonwealth Companies), but is not mandatory. Entities may share information with other Commonwealth entities provided the information is transferred in accordance with the PSPF, the need-to-know principle is applied, the recipient holds the appropriate security clearance, and agrees to adhere to the Minimum Protections and Handling Requirements.

12.2.2 Sharing with Australian State and Territory Agencies

A Memorandum of Understanding (MOU) between the Commonwealth, States and Territories is in place for the protection of security classified information and to support national cooperation between jurisdictions. Under the MOU, state and territory government agencies that hold or access Australian Government security classified information are required to apply the relevant protective security measures contained in the PSPF to that information.

Requirement 0076 | INFO | All entities | 31 October 2024

The Memorandum of Understanding between the Commonwealth, States and Territories is applied when sharing information with state and territory government agencies.

12.2.3 Sharing with Non-Government Stakeholders

Risks arise when sharing information outside of government as the PSPF Minimum protections and handling requirements apply only to non-corporate Commonwealth entities. These arrangements therefore need an agreement, contract or deed in place to provide assurance that the non-government stakeholder understands the obligations to protect government information.

OFFICIAL information (i.e. non-classified information) may be shared with non-government stakeholders without an agreement or arrangement for its protection.

Requirement 0077 | INFO | All entities | 01 July 2025

An agreement or arrangement, such as a contract or deed, that establishes handling requirements and protections, is in place before security classified information or resources are disclosed or shared with a person or organisation outside of government, unless the entity is returning or responding to information provided by a person or organisation outside of government, or their authorised representative, which the government entity subsequently classified as OFFICIAL: Sensitive.

12.3 International Information Sharing

The Department of Home Affairs, as the National Security Authority for the Australian Government, is responsible for general oversight of General Security Agreements and other international arrangements where Australian Government classified information sharing provisions are present, including for determining the policy for protecting and sharing security classified information and resources.

The Department of Home Affairs provides advice on the equivalent international protections for security classified information to be applied when sharing information with international partners.

Australia has international treaty-level agreements, or less-than-treaty-status arrangements, that provide for equivalent international protection of Australian Government OFFICIAL and security classified information or resources:

- an international agreement constitutes a treaty and is binding under international law, and
- an international arrangement has less-than-treaty status, such as a Memorandum of Understanding, and does not create legal rights or obligations. Arrangements do, however, create commitments that are politically and morally binding.

Australian Government security classified information and resources must not be shared with a foreign entity unless explicit legislative provisions, international agreements or arrangements for protection of classified information and resources are in place.

There are generally two types of international agreements:

- Whole of government international agreement – referred to as General Security Agreements (GSA).
- Entity-to-entity specific international agreements – these vary in format and substance.

Australian Government security classified information or resources must not be shared with a foreign entity that is subject to extensive data collection powers or exposure to extrajudicial directions from a foreign government that conflict with Australian law.

Requirement 0078 | INFO | All entities | 31 October 2024

Provisions are met concerning the security of people, information and resources contained in international agreements and arrangements to which Australia is a party.

Requirement 0079 | INFO | All entities | 31 October 2024

Australian Government security classified information or resources shared with a foreign entity is protected by an explicit legislative provision, international agreement or international arrangement.

Requirement 0080 | INFO | All entities | 01 July 2025

Australian Government security classified information or resources bearing the Australian Eyes Only (AUSTEO) caveat is never shared with a person who is not an Australian citizen, even when an international agreement or international arrangement is in place, unless an exemption is granted.

AUSTEO Exemption Process

The Accountable Authority may grant an exemption to Requirement 0080 to give a non-Australian appointee access to AUSTEO material, provided they:

- advise the Department of Home Affairs before a Cabinet decision is made to appoint the individual
- co-ordinate with relevant AUSTEO producing entities, and
- ensure the individual:
  - is appointed by a Cabinet process to a position that requires access to AUSTEO information
  - is a citizen of a Five-Eyes country (New Zealand, United Kingdom, United States of America or Canada)
  - holds the appropriate security clearance (either Australian or recognised Five-Eyes security clearance), and
  - signs a non-disclosure agreement that prevents on-sharing of AUSTEO information.

Requirement 0081 | INFO | All entities | 31 October 2024

Australian Government security classified information or resources bearing the Australian Government Access Only (AGAO) caveat is not shared with a person who is not an Australia citizen, even when an international agreement or international arrangement is in place, unless they are working for, or seconded to, an entity that is a member of National Intelligence Community, the Department of Defence or the Australian Submarine Agency.

Requirement 0082 | INFO | All entities | 31 October 2024

Where an international agreement or international arrangement is in place, security classified foreign entity information or resources are safeguarded in accordance with the provisions set out in the agreement or arrangement.

12.3.1 Sharing with Non-Government International Stakeholders

Sharing of Australian Government security classified information and resources with a foreign entity (including non-government individuals, companies or organisations) is prohibited unless explicit legislative provisions, international agreements or arrangements for protection of classified information and resources are in place.

These arrangements ensure that the appropriate mutual arrangements for the protection of information and resources have been considered and agreed.

Risk-based approaches to ad hoc or one-off sharing of Australian Government security classified information and resources can be made through arrangements such as a letter of assurance or using temporary access provisions at Access to Resources.

If agreed by the Accountable Authority, these ad hoc arrangements must be:

- documented, including the date the accountable authority approved the arrangements
- for a limited/specific period of time only, i.e. not ongoing or enduring
- for a specific purpose, project or activity, and
- inclusive of protections for use and storage of security classified and caveated information in accordance with the Minimum Protections and Handling Requirements and the Australian Government Security Caveat Standards.

Australian Government security classified information or resources must not be shared with foreign non-government stakeholders that are subject to extensive data collection powers or exposure to extrajudicial directions from a foreign government that conflict with Australian law.

Requirement 0083 | INFO | All entities | 31 October 2024

Australian Government security classified information or resources shared with a foreign non-government stakeholder is protected by an explicit legislative provision, international agreement or international arrangement.

Related Standards – Information Sharing

- Standard: Australian Government Security Caveat Standard (on GovTEAMS)
- Memorandum of Understanding (MOU) between the Commonwealth, States and Territories for the protection of security classified information (on GovTEAMS)
- Reference: Australian Treaties Database

Part Four

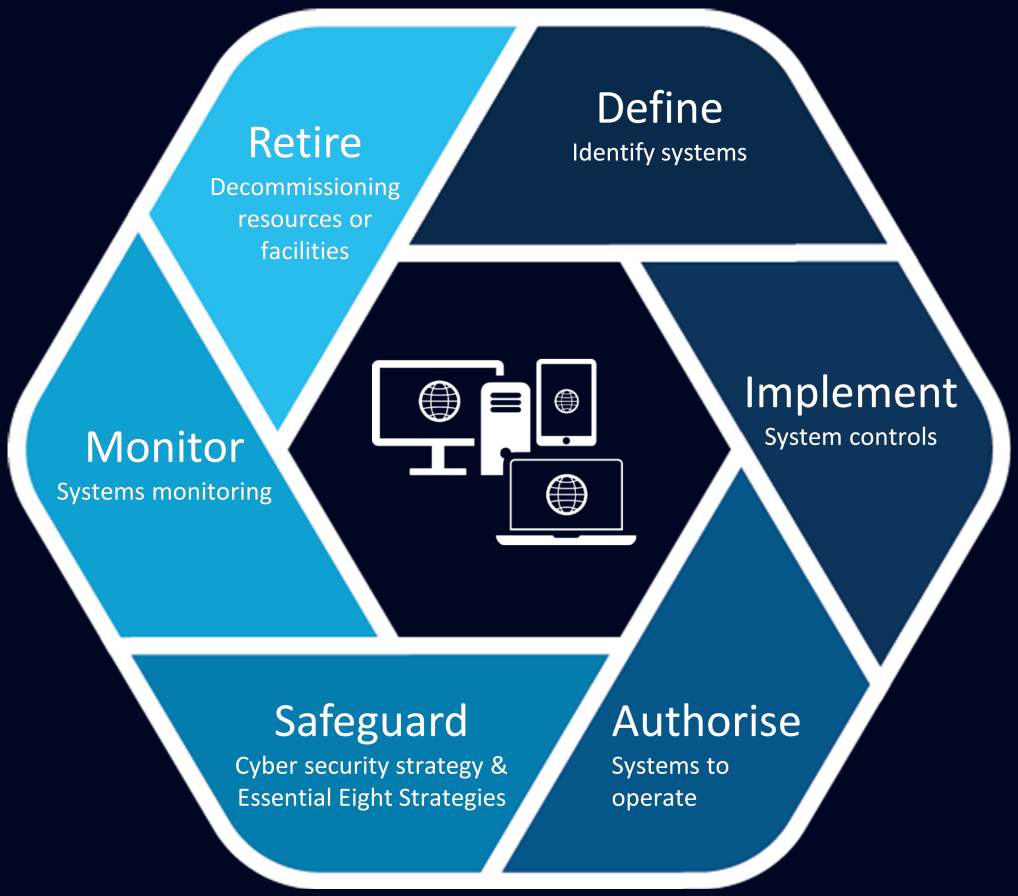
Technology

Technology Lifecycle Management

Cyber Security Strategies

Cyber Security Programs

Technology Lifecycle



13 Technology Lifecycle Management

Technology lifecycle management is the approach to managing the entity's information technology and operational technology systems (technology systems) across designing, developing, planning, procurement, deployment and maintenance through to retirement of the systems.

13.1 Information Security Manual

The Australian Signals Directorate's Information Security Manual outlines the controls to protect the entity's technology systems and data from cyber threats, using a risk management framework. Broadly the Information Security Manual's risk management framework has six steps: define the system, select controls, implement controls, assess controls, authorise the system and monitor the system.

Non-corporate Commonwealth entities should interpret the ISM's references to 'board of directors or executive committee' as the Accountable Authority as defined by the PGPA Act.

Requirement 0084 | TECH | All entities | 31 October 2024

The Australian Signals Directorate's Information Security Manual cyber security principles are applied during all stages of the lifecycle of each system

Requirement 0085 | TECH | All entities | 31 October 2024

The Australian Signals Directorate's Information Security Manual controls and cyber security guidelines are applied on a risk-based approach.

13.2 Technology Estate

The technology estate encompasses all of an entity's technology systems including the related set of hardware, software, supporting infrastructure, and the governance framework in which the technology systems operate, IT assets and equipment, applications, mobile devices, and services that process, store or communicate official and security classified information and data. This includes outsourced systems and cloud services provided to or by the entity.

Understanding the scope of an entity's technology estate allows the entity to identify assets and technology systems that are at high risk of cyber security vulnerabilities, particularly those that can be accessed by unknown and unauthorised people, and provide access to the entity's wider, non-internet-facing network.

13.2.1 Technology Asset Stocktake and Technology Security Risk Management Plan

All Internet-facing systems, services and devices are vulnerable to compromise, particularly if they connect to the entity's wider technology estate. Systems, services and devices that can be accessed by unknown and unauthorised people, including members of the public, are particularly susceptible to compromise and exploitation, they may allow unauthorised access to the entity's wider, non-internet-facing network.

A Technology Asset Stocktake provides visibility of the scope of the entity's technology estate and includes internet-facing systems or services that are particularly at risk.

A Technology Security Risk Management Plan is a structured approach to assess and manage the risks associated with technology assets identified in the Technology Asset Stocktake. Assessing risk and applying mitigations for technology assets will support the secure and continuous delivery of government business. This is critical to maintaining public and stakeholder trust in transacting with the Australian Government.

Requirement 0211 | TECH | All entities | 01 July 2025

A Technology Asset Stocktake and Technology Security Risk Management Plan is created to identify and manage the entity's internet-facing systems or services to ensure continuous visibility and monitoring of the entity's resource and technology estate.

13.2.2 Network Documentation

Network documentation is developed to accurately depict the current state of the entity's networks across the entity's technology estate, and includes high-level network diagrams showing all connections into networks; logical network diagrams showing all critical servers, high-value servers, network devices and network security appliances; and device settings for all critical servers, high-value servers, network devices and network security appliances.

Network documentation can assist in troubleshooting network problems as well as responding to and recovering from cyber security incidents. As network documentation could be used by malicious actors to assist in compromising networks, it is important that it is appropriately protected.

Entities may want to use vulnerability, network or attack surface scanning tools and explore how these could be leveraged for mitigating security risks posed by inadequate information technology and operational technology asset inventories or shadow IT. See Guidelines for System Management (cyber.gov.au) and Managing the Risks of Legacy IT (cyber.gov.au).

13.3 Technology System Authorisation

The effective implementation of the Information Security Manual's cyber security principles, controls and guidelines are key to safeguarding entity technology and systems from cyber threats and managing the associated security risks.

All technology systems require authorisation to operate or be used in the entity. The authorisation process ensures that an appropriate level of security is being applied to the technology system and that residual security risks have been accepted by the relevant authority. This approach also provides confidence that the technology system meets security objectives, and addresses known security vulnerabilities. An impartial (and in some cases independent) security assessment can be a valuable tool in authorisation decisions.

Obligations for protecting Australian Government information and data that is processed, stored or communicated via an outsourced managed service provider or cloud service provider are no different than those using an internal entity service. The same authorisation to operate framework for managing security risks during the lifecycle of the technology system still applies.

Table 21: Authorising Officer and Security Assessor for Technology System Authorisation

Type	Role	TOP SECRET[11]	SECRET	PROTECTED	OFFICIAL: SENSITIVE	OFFICIAL
Systems	Security Assessor	Australian Signals Directorate assessor (or their delegate)	Entity assessor or IRAP assessor	Entity assessor or IRAP assessor	Entity assessor or IRAP assessor	Entity assessor or IRAP assessor
	Authorising Officer	Director-General Australian Signals Directorate (or their delegate)	Accountable Authority or CISO (or their delegate) of entity system owner	Accountable Authority or CISO (or their delegate) of entity system owner	Accountable Authority or CISO (or their delegate) of entity system owner	Accountable Authority or CISO (or their delegate) of entity system owner
Outsourced Systems and Information Technologies	Security Assessor	Australian Signals Directorate assessor (or their delegate)	IRAP assessor	IRAP assessor	IRAP assessor	IRAP assessor
	Authorising Officer	Director-General Australian Signals Directorate (or their delegate)	Accountable Authority or CISO (or their delegate) of entity system owner	Accountable Authority or CISO (or their delegate) of entity system owner	Accountable Authority or CISO (or their delegate) of entity system owner	Accountable Authority or CISO (or their delegate) of entity system owner
Cloud services	Security Assessor	Australian Signals Directorate assessor (or their delegate)	IRAP assessor	IRAP assessor	IRAP assessor	IRAP assessor
	Authorising Officer	Director-General Australian Signals Directorate (or their delegate)	Accountable Authority or CISO (or their delegate) of entity system owner	Accountable Authority or CISO (or their delegate) of entity system owner	Accountable Authority or CISO (or their delegate) of entity system owner	Accountable Authority or CISO (or their delegate) of entity system owner
Gateways	Security Assessor	Australian Signals Directorate assessor (or their delegate)	IRAP assessor	IRAP assessor	IRAP assessor	IRAP assessor
	Authorising Officer	Director-General Australian Signals Directorate (or their delegate)	Accountable Authority or CISO (or their delegate) of entity system owner	Accountable Authority or CISO (or their delegate) of entity system owner	Accountable Authority or CISO (or their delegate) of entity system owner	Accountable Authority or CISO (or their delegate) of entity system owner
Multinational and multi-entity systems	Security Assessor	Determined by a formal agreement between the parties involved.				
	Authorising Officer	Determined by a formal agreement between the parties involved.				

[11] Including sensitive compartmented information systems, outsourced systems and information technologies, and cloud services.

Requirement 0086 | TECH | All entities | 31 October 2024

The Authorising Officer authorises each technology system to operate based on the acceptance of the residual security risks associated with its operation before that system processes, stores or communicates government information or data.

Requirement 0087 | TECH | All entities | 31 October 2024

Decisions to authorise (or reauthorise) a new technology system or make changes to an existing technology system are based on the Information Security Manual's risk-based approach to cyber security.

Requirement 0088 | TECH | All entities | 31 October 2024

The technology system is authorised to the highest security classification of the information and data it will process, store or communicate.

Requirement 0089 | TECH | All entities | 31 October 2024

A register of the entity's authorised technology systems is developed, implemented and maintained, and includes the name and position of the Authorising Officer, system owner, date of authorisation, and any decisions to accept residual security risks.

13.3.1 Technology System Reauthorisation

During the lifecycle of a technology system, it may require a reassessment to continue operation or eventually be decommissioned (i.e. disposal at the end of its life). Examples of events that may trigger additional risk management activities for a technology system include:

- changes of application in the Information Security Manual's controls or security policies relating to the technology system
- detection of new or emerging cyber threats to the technology system or its operating environment
- the discovery that security controls for the technology system are not as effective as planned
- a major cyber security incident involving the technology system, or
- major functionality or architectural changes to the technology system.

Requirement 0090 | TECH | All entities | 31 October 2024

Each technology system's suitability to be authorised to operate is reassessed when it undergoes significant functionality or architectural change, or where the system's security environment has changed considerably.

13.3.1.1. Continued Authorisation

Authorisation to operate is generally ongoing once the system is operational. However, the system owner monitors to ensure that the risks of operating the system do not exceed the entity's risk tolerances. Where a risk level has been exceeded, the system owner must take appropriate steps to identify the level of mitigation required and whether the Authorising Officer needs to accept the risk or sign off on the proposed mitigations. If multiple risks are exceeded simultaneously, the system owner must consider if one or more of the triggers from the above section are warranted, triggering a full reassessment and reauthorisation.

13.3.2 System Owners

System owners are responsible for ensuring the secure operation of their technology systems. System owners may delegate the day-to-day management and operation of their technology systems to other personnel.

See PSPF Guidelines and the Information Security Manual for the authorisation process steps.

13.4 Applications Management

All applications require approval to be installed or used on resources that access Australian Government technology systems or data.

13.5 Social Media Applications

Social media applications can pose significant security and privacy risks to the Australian Government due to the potential collection and exploitation of user and device data. Decisions to install social media applications need to be made on an assessment of the risk, in cases where the application is produced by vendors that are subject to extrajudicial directions from a foreign government whose laws conflict with Australian law.

Extensive data collection – Social media applications typically collect extensive data as part of their business model. These applications may also collect additional data from individuals' devices, which extends beyond the content of messages, videos and voice recordings. The type of data collected may change over time, including when new versions or features are released. The terms of use and privacy policies relating to what data is collected, as well as how and when it can be used, may also change at short notice or be difficult to understand. Sometimes this data is stored outside of Australia and may be subject to lawful access or covert collection by other countries. In such cases, current Australian legislation and privacy or consumer laws may not apply.

Exploitation of personal information – Personal information posted to social media can be exploited. Even seemingly benign posts, messages, photos or videos can be used to develop detailed profiles of individuals. This information could be used in extortion or social engineering campaigns aimed at eliciting sensitive information, or influencing individuals to compromise organisations' activities or technology systems.

In addition, social media content may not come from reputable or trustworthy sources and may contain disinformation.

See Procurement, Outsourcing and Contract Management.

13.6 TikTok Application

The TikTok application poses significant security and privacy risks to non-corporate Commonwealth entities arising from extensive collection of user data and exposure to extrajudicial directions from a foreign government that conflict with Australian law.

Use of the TikTok application is not permitted on government devices and existing instances must be removed unless a legitimate business reasons exists. Legitimate business reason means a need to install or access the TikTok application on a government device to conduct business and/or achieve a work objective of an entity.

Entities that accept the risks of the use of personal devices to access official or security classified system data, up to and including PROTECTED, (i.e. pursuant to remote access arrangements including Bring Your Own Device (BYOD) or equivalent policies), must provide access to that data through non-persistent and full remote access solutions, approved by the CISO, as opposed to using the native storage and applications on the personal device.

Requirement 0091 | TECH | All entities | 31 October 2024

The TikTok application is prevented from being installed, and existing instances are removed, on government devices, unless a legitimate business reason exists which necessitates the installation or ongoing presence of the application.

Requirement 0092 | TECH | All entities | 31 October 2024

The Chief Security Officer or Chief Information Security Officer approves any legitimate business reason for the use of the TikTok application on government devices and ensures the following mitigations are in place to manage security risks:

- Ensure the TikTok application is installed and accessed only on a separate, standalone device without access to services that process or access official and classified information.
- Ensure the separate, standalone device is appropriately stored and secured when not in use. This includes the isolation of these devices from sensitive conversations and information.
- Ensure metadata has been removed from photos, videos and documents when uploading any content to TikTok.
- Minimise, where possible, the sharing of personal identifying content on the TikTok application.
- Use an official generic email address (for example, a group mailbox) for each TikTok account.
- Use multi-factor authentication and unique passphrases for each TikTok account.
- Ensure that devices that access the TikTok application are using the latest available operating system in order to control individual mobile application permissions. Regularly check for and update the application to ensure the latest version is used.
- Only install the TikTok application from trusted stores such as Microsoft Store, Google Play Store and the Apple App Store.
- Ensure only authorised users have access to corporate TikTok accounts and that access (either direct or delegated) is revoked immediately when there is no longer a requirement for that access.
- Carefully and regularly review the terms and conditions, as well as application permissions with each update, to ensure appropriate risk management controls can be put in place or adjusted as required.
- Delete the TikTok application from devices when access is no longer needed.

13.7 Legacy Information Technology Management

An Information Technology (IT) product (i.e. hardware, software, services, protocols, and/or systems) is considered to be 'legacy' when it meets one or more criteria in both Category A and Category B below.

13.7.1 Category A

- Considered an end-of-life product, or
- Out of support, and extended support from the manufacturer, vendor or developer.

13.7.2 Category B

- Impractical to update or support within the entity, or
- No longer cost-effective, or
- Considered to be above the current acceptable risk threshold, or
- Offers diminishing business utility, or
- Prevents or obstructs fulfilment of the entity's IT strategies.

Legacy IT presents significant and enduring risks to the cyber security posture of Australian Government. Its presence can increase the risk of a cyber security incident, and make any incident that does occur much more impactful. All IT will eventually become legacy and present these acute cyber security risks.

The most effective method to mitigate the risk posed by legacy IT is to replace it before it expires with IT that is still supported. Where legacy IT cannot immediately be replaced, the entity must apply the Australian Signals

Directorate's guidance on managing the risks posted by legacy IT. This guidance provides a list of temporary mitigations that entities must consider implementing in addition to any additional mitigations that are relevant to the entity's IT environment. These mitigations are only suitable for temporary fixes as the only long-term solution is replacement of legacy IT. See Managing the Risks of Legacy ICT: Practitioner Guidance | Cyber.gov.au

Requirement 0093 | TECH | All entities | 31 October 2024

The Australian Signals Directorate's temporary mitigations for legacy IT are applied to manage legacy information technology that cannot yet be replaced.

13.8 Technology Asset Storage

A technology asset is defined as any hardware, software or information system, platform, mobile application or 'as-a-service' offering, which stores, processes, transmits or communicates official or security classified information or data belonging to, or utilised by, the Australian Government.

A technology asset storage facility is a designated space or floor of an entity's building used to house the entity's technology systems, information technology and operational technology equipment and their components. These facilities include:

- server and gateway rooms
- datacentres
- storage areas for equipment that hold, store, process or communicate official information, and
- communication and patch rooms.

See Construct or Lease Entity Facilities.

Requirement 0094 | TECH | All entities | 31 October 2024

Technology assets and their components, classified as SECRET or below are stored in the appropriate Security Zone based on their aggregated security classification or business impact level.

Requirement 0095 | TECH | All entities | 31 October 2024

Technology assets and their components classified as TOP SECRET are stored in suitable SCEC-endorsed racks or compartments within an accredited Security Zone Five area meeting ASIO Technical Note 5/12 – Compartments within Zone Five areas requirements.

Requirement 0096 | TECH | All entities | 31 October 2024

Outsourced facilities that house technology assets and their components with a catastrophic business impact level are certified by ASIO-T4 physical security and accredited by ASD before they are used operationally.

13.8.1 Technology Asset Housed in Security Zone

The physical security requirements of containers required to house technology assets and their components, other than mobile devices, in security zones are detailed in Table 22. See Minimum Protections and Handling Requirements for storage of mobile devices.

See International Entity Facilities (including Missions and Posts) for arrangements.

Table 22: Storage Container Requirements for Technology Assets (other than mobile devices)

Business Impact Level of Aggregated Information	Security Zone	Security Container
OFFICIAL – Low business impact	Zone Two	Lockable commercial cabinet

Business Impact Level of Aggregated Information	Security Zone	Security Container
	Zone One	Lockable commercial cabinet
OFFICIAL: Sensitive – Low to medium business impact	Zone Two	Lockable commercial cabinet
	Zone One	SCEC Class C
PROTECTED – High business impact	Zone Four and Five	Lockable commercial cabinet
	Zone Three	SCEC Class C (recommended)
	Zone Two	SCEC Class C
SECRET – Extreme business impact	Zone Four	SCEC Class C
	Zone Three	SCEC Class B
TOP SECRET – Catastrophic business impact	Zone Five	SCEC Class B

13.8.2 Technology Asset Housed in Layered Security Zones

The physical security of containers required to house technology assets and their components may be lowered when the facility is a separate Security Zone (secondary Security Zone) within an existing Security Zone (primary Security Zone) that is suitable for the aggregation of the information held.

Table 23: Layered Storage Container Requirements for Technology Assets (other than mobile devices)

Classification/Business Impact Level of Aggregated Information	Primary Security Zone	Layered Security Zones (additional Security Zone housed in primary Security Zone)	
		Secondary Security Zone	Security Container in Secondary Security Zone
OFFICIAL – Low business impact	Zone Two	No additional zone required	Lockable commercial cabinet
	Zone One	Zone Two or above	Lockable commercial cabinet
OFFICIAL: Sensitive – Low to medium business impact	Zone Two	No additional zone required	Lockable commercial cabinet
	Zone One	Zone Two or above	Lockable commercial cabinet
PROTECTED – High business impact	Zone Four and Five	No additional zone required	Lockable commercial cabinet
	Zone Three	No additional zone required	SCEC Class C (recommended)
	Zone Two	Zone Three or above	Lockable commercial cabinet
		Zone Two	SCEC Class C
SECRET – Extreme business impact	Zone Four	Zone Three or above	Lockable commercial cabinet
		Zone Two	SCEC Class C
	Zone Three	Zone Four or above	Lockable commercial cabinet
		Zone Three	SCEC Class C
		Zone Two	SCEC Class B
TOP SECRET – Catastrophic business impact	Zone Five	Sensitive Compartmented Information Facilities	SCEC Class C

13.9 Technology Assets Disposal

Entities may need to dispose of physical technology assets due to advances in technology, the end of the usable life of the physical technology asset, downsizing or changes in business requirements.

Entities must dispose of physical technology assets securely. Prior to decommissioning and disposal of physical technology assets such as security containers, cabinets, vaults, strongrooms and secure rooms, the combination

locks (electronic and mechanical) need to be reset to factory settings and the asset is visually inspected to remove all contents from the asset.

Secure disposal of technology assets may be achieved through either sanitisation or destruction in accordance with the Information Security Manual. Entities may also set their own destruction requirements in addition to those detailed in the Information Security Manual.

Requirement 0097 | TECH | All entities | 31 October 2024

Technology assets are disposed of securely in accordance with the Information Security Manual.

13.9.1 Destruction equipment

Destruction equipment is used for security classified information and IT media) so that resultant waste particles cannot be reconstructed to enable the recovery of information.

See the Minimum Protections and Handling Requirements for information on the destruction equipment required for each security classification. See also Information Disposal for details on the methods for secure destruction of information in physical form, including the destruction of security classified information.

13.10 Innovative Technologies

The Australian Government embraces innovative and emerging technologies that support efficiencies and new ways of working. There are many projects across government seeking to harness these technologies to deliver world-class capabilities and services for Australians.

Innovative technologies encompasses a wide range of fields and types and present both an opportunity and a risk. Due to the rapid pace of their development and adoption, they can present significant security risks that must be appropriately managed to ensure the protection of Australian Government people, information and resources.

Examples of innovative technologies include:

- artificial intelligence (AI) technologies
- quantum technologies, and
- connected peripheral technologies.

This list is non-exhaustive and will continue to grow as Australia's technology estate develops and expands.

13.10.1 Artificial Intelligence

Artificial Intelligence (AI) is a broad field of technologies that enable machines to perform tasks that replicate human cognitive abilities such as problem solving, decision making, comprehension and learning. AI technologies present significant opportunities but must be managed to protect against security and privacy risks to the Australian Government due to the potential collection and exploitation of user and device data.

The Organisation for Economic Co-operation and Development defines AI technologies as any machine-based technology that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.

AI technologies can perform both simple and complex tasks with varying levels of autonomy in decision-making and adaptability. These tasks may traditionally require human intelligence, such as visual perception and speech recognition, or may extend beyond human capabilities such as quickly reading and summarising vast quantities of data.

The Digital Transformation Agency (DTA) is responsible for coordinating whole of government policy on the safe and responsible adoption of AI by the APS. The DTA's Policy for the Responsible Use of AI in Government applies, with some exceptions, to all entities and is the first step to position government as an exemplar in the safe and responsible use of AI, in line with the Australian community's expectations.

AI technologies, like any other technologies in the Commonwealth, is required to follow the technology system authorisation process, regardless of whether they are internally or externally hosted or managed. Table 21 details the security assessment and authorisation required for technology systems to operate or be used by an entity. The relevant security assessor and authorising officer required for an AI technology to operate will depend on whether it is internally or externally hosted and managed.

In addition to Table 21, the following PSPF Requirements also apply when adopting AI technologies, including those located outside of the entity's direct control (i.e. outside of the entity's network or security domain):

- PSPF Requirement 0039 to ensure procurement and contract decisions do not expose the entity or the Australian Government to an unacceptable level of risk (see Procurement, Outsourcing and Contract Management).
- PSPF Requirement 0040 to ensure procurement, contracts and third-party outsourced arrangements, contain proportionate security terms and conditions to ensure service providers, contractors and subcontractors comply with relevant PSPF Requirements and avoid exposing the entity or the Australian Government to an unacceptable level of risk (see Procurement, Outsourcing and Contract Management).
- PSPF Requirement 0046 to ensure procurement and contract decisions consider the security risks before engaging providers operating under foreign ownership, control or influence, and in response to any developments during the contract period that may give rise to foreign ownership, control or influence risks (see Foreign Ownership, Control or Influence in Procurement).
- PSPF Requirement 0049 to manage the security risk associated with engaging foreign partners if the AI technology is not Australian owned and operated (see Recognising Foreign Interference and Espionage).
- PSPF Requirement 0062 to protect security classified information (see Minimum Protections and Handling Requirements).
- PSPF Requirement 0086 to authorise the AI technology system to operate (see Technology System Authorisation).
- PSPF Requirement 0087 to inform decisions to authorise (or reauthorise) a new technology system or make changes to an existing technology system based on the Information Security Manual's risk-based approach to cyber security (see Technology System Authorisation).

13.10.2 Quantum Computing

Quantum computing is able to perform mathematic computations simultaneously and process vast amounts of data at speeds greater than is possible for classical computers. Quantum computing has the potential to enhance AI technologies and machine learning capabilities due to the computation power provided by quantum computing processing.

13.10.2.1. Cryptographically Relevant Quantum Computers

Cryptographically relevant quantum computers (CRQC) are capable of successfully executing attacks against traditional cryptographic systems. The most commonly used encryption for securing communications and data

are enabled through asymmetric and symmetric cryptographic algorithms, commonly known as public-key and private-key cryptography, respectively.

Public-key cryptographic technology is ubiquitous in contemporary secure communications technologies and encryption standards. Many of the most commonly used algorithms are theoretically not secure against cryptographically relevant quantum computing attacks.

Cryptographically relevant quantum computers pose a significant risk to security classified information that is stored on technology resources that rely on public-key cryptography. Australian Government security classified information is encrypted and therefore currently remains secure if it is intercepted or stolen by malicious threat actors. However, this information is at risk if stored until a cryptographically relevant quantum computer is developed, as it could then be decrypted and exposed to compromise.

Post-Quantum encryption algorithms have been designed to ensure encrypted information and data is secure against cryptographically relevant quantum computers.

13.10.2.2. Post-Quantum Cryptographic Algorithms

Post-quantum cryptographic (PQC) algorithms are designed to be resistant to both classical and cryptographically relevant quantum computers and allow technology systems to remain secure if intercepted or stolen. PQC algorithms are able to operate on classical information technology assets and systems and do not require specialised quantum computers to use PQC encryption.

Entities must adopt PQC algorithms during the procurement of new cryptographic equipment and software to ensure Australian Government technology systems are quantum-safe.

See Minimum Protections and Handling Requirements for mandatory encryption required during transmission of security classified information.

Requirement 0212 | TECH | All Entities | 01 July 2025

Approved post-quantum cryptographic encryption algorithms are used for newly procured cryptographic equipment and software in accordance with the Information Security Manual's guidelines for cryptography.

13.10.3 Connected Peripheral Technologies

Peripheral technologies are external assets that can be connected to computers and mobile devices to expand their capabilities and are not a core, non-removable component of the technology.

Connected peripheral technologies are peripheral technology assets that are able to connect to Australian Government technology systems and devices and are also able to connect to the internet through either wireless or wired connections, including through Wi-Fi or cellular networks such as 4G and 5G.

Examples of connected peripheral technologies include connected and autonomous vehicles, drones, and wireless security cameras.

Connected peripheral technologies significantly increase the potential attack surface of Australian Government technology systems and may allow malicious threat actors to utilise cyber security vulnerabilities to expose or extract Australian Government official and security classified information or discussions, or may result in the loss, damage or corruption of Australian Government resources.

Information that is entered into, or is allowed to be accessed by, connected peripheral technologies outside of the entity's controlled technology systems and devices is subject to the privacy policies of the entity that owns and operates the technology. It may also be subject to the extrajudicial directions from a foreign government whose laws conflict with Australian law.

Entities should minimise their exposure to the risks posed by connected peripheral technologies by educating their personnel on the potential vectors of compromise and the appropriate strategies to minimise the harm. Refer to Security Awareness Training.

See PSPF Guidelines for a case study on addressing the security risks of connected peripheral technologies.

Related Standards – Technology Lifecycle Management

- Standard: ASD's Information Security Manual
- Guidance: ASD's Managing the Risks of Legacy ICT: Practitioner Guidance | Cyber.gov.au
- Guidance: DISR's List of Critical Technologies in the National Interest
- Government policy: DTA's Policy for the Responsible Use of AI in Government
- Guidance: Department of Industry, Science and Resources (DISR) Australia's AI Ethics Principles
- Standard: DISR's Voluntary AI Safety Standard | 10 Voluntary Guardrails
- Guidance: Finance's National Framework For The Assurance Of Artificial Intelligence In Government
- Guidance: ASD's An Introduction to Artificial Intelligence and Engaging with Artificial Intelligence
- Guidance: ASD's Deploying AI Systems Securely
- Guidelines: DISR's National Quantum Strategy
- Guidelines: DISR's Guiding Principles for a Global Quantum Ecosystem Informed by Science
- Guidelines: ASD's Guidelines for Cryptography

  Guidelines: ASD's Planning for Post-Quantum Cryptography

14 Cyber Security Strategies

14.1 Cyber Security Strategy

Cyber threats faced by the Australian Government include both external and internal malicious actors that steal data, destroy data or attempt to prevent technology systems from functioning. The most common cyber threat entities face is external malicious actors who attempt to steal data. Often these malicious actors attempt to access technology systems and data through malicious emails and websites. It is critical that entities safeguard the data held on technology systems that can receive emails or browse internet content.

A cyber security strategy articulates the entity's plans and priorities for cyber security uplift to manage cyber security risks. Achieving and maintaining effective cyber security mitigations requires investment, sufficient capability and clear objectives.

The CISO's biannual update to the Audit Committee on the entity's cyber security strategy and uplift plan should be provided as a report for the Committee's consideration. The progress reports at each Audit Committee meeting may be provided verbally if preferred.

Requirement 0098 | TECH | All entities | 01 July 2025

A cyber security strategy and uplift plan is developed, implemented and maintained to manage the entity's cyber security risks in accordance with the Information Security Manual and the Guiding Principles to Embed a Zero Trust Culture.

Requirement 0213 | TECH | All entities | 01 July 2025

The Chief Information Security Officer reports on the entity's cyber security risk at each meeting of the Audit Committee and biannually on the progress of the cyber security strategy and uplift plan.

14.1.1 Zero Trust Culture

PSPF Requirement 0098 requires that a cyber security strategy and uplift plan is developed, implemented and maintained to manage the entity's cyber security risks in accordance with the ISM and the Guiding Principles to Embed a Zero Trust Culture. These principles are outlined in Table 24.

Entities must embed a Zero Trust Culture through the Guiding Principles to ensure that current and emergent risks stemming from a rapidly evolving cyber threat landscape and expansion of an entity's digital attack surface are appropriately managed through entity-wide transformation. An effective Zero Trust Culture provides personnel with a clear understanding of roles and responsibilities and provides a consistent experience across information technology systems.

The Guiding Principles to Embed a Zero Trust Culture define governance principles that establish an entity's organisational-wide functions and activities required to underpin successful application of the Zero Trust concepts beyond purely technical cyber security strategies. These principles draw from existing best practices and frameworks, and reflect key areas that need to be strengthened to ensure cyber security resilience across the Commonwealth.

Table 24: Guiding Principles to Embed a Zero Trust Culture

Principles	Description
Principle 1 - Identify and manage cyber security risk at an enterprise level	Principle 1 increases the resiliency of the resiliency of the Australian Government's digital landscape by ensuring cyber security risk is considered at an enterprise level. In a world of digitalising services, managing cyber security risk should not

Principles	Description
	be considered the responsibility of the CISO, but should be managed at the enterprise level.
Principle 2 - Understand accountabilities and responsibilities at all levels	Principle 2 enacts clearly defined roles and responsibilities as they are fundamental in establishing strong governance and maintaining accountability mechanisms. This enforces a commitment for cultural change from the top down and implements well defined reporting pathways to circulate information on incidents, identified risks, and emerging trends, allowing swift response and adaptation to evolving threat environment.
Principle 3 - Know and understand your most critical and sensitive technology assets	Principle 3 drives understanding and appropriate protection to give context on entity's critical and sensitive technology assets. This supports prioritisation and mitigation of critical risk. To ensure proper protection of critical assets, it's crucial to implement continuous education and training, ensuring staff at all levels can respond to cyber threats in the moment. This enables a proactive, risk-based approach, rather than reactive compliance.
Principle 4 - Maintain resiliency through a comprehensive cyber strategy and uplift plans	Principle 4 focuses on uplifting cyber security resilience which requires development and maintenance of a robust cyber strategy. The strategy needs to be constructed on current and predicted future threat trends, as well as risks and dependencies tied to key third-party suppliers. The strategy should be incorporated through investment plans, ensuring uplift activities are comparable to planned digital investment and business operation changes.
Principle 5 - Go beyond incident planning	Principle 5 ensures incident management goes beyond a traditional preparation, containment and eradication focus, while also driving continuous improvement in the entity's cyber posture. Cyber incident planning must be built on the premise that no system or user is inherently secure, and all system access should be continuously verified. This mentality should be ingrained in an entity's entire operational framework.

14.2 Essential Eight Strategies

The Australian Signals Directorate has developed prioritised mitigation strategies, Strategies to Mitigate Cyber Security Incidents, to help protect against various cyber threats. The most effective of these mitigation strategies are the Essential Eight.

The Essential Eight is designed to protect internet-connected information technology networks. While the principles behind the Essential Eight may be applied to enterprise mobility and operational technology networks, it was not designed for such purposes and alternative mitigation strategies may be more appropriate to defend against unique cyber threats to these environments.

Entities are required to implement the Essential Eight strategies to Maturity Level Two under ASD's Essential Eight Maturity Model and consider which of the remaining 29 Strategies to Mitigate Cyber Security Incidents are required to address the entity's threats.

14.2.1 Patch Applications

A patch is a piece of software designed to fix problems or update an application or operating system. This includes fixing security vulnerabilities or other deficiencies as well as improving the usability or performance of an application or operating system.

Temporary workarounds or alternative mitigations are required for applications that are no longer supported by vendors to prevent exposing the government to high risk.

Requirement 0099 | TECH | All entities | 31 October 2024

Patch applications mitigation strategy is implemented to Maturity Level Two under ASD's Essential Eight Maturity Model.

14.2.2 Patch Operating Systems

Applying patches to operating systems is critical to ensuring the security of technology systems.

Temporary workarounds or alternative mitigations are required for operating systems that are no longer supported by vendors to prevent exposing the government to high risk.

Requirement 0100 | TECH | All entities | 31 October 2024

Patch operating systems mitigation strategy is implemented to Maturity Level Two under ASD's Essential Eight Maturity Model.

14.2.3 Multi-Factor Authentication

Multi-factor authentication is used to authenticate users to the entity's online services and technology systems that process, store or communicate OFFICIAL and security classified data. Multi-factor authentication uses two or more different authentication factors. This mitigation is one of the most effective controls an entity can implement to prevent an adversary from gaining access to an online service or technology system and accessing OFFICIAL or security classified data. When implemented correctly, multi-factor authentication can make it significantly more difficult for an adversary to steal legitimate credentials to facilitate further malicious activities on an online service or technology system.

Requirement 0101 | TECH | All entities | 31 October 2024

Multi-factor authentication mitigation strategy is implemented to Maturity Level Two under ASD's Essential Eight Maturity Model.

14.2.4 Restrict Administrative Privileges

User accounts with administrative privileges are an attractive target for malicious actors because they have a high level of access to an entity's technology systems and data. Restricting administrative privileges makes it difficult for malicious actors to spread or hide their existence.

Privileged accounts that cannot access emails or open attachments, cannot browse the internet, or obtain files via internet services (such as instant messaging or social media) minimise opportunities for these accounts to be compromised.

Requirement 0102 | TECH | All entities | 31 October 2024

Restrict administrative privileges mitigation strategy is implemented to Maturity Level Two under ASD's Essential Eight Maturity Model.

14.2.5 Application Control

Malicious code (malware) often aims to exploit vulnerabilities in existing applications and does not need to be installed on workstations or servers to be successful. If appropriately configured, application control helps to prevent undesired execution of software regardless of whether the software was downloaded from a website, clicked on as an email attachment or introduced via CD/DVD/USB removable storage media.

Requirement 0103 | TECH | All entities | 31 October 2024

Application control mitigation strategy is implemented to Maturity Level Two under ASD's Essential Eight Maturity Model.

14.2.6 Restrict Microsoft Office Macro Settings

Microsoft Office files can contain embedded code known as a macro. A macro can contain a series of commands that can be coded or recorded, and replayed at a later time to automate repetitive tasks. An adversary can also create macros to perform a variety of malicious activities, such as assisting to compromise workstations in order to exfiltrate or deny access to OFFICIAL or security classified data.

Requirement 0104 | TECH | All entities | 31 October 2024

Restrict Microsoft Office macros mitigation strategy is implemented to Maturity Level Two under ASD's Essential Eight Maturity Model.

14.2.7 User Application Hardening

This mitigation strategy significantly helps to reduce the attack surface of users' workstations. It also helps to mitigate malicious actors using malicious content in an attempt to evade application control by either exploiting an application's legitimate functionality, or exploiting a vulnerability for which a vendor patch is unavailable.

Requirement 0105 | TECH | All entities | 31 October 2024

User application hardening mitigation strategy is implemented to Maturity Level Two under ASD's Essential Eight Maturity Model.

14.2.8 Regular Backups

Regular backups ensure that entities are able to recover their technology systems and data in the event of a disruptive or destructive cyber security incident. The backups include all important data, software and configuration settings for software, network devices and other IT equipment.

Requirement 0106 | TECH | All entities | 31 October 2024

Regular back-ups mitigation strategy is implemented to Maturity Level Two under ASD's Essential Eight Maturity Model.

14.2.9 Remaining Strategies

While the remaining mitigation strategies from the Strategies to Mitigate Cyber Security Incidents are not mandatory, entities must consider each of these strategies and implement those that are needed to protect the entity.

The suggested implementation order for the remaining strategies is:

- targeted cyber intrusions and other external malicious actors who steal data
- ransomware denying access to data for monetary gain, and external malicious actors who destroy data and prevent computers/networks from functioning
- malicious insiders who steal data such as customer details or intellectual property, and
- malicious insiders who destroy data and prevent computers/networks from functioning.

When implementing a mitigation strategy, first implement it for high risk users and computers such as those with access to important (security classified or high-availability) data, and then implement it for all other users and computers.

Requirement 0107 | TECH | All entities | 31 October 2024

The remaining mitigation strategies from the Strategies to Mitigate Cyber Security Incidents are considered and, where required, implemented to achieve an acceptable level of residual risk for their entity.

14.3 Alternate Cyber Security Standards

There are a number of other Australian and International Standards that aim to protect against cyber security-related risks, including ISO/IEC 27001 Information Technology – Security Techniques - Information Security Management Systems. While alternative standards are useful as a resource, they are not specifically targeted for the Australian Government and are not suitable for use as an alternative authorisation to operate pathway.

Entities that elect to rely on these alternate standards are required to detail why it was necessary to deviate from ASD's Information Security Manual and Strategies to Mitigate Cyber Security Incidents in their annual report on security to their minister and the Department of Home Affairs.

Related Standards – Cyber Security Strategies

- Standard: ASD's Strategies to Mitigate Cyber Security Incidents
- Standard: ASD's Essential Eight Maturity Model
- Guidance: ASD's Secure-by-Design Foundations
- Guidance: ASD's Modern Defensible Architecture
- Guidance: ASD's Foundations for Modern Defensible Architecture | Zero Trust Principles
- Guidance: ISO/IEC 27001 Information Technology – Security Techniques - Information Security Management Systems (available to purchase from International Organization for Standardization)

15 Cyber Security Programs

15.1 Whole of Government Cyber Security Services

Protective Domain Name System (PDNS) services, or other security mechanisms that use reputation or content categorisation, must be used to block connections to and from known malicious endpoints.

A PDNS service can be an effective way of blocking connection made by an entity's technology system, or a malicious actor on an entity's technology system, to known malicious domains – either as part of an initial compromise or subsequent command and control activities. Domain Name System (DNS) event logs captured by a PDNS service can also be useful for investigating an exploitation attempt or successful compromise of a technology system.

The Australian Signals Directorate offers select Commonwealth entities a PDNS service, known as Australian Protective Domain Name Service (AUPDNS), free of charge. Commercial offerings are also available.

Requirement 0108 | TECH | All entities | 31 October 2024

A Protective Domain Name System service or other security mechanisms is used to prevent connections to and from known malicious endpoints.

15.2 Secure Cloud

The Department of Home Affairs' Secure Cloud Strategy and ASD's suite of cloud security publications provides guidance on adopting cloud computing. At its core, cloud computing involves outsourcing a part, or all, of an entity's IT capability to a cloud service provider. This outsourcing brings a reduction in control and oversight of the technology stack, as the service provider dictates both the technology and operational procedures available to the cloud consumers using its cloud services.

Requirement 0109 | TECH | All entities | 31 October 2024

Cloud Service Providers that have completed an IRAP assessment against the latest version of ASD's Information Security Manual within the previous 24 months are used.

Requirement 0110 | TECH | All entities | 31 October 2024

Entities consider IRAP assessment recommendations and findings, and implement on a risk-based approach.

15.2.1 Hosting Certification Framework

The Department of Home Affairs' Australian Government Hosting Certification Framework provides policy guidance on securely hosting government data using cloud services or data centres and associated infrastructure. The Hosting Certification Framework reduces risks associated with access to information and data, supply chain of processed, stored or communicated information and data, and ownership and control of services providers.

While using outsourced data centre services or cloud computing can significantly enhance an entity's cyber security, they also presents other risks that need to be considered and managed. Entities electing to use cloud computing services or data centre services are required to use Hosting Certification Framework certified suppliers for security classified government information and data, a whole of government system or system rated at the classification levels of OFFICIAL: Sensitive and PROTECTED. Entities may use the services of an uncertified provider for non-sensitive government information (OFFICIAL) and commercial information and data.

Entities seeking to use SECRET or TOP SECRET cloud services must only use community or private clouds in accordance with the Information Security Manual.

Requirement 0111 | TECH | All entities | 01 July 2025

Security classified or systems of government significance information and data is securely hosted using a Cloud Service Provider and Data Centre Provider that has been certified against the Australian Government Hosting Certification Framework.

15.2.2 Data Centres

The Department of Home Affairs assesses outsourced data centre providers and cloud service providers against the Hosting Certification Framework, and maintains a list of certified service providers.

When buying data centre space and services, non-corporate Commonwealth entities are required to use the DTA's Data Centre Facilities Supplies Panel. DTA's 'BuyICT Portal' leverages the Data Centre Facilities Supplies Panel for buying certified data centre space and services.

See Procurement, Outsourcing and Contract Management.

Requirement 0112 | TECH | All entities | 31 October 2024

The Data Centre Facilities Supplies Panel is used when procuring certified data centre space and services.

15.2.3 Offshore or Foreign-Owned Cloud Services and Managed Service Providers

Foreign ownership of a managed service provider or cloud service provider presents risks to data. An entity's ability to manage and control resources in an outsourced, offshore or supply chain arrangement is impacted by the service provider's locality, ownership and control. These arrangements need to be considered as part the entity's assessment to determine if the service provider is suitable for handling its data.

Foreign-owned service providers may be subject to extrajudicial control and interference by a foreign entity. This could include a foreign entity compelling a service provider to disclose its customers' data unbeknownst to its customers.

The service provider's administration arrangements and location where support is provided from should also be considered. Depending on the locations, this can impact personnel pre-employment screening practices, as different countries have different laws about the degree of data that employers can request from their employees.

See Australian Signals Directorate's Cloud Assessment and Authorisation and ASIO's Protective Security Circular 149— Physical security certification of outsourced information and communications technology facilities (on GovTEAMS).

15.3 Gateway Security

The Department of Home Affairs' Australian Government Gateway Security Standard details security protections and capabilities between security domains. A gateway is a data flow control mechanism that has a set of capabilities responsible for securely managing data flows between connected networks from different security domains within an entity's technology systems. The Australian Government Gateway Security Standard details the strategic direction and minimum standards for gateways and security service edges across the Australian Government.

Gateways play a vital role in securing a technology system by providing entities with protection at its perimeter. However, they are only one element of a layered defensive strategy. Gateways can be shared between multiple

entities, providing the benefits of a common suite of cyber security defences. As such, threats to technology systems (for example, distributed denial of service attacks, botnets, malware, web application attacks and web-based attacks) can be efficiently mitigated through appropriately configured gateways. At the same time, entities may require the flexibility to source additional security services in a manner that best suits their operational needs and risk environment.

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.

15.4 Vulnerability Disclosure Program

A vulnerability disclosure program (VDP) is a collection of processes and procedures designed to identify, verify, resolve and report on vulnerabilities disclosed by both internal and external sources.

Implementing a vulnerability disclosure program, based on responsible disclosure, can assist entities, vendors and service providers to improve the security of their products and services as it provides a way for security researchers, customers and members of the public to responsibly notify them of potential vulnerabilities in a coordinated manner. Furthermore, following the verification and resolution of a reported vulnerability, it can assist entities, vendors and service providers in notifying their customers of any vulnerabilities that have been discovered in their products and services and any recommended security patches, updates or mitigations.

Requirement 0115 | TECH | All entities | 31 October 2024

A vulnerability disclosure program and supporting processes and procedures are established to receive, verify, resolve and report on vulnerabilities disclosed by both internal and external sources.

15.5 Cyber Security Partnership Program

ASD's Cyber Security Partnership Program enables Australian organisations and Government entities to engage with the ASD's Australian Cyber Security Centre (ACSC) and fellow partners, drawing on collective understanding, experience, skills and capability to uplift cyber security and resilience across the Australian economy.

The program is available free-of-charge to cyber security professionals across government, industry, academia and research sectors. It provides access to threat information, news, advice, collaboration opportunities, and resilience building activities.

See ASD's Cybersecurity Partnership Program for more details.

Requirement 0215 | TECH | All entities | 01 July 2025

Participate in the Australian Signals Directorate's Cyber Security Partnership Program and notify ASD in the event of a change in the entity's risk profile.

15.6 Cyber Threat Intelligence Sharing Platform

ASD's Cyber Threat Intelligence Sharing (CTIS) platform is a two-way sharing platform that enables government and industry partners to receive and share information about malicious cyber activity at machine speed. CTIS conveys unclassified structured threat intelligence in multiple formats: Structured Threat Information eXpression (STIX) v2.1 and Malware Information Sharing Platform (MISP).

Connecting to the CTIS platform does not give ASD access to the entity's system. The sharing process is a push request from the entity. Entities have the authority to share, or not share, the data and the malicious indicators of compromise or sightings. However, entities are strongly encouraged to share with ASD and it will assist ASD to build the threat landscape.

Connecting to CTIS enables entities to receive and share threat intelligence with ASD, industry and government partners.

Requirement 0216 | TECH | All entities | 01 July 2025

Connect to the Australian Signals Directorate's Cyber Threat Intelligence Sharing platform.

15.7 Systems of Government Significance

The Department of Home Affairs' Australian Government Systems of Government Significance Standard (available on GovTEAMs) details the mandatory cyber security obligations for protecting systems or services that are declared as Systems of Government Significance (SoGS).

The SoGS regime identifies and priorities the Australian Government's most critical digital services and the underlying supporting systems. SoGS are declared based on an assessment of their centrality to government functions and services, the scale of interdependencies to other systems and the potential for significant and cascading consequences to Australia's national security, economic prosperity or social cohesion if disrupted.

SoGS are declared by the Department of Home Affairs and the list is not publicly available.

Entities operating declared SoGS are required to mitigate the risk of undesirable social, economic or national security consequences.

Requirement 0217 | TECH | SOGS | 01 July 2025

Declared Systems of Government Significance are protected in accordance with the Australian Government Systems of Government Significance Standard.

Related Standards – Cyber Security Programs

- Standard: ASD's Information Security Manual
- Standard: Hosting Certification Framework
- Standard: Australian Government Gateway Security Standard
- Standard: Systems of Government Significance Standard (on GovTEAMS)
- Guidance: ASD's Blueprint for Secure Cloud
- Guidance: ASD's Cloud Assessment and Authorisation
- Guidance: ASD's Cloud Computing Security for Executives
- Guidance: ASD's Cloud Computing Security for Tenants
- Guidance: ASIO T4 Security Manager's Guide – Data centre security (on GovTEAMS)

- Guidance: ASIO's Protective Security Circular 149— Physical security certification of outsourced information and communications technology facilities (on GovTEAMS)
- Guidance: Cyber and Infrastructure Security Centre Factsheet - Risks Associated with Offshoring of Data
- Guidance: Cyber and Infrastructure Security Centre Factsheet - Risk Assessment Advisory for critical infrastructure - Data Storage or Processing sector

Part Five

Personnel

Pre-Employment Eligibility

Access to Resources

Security Clearances

Security Vetting Process

Australian Officials and Office Holders

Maintenance and Ongoing Assessment

Separation

Personnel Lifecycle

16 Pre-Employment Eligibility

16.1 Pre-Employment Screening

All personnel working in and for Australian Government entities are required to undergo pre-employment screening, regardless of whether the position requires a security clearance or not. Personnel includes security cleared and non-security cleared personnel, contractors and others who will have access to Australian Government resources (that is technology systems, assets and facilities).

Pre-employment screening provides a level of assurance that personnel are suitable to access Australian Government resources and is a primary activity used to mitigate an entity's personnel security risks. PSPF pre-employment screening checks may be supplemented by entity-specific screening where required.

Pre-employment screening takes place after the conclusion of the merit selection process but prior to an offer of employment or contract. Completing screening prior to engagement is particularly important for positions that have been identified as requiring a security clearance. If an individual is found to be unsuitable as part of the pre-employment and entity-specific screening, entities must not seek a security clearance for the individual. Where checks are not completed prior to engagement, it is recommended that entities make the employment or contract conditional on satisfying the required checks within a reasonable timeframe.

Individuals cannot obtain a security clearance unless they are expected to be engaged in a role requiring a security clearance. Therefore, it is not reasonable to expect an individual to hold a security clearance prior to being selected for a designated role. Selection based on existing clearance status is not merit based and may be contrary to an entity's enabling legislation. Entities that are legislatively required to make employment decisions in accordance with the merit principle cannot discriminate against individuals who do not hold a current security clearance where they indicate a willingness and ability to gain a clearance prior to engagement.

Requirement 0116 | PER | All entities | 31 October 2024

The eligibility and suitability of personnel who have access to Australian Government people and resources is ensured.

16.1.1 Pre-Employment Screening Checks

Pre-employment screening checks, including related security clearance vetting and ongoing suitability checks, are conducted in accordance with the Australian Privacy Principles.

Authorised Vetting Agencies may conduct pre-employment screening concurrently with security vetting to permit streamlined engagement of personnel. If conducted concurrently, the Authorised Vetting Agency should record the vetting determination against the criteria and identify whether a decision relates to a pre-employment screening threshold or a security clearance threshold.

Pre-employment screening checks for personnel transferring within the Australian Government may have already been conducted. The gaining entity should confirm what checks have been undertaken by the losing entity. Additional checks can be done to meet the specific entity employment requirements of the gaining entity or if the check needs to be revalidated.

See Locally Engaged Staff for advice on pre-employment screening arrangements.

16.1.1.1. Identity Checks

An identity check helps to establish confidence in a person's identity and provides entities with a level of assurance about the prospective employee.

The National Identity Proofing Guidelines provide a more robust approach to identity proofing than the traditional '100 point check', and aligns with international best-practice standards.

The National Identity Proofing Guidelines have four levels of assurance. Level of Assurance 3 (high) is the minimum for pre-employment screening identity checks, and includes:

- the uniqueness of the identity in the intended context
- the claimed identity is legitimate
- the operation of the identity in the community over time
- the linkage between the identity and the person claiming the identity, and
- the identity is not known to be used fraudulently.

Verification of a person's claimed identity where no prior government records exist, may be verified with a reputable organisation, trusted referee or bodies known to them. For example, Aboriginal and Torres Strait Islander organisations may not hold, or be able to verify, the identity of clients where no prior government record exists. A trusted referee is a person or organisation that holds a position of trust in the community and does not have a conflict of interest, such as an Aboriginal elder or reputable organisation that the person is a customer, employee or contractor of, and is known and listed by the enrolling agency to perform the function of a referee. The *Statutory Declarations Act 1959* provides a list of people who hold a position of trust in the community. Similar lists are also generally included in state and territory legislation. Trusted referees may also include guardians or other people nominated to act on a person's behalf whose identities have been verified.

Requirement 0117 | PER | All entities | 31 October 2024

The pre-employment screening identity check is conducted for all personnel, to verify identity to at least Level 3 (High) of Assurance of the National Identity Proofing Guidelines.

The *Identity Verification Services Act 2023* (Cth) provides a legislative basis for the operation of the identity verification services. A key element of the identity check is verifying whether the biographic information on the identity document matches the original record through an identity verification solution that checks source documents.

The Document Verification Service's (DVS) identity matching service can verify 14 different types of identity documents, including birth certificates, driver licences and Medicare cards. For information on how to access the DVS, see the Identity Matching Services website. Other source identity verification solutions may be used if they meet the same standard as the DVS.

The entity may omit the identity check in circumstances where obtaining a security clearance prior to engagement is a condition of employment and pre-employment screening is unlikely to be predictive of security clearance suitability.

Requirement 0118 | PER | All entities | 31 October 2024

Biographic information in identity documents is verified to ensure the information matches the original record.

16.1.1.2. Eligibility Check

An eligibility check confirms whether a person is eligible to work in Australia. This requires confirmation that a person holds Australian Citizenship, or if the person is not an Australian citizen, confirming that they have a valid work visa. For information see the *Migration Act 1958*.

Further eligibility conditions, including requirements relating to Australian citizenship, are covered in the *Public Service Act 1999* and in the enabling legislation of many entities.

Australian citizenship is obtained either automatically or by application. Section 17 of the *Australian Citizenship Act 1948* provides that Australians over the age of 18 who took action to acquire the nationality or citizenship of a foreign country between 26 January 1949 and 3 April 2002, automatically ceased to be an Australian citizen. Australians impacted by this change can apply to resume their Australian citizenship. On 4 April 2002, section 17 of the 1948 Act was repealed. This enabled Australian citizens to acquire dual citizenship without losing their Australian citizenship. A dual citizen is a person who holds citizenship of two or more countries.

Information on how to confirm Australian citizenship, apply to resume citizenship and verify visas is available on the Department of Home Affairs website.

Requirement 0119 | PER | All entities | 31 October 2024

The pre-employment screening eligibility check is conducted for all personnel, to confirm their eligibility to work in Australia and for the Australian Government.

Requirement 0120 | PER | All entities | 31 October 2024

The entity obtains assurance of each person's suitability to access Australian Government resources, including their agreement to comply with the government's policies, standards, protocols and guidelines that safeguard resources from harm, during pre-employment screening.

16.1.2 Personnel Transferring within the Australian Government

Pre-employment screening checks for personnel transferring within the Australian Government may have already been conducted. The gaining entity should confirm what checks have been undertaken by the losing entity. Additional checks can be done to meet the specific entity employment requirements of the gaining entity or if the check needs to be revalidated.

Related Standards – Pre-Employment Screening

- Standard: National Identity Proofing Guidelines
- Standard: Office of the Australian Information Commissioner's Australian Privacy Principles
- Service: Australian Government Document Verification Service

17 Access to Resources

The need-to-know principle applies to all security classified information and resources. It reflects the need for personnel to access this information only where there is an operational requirement to do so. The practice helps personnel understand their responsibility to protect information, including the correct methods for storage, handling and dissemination.

17.1 Temporary Access to Resources

Temporary access to classified information may be required in some limited circumstances. Temporary access may be provided up to and including PROTECTED level information without a security clearance, after the risks of doing so have been assessed and for limited time periods. Temporary access to TOP SECRET information requires an existing Negative Vetting 1 security clearance.

There are two types of temporary access to security classified information:

- Short-term temporary access – where the person does not hold a clearance at the appropriate level (but has a valid need-to-know and requires immediate access to relevant information, system or resources) and the risks can be managed. This may include, but is not limited to:
  - new starters
  - people on short-term projects
  - people who are reasonably expected to have only incidental or accidental contact with security classified information (e.g. security guards, cleaners, external IT personnel, researchers and visitors such as children who do not have an ability to comprehend the classified information, that is children aged under 10 years of age)
- Provisional temporary access – where the person has commenced a clearance process by providing the relevant details for assessment by an Authorised Vetting Agency, and immediate access is urgently required. Provisional temporary access can be maintained until a security clearance is granted or denied.

Short-term access can be changed to provisional once the Authorised Vetting Agency has confirmed that the completed security clearance pack has been received and advises the entity that no initial concerns have been identified.

See Australian Government Personnel Security Adjudicative Standard for further guidance.

Requirement 0121 | PER | All entities | 31 October 2024

Prior to granting temporary access to security classified information or resources, pre-employment checks are completed, and an existing Negative Vetting 1 security clearance is confirmed prior to granting temporary access to TOP SECRET information data or resources.

17.1.1 Temporary Access Risk Assessment

Temporary access may only be granted after a security risk assessment has been completed and if security risks arising from the proposed action are identified, they are assessed as manageable.

When conducting a risk assessment for temporary access, the entity must consider:

- the need for temporary access, including if the role can be performed by a person who already holds the necessary clearance

- confirmation from the Australian Government Security Vetting Agency (AGSVA) of the person's security clearance and status ensuring that they haven't previously had a security clearance cancelled or denied, separate from PSPF Requirement 0125potential conflicts of interest
- the period of access under consideration, noting the time limitations imposed on short-term access
- proposed risk management measures, including any conditions placed on the clearance holder subject to the waiver or temporary access.
- the quantum and classification level of matters that could be accessed, and the potential business impact if these matters were compromised
- how access to classified information will be supervised, including how access to caveat or compartmented classified information will be prevented, and
- other risk mitigating factors such as pre-engagement screening, entity specific character checks, and knowledge of personal history, previous security clearance issues of concern, and security breaches.

Requirement 0122 | PER | All entities | 31 October 2024

A risk assessment determines whether a person is granted temporary access to security classified information or resources.

17.1.2 Supervise Temporary Access

Entities must supervise all temporary access. Examples include:

- escorting visitors in premises where classified information is being stored or used
- oversight of the work completed by personnel with temporary access, and
- monitoring or audit logging of incidences of contact with security classified information (e.g. contract conditions that require service providers to report when any of their contractors have had contact with security classified information or activities).

Requirement 0123 | PER | All entities | 31 October 2024

Temporary access to security classified information, resources and activities is supervised.

17.1.3 Limit Duration of Temporary Access

Entities must limit the duration of access to security classified information as follows:

- Short-term access – an individual can be granted access for a total combined maximum of 3-months in a 12-month period for all entities (e.g. Entity A: 2 months, and Entity B: one month), and
- Provisional access – an individual can be granted access until a security clearance is granted or denied.

Requirement 0124 | PER | All entities | 31 October 2024

Short-term temporary access to security classified information, resources and activities is limited to the period in which an application for a security clearance is being processed for the particular person, or up to a total combined maximum of three months in a 12-month period[12] for all entities.

[12] 12-months refers to the preceding 12-months from the date the short-term access would be granted.

Short-term access can be changed to provisional once the Authorised Vetting Agency has confirmed that the completed security clearance pack has been received and advises the entity that no initial concerns have been identified.

Requirement 0125 | PER | All entities | 31 October 2024

The Authorised Vetting Agency confirms that the completed security clearance pack has been received, and that no initial concerns have been identified for the clearance subject, before short-term temporary access is changed to provisional temporary access.

In exceptional circumstances, short-term or provisional access to caveated classified information may be granted by the originator and caveat owner (controlling authority) based on the assessed risk and granted on a case-by-case basis.

Requirement 0126 | PER | All entities | 31 October 2024

Temporary access to classified caveated information, resources or activities is not granted, other than in exceptional circumstances, and only with the approval of the caveat controlling authority.

Requirement 0127 | PER | All entities | 31 October 2024

Prior to granting temporary access, the entity obtains an undertaking from the person to protect the security classified information, resources and activities they will access.

Requirement 0128 | PER | All entities | 31 October 2024

Prior to granting temporary access, the entity obtains agreement from any other entity (or third party) whose security classified information, resources and activities will be accessed by the person during the temporary access period.

17.2 Ongoing Access to Resources

Ongoing access to government information or resources must be appropriately controlled, especially when accessing security classified information outside the entity's facilities or providing access to non-government personnel.

In addition to requiring a need-to-know basis, ongoing access to security classified information is limited to personnel with the necessary security clearance. See Table 25 for details on the Australian Government security clearance levels required for ongoing access security classified information, resources and activities.

Personnel require an appropriate employment screening check for access to OFFICIAL: Sensitive information.

Some Australian office holders are not required to hold a security clearance. See Clearance Exemptions for Australian Officials and Office Holders.

Requirement 0129 | PER | All entities | 31 October 2024

Access to official information is facilitated for entity personnel and other relevant stakeholders.

Requirement 0130 | PER | All entities | 31 October 2024

Appropriate access to official information is enabled, including controlling access (including remote access) to supporting technology systems, networks, infrastructure, devices and applications.

Requirement 0131 | PER | All entities | 31 October 2024

Access to security classified information or resources is only given to entity personnel with a need-to-know that information.

Requirement 0132 | PER | All entities | 31 October 2024

Personnel requiring ongoing access to security classified information or resources are security cleared to the appropriate level.

Requirement 0133 | PER | All entities | 31 October 2024

Personnel requiring access to caveated information meet any clearance and suitability requirements imposed by the originator and caveat controlling authority.

Requirement 0134 | PER | All entities | 31 October 2024

A unique user identification, authentication and authorisation practice is implemented on each occasion where system access is granted, to manage access to systems holding security classified information.

17.3 Remote Access to Resources

A service-wide, principles-based approach to working flexibility in the APS was endorsed by the Secretaries Board in March 2023. A common clause on flexible working arrangements has been included in all APS enterprise agreements.

17.3.1 Working Remotely in Australia

Working remotely for the purposes of the PSPF, is defined as all work outside of the entity's facilities in Australia using either portable mobile devices or remote access to the entity's services, information and technology systems. Working remotely includes home-based work, working in another government entity's facilities in Australia, and field work undertaken on behalf of the entity by contractors, but does not include any work undertaken by contractors in their own facilities.

17.3.1.1. Working from Home

Flexible work is a core part of the way the APS does business, including access to working from home arrangements where it is agreed to do so. Under the *Fair Work Act 2009* and the common clause on flexible working arrangements, which has been largely replicated in APS enterprise agreements, requests to work from home can only be denied on reasonable business grounds. The common clause provides examples of reasonable business grounds, including where it would not be possible to accommodate the working arrangements without significant changes to security requirements. In making decisions about working from home arrangements, the delegate must comply with the *Fair Work Act 2009* and the relevant entity's enterprise agreement. This supports the Accountable Authority to ensure operational requirements are met and the entity's services continue to be delivered.

Remote working arrangements to support home-based work must adhere to the Minimum Protections and Handling Requirements mandated for Working Remotely in Australia (including home-based work).

17.3.1.2. Working in Another Government Entity's Facilities in Australia (Hosted or Co-location Arrangements)

The Accountable Authority is responsible for safeguarding the entity's people and resources from harm or compromise. In order to fulfil these requirements, the Accountable Authority needs to maintain control over where the entity's people and resources are located, and the security decisions relating to these locations.

When making property decisions in line with the Commonwealth Property Management Framework (such as the effective and efficient use of office space through co-locating staff within another entity's property, locating another entity's staff in their property or wholly assigning a lease to or from another entity) the accountable authority needs to assess the security risks associated with these arrangements, and consider the environment in

which the other entity operates, its security culture and practice and the type of information that will be used in the facilities. Co-location or hosted arrangements must adhere to the Minimum Protections and Handling Requirements. The Accountable Authority, with support from the CSO, remains responsible even where personnel or resources are located or hosted in another Government entity's facilities.

Requirement 0135 | PER | All entities | 31 October 2024

A security risk assessment of the proposed location and work environment informs decisions by the Chief Security Officer to allow personnel to work in another government entity's facilities in Australia.

Requirement 0136 | PER | All entities | 31 October 2024

An agreement is in place to manage the security risks associated with personnel working in another government entity's facilities in Australia.

17.3.2 Working Remotely Outside of Australia (International)

Working remotely outside of Australia includes working at entity facilities located internationally, Australian Government international missions and international posts, including those managed by Department of Foreign Affairs and Trade (DFAT), and remote home-based work outside of an Australian Government entity facility, mission or post.

17.3.2.1. Working Inside an Australian Government International Entity Facility, Mission or Post

In accordance with the Prime Minister's Directive on Guidelines for Management of the Australian Government Presence Overseas, DFAT is responsible for all aspects of security policy affecting Australian missions and staff attached to DFAT-managed missions. International entity facilities managed entities other than DFAT are the responsibility of the entity managing the facility.

All Australian Government international missions and international posts, including those managed by DFAT are required to meet the PSPF requirements, unless a specific legislative provision allows for alternative arrangements. See International Entity Facilities (including Missions and Posts).

17.3.2.2. Working Outside of an Australian Government International Entity Facility, Mission or Post

Security considerations are key when making decisions about the geographic location of personnel, particular in working overseas.

Not all locations are suitable for international remote work arrangements, particularly countries that have extensive collection of user data or are subject to extrajudicial directions from a foreign government that conflict with Australian law. Contact ASIO for country-specific threat assessment advice from the National Intelligence Community.

Decisions to approve extended working remotely at international location arrangements must not expose government information, data or systems to compromise or unacceptable risk. Entities that choose to allow their personnel to work remotely at international locations for extended periods (i.e. not for short-term travel) must assess and record the risk in each instance and ensure the remote facilities meet the minimum protections and handling requirements for the classification of information.

The Minimum Protections and Handling Requirements for Australian Government security classified information and resources do not change when personnel are working overseas. The same PSPF requirements must be met. In fact, international remote working arrangements are likely to increase the security risks and may lead to unexpected exposure to insider threat and compromise of information's confidentiality.

Each request requires a risk assessment to determine whether the country and the proposed work environment (including the workspace, IT equipment, access, storage facilities and connectivity) are sufficient to meet the requirements of the PSPF and ISM. It would be challenging to work with information and mobile devices at the PROTECTED level and above, in workspaces outside of an Australian Government international facility, post, chancery, embassy or consulate.

Contact the DFAT for advice, as it is responsible for security arrangements at international posts, including providing security awareness training for Australian Government personnel deployed or posted overseas.

Requirement 0137 | PER | All entities | 31 October 2024

Approval for remote access to TOP SECRET information, data or systems in international locations outside of facilities meeting PSPF requirements is only granted if approved by the Australian Signals Directorate.

Requirement 0138 | PER | All entities | 31 October 2024

A security risk assessment of the proposed location and work environment informs decisions to allow personnel to work remotely in international locations.

Requirement 0139 | PER | All entities | 31 October 2024

Personnel are not granted approval to work remotely in locations where Australian Government information, or resources are exposed to extrajudicial directions from a foreign government that conflict with Australian law, unless operationally required, and the residual risks are managed and approved by the Chief Security Officer.

Related Standards – Access to resources

- Standard: Commonwealth Property Management Framework
- Standard: Australian Government Personnel Security Adjudicative Standard

18 Security Clearances

Security vetting is conducted to determine whether an individual is eligible and suitable to hold a security clearance in order to access security classified government information, resources and activities. To be eligible for an Australian Government security clearance, an individual must be an Australian citizen, have a checkable background and possess and demonstrate integrity and trustworthiness commensurate with the security classified information, resources and activities they will be expected to protect.

The security vetting process details the standardised vetting practices to be undertaken when employing personnel and contractors. These practices provide a high-quality and consistent approach to managing personnel eligibility and suitability risk across government. Security vetting applies to Australian Government Baseline, Negative Vetting 1, Negative Vetting 2 and Positive Vetting security clearances.

The security vetting process establishes confidence that an individual possesses a sound and stable character, and they are not unduly vulnerable to key national security threats such as:

- espionage – a form of theft,
- sabotage – violence or damage (physical or other) aimed at destroying, degrading, corrupting or delaying access to information or capabilities
- foreign interference – including influence and corruption operations, and
- political violence.

These activities could overlap with each other and with non-national security threats. Non-national security threats that may also be protected by these security measures include theft, fraud, criminal damage or criminal violence.

Individuals who require ongoing access to Australian Government security classified information, technology systems and resources must hold a security clearance, commensurate with the security classification, unless the entity specifies a higher security clearance is necessary for operational requirements. The security clearance level required is not based on the person's rank, seniority or status.

18.1 Security Clearances

A security clearance is a statement of assurance that a person is both eligible and, so far as can be determined at the time that the clearance is issued, suitable to hold a position of trust that gives them access to security classified Australian Government information, resources and activities.

It is a point in time judgement that must be accompanied by ongoing security management of those holding clearances to ensure that they remain suitable.

Individuals who require ongoing access to Australian Government security classified information, resources and activities must hold a security clearance, commensurate with their security classification. The security clearance level required is not based on the person's rank, seniority or status, but on the necessary access required to perform their identified position (see Identifying and Recording Positions that Require a Security Clearance).

18.1.1 Security Clearance Levels

The Australian Government has four security clearance levels, noting Positive Vetting security clearances are being phased out and replaced with TS-PA security clearances. Clearances are linked to and reflective of the

security classification system. This system applies a security classification to information, resources and activities that require security protection.

Table 24 details the Australian Government security clearance levels required to access security classified information, resources and activities.

Table 25: Australian Government Security Clearances Levels

Security Clearance Level	Level of Access
Baseline	Permits ongoing access up to and including PROTECTED.
Negative Vetting 1 (NV1)	Permits ongoing access up to and including SECRET, and temporary access to TOP SECRET in certain circumstances.
Negative Vetting 2 (NV2)	Permits ongoing access up to and including TOP SECRET.
Positive Vetting (PV)	Permits ongoing access up to and including TOP SECRET, including security caveated information, resources or activities, where authorised. Note: The PV security clearance is being progressively replaced by the TS-PA security clearance. During the transition, some Authorised Vetting Agencies will continue to issue PV clearances in accordance with the existing Sensitive Material Security Management Protocol – Personnel Security – Positive Vetting Guidelines (SMSMP-PVG).
TOP SECRET-Privileged Access (TS-PA)	Permits ongoing access to classified resources up to and including TOP SECRET, including security caveated information, resources or activities, where authorised. The TS-PA clearance was introduced in November 2021 and is being phased in to replace the Positive Vetting clearance.

18.1.2 Security Clearance Status

Table 26: Australian Government Security Clearances Status

Security Clearance Status	Definition
Active	An active security clearance is: • sponsored by an Australian Government entity, and • being maintained by a clearance holder and sponsoring entity
Inactive	An inactive security clearance that is within the revalidation period, however, the clearance is: • not sponsored by an Australian Government entity, or • not being maintained by the clearance holder for a period greater than six months due to long term absence from their role (e.g. maternity leave, extended leave without pay). However, the sponsoring entity has the discretion to allow people on long term leave to maintain their security clearance provided the clearance holder continues to meet their clearance requirements, including to report any changes in circumstances, and maintains periodic contact with the sponsoring entity throughout the leave period. For PV clearances, the SMSMP-PVG requires a security check to have been completed within the last two years, if not, the clearance is inactive. For TS-PA security clearances, refer to the TS-PA Standard.
Expired	An expired security clearance is: • outside the revalidation period, or

Security Clearance Status	Definition
	• a PV clearance and an annual security check has not been completed within the last two years. The Authorised Vetting Agency has the discretion to extend the expiry date of a security clearance beyond the standard revalidation period in circumstances where the revalidation or upgrade process takes longer than expected, provided the delay is not due to the clearance subject or sponsoring entity, and where there are no known concerns with the suitability of the clearance subject. For TS-PA security clearances, refer to the TS-PA Standard. It is not possible to request sponsorship of an expired clearance. If an Australian Government entity requests sponsorship after a clearance has expired, a new initial security clearance assessment process will be initiated.
Ceased	A ceased security clearance (or in some circumstances vetting process): • that has been denied or revoked, or • that has time-based conditions on when the clearance subject or holder can reapply for a security clearance, or • where the clearance subject or holder is ineligible to hold or maintain a security clearance.

18.2 Authorised Vetting Agencies

Security vetting may only be performed by Authorised Vetting Agencies authorised to assess, process and grant security clearances for Australian Government entities.

The Australian Government Security Vetting Agency (AGSVA) conducts security vetting for Australian Government entities, unless the entity has been authorised to conduct security vetting for its own personnel. Authorised Vetting Agencies must conduct security vetting in a manner consistent with the PSPF and the Australian Government Personnel Security Adjudicative Standard.

The term 'vetting analyst' denotes a person within an Authorised Vetting Agency who conducts vetting assessments. The term 'security clearance delegate' denotes a person formally authorised to make decisions on the outcome of a vetting process (i.e. to grant, deny, grant-conditional, revoke or cancel a security clearance).

Requirement 0140 | PER | All entities | 31 October 2024

The Australian Government Security Vetting Agency (AGSVA) or the TOP SECRET-Privileged Access Vetting Authority is used to conduct security vetting, or where authorised, the entity conducts security vetting in a manner consistent with the Personnel Security Vetting Process and Australian Government Personnel Security Adjudicative Standard.

See Authorised Vetting Agencies and TOP SECRET-Privileged Access Authority.

18.2.1 Competencies of Vetting Personnel

Authorised Vetting Agencies are required to ensure vetting personnel (i.e. vetting analysts and security clearance delegates) maintain the required skills and competencies for their role. See PSPF Guidelines for a list of recommended competencies and skills. These competencies and skills can be attained through formal qualifications, such as the Certificate IV or Diploma in Government Security (Personnel Vetting), or equivalent qualifications. Where Authorised Vetting Agencies determine that a formal qualification is required for vetting personnel in the entity, this should be obtained from a registered training organisation. A list of registered training organisations is available at www.training.gov.au.

Requirement 0141 | PER | AVA | 31 October 2024

All vetting personnel attain and maintain the required skills and competencies for their role.

The TS-PA Standard establishes the minimum qualifications and specific competencies for practitioners for TS-PA security clearances.

See PSPF Guidelines for recommended competencies and skills.

18.3 Recognition of Existing Security Clearances

Where an individual holds, or has previously held, a security clearance issued by an Authorised Vetting Agency[13] at the level required for the identified position (or higher), an entity may assume sponsorship of that security clearance.

Prior to seeking a new security clearance, the sponsoring entity must identify whether the clearance subject already holds, or has previously held, a security clearance, and advise the Authorised Vetting Agency accordingly. The Authorised Vetting Agency will confirm the clearance details with the granting agency, obtain the clearance subject's personal security file and record the new sponsorship of the security clearance on the file.

A security clearance held by the clearance subject cannot be recognised if:

- the clearance has expired due to the period since the clearance being granted (or last revalidated) exceeding:

Table 27: Security Clearance Expiration Periods

Security Clearance	Expiration Period
Baseline	15 years
Negative Vetting 1 (NV1)	10 years
Negative Vetting 2 (NV2)	7 years
Positive Vetting (PV)	7 years, or if a security clearance has not been completed in the previous two years. T The Sensitive Material Security Management Protocol – Personnel Security – Positive Vetting Guidelines (SMSMP-PVG) also requires an annual security appraisal to have been completed within the last two years. The SMSMP-PVG is available to entity security practitioners or by request via the PSPF community on GovTEAMS.
TOP SECRET-Privileged Access (TS-PA)	See the TS-PA Standard for details. This Standard is available to TOP SECRET-Privileged Access practitioners via the TOP SECRET-Privileged Access Quality Assurance Office.

- the Authorised Vetting Agency has concerns that the incoming clearance subject is no longer eligible or suitable to access Australian Government security classified resources at that clearance level
- the clearance was granted on the basis of an eligibility (citizenship or checkable background) waiver

[13] This includes a security clearance issued by a state or territory government in accordance with the *Memorandum of Understanding for the Protection of National Security Information* between the Commonwealth, states and territories, where the personal security file is transferred to an Authorised Vetting Agency.

- the clearance was granted subject to clearance conditions, or
- the clearance has ceased.

If a clearance is subject to an eligibility waiver or clearance conditions, the Authorised Vetting Agency will advise the gaining sponsoring entity.

Requirement 0142 | PER | All entities | 31 October 2024

The gaining sponsoring entity establishes new clearance conditions before assuming sponsorship of an existing security clearance that is subject to clearance conditions.

Requirement 0143 | PER | All entities | 31 October 2024

The gaining sponsoring entity undertakes the exceptional business requirement and risk assessment provisions prior to requesting transfer of sponsorship of an existing security clearance that is subject to an eligibility waiver.

18.4 Sponsoring Security Clearances

Security clearances must be sponsored by an Australian Government entity or an organisation otherwise authorised by the Australian Government.

State and territory governments may request that AGSVA conduct security clearances for their personnel up to and including Negative Vetting 2, in accordance with the 2007 Memorandum of Understanding for the Protection of National Security Information (available on GovTEAMS). States and territories require an Australian Government entity to sponsor all Positive Vetting security clearances for their personnel.

Requirement 0144 | PER | All entities | 31 October 2024

The Authorised Vetting Agency only issues a security clearance where the clearance is sponsored by an Australian Government entity or otherwise authorised by the Australian Government.

18.4.1 Identifying and Recording Positions that Require a Security Clearance

Sponsoring entities are required to identify and document the positions that require a security clearance to have ongoing access to Australian Government classified information, resources and activities. Recruitment for positions identified as requiring a security clearance must specify eligibility to obtain a security in the conditions of employment.

Given the interrelationships and complementarity of security classification, security information, resources and activities that require protection must be appropriately classified.

Entities may use security clearances where they need additional assurance of the suitability and integrity of personnel. This could be for access to security classified information, or to provide greater assurance for designated positions.

Requirement 0145 | PER | All entities | 31 October 2024

Positions that require a security clearance are identified and the level of clearance required is documented.

Requirement 0146 | PER | All entities | 31 October 2024

Each person working in an identified position has a valid security clearance issued by the relevant Authorised Vetting Agency.

See Clearance Exemptions for Australian Officials and Office Holders.

18.5 Eligibility for a Security Clearance

To be eligible for an Australian Government security clearance, an individual must be an Australian citizen and have a checkable background. Australian citizenship is determined by the sponsoring entity before requesting a security clearance.

General checkable background is determined by the Authorised Vetting Agency as part of the vetting assessment. ASIO may also deem a background as 'security uncheckable' as part of the Security Clearance Suitability Assessment (SCSA) process.

Pre-employment screening is the first 'vetting' activity, used to establish a person's eligibility to be employed by or for the Australian Government. It provides limited assurance on personnel security risks. Sponsoring entities are required to confirm that the mandatory pre-employment screen checks are completed before they seek a security clearance from their Authorised Vetting Agency.

Requirement 0147 | PER | All entities | 31 October 2024

Australian citizenship is confirmed and pre-employment screening is completed before the entity seeks a security clearance for a person in a position identified as requiring a security clearance.

See Pre-Employment Eligibility and Pre-Employment Screening.

18.5.1 Checkable and Uncheckable Backgrounds

A 'checkable background' is established when an Authorised Vetting Agency:

- has completed the minimum checks required for the checkable period,
- is satisfied that the checks provide an appropriate level of assurance in order to assess the clearance subject's life or background, and
- has validated the information provided by the clearance subject with respect to their identity and background from independent and reliable sources.

An 'uncheckable background' is where the Authorised Vetting Agency is unable to validate the information provided by a clearance subject with respect to their background from independent and reliable sources or authorities. There are generally two forms of uncheckable background:

- Uncheckable identity – clearance subject is born and substantially raised in a country where the Authorised Vetting Agency cannot reliably check the clearance subject's identity.
- Uncheckable period –clearance subject's identity can be confidently established, but the Authorised Vetting Agency is unable to check the clearance subject's activities and associations as they have spent a significant period of time in a high-security risk country where reliable checking is not possible.

The implications and significance of an uncheckable background will depend on a number of factors, including the security risk associated with the country in which the uncheckable time was spent, the reason the background is uncheckable, or the nature of the clearance subject. If an uncheckable background prevents the Authorised Vetting Agency from positively identifying the clearance subject, this may prevent them from identifying and responding to attempts by a foreign intelligence service, or other threat source, to insert their people into a position of access to Australian Government information, resources or activities. An uncheckable background may also conceal a clearance subject's activities, associations, or beliefs that might be of concern or otherwise relevant to their suitability to hold a security clearance.

The degree of confidence the Authorised Vetting Agency has in checks with international countries will vary depending on the relationship Australia has with the government of that country and the level of security risk

associated with that country. For example, high confidence in authorities from low-security risk countries that have similar values and government arrangements, and low to no confidence in authorities from high-security risk countries that have authoritarian and undemocratic values that are hostile to Australia. Periods spent in the latter are usually uncheckable.

18.5.2 Checkable Background Gaps

Gaps in a clearance subject's checkable background information due to a period overseas reduces confidence in assessments of suitability but does not necessarily point to a concern to be resolved.

Gaps in a subject's checkable background in low-security risk countries may be satisfactorily resolved by using documentary evidence from another reliable source, such as an employer or academic institution, or by information provided by a reliable referee who had first-hand knowledge of the subject and their activities in that location.

Gaps relating to a period in a high-security risk country, particularly countries which host or pose a security threat to Australia, is of greater concern and may be indicative of specific security issues requiring resolution. Where the Authorised Vetting Agency determines that despite any gaps, the clearance subject's background is 'checkable' and all vetting issues are dealt with exhaustively, any potential concerns arising from the gaps may be considered as part of ASIO's SCSA.

18.6 Eligibility Waivers

An eligibility waiver is a determination by the Accountable Authority that the advantage to the entity of allowing access to security classified information, resources or activities by a person that does not meet either the required citizenship or checkable background requirements, outweighs the risk involved.

The Accountable Authority (or Chief Security Officer if delegated) may waive the citizenship or checkable background requirements if there is an exceptional business requirement and after conducting a risk assessment, taking into account the ASIO threat assessments relating to the clearance subject's current or former country (or countries) of residence, and where the residual risks of waiving these requirements are assessed and have been accepted.

The Accountable Authority's decision to approve an exceptional business requirement is informed by whether the role:

- is critical to meeting the Sponsoring Entity's outcomes
- can be performed by a person who meets the eligibility requirements (i.e. is there another person capable of performing the role who is an Australian citizen and/or has a checkable background), or
- can be redesigned, so that the access to security classified resources is restricted to a person who already holds, or is eligible to hold, the appropriate security clearance.

The risk assessment for a citizenship or checkable background waiver is based on a specific position and entity. As such, security clearances granted on the basis of a citizenship or checkable background waiver cannot be transferred to a new position or entity unless the exceptional business requirement and risk assessment provisions are undertaken and accepted for the new position or entity.

The granting of a waiver does not lead to the presumption that a security clearance will be granted. Where an eligibility waiver has been issued, the Authorised Vetting Agency can still deny a security clearance if there are significant concerns about the clearance subject's eligibility or suitability to hold the clearance that cannot be mitigated. This includes concerns relating to the eligibility condition that was waived.

Where the Accountable Authority has waived the citizenship or checkable background requirements for any security clearances sponsored by the entity, the number of personnel in the entity with active waivers and the type of waivers are reportable in the annual report on security.

There are two types of eligibility waivers – citizenship and checkable background.

Requirement 0218 | PER | All entities | 01 July 2025

The Sponsoring Entity ensures clearance subjects with an eligibility waiver or where a waiver is being considered, are not given temporary or provisional access to security classified information or resources until the security vetting process is complete.

18.6.1 Citizenship Eligibility Waiver

This type of waiver may be used when a clearance subject is not an Australian Citizen but has a valid visa with work rights.

Requirement 0148 | PER | All entities | 31 October 2024

The Sponsoring Entity establishes an exceptional business need and conducts a risk assessment before a citizenship eligibility waiver is considered for a non-Australian citizen who has a valid visa and work rights to work in an identified position.

Requirement 0149 | PER | All entities | 01 July 2025

The Accountable Authority (or the Chief Security Officer if delegated) approves a citizenship eligibility waiver (after accepting the residual risk of waiving the citizenship requirement for that person and confirming that a checkable background eligibility waiver is not in place), and maintains a record of all citizenship eligibility waivers approved.

18.6.2 Checkable Background Eligibility Waiver

This type of waiver may be used when the Authorised Vetting Agency assesses that a clearance subject has an uncheckable background as they cannot complete the minimum checks and inquiries for the required period, or the checks and inquiries made do not provide an adequate basis to assess the clearance subject's life or background.

In these circumstances, and if no checkable background eligibility waiver is in place from the sponsoring entity, the Authorised Vetting Agency will deny the request for a clearance.

Requirement 0150 | PER | All entities | 31 October 2024

The Sponsoring Entity establishes an exceptional business need and conducts a risk assessment (including seeking advice from the Authorised Vetting Agency), before a checkable background eligibility waiver is considered for a clearance subject assessed as having an uncheckable background.

Requirement 0151 | PER | All entities | 01 July 2025

The Sponsoring Entity's Accountable Authority (or the Chief Security Officer if delegated) approves checkable background eligibility waivers (after accepting the residual risk of waiving the checkable background requirement for each person and confirming that a citizenship eligibility waiver is not in place), and maintains a record of all checkable background eligibility waivers approved.

Requirement 0152 | PER | AVA | 31 October 2024

The Authorised Vetting Agency provides the Sponsoring Entity with information to inform a risk assessment if a clearance subject has an uncheckable background and only issues a clearance if the Accountable Authority

waives the checkable background requirement and provides the Authorised Vetting Agency with a copy of the waiver.

18.6.3 Eligibility Waivers Risk Assessment

Entities granting eligibility waivers must only do so after conducting an assessment of the security risks arising from the proposed action in accordance with the Australian Government Personnel Security Adjudicative Standard. Risk assessments to inform eligibility waivers are role-specific and not portable or transferrable. Gaining sponsoring entities cannot rely on the assessment of the losing sponsoring entity, rather they must conduct their own assessment of the security risks of an eligibility waiver and where approved, reissue a waiver.

When conducting a risk assessment for eligibility waivers, the Sponsoring Entity must consider:

- potential conflicts of interest
- advice from the Authorised Vetting Agency and ASIO, including any known concerns about the clearance subject
- the period of access under consideration, and
- proposed risk management measures, including any conditions placed on the clearance holder subject to the waiver or temporary access.

For uncheckable background eligibility waivers, also consider:

- details of any concerns associated with the subject's uncheckable background and assessment of the impact of this uncheckable period against the whole-of-person assessment, and
- any threat assessments from ASIO on the clearance subject's country(ies) of citizenship or the country(ies) that gave rise to issues of checkability.

For citizenship eligibility waivers, also consider:

- details of the clearance subject's visa status and whether they are actively seeking Australian citizenship, or plan to
- the sponsoring entity's plan to ensure the clearance subject does not access caveated AUSTEO information, and
- any threat assessments from ASIO on the clearance subject's country(ies) of citizenship or the country(ies) that gave rise to issues of checkability.

18.7 Clearance Subject Responsibilities

Clearance subjects who agree to undertake the security clearance process for the purposes of gaining employment, transfer or promotion to a position, securing a service provision contract, or to complete additional tasks within an existing position must disclose all relevant and required information. They must also co-operate in the collection of personal documentation and corroborating evidence. Clearance subjects must answer questions fully and honestly, and provide accurate information and personal documentation.

Sponsoring Entities must deny or withdraw a security clearance if a clearance subject fails or refuses to complete the required forms or to comply with reasonable requests from the Authorised Vetting Agency. This could result in a reduction of or an alteration to, duties or termination of employment. Before an entity denies a security clearance for this reason, they must inform the clearance subject of the likely consequences of not co-operating.

18.8 Locally Engaged Staff

Locally engaged staff are employed to support and complement the capacity of APS employees posted as representatives of the Australian Government at international posts (Australian embassies, high commissions and consulates). Locally engaged staff are not APS personnel but provide essential in-country knowledge, networks and continuity at an international post.

Locally engaged staff who are not Australian citizens may be granted a diplomatic mission clearance in accordance with the *Prime Minister's Directive on Guidelines for the Management of the Australian Government Presence Overseas.* These clearances are only recognised for the mission they are granted, are role-specific and are not portable or transferrable.

The Department of Foreign Affairs and Trade is responsible for the security vetting of their locally engaged staff. The Australian Trade and Investment Commission is a managing entity under this directive and conducts security screening for its locally engaged staff and for those of attached entities.

The Accountable Authority (or Chief Security officer if delegated) may grant a waiver for citizenship eligibility to locally engaged staff working for an Australian Government entity in an international facilities not managed by DFAT, where the preferred person is not an Australian citizen, and the entity understands and agrees to manage that risk. Such waivers must be subject to a suitable risk assessment.

Related Standards – Security Clearances

- Standard: Australian Government Personnel Security Adjudicative Standard.
- Standard: TOP SECRET Privileged Access Standard (available to relevant entities through the Quality Assurance Office).
- Standard: Sensitive Material Security Management Protocol – Personnel Security – Positive Vetting Guidelines (on GovTEAMS).

19 Personnel Security Vetting Process

Security vetting is conducted to ensure personnel are eligible and suitable to access classified government resources. The security vetting process results in a determination of the clearance subject's eligibility and suitability to hold a security clearance.

Security vetting of an individual establishes confidence that they possess an appropriate level of integrity, a sound and stable character, and they are not unduly vulnerable to influence or coercion.

The determination is based on:

- an assessment against the Australian Government Personnel Security Adjudicative Standard
- minimum personnel security checks, and
- a resolution of any doubt in the national interest.

The personnel security vetting process details the standardised vetting practices to be undertaken when employing personnel and contractors. These processes provide a high-quality and consistent approach to managing personnel eligibility and suitability risk across government.

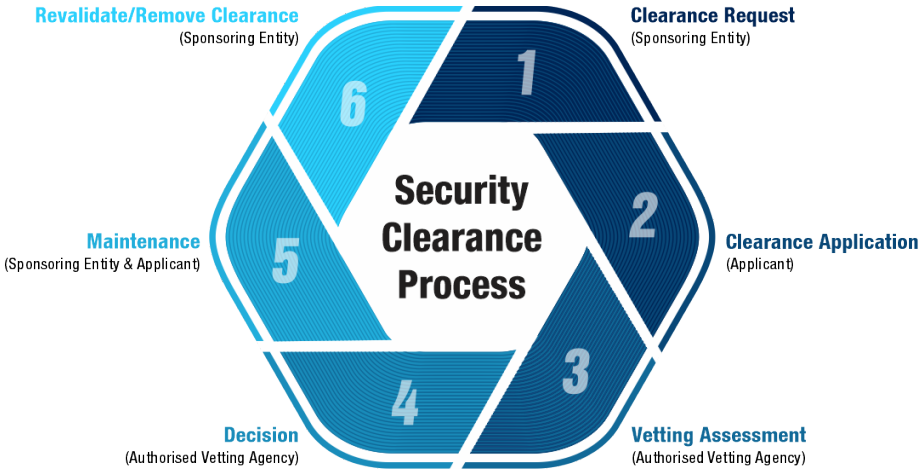
In the security context, integrity is defined as a range of character traits that indicate the individual is able to protect Australian Government security classified information, resources and activities.

These character traits are:

- honesty
- trustworthiness
- maturity
- tolerance
- resilience, and
- loyalty.

The security vetting process is summarised in Figure 3. The vetting assessment phase includes all the mandatory minimum personnel security checks, including ASIO's security clearance suitability assessment (SCSA) which applies to all security clearance applications (other than Baseline security clearance applications as ASIO's SCSA is optional but not mandatory for Baseline security clearances).

Figure 3: Security Clearance Process



19.1.1 Informed Consent

The Authorised Vetting Agency is required to seek informed consent from the clearance subject to collect, use and disclose their personal information for the purposes of assessing and managing their eligibility and suitability to hold a security clearance.

Personal information received or used during security clearance vetting and ongoing suitability checks must be conducted in accordance with the Australian Privacy Principles (unless these principles do not apply to the entity).

Due to the nature of its content, personal information will always be classified at least OFFICIAL: Sensitive and must be protected in accordance with the minimum protections and handling requirements for this classification.

Sharing relevant information, even when it is sensitive personal information, will not breach an individual's privacy provided that informed consent is received and the information is used for the purpose for which consent is provided. To be able to meet the PSPF obligations to share information of concern, Authorised Vetting Agencies are required to obtain informed consent from all clearance subjects to share information with other entities. This includes but is not limited to the Sponsoring Entity and other Authorised Vetting Agencies. Consent is recommended to be obtained at key information collection points, such as application for a security clearance, and that consent is updated at reasonable intervals.

It is ideal for entities to also include a privacy statement in their recruitment and pre-recruitment paperwork detailing how personal information will be collected, used and disclosed. This should note that information gathered through the security vetting process may be shared to inform other decisions related to law enforcement or counter intelligence.

Entities are exempt from the provisions of the Privacy Act when communicating personal information to ASIO in support of ASIO's functions.

Requirement 0153 | PER | AVA | 31 October 2024

The clearance subject's informed consent is given to collect, use and disclose their personal information for the purposes of assessing and managing their eligibility and suitability to hold a security clearance.

19.2 Personnel Security Adjudicative Standard

The Australian Government Personnel Security Adjudicative Standard applies to Australian Government Baseline, Negative Vetting 1, Negative Vetting 2, and Positive Vetting security clearances. Positive Vetting security clearances will be progressively replaced by TS-PA security clearances, issued in accordance with the TS-PA Standard.

Authorised Vetting Agencies must assess an individual's eligibility and suitability from a whole-of-person perspective to hold a security clearance. This includes consideration of their integrity in accordance with the Personnel Security Adjudicative Standard. For the purposes of security vetting, integrity is defined as the character traits of honesty, trustworthiness, maturity, tolerance, resilience and loyalty.

The Australian Government Personnel Security Adjudicative Standard provide the common risk factor areas against which a clearance subject's eligibility and suitability is assessed. These areas may have a bearing on one or more of a clearance subject's character traits. Authorised Vetting Agencies should use a process of structured professional judgement to achieve an overall decision or a decision based on the available information.

Requirement 0154 | PER | AVA | 31 October 2024

The clearance subject's eligibility and suitability to hold a Baseline, Negative Vetting 1, Negative Vetting 2 or Positive Vetting security clearance is assessed by considering their integrity (i.e. the character traits of maturity, trustworthiness, honesty, resilience, tolerance and loyalty) in accordance with the Australian Government Personnel Security Adjudicative Standard.

19.2.1 TOP-SECRET Privileged Access

The TS-PA Standard establishes the requirements that apply to TS-PA clearances. The Standard is a classified document that is only available to qualified practitioners conducting TS-PA vetting, psychological assessments or insider threat management activities in the TOP SECRET-Privileged Access Authority, Quality Assurance Office, or sponsoring entities (referred to as TS-PA practitioners).

Only entities with an insider threat program that meets the TS-PA Standard are able to sponsor TS-PA security clearances.

All personnel who obtain a TS-PA security clearance will be provided with a copy of the annex to the TS-PA Standard that outlines their obligations for maintaining their security clearance.

The TOP SECRET-Privileged Access Vetting Authority is required to assess an individual's suitability to hold TS-PA security clearance by considering their trustworthiness and commitment to Australia, its values, and its democratic system of government in accordance with the TS-PA Standard.

Requirement 0155 | PER | AVA | 31 October 2024

The clearance subject's eligibility and suitability to hold a TOP SECRET-Privileged Access security clearance is assessed in accordance with the TOP SECRET-Privileged Access Standard.

19.3 Minimum Personnel Security Checks

The purpose of minimum personnel security checks is to verify identity and collect relevant information necessary to obtain an accurate picture of the clearance subject's background, lifestyle and character. These checks establish the clearance subject's eligibility and suitability to hold a security clearance.

The effectiveness of these minimum personnel security checks relies on complete, consistent and accurate information provided by the clearance subject.

Requirement 0156 | PER | AVA | 31 October 2024

The clearance subject's eligibility and suitability to hold a Baseline, Negative Vetting 1, Negative Vetting 2 or Positive Vetting security clearance is assessed by conducting the minimum personnel security checks for the commensurate security clearance level.

Table 28: Minimum Personnel Security Checks

Check	Security Clearance Level				
	Baseline Vetting	Negative Vetting 1	Negative Vetting 2	Positive Vetting	TOP SECRET-Privileged Access [14]
Identity check	Required	Required	Required	Required	TS-PA Standard
	Entities must verify the person's identification documents with the issuing authority by using the Document Verification Service (or other source identity verification solution) for Australian issued primary identification documents.				TS-PA Standard

[14] See the TOP SECRET-Privileged Access Standard.

Check	Security Clearance Level				
	Baseline Vetting	Negative Vetting 1	Negative Vetting 2	Positive Vetting	TOP SECRET-Privileged Access [14]
Confirmation of Australian citizenship and status of any other citizenships	Required	Required	Required	Required	TS-PA Standard
Background assessment	Required for the checkable period of 5 years	Required for the checkable period of 10 years	Required for the checkable period of 10 years	Required for the checkable period that is greater of 10 years or from the age of 16	TS-PA Standard
Acknowledgement of relevant legislation (secrecy of information)	Required	Required	Required	Required	TS-PA Standard
Referee checks	Required	Required	Required	Required	TS-PA Standard
Digital footprint check	Required	Required	Required	Required	TS-PA Standard
National police check/criminal history check	Required, no exclusion	Required, full exclusion	Required, full exclusion	Required, full exclusion	TS-PA Standard
Financial history assessment	Required	Required	Required	Required	TS-PA Standard
Financial statement	Not required	Required	Required	Required with supporting documents	TS-PA Standard
Financial probity assessment	Not required	Not required	Not required	Required	TS-PA Standard
Comprehensive financial assessment	Not required	Not required	Not required	Not required	TS-PA Standard
ASIO security clearance suitability assessment	Not required	Required	Required	Required	TS-PA Standard
Security interview	Not required	Not required	Required	Required	TS-PA Standard
Psychological assessment	Not required, however optional where deemed necessary by the Authorised Vetting Agency.			Required	TS-PA Standard
Overseas travel check	Not required	Not required	Not required	Not required	TS-PA Standard
Statutory declaration (only when vetting is conducted by a state or territory agency)	Required	Required	Required	Not required	TS-PA Standard

See PSPF Guidelines for detailed information on each of these mandatory minimum checks.

19.4 National Interest

The national interest is Australia's sovereignty, security, prosperity, independence of decision-making and the freedom and social cohesion of its people.

All people working in and on behalf of Australian Government must have a primary and overriding commitment to the democratic process and a respect for the processes by which the elected government functions. If a clearance subject expresses political or personal views incompatible with Australia's constitutional, democratic system of government, doubts arise over whether they are loyal to the Australian Government. Conflict of views or conscientious objections could arise in some cases. However, the issue is whether a clearance subject recognises their responsibilities to their employing entity, the elected government and the public interest. When a clearance subject acts in ways that indicates a preference for a foreign country over Australia, then they may be prone to act in ways that are harmful to the national interest of Australia.

The determination of whether an individual is suitable to hold a security clearance, consistent with the national interest, is based on careful consideration of the whole person in the context of the following risk factor areas:

- external loyalties, influences and associations
- personal relationships and conduct
- financial considerations
- alcohol and drug usage
- criminal history and conduct
- security attitudes and violations, and
- mental health disorders.

These factor areas may have a bearing on one or more of a clearance subject's character traits.

Each clearance subject is assessed on their own merits, and the final determination of their suitability rests with the Authorised Vetting Agency delegate. Any doubt concerning the clearance subject's suitability must be resolved in favour of the national interest

See PSPF Guidelines for further information on national interest risk factors.

Requirement 0157 | PER | AVA | 31 October 2024

The clearance subject's eligibility and suitability to hold a Baseline, Negative Vetting 1, Negative Vetting 2 or Positive Vetting security clearance is assessed by resolving any doubt in the national interest.

19.5 Security Vetting Outcomes

A vetting analyst conducts the assessment and provides a security clearance delegate with a recommended outcome. The outcome of a security vetting process is a decision of the clearance subject's eligibility and suitability to hold a security clearance based on an assessment:

- against the Personnel Security Adjudicative Guidelines (for Baseline, Negative Vetting 1, Negative Vetting 2 and Positive Vetting)
- against the TOP SECRET-Privileged Access Standard (for TS-PA)
- taking into account all relevant, reliable and independently verified information obtained through the minimum personnel security checks, and any additional checks required

- taking into account ASIO's security clearance suitability assessment (for Baseline, Negative Vetting 1, Negative Vetting 2 and Positive Vetting), and
- resolving any doubt in the national interest.

In determining the security clearance outcome based on the recommendation from the vetting analyst, the delegate:

- satisfies themselves that all issues raised in the clearance process have been addressed, and
- provides the clearance subject with the opportunity to respond to any adverse information, if appropriate.

Authorised Vetting Agencies are asked to use consistent language to describe the outcomes of security vetting processes in personal security files.

Table 29: Determinative Security Vetting Outcomes

Outcome	Description
Denied	The clearance subject is not suitable to hold an Australian Government security clearance at the requested level.
Granted	The clearance subject is eligible and suitable to hold an Australian Government security clearance.
Granted–conditional	The clearance subject is eligible and suitable to hold an Australian Government security clearance if they comply with clearance conditions.

Administrative outcomes of the security vetting process apply where no vetting assessment or security clearance decision has been made.

Table 30: Administrative Security Vetting Outcomes

Outcome	Description
Ineligible	The clearance subject is not eligible for an Australian Government security clearance as they: • do not hold Australian citizenship • do not have a checkable background.
Cancelled	The security clearance could not be completed by the vetting agency because: • sponsorship of the clearance was removed at the request of the sponsoring entity • sponsorship or clearance requirement could not be confirmed, or • the clearance subject was non-compliant.

19.5.1 Conditional Security Clearances

Security clearance conditions enable the sponsoring entity to manage ongoing risks affecting the clearance subject's eligibility and suitability to hold a security clearance. This may include access restrictions or other risk mitigations measures.

Conditions may be placed on a security clearance at the instigation of the Sponsoring Entity, or the Authorised Vetting Agency, or on the recommendation of ASIO's security clearance suitability assessment.

Monitoring a clearance subject's compliance with security clearance conditions is addressed in Requirement 165. Non-compliance with conditions may trigger a review for cause.

Requirement 0158 | PER | AVA | 31 October 2024

Concerns that are identified during the vetting or security clearance suitability assessment process, that are not sufficient to deny a security clearance and where the related risks can be managed through conditions attached to the security clearance, the Authorised Vetting Agency must:

- identify the clearance conditions
- provide the sponsoring entity with information about the concerns to inform a risk assessment
- only issue a conditional security clearance if the Accountable Authority and the clearance subject accept the clearance conditions. The Accountable Authority may delegate this decision to the Chief Security Officer, however the Chief Security Officer is required to notify the Accountable Authority of the clearance conditions.

19.6 Sharing Information of Concern

Authorised Vetting Agencies are required to provide relevant information of concern obtained during the security vetting process to the sponsoring entity. Information of concern includes information of security concern (such as issues relating to the protection of security classified information, resources or activities such as compromise, espionage, sabotage, foreign interference.) and information of non-security concern (such as integrity or allegiance to Australia or the Australian Government's interest). This is particularly important if identified concerns may lead to an adverse recommendation, or where vetting uncovers information likely to impact on the clearance subject's suitability to hold the role. For example, current drug use in an entity with a zero drug-use policy.

Where a security clearance decision is pending, including in circumstances where a response has been invited from the clearance subject in relation to the identified risks, the Authorised Vetting Agency only shares relevant information with the sponsoring entity to enable temporary measures until a decision is made.

Not all information of concern obtained during the security vetting process will disqualify the security clearance applicant from obtaining a security clearance or require conditions to be imposed on the security clearance. However, where this type of information is identified, the Authorised Vetting Agency should consider the merits of sharing this information with the sponsoring entity, noting the decision to share this type of information is at their discretion. For example, the clearance subject has falsified their qualifications, however during the vetting process the Authorised Vetting Agency determines that this is manageable from a security clearance perspective but considers this renders the applicant ineligible for the particular role for which they have been recruited. By sharing this information with the sponsoring entity, the Authorised Vetting Agency supports the sponsoring entity to make sound risk-based decisions on whether to proceed with the clearance.

When advising the sponsoring entity of the security clearance outcome, the Authorised Vetting Agency should include information relating to any vulnerabilities, risk factors or risk mitigation measures that were applied by the vetting agency. The sponsoring entity can then understand and manage any risks relating to the clearance holder's ongoing access to Australian Government resources.

Requirement 0159 | PER | AVA | 31 October 2024

The Authorised Vetting Agency provides the sponsoring entity any relevant information of concern, when advising them of the outcome of the security vetting process, to inform the sponsoring entity's risk assessment.

19.7 Procedural Fairness

Procedural fairness applies to Baseline, Negative Vetting 1, Negative Vetting 2 and Positive Vetting security clearance processes. The TS-PA Standard provides guidance on procedural fairness for TS-PA security clearance processes.

Procedural fairness is concerned with the procedures followed by a decision maker in reaching an outcome, rather than the actual outcome reached – it is a matter of administrative law. Procedural fairness requires a fair and proper procedure be used when making a decision. A decision maker who follows a fair procedure is more likely to reach a fair and correct decision.

Authorised Vetting Agencies must apply procedural fairness to security clearance decisions that are adverse to a clearance subject, without compromising the national interest or betraying the confidentiality of the source of any adverse information. When the principles of procedural fairness are applied in a security clearance process, it protects the rights of the individual and reduces the possibility of a new clearance process being ordered on review or appeal.

If the vetting analyst intends to recommend against the approval of a clearance at the level sought, or to recommend that the clearance be approved with clearance conditions, the clearance subject should be provided with an opportunity to respond before the final recommendation is made. Any information used to make a decision must be substantiated, particularly when the information is from a referee who may be biased or have a conflict of interest.

The essential elements of providing procedural fairness are:

- the hearing rule, which requires a person be provided with a clear understanding of the matters at issue (the allegations or charges against them) and an opportunity to be heard and express their views to a decision maker
- the bias rule, which requires a decision maker to be impartial.
- a sound (reliable and sufficient) evidentiary base for decisions, and
- diligent inquiry into and, where possible, resolution of any matters in dispute.

The term procedural fairness is preferred when referring to administrative decision-making because the term 'natural justice' is associated with procedures used by courts of law. However, the terms have similar meaning and are commonly used interchangeably. For consistency, the term 'procedural fairness' is used in this standard.

Requirement 0160 | PER | AVA | 31 October 2024

The Authorised Vetting Agency applies the rules of procedural fairness to security clearance decisions that are adverse to a clearance subject, including decisions to deny a security clearance (including grant lower level) or grant a conditional security clearance, without compromising the national interest.

Note: Separate arrangements ensure procedural fairness and national security are preserved where denial of a clearance is based on an ASIO security clearance suitability assessment.

19.7.1 Procedural Fairness and Security Clearance Decisions

To comply with administrative law principles, Authorised Vetting Agencies must apply the rules of procedural fairness to security clearance decisions that are adverse to a clearance subject, including decisions to deny or revoke a security clearance.

As part of the security clearance decision-making process and in accordance with the hearing rule, where an adverse decision is proposed, the Authorised Vetting Agencies should advise the clearance subject of this potential outcome and the reasons why an adverse decision is being considered (to the fullest extent possible consistent with national security) and give them an opportunity to reply before the delegate makes a decision. The Authorised Vetting Agencies should ensure that the clearance subject:

- is told of the potential adverse finding before preparing their reply, including being provided with a description of the proposed decision, the criteria for making that decision and the information on which

any such decision would be based. It is recommended that the Authorised Vetting Agency discloses any negative information they have about the clearance subject to the extent possible consistent with national security. It is sufficient that a summary of the information being considered is provided to the clearance subject – original documents and the identity of confidential sources do not have to be provided

- is provided with a reasonable opportunity to consider their position and prepare a response, and
- have their reply considered by the delegate before the decision is made.

The bias rule requires that a delegate making a security clearance decision:

- does not have an interest (either direct or indirect) in the matter being decided, and
- does not bring, or appear to bring, a biased or prejudiced mind to making the decision.

A delegate must be impartial. Authorised Vetting Agencies must maintain processes to ensure application of the bias rule to comply with administrative law principles.

19.7.2 Procedural Fairness and Delegate

In making a security clearance decision that complies with administrative law principles, a delegate must comply with the rules of procedural fairness and ensure that:

- a clearance subject has been provided with an opportunity to be heard to make submissions if this has not already occurred and it is not prejudicial to security to do so
- they act fairly and impartially, including by ensuring there is no reasonable perception of bias on the part of the delegate, and
- any information used to make a decision can be substantiated, particularly when the information is from a referee who may be biased or have a conflict of interest.

19.7.3 Procedural Fairness and Negative Delegate Decisions

If a clearance subject is negatively affected by a delegate's decision, they can expect that the vetting analyst and delegate will follow the rules of procedural fairness before reaching a conclusion. In particular, a clearance subject is entitled to:

- be told the case to be met (e.g. that an Authorised Vetting Agency is considering denying a clearance, ceasing a clearance, or imposing conditions on the clearance), including being provided with a description of the proposed decision, the criteria for making that decision and the information on which the decision would be based, except where to do so would be inconsistent with national security, and
- an opportunity to reply to the case to be met by a written reply or submission or, in certain circumstances, through a face-to-face or phone interview.

In responding to concerns, a clearance subject may:

- deny the allegations
- provide evidence they believe disproves the allegations
- explain the allegations or present an innocent explanation, or
- provide details of any special circumstances they believe need to be taken into account.

19.7.4 Procedural Fairness and Vetting Analysts

A vetting analyst must take into account the requirements of procedural fairness during the clearance process, including when undertaking a security clearance assessment and preparing a recommendation for a delegate.

To comply with administrative law principles when making a recommendation to a delegate, a vetting analyst must:

- consider all submissions made by a clearance subject
- take into account only relevant information
- ensure that any recommendation made is based on a sound (reliable and sufficient) evidentiary base
- act fairly and impartially
- conduct the clearance process without unnecessary delay, and
- ensure that a full record of the clearance process has been made.

19.8 Review of Decisions

The denial or granting of a security clearance, with or without clearance conditions, is an administrative decision and is reviewable. The avenues for review vary depending on the applicable Authorised Vetting Agency, Sponsoring Entity and the status of the clearance subject.

Table 31: Administrative Review Process by Sponsoring Entity

Employer	Administrative Review Process
APS employees	Primary review by the Authorised Vetting Agency – an employee can seek an initial review conducted by the Authorised Vetting Agency. The employee has 60 days from notification of the security decision to request a review under subsection 38(1) 5.24(1) of the *Public Service Regulations 2023*. Primary review by the Merit Protection Commissioner – an employee can seek an initial review conducted by the Merit Protection Commissioner. The employee has 60 days from notification of the security decision to request a review under subsection 38(3) of the *Public Service Regulations 2023*. Secondary review by the Merit Protection Commissioner – an employee can seek an independent review if they are dissatisfied with a decision arising from the Authorised Vetting Agency's review or have been advised that the matter is not reviewable. An employee has 60 days from the time they are advised of the decision of the relevant Authorised Vetting Agency's review to make an application for review by the Merit Protection Commissioner under section 43(1) (a of the *Public Service Regulations 2023*. An employee seeking review must lodge their application with the vetting agency. The agency has 14 days to forward the application to the Merit Protection Commissioner with all of the relevant paperwork from the primary review. Employees may also lodge a complaint with the Commonwealth Ombudsman. An Ombudsman will generally only investigate a complaint if other review processes have been completed within the relevant agency. If an employee is dissatisfied with the Ombudsman's decision whether to investigate a complaint, they can seek an internal review of the decision within 3 months.
Australian Defence Force members	Members may seek an internal review via the procedures outlined in Defence Complaints and Resolution Manual that is available to Australian Defence Force members. Australian Defence Force members can also seek review by the Defence Force Ombudsman.

Employer	Administrative Review Process
Non-APS employees	Employees may have access to internal review procedures set by the relevant vetting agency. Employees may also lodge a complaint with the Commonwealth Ombudsman. An Ombudsman will generally only investigate a complaint if other review processes have been completed within the relevant agency. If an employee is dissatisfied with the Ombudsman's decision whether to investigate a complaint, they can seek an internal review of the decision within 3 months.

A secondary review by the Merit Protection Commissioner cannot reverse a decision made by the delegate, under section 42 of the *Public Service Regulations 2023*. Instead, under the regulations the Commissioner must make a recommendation to the relevant Authorised Vetting Agency. Under section 46, the Authorised Vetting Agency may confirm the action, vary it or set the action aside and substitute a new action in response to the recommendation. The Authorised Vetting Agency must advise the Merit Protection Commissioner of its decision and the reasons for the decision. If the Merit Protection Commissioner is not satisfied with the Authorised Vetting Agency's response, subsection 33(6) of the *Public Service Act 1999* allows for the matter to be reported to the entity's minister, the Prime Minister and the Parliament.

Security clearance decisions made by ASIO may be internally reviewable and reviewable by the Administrative Review Tribunal or an independent reviewer appointed by the Attorney-General. Information about review rights is provided to eligible clearance subjects.

The clearance subject may appeal in the Administrative Review Tribunal against certain prejudicial ASIO security clearance suitability assessments. The subject must be advised in writing (usually within 14 days of furnishing of the assessment. The review process is conducted through the Security Division of the Administrative Review Tribunal. For information about how to apply for a review of a decision in the Security Division, see Administrative Review Tribunal (art.gov.au).

Authorised Vetting Agencies should ensure the clearance subject has been given a chance to respond to any other suitability concerns. Any responses by the clearance subject will be included on the clearance subject's personal security file.

The clearance subject may also make a formal complaint to:

- the Privacy Commissioner, if they feel there was a breach of the *Privacy Act 1988* in the way information was handled, or
- the Human Rights Commissioner, if they feel they have been unfairly discriminated against. Under section 20 of the *Human Rights Commission Act 1986*, the Commissioner will investigate a complaint or provide written notice explaining why the complaint will not be investigated. If the complaint refers to an action by an intelligence agency, the Commissioner will refer the complaint to the Inspector-General of Intelligence and Security.

The clearance subject may also seek judicial review of a vetting decision in the Federal Court of Australia or High Court of Australia under section 39B of the *Judiciary Act 1903* or section 75(v) of the Constitution.

Related Standards – Personnel Security Vetting Process

- Standard: Australian Government Personnel Security Adjudicative Standard.
- Standard: TOP SECRET Privileged Access Standard (available to relevant entities through the Quality Assurance Office).
- Standard: Sensitive Material Security Management Protocol – Personnel Security – Positive Vetting Guidelines (on GovTEAMS).

20 Australian Officials and Office Holders

20.1 Clearance Exemptions for Australian Officials and Office Holders

Some Australian officials and office holders are not required to hold a security clearance to access security classified information while exercising the duties of the office:

- members and senators of the Commonwealth (including Ministers, shadow ministers and backbenchers[15]) and state parliaments and territory legislative assemblies members
- judges of federal courts and the Supreme Courts of the states and territories
- royal commissioners
- the Governor-General, state governors, the Northern Territory administrator
- members of the Executive Council, and
- appointed office holders with enabling legislation that gives the same privileges as the office holders already identified e.g. members of the Administrative Review Tribunal.

Staff of the above are not exempt from security clearance requirements.

20.2 PSPF Obligations for Australian Officials and Office Holders

An Australian officer holder's exemption from the requirements of the PSPF is limited to the requirement for a security clearance.

Departments of State responsible for managing protective security for Australian office holders are to ensure that classified information, devices and resources in their possession are appropriately safeguarded at all times in accordance with the PSPF.

20.3 Members of Parliament (Staff) Act Employees

Parliamentarians employ staff under the *Members of Parliament (Staff) Act 1984* (MOP(S) Act). Staff are referred to as MOP(S) Act employees. This Act covers electorate employees, personal employees (Ministerial) and personal employees (non-Ministerial for example staff members of shadow ministers and backbenchers).

The power to employ, and the terms and conditions of employment, may be affected by arrangements and determinations made by the Prime Minister. Further, successive responsible Ministers have made determinations and authorisations under the authority provided by the MOP(S) Act to assist in the administration of entitlements of employees.

Once such determination, the *Special Minister of State - Members of Parliament (Staff) (Employment Arrangements) Determination 2025,* requires that electorate or personal staff (ministerial staff), excluding casual electorate employees of an office-holder who is a Minister or Parliamentary Secretary, employed under Part III of the MOP(S) Act, must obtain and maintain a Negative Vetting 2 security clearance.

The Australian Government Security Vetting Agency is the Authorised Vetting Agency responsible for the security clearances of ministerial staff.

[15] Backbencher is a Member of Parliament who is not a minister or special officer holder.

The responsibilities for sponsorship and management of the security clearances of ministerial staff are shared between the Department of Finance, the Department of State in the relevant portfolio (or another entity in the portfolio as their delegate) and the relevant Minister (or Chief of Staff as their delegated authorised officer).

The key responsibilities are detailed below.

Table 32: Key Stakeholder Responsibilities for Ministerial Staff Security Clearances

Department of Finance	Department of State (or delegate)	Minister/Chief of Staff
• Initiate clearance process • Manage separation process	• Assess temporary access requests • Coordinate eligibility waivers and conditional clearances • Manage clearance maintenance	• Notify Finance of the commencement and separation of ministerial staff • Encourage submission of clearance paperwork • Advise on personnel security risks

20.3.1 Variation of Special Minister of State's Determination for a Minister's electorate officer

- The *Special Minister of State - Members of Parliament (Staff) (Employment Arrangements) Determination 2025* requires that staff of Ministers employed under Part III of the MOP(S) Act obtain and maintain a Negative Vetting 2 security clearance. Under section 8(1) of the Determination, a Minister's Chief of Staff may request a variation of the security clearance requirement from the Secretary of the Department of Home Affairs.

Table 33: Possible Variations for Electorate Officers Employed by a National Security Committee Minister

Staff	Information Access	Security Clearance Variation
Electorate officers employed by a National Security Committee Minister	TOP SECRET or SECRET	No variation. Negative Vetting 2 security clearance required.
	PROTECTED, OFFICIAL: Sensitive or OFFICIAL	Variation to Baseline security clearance may be sought.
Electorate officers employed by a non-National Security Committee Minister	TOP SECRET	No variation. Negative Vetting 2 security clearance required.
	SECRET	Variation to Negative Vetting 1 security clearance may be sought.
	PROTECTED, OFFICIAL: Sensitive or OFFICIAL	Variation to Baseline security clearance may be sought.

The Secretary, Department of Home Affairs will consider a request to vary the requirement for a Negative Vetting 2 security clearance following endorsement by the relevant Department of State. Please complete the variation request form in PSPF Guidelines and send to PSPF@homeaffairs.gov.au

20.4 Other Commonwealth Officials

Commonwealth Officials such as Australian High Officer Holders, Statutory Office Holders, Special Envoys, Royal Commissioners and Judges, may be exposed to additional security risks by virtue of their position, profile or employment.

Where a Commonwealth Official is working within a portfolio, or as part of a Ministerial Directive, the Accountable Authority of the responsible entity is required to assess and address the security risks posed to these individuals.

Where appropriate, entities should consider providing security training, enhanced security and safety measures in the workplace, and addressing the physical security of Commonwealth Officials in transit whilst travelling and in their homes.

The Australian Federal Police and Home Affairs can provide guidance for entities and Commonwealth Officials to support security training and awareness, as well as insights regarding home security risk assessment and controls. Contact physec@homeaffairs.gov.au for advice.

Related Standards – Australian Officials and Office Holders

- Legislation: Departments of Staff - List of Commonwealth Entities
- Standard: Special Minister of State - Members of Parliament (Staff) (Employment Arrangements) Determination 2025
- Guidance: National Security Committee members

21 Maintenance and Ongoing Assessment

Effectively assessing and managing ongoing suitability ensures that entity personnel, including contractors, continue to meet eligibility and suitability requirements established at the point of engagement.

Entitles must maintain confidence in their personnel's ongoing suitability to access Australian Government resources, and manage the risk of malicious or unwitting insiders. It is critical that entities are aware of changes in their personnel's circumstances and workforce behaviours. This awareness is facilitated by effective information sharing and a positive security culture, recognising that security is everyone's responsibility.

Entities that sponsor Australian Government security clearances (Sponsoring Entity) and Authorised Vetting Agencies play a critical role in assuring ongoing suitability of personnel occupying positions that require access to security classified resources or additional levels of assurance.

21.1 Security Clearance Maintenance

A security clearance is based on a point in time assessment and the reliability of that assessment begins to decay from that point in time. Ongoing security management of clearance holders is essential to ensuring suitability from that point on. Effectively assessing and managing ongoing suitability ensures that entity personnel, including contractors, continue to meet eligibility and suitability requirements established at the point of engagement.

Entitles must maintain confidence in their personnel's ongoing suitability to access Australian Government resources, and manage the risk of malicious or unwitting insiders. It is critical that entities are aware of changes in their personnel's circumstances and workforce behaviours. This awareness is facilitated by effective information sharing and a positive security culture, recognising that security is everyone's responsibility.

Entities that sponsor Australian Government security clearances (Sponsoring Entity) and Authorised Vetting Agencies play a critical role in assuring ongoing suitability of personnel occupying positions that require access to security classified resources or additional levels of assurance.

Departments of State also have responsibilities for the assessment and management of the ongoing suitability of the ministerial staff of their portfolio ministers employed under Part III of the *Members of Parliament (Staff) Act 1984*. This includes the monitoring and management of the clearance holder.

Ensuring the ongoing eligibility and suitability of security cleared personnel to hold an Australian Government security clearance is the joint responsibility of Authorised Vetting Agencies, the Sponsoring Entity and the individual clearance holder. For details on the responsibilities for the ongoing assessment of ministerial staff employed under Part III of the *Members of Parliament (Staff) Act 1984*, see Members of Parliament (Staff) Act Employees.

21.2 Authorised Vetting Agencies Maintenance Responsibilities

Authorised Vetting Agencies are responsible for assessing how information relates to an individual's eligibility and suitability to hold a clearance.

21.2.1 Share Information of Concern

Authorised Vetting Agencies are required to share relevant information about security clearance holder's ongoing eligibility and suitability for employment or to hold an Australian Government security clearance. Authorised Vetting Agencies must share all information relating, or appearing to relate, to the ongoing suitability of personnel so the entity receiving the information can determine whether it is relevant.

This includes in relation to transfers of personnel, including temporary and permanent transfers within entities and to other entities. Note that information sharing may be limited by legislation, including the Australian Privacy Principles and an entity-enabling legislation. Sharing relevant information, even when it is sensitive personal information, does not breach an individual's privacy provided that informed consent is received and the information is used for the purpose for which consent was given.

21.2.2 Assess and Respond to Information of Concern

Authorised Vetting Agencies must assess and respond to information of concern about security clearance holders, which includes reports from sponsoring entities.

21.2.3 Review Conditional Security Clearances

The Authorised Vetting Agency must review the conditions of conditional security clearances annually. This ensures the conditions remain appropriate and continue to mitigate the identified concerns. As part of this review it may be necessary for the Authorised Vetting Agency to confirm with the Sponsoring Entity and clearance subject that the agreed conditions are still able to be met. Where concerns relevant to the clearance conditions have changed, the Authorised Vetting Agency will need to reassess the clearance holder's suitability to hold a security clearance.

Requirement 0161 | PER | AVA | 31 October 2024

The Authorised Vetting Agency reviews the conditions of conditional security clearances annually.

21.2.4 Review for Cause

Authorised Vetting Agencies must review a clearance holder's eligibility and suitability to hold a security clearance where concerns are identified. This process is known as a review for cause.

Concerns may arise from:

- advice from the clearance subject of a change in circumstances
- concern raised by the clearance subject's sponsoring entity
- a security incident involving the clearance subject
- non-compliance with clearance conditions, or
- other information or advice of concern received by the Authorised Vetting Agency about the clearance subject.

A review for cause may entail an investigation into specific concerns in the context of the whole person, or may prompt bringing forward a full revalidation of the security clearance.

In conducting a review for cause, Authorised Vetting Agencies are encouraged to:

- assess if a review for cause is warranted
- check with the sponsoring entity whether an ongoing investigation is underway that might be compromised by the review for cause and negotiate how to proceed
- advise the clearance subject any reviews for cause and provide the reasons for the review prior to starting, and
- undertake the checks required to resolve the concerns that led to the initiation of the review for cause, for example:

- targeted checks to resolve an issue
- a full revalidation if the concerns are wide ranging

- advise both the clearance subject and the sponsoring entity of the review for cause outcome.

ASIO may also undertake a review for cause of a security clearance suitability assessment on the basis of information of concern provided by the sponsoring entity, Authority Vetting Agency, other sources or as a result of its own security investigations.

Requirement 0162 | PER | AVA | 31 October 2024

The Authorised Vetting Agency reviews the clearance holder's eligibility and suitability to hold a security clearance, where concerns are identified (review for cause).

21.2.5 Implement TS-PA Standard

Authorised TOP SECRET-Privileged Access (TS-PA) Vetting Agencies are to implement specific requirements in the TS-PA Standard to assess and manage the ongoing suitability of TS-PA security clearance holders. This includes, but is not limited to, assessing information provided by sponsoring entities and other sources (including changes of circumstances), and conducting annual clearance reviews of all TS-PA security clearances, reviews for cause, and revalidation of TS-PA security clearances.

Requirement 0163 | PER | AVA | 31 October 2024

The Authorised TOP SECRET-Privileged Access Vetting Agency implements the TOP SECRET-Privileged Access Standard in relation to the ongoing assessment and management of personnel with TOP SECRET-Privileged Access security clearances.

21.3 Sponsoring Entities Maintenance Responsibilities

Sponsoring Entities are responsible for assessing how information relates to an entity's security risks, as well as a person's suitability for employment by the entity. This is particularly relevant where there are entity-specific employment requirements, such as a zero-tolerance drug and alcohol policy. Sponsoring entities must also share relevant information of concern and assess whether information is relevant to share.

The potential for insiders (employees, contractors and others with access to Australian Government resources) to betray the trust placed in them presents an enduring security risk. Insiders who compromise security may be unwitting or malicious. Possible motives are complex and can be driven by a mix of personal vulnerabilities, life events and situational factors.

While pre-employment screening and security clearance vetting provide an assessment of a person's suitability at a point in time, ongoing awareness of changes in the person's circumstances and workplace behaviours is essential to manage the risk of insider threat.

Entities are responsible for ensuring their personnel remain suitable to access Australian Government information, resources and activities for the entire period of their engagement. However, ensuring the ongoing eligibility and suitability of security cleared personnel to hold an Australian Government security clearance is the joint responsibility of Authorised Vetting Agency, the Sponsoring Entity and the individual clearance holder.

Effective assessment of personnel's ongoing suitability relies on entities encouraging and facilitating reporting of concerns, as well as collating and assessing information on personnel from a range of sources, including their management and colleagues. The way entities assess and manage ongoing suitability will depend on:

- the type of personnel (employees and contractors, security clearance holders or uncleared personnel) within the entity

- their access to classified and unclassified Australian Government information, resources and activities
- the entity's tolerance for security risks
- any risks that may be specific to the position, and
- the individual's personal risk profile.

Requirement 0164 | PER | All entities | 31 October 2024

The Sponsoring Entity actively assesses, monitors and manages the ongoing suitability of personnel.

Requirement 0165 | PER | All entities | 31 October 2024

The Sponsoring Entity monitors and manages compliance with any conditional security clearance requirements and reports any non-compliance to the Authorised Vetting Agency.

Requirement 0166 | PER | All entities | 31 October 2024

The Sponsoring Entity monitors and manages compliance with security clearance maintenance obligations for the clearance holders they sponsor.

21.3.1 Procedures for Assessing Managing Ongoing Suitability

The procedures for assessing and managing the ongoing suitability of personnel are listed below. Entities should include periodic employment suitability checks, as well as mechanisms to support reporting of concerns.

Table 34: Procedures for Assessing and Managing Ongoing Suitability

Procedure	Uncleared Personnel	Security Cleared Personnel
Building personnel security into performance management	Mandatory	Mandatory
Periodic employment suitability check	Mandatory	Mandatory
Annual security check	Recommended	Mandatory
Contact reporting obligations	Recommended	Mandatory
Security incident reporting and follow-up	Recommended	Mandatory
Collecting and assessing information on changes in personal circumstances	Recommended	Mandatory
Annual reviews of eligibility waivers	Not applicable	Mandatory for holders of a clearance subject to an eligibility waiver
Monitoring compliance with clearance conditions	Not applicable	Mandatory
Positive Vetting maintenance obligations in accordance with the SMSMP-PVG	Not applicable	Mandatory for Positive Vetting holders
TOP SECRET-Privileged Access clearance management in accordance with the TOP SECRET-Privileged Access Standard	Not applicable	Mandatory for TS-PA holders

21.3.2 Share Information of Concern

Sponsoring Entities are required to share relevant information about security clearance holders' ongoing eligibility and suitability for employment or to hold an Australian Government security clearance. This includes in relation to transfers of personnel, including temporary and permanent transfers within entities and to other entities. Note that information sharing may be limited by legislation, including the Australian Privacy Principles and an entity-enabling legislation.

Sharing relevant information, even when it is sensitive personal information, does not breach an individual's privacy provided that informed consent is received and the information is used for the purpose for which

consent was given. It is therefore critical that entities obtain informed consent from all personnel (existing and potential) to share sensitive personal information with other entities and the Authorised Vetting Agency for the purposes of assessing their ongoing eligibility and suitability. This consent is best obtained at key information collection points, such as pre-employment screening and at application for a security clearance, and updated at reasonable intervals, such as when conducting periodic employment checks and revalidation of a security clearance.

Requirement 0167 | PER | All entities | 31 October 2024

The Sponsoring Entity shares relevant information of concern, where appropriate.

21.3.3 Annual Security Checks

Sponsoring entities must conduct an annual security check with all security cleared personnel. An annual security check provides an opportunity to discuss any identified behavioural concerns, improve awareness and understanding of security obligations, and reinforces a positive security culture.

An annual security check addresses the person's:

- compliance with general security clearance obligations, as well as any conditions associated with a conditional security clearance. General security clearance obligations for clearance holders include compliance with entity security procedures, in particular:
  - reporting:
    - changes in circumstances
    - security incidents
    - suspicious, ongoing, unusual or persistent contact with foreign and Australian nationals who are seeking information that they do not need to know, as well as suspicious, ongoing, unusual or persistent incidents (e.g. such as social media contact)
  - completing security awareness training
- workplace behaviours to identify behaviours of concern.

Line managers are well placed to conduct an annual security check as they are likely to have the best knowledge of the behaviour of their personnel. Where appropriate, checks may be conducted in consultation with a security practitioner or an appropriate representative from the entity's human resources area. This may be particularly relevant where clearance conditions exist.

Entities may include the annual security check as part of their annual performance management process or as a stand-alone requirement. The annual security check does not replace an entity's responsibility to monitor and evaluate ongoing suitability through performance management, including code-of-conduct investigations.

If the sponsoring entities' annual security check identifies any concerns about a security clearance holder, they must share those concerns with the relevant Authorised Vetting Agency in addition to reporting any changes in circumstances, security incidents, and suspicious, ongoing, unusual or persistent contact reports as they occur.

Personnel holding a Positive Vetting security clearance are subject to additional requirements for annual security appraisals, which are set out in the SMSMP-PVG.

For personnel holding a TS-PA security clearance, the sponsoring entity is required to provide the relevant Authorised Vetting Agency with information from the annual security check and any information obtained as part of the insider threat program to inform the annual clearance review as set out in the TS-PA Standard.

Requirement 0168 | PER | All entities | 31 October 2024

The Sponsoring Entity conducts an annual security check with all security cleared personnel.

21.3.4 Review Eligibility Waivers

Sponsoring entities must review security clearance eligibility waivers at least annually and before revalidation of a security clearance.

An eligibility waiver is role-specific, non-transferable, finite and subject to review. In other words, the waiver applies only while the clearance holder remains in the position for which the clearance was granted. The waiver does not follow the clearance holder to any other position without review. An eligibility waiver is not open ended and is subject to regular review to confirm that there is a continuing requirement for the waiver.

It is important that personnel with a clearance subject to a waiver (as well as their line manager and in the case of ministerial staff their Chief of Staff or Minister, and potentially, co-workers) are informed of the limitations and conditions of the security clearance.

Requirement 0169 | PER | All entities | 31 October 2024

The Sponsoring Entity reviews eligibility waivers at least annually, before revalidation of a security clearance, and prior to any proposed position transfer.

21.3.5 Implement TS-PA Standard

Sponsoring agencies are to implement specific requirements in the TS-PA Standard to assess and manage the ongoing suitability of TS-PA security clearance holders. This includes, but is not limited to, conducting annual security checks, facilitating contact reporting, collecting and assessing information of concern (including changes of circumstances), monitoring compliance with conditional security clearances and reviewing eligibility waivers at least annually.

The TS-PA Standard requires all entities that manage TS-PA security clearance subjects to implement an insider threat program. Insider threat programs enable organisations to identify and manage insider risk in a holistic and coordinated way. An effective insider threat program can protect critical resources, counter unintentional and malicious incidents, prevent loss of data and prevent reputational damage. To be effective, these programs should be both proactive and prevention focussed.

Requirement 0170 | PER | All entities | 31 October 2024

The Sponsoring Entity monitors, assesses and manages personnel with TOP SECRET-Privileged access security clearances in accordance with the TOP SECRET-Privileged Access Standard.

21.4 Clearance Holder Maintentance Obligations

Holders of an Australian Government security clearance must meet obligations in order to retain their clearance. These obligations are established by the Authorised Vetting Agency at the time the clearance is granted.

The obligations include:

- maintain a standard of behaviour that the public would reasonably expect of someone who holds a position of public trust and who has found to meet the requirements to hold a security clearance
- avoid the intake of excessive amounts of alcohol
- not take illegal recreational or non-prescribed prescription drugs

- notify the Authorised Vetting Agency of any reportable changes in personal circumstances
- keep up-to-date with security clearance holder requirements
- cooperate with security clearance assurance activities and undertake required security awareness training
- protect classified information, resources and activities, including adherence to the need-to-know principle
- report any suspicious or unusual occurrences in or around the workplace to your entity's security unit immediately
- report all adverse changes in personality or suspicious behaviour displayed by work colleagues to the entity's security unit or Authorised Vetting Agency
- report suspicious, unusual or persistent contacts and incidents (contact reporting) with the entity's security unit
- act with honesty and integrity
- act in accordance with applicable laws, regulations, determinations and comply with any lawful and reasonable direction given by a person who has the authority to give it
- perform duties with care, diligence and with adherence to relevant security requirements
- use official information, equipment and facilities in a proper and secure manner
- disclose correct personal information when it is required for official purposes
- disclose and avoid real or apparent conflicts of interest, financial or otherwise, and
- not take advantage of a position or level of authority to seek or obtain a benefit, or to avoid a liability or penalty.

21.4.1 Reportable Changes in Circumstances

Clearance holders must report any changes in circumstances that may affect their suitability to hold a security clearance. The Authorised Vetting Agency or Sponsoring Entity will provide the clearance holder with a list of reportable changes in circumstances at the time the clearance is granted.

Reportable changes in circumstances include:

- change of name or identity, including gender
- change in citizenship or nationality, including dual-citizenship
- change in significant relationships, including entering into, or ceasing, a marriage, domestic partnership or significant personal relationship
- involvement or association with any group, society or organisation that may be a security concern
- involvement with any individual that may be a security concern
- suspicious, unusual, persistent, regular or ongoing contact with foreign nationals
- relatives residing in a foreign country
- changes of address or share-housing arrangements
- residence in a foreign country

- change in financial circumstances, including entering into a mortgage, incurring a significant debt, significant change to household income, receiving a lump sum payment or other financial windfall
- change of employer
- external business interests, including business activities with overseas individuals and entities
- change in health or medical circumstances
- change in criminal history, police involvement and association with criminal activity
- disciplinary procedures
- illicit or illegal drug use or alcohol problems
- changes in religious beliefs
- security incidents
- international travel, and
- identity document replacement following a cyber-hack, including driver's licence, passport and Medicare card.

21.5 Security Clearance Revalidation

Revalidation assesses a clearance holder's ongoing eligibility and suitability to hold a security clearance by repeating many of the checks undertaken to determine their initial suitability, and considering again the required character traits.

The revalidation covers the period since the initial clearance or last revalidation was completed, unless there are significant security concerns that raise doubts about the previous assessment, or indication of an enduring pattern of behaviour.

The Authorised Vetting Agency is responsible for commencing the revalidation process and should allow sufficient time to complete the revalidation before the due date so that the security clearance does not lapse. Where cases are complex or new security concerns are identified during the revalidation process, this may require additional time.

The Authorised Vetting Agency is required to share information of security concern about security clearance holders with the Sponsoring Entity so they can decide whether to suspend or limit the clearance holder's access to Australian Government classified information, systems or resources until the concerns are resolved.

Requirement 0171 | PER | AVA | 31 October 2024

The Authorised Vetting Agency reassesses a clearance holder's eligibility and suitability to hold a security clearance by revalidating minimum personnel security checks for a security clearance.

Requirement 0172 | PER | AVA | 31 October 2024

The Authorised Vetting Agency reassesses a clearance holder's eligibility and suitability to hold a Baseline, Negative Vetting 1, Negative Vetting 2 or Positive Vetting security clearance by considering their integrity in accordance with the Australian Government Personnel Security Adjudicative Standard.

Requirement 0173 | PER | AVA | 31 October 2024

The TOP SECRET-Privileged Access Vetting Authority reassesses a clearance holder's eligibility and suitability to hold a TOP SECRET-Privileged Access security clearance by assessing their trustworthiness in accordance with the TOP SECRET-Privileged Access Standard.

Requirement 0174 | PER | AVA | 31 October 2024

The Authorised Vetting Agency reassesses a clearance holder's eligibility and suitability to hold a security clearance by resolving any doubt in the national interest.

Table 35: Minimum Personnel Security Checks for Revalidation of Security Clearances

Check	Security Clearance Level				
	Baseline Vetting	Negative Vetting 1	Negative Vetting 2	Positive Vetting	TOP SECRET-Privileged Access [16]
Revalidation undertaken at least every:	15 years	10 years	5 to 7 years	5 to 7 years	TS-PA Standard
Updated personal particulars	Required	Required	Required	Required	TS-PA Standard
	Entities **must** confirm any changes to a clearance holder's personal particulars using identification documents verified with the issuing authority by using the Document Verification Service (or other source identity verification solution) for Australian-issued primary identification documents.				
Background assessment covering period since the initial clearance or last revalidation	Required	Required	Required	Required	TS-PA Standard
Referee checks covering period since the initial clearance or last revalidation	Required	Required	Required	Required	TS-PA Standard
Digital footprint check covering period since the initial clearance or last revalidation	Required	Required	Required	Required	TS-PA Standard
National police check/criminal history check	Required, no exclusion	Required, full exclusion	Required, full exclusion	Required, full exclusion	TS-PA Standard
Financial history assessment	Required	Required	Required	Required	TS-PA Standard
Financial statement	Not required	Required	Required	Required with supporting documents	TS-PA Standard
Financial probity assessment	Not required	Not required	Not required	Required	TS-PA Standard
Comprehensive financial assessment	Not required	Not required	Not required	Not required	TS-PA Standard
ASIO security clearance suitability assessment	Not required	Required	Required	Required	TS-PA Standard
Security interview	Not required	Not required	Required	Required	TS-PA Standard
Psychological assessment	Not required, however optional where deemed necessary by the Authorised Vetting Agency.			Required	TS-PA Standard
Overseas travel check	Not required	Not required	Not required	Not required	TS-PA Standard

[16] See the TOP SECRET-Privileged Access Standard.

21.5.1 Revalidation Timeframes

The Authorised Vetting Agency is responsible for commencing the revalidation process and should allow sufficient time to complete the revalidation before the due date so that the security clearance does not lapse. Where cases are complex or new concerns are identified during the revalidation process, this may require additional time.

Requirement 0175 | PER | AVA | 31 October 2024

The Authorised Vetting Agency commences the security clearance revalidation process in sufficient time to complete the revalidation before the due date so that the security clearance does not lapse.

Requirement 0176 | PER | AVA | 31 October 2024

The Authorised Vetting Agency shares information of concern about security clearance holders with the Sponsoring Entity so they can decide whether to suspend or limit the clearance holder's access to Australian Government classified information, resources or activities until the concerns are resolved.

See Table 35 for revalidation timeframes.

21.6 Information Sharing on Security Clearances

Sponsoring Entities and Authorised Vetting Agencies are required to share relevant information about security clearance holder's ongoing eligibility and suitability for employment or to hold an Australian Government security clearance. This includes in relation to transfers of personnel, including temporary and permanent transfers within entities and to other entities. Note that information sharing may be limited by legislation, including the Australian Privacy Principles and an entity-enabling legislation.

Sharing relevant information, even when it is sensitive personal information, does not breach an individual's privacy provided that informed consent is received and the information is used for the purpose for which consent was given. It is therefore critical that entities obtain informed consent from all personnel (existing and potential) to share sensitive personal information with other entities and the Authorised Vetting Agency for the purposes of assessing their ongoing eligibility and suitability. This consent is best obtained at key information collection points, such as pre-employment screening and application for a security clearance, and updated at reasonable intervals, such as when conducting periodic employment checks and revalidation of a security clearance.

Requirement 0177 | PER | All entities | 31 October 2024

The Sponsoring Entity shares relevant information of security concern, where appropriate with the Authorised Vetting Agency.

Requirement 0178 | PER | AVA | 31 October 2024

The Authorised Vetting Agency shares information of security concern about security clearance holders with the Sponsoring Entity.

Requirement 0179 | PER | AVA | 31 October 2024

The Authorised Vetting Agency assesses and responds to information of security concern about security clearance holders, including reports from Sponsoring Entities.

21.7 International Travel

Holding a security clearance is a privilege that comes with some restrictions. Negative Vetting 2, Positive Vetting and TOP SECRET-Privileged Access security clearances have specific obligations in relation to international

travel. Security clearance holders briefed into compartments for codeword material, will be advised of other obligations, including those related to international travel.

All personnel who obtain a TS-PA security clearance are provided with a copy of the annex to the TS-PA Standard that outlines their obligations for maintaining their security clearance. These obligations include approval of all international travel. Additional information on these obligations is available from the insider threat team in each Sponsoring Entity.

Requirement 0180 | PER | All entities | 31 October 2024

Negative Vetting 2 and higher clearance holders receive appropriate departmental travel briefings when undertaking international personal and work travel.

Related Standards – Maintenance and Ongoing Assessment

- Standard: Australian Government Personnel Security Adjudicative Standard.
- Standard: TOP SECRET-Privileged Access Standard (available to relevant entities through the Quality Assurance Office).
- Standard: Australian Government Security Caveat Standard (on GovTEAMS).

22 Separation

Separation processes are vital to protect Australian Government people, information and resources when personnel permanently or temporarily leave their employment with an entity. Effectively managing personnel security includes ensuring departing personnel fulfil their obligations to safeguard Australian Government resources; this limits the potential for the integrity, availability and confidentiality of those resources to be compromised.

Separating personnel include:

- security cleared personnel, non-security cleared personnel, contractors and third parties
- personnel voluntarily leaving an entity
- personnel whose employment has been terminated for misconduct or other adverse reasons
- personnel transferring temporarily or permanently to another Australian Government entity (including machinery of government changes)
- personnel taking extended leave for 6 months or longer, and
- personnel on leave without pay for 6 months or longer.

See Security Clearance Status.

22.1 Debriefing Procedures

Separating personnel are to be advised of their continuing obligations under the Commonwealth Criminal Code and other relevant legislation, and to acknowledge these obligations prior to separation from the entity. This acknowledgement helps safeguard Australian Government resources and limit the potential for the compromise of the integrity, availability and confidentiality of security classified information.

Separating personnel who have access to security classified information and caveated information where additional compartment briefing requirements apply, are required to be debriefed to ensure they understand their continuing obligations. See the Australian Government Security Caveat Standard for further information on compartment briefing.

Requirement 0181 | PER | All entities | 31 October 2024

The Chief Security Officer, Chief Information Security Officer (or other relevant security practitioner) is advised prior to separation or transfer of any proposed cessation of employment resulting from misconduct or other adverse reasons.

Requirement 0182 | PER | All entities | 31 October 2024

Separating personnel are informed of any ongoing security obligations under the *Commonwealth Criminal Code* and other relevant legislation and those holding a security clearance or access security classified information are debriefed prior to separation from the entity.

Requirement 0183 | PER | All entities | 31 October 2024

Separating personnel transferring to another Australian Government entity, the entity, when requested, provides the receiving entity with relevant security information, including the outcome of pre-employment screening checks and any periodic employment suitability checks.

Requirement 0184 | PER | All entities | 31 October 2024

Separating personnel transferring to another Australian Government entity, the entity reports any security concerns (as defined in the *Australian Security Intelligence Organisation Act 1979*) to the Australian Security Intelligence Organisation.

Requirement 0185 | PER | All entities | 31 October 2024

A risk assessment is completed to identify any security implications in situations where it is not possible to undertake the required separation procedures.

22.2 Withdrawal of Access

Separating personnel, including those on extended leave or transferring from the entity, are required to have their access to access to Australian Government resources withdrawn, removed or suspended as soon as there is no longer a legitimate business requirement for the access. This may also include where personnel performing malicious activities are detected.

It is important to ensure that all access is withdrawn, removed or suspended including access to physical facilities, technology systems access, non-standard system access (e.g. administration privileges, remote access, SECRET or TOP SECRET network access), and any other special access arrangements.

Requirement 0186 | PER | All entities | 31 October 2024

Separating personnel have their access to Australian Government resources withdrawn upon separation or transfer from the entity, including information, technology systems, and resources.

22.3 Post-Separation Security Clearance Actions

Security clearance actions only apply to personnel who hold a security clearance and take place after separation or transfer.

Requirement 0187 | PER | All entities | 31 October 2024

The Sponsoring Entity advises the relevant Authorised Vetting Agency of the separation of a clearance holder, including any relevant circumstances (e.g. termination for cause) and any details, if known, of another entity or contracted service provider the clearance holder is transferring to, along with any identified risks or security concerns associated with the separation.

Examples of identified risks or security concerns include:

- the individual's employment or contract is terminated for cause
- the individual was subject to a code of conduct investigation, whether completed or not
- the individual departed without a security debrief, and
- any outstanding security issues, including any risks or issues identified through a risk assessment completed where separation procedures are not possible.

Requirement 0188 | AVA | All entities | 31 October 2024

The Authorised Vetting Agency manages and records changes in the security clearance status of separating personnel, including a change of Sponsoring Entity, and transfer personal security files where a clearance subject transfers to an entity covered by a different Authorised Vetting Agency, to the extent that their enabling legislation allows.

Related Standards and Guidance – Separation

- Legislation: *Criminal Code Act 1995*
- Standard: Australian Government Security Caveat Standard (on GovTEAMS)
- Guidance: Commonwealth Criminal Code: A Guide for Practitioners

Part Six

Physical

Physical Security Lifecycle

Security Zones

Physical Security Measures and Controls

Event Security

Physical Lifecycle

23 Physical Security Lifecycle

Protective security must be integrated during all stages of the physical security lifecycle – planning, selecting, designing, approving, operating, modifying, reviewing and retiring entity facilities.

Entities need to adopt a consistent and structured approach to ensure protective security building construction, security zoning and physical security control measures of entity facilities. This ensures the protection of Australian Government people, information and physical resources secured by those facilities.

Requirement 0189 | PHYS | All entities | 31 October 2024

Protective security is integrated in the process of planning, selecting, designing and modifying entity facilities for the protection of people, information and resources.

23.1 Plan Entity Facilities

Site security planning includes assessing the suitability of the physical security environment of a proposed site for entity facilities and whether a facility can be constructed or modified to incorporate security measures that provide appropriate risk mitigation strategies. While security measures prevent or reduce the likelihood of events, the site and design also need to accommodate normal business.

An entity facility is the designated space, building or floor of a building that is designed and constructed in accordance with the PSPF and ASIO Technical Notes.

23.1.1 Facility Security Plan

A facility security plan is required for all sites (including new facilities under construction or existing facilities undergoing major refurbishment) to assess the security risks associated with the facilities':

- location and nature of the site
- ownership or tenancy of the site (sole or shared, including multiple entities sharing the same space)
- collateral exposure, such as the presence nearby of other 'attractive targets'
- access to the site for authorised personnel and the public (if necessary) and preventing access as required
- security classification of information and resources, including technology assets and related equipment, to be stored, handled or processed in each part of the site, this includes considering the need to hold security classified discussions and meetings
- other resources that will be on the site, and
- protective security measures required for:
    - the site as a whole
    - particular areas within the site (e.g. a floor or part of a floor that will hold information of a higher classification than the rest of the site)
    - storage, handling and processing of security classified information
    - security classified and other security classified discussions and meetings

- business hours and out-of-hours, as they are likely to be different, for example increased risks from public and client contact during business hours, and external threats such as break and enters or insider threat that may pose a greater risk out-of-hours.

Requirement 0190 | PHYS | All entities | 31 October 2024

A facility security plan is developed for new facilities, facilities under construction or major refurbishments of existing facilities.

23.1.2 Facility Site Selection

Site selection is an important part of planning and needs to factor in the suitability of the physical security environment of a proposed site. This assessment needs to consider the proposed entity facilities and whether a facility can be constructed or modified to incorporate security measures that provide appropriate risk mitigation strategies. While security measures prevent or reduce the likelihood of events, the site and design also need to accommodate normal business.

Security-in-depth is a multi-layered system in which security measures combine to make it difficult for intruders or authorised personnel to gain unauthorised access.

Table 36: Site Selection Factors for Australian Government Facilities

Factor	Description
Neighbourhood	Local threat environment from neighbourhood-related issues such as local criminal activity, risks from neighbouring entities and businesses, suitability of neighbours, oversight of entity operations.
Standoff perimeter	Standoff perimeter distances where there is an identified threat from pedestrians and vehicle-based improvised explosive devices (IED). However, it may not be possible in urban areas to achieve an effective standoff distance for some threats. Entities are encouraged to seek additional advice, for example, blast engineering advice.
Site access and parking	Need and ability to control access of pedestrians and vehicles to the site including the facility, parking and standoff perimeter.
Building access point	Ability to secure all building access points including entries and exits, emergency exits, air intakes and outlets and service ducts.
Security Zones	Ability of the site to establish Security Zones based on: • entity risk assessment • business impact levels, and • security-in-depth at the site.
Environmental risks	Seek specialist advice about the risk of natural disasters and suitable mitigation strategies and security products.

Requirement 0191 | PHYS | All entities | 31 October 2024

Decisions on entity facility locations are informed by considering the site selection factors for Australian Government facilities.

23.2 Design and Modify Entity Facilities

Protection of people, information and resources is achieved through a combination of physical and procedural security measures that prevent or mitigate threats and attacks. Successive layers of physical security are required when planning for new entity facilities or modifying existing facilities.

Protection of people, information and resources is achieved through a combination of physical and procedural security measures that prevent or mitigate threats and attacks. Facilities should be designed or modified using successive layers of physical security:

- **Deter** — measures that cause significant difficulty or require specialist knowledge and tools for adversaries to defeat.
- **Detect** — measures that identify unauthorised action are being taken or have already occurred.
- **Delay** — measures to impede an adversary during attempted entry or attack, or slow the progress of a detrimental event to allow a response.
- **Respond** — measures that resist or mitigate the attack or event when it is detected.
- **Recover** — measures to restore operations to normal levels following an event.

Facilities are designed and modified in order to define restricted access areas according to the five Security Zones, with increasing restrictions and access controls as the zones progress from Zone One to Zone Five.

Requirement 0192 | PHYS | All entities | 31 October 2024

When designing or modifying facilities, the entity secures and controls access to facilities to meet the highest risk level to entity resources in accordance with Security Zone restricted access definitions.

Table 37: Security Zone Restricted Access Definitions

Security Zone	Restricted Access Definition
Zone One	• Unrestricted public access
Zone Two	• Restricted public access • Unrestricted access for authorised personnel • May use single factor authentication for access control
Zone Three	• No public access • Visitor access only for visitors with a need-to-know and with close escort • Restricted access for authorised personnel • Single factor authentication for access control
Zone Four	• No public access • Visitor access only for visitors with a need-to-know and with close escort • Restricted access for authorised personnel with appropriate security clearance • Single factor authentication for access control
Zone Five	• No public access • Visitor access only for visitors with a need-to-know and with close escort • Restricted access for authorised personnel with appropriate security clearance • Dual factor authentication for access control

See Minimum Protections and Handling Requirements for details of security classified information and resources that can be used and stored in each Security Zone.

See Security Zones.

23.3 Construct or Lease Entity Facilities

All building work in Australia (including new buildings and new building work in existing buildings) must comply with the requirements of the Building Code of Australia (BCA).[17] Some older buildings may not comply with the current codes. The BCA classifies buildings according to the purpose for which they are designed, constructed or adapted to be used. The BCA requirements for commercial buildings, including facilities used by entities, provide an increased level of perimeter protection as well as protection for resources and information where the compromise, loss of integrity or unavailability would have a business impact level of medium or below.

Entities may include additional building elements to address specific risks identified in their risk assessment where building hardening[18] may provide some level of mitigation. For example:

- blast mitigation measures
- forcible attack resistance
- ballistic resistance
- siting of road and public access paths, and
- lighting (in addition to security lighting).

See Physical Security Measures for building construction protections for Security Zones. See Security Zone Certification and Accreditation.

Requirement 0193 | PHYS | All entities | 31 October 2024

Facilities are constructed in accordance the applicable ASIO Technical Notes to protect against the highest risk level in accordance with the entity security risk assessment in areas:

- accessed by the public and authorised personnel, and
- where physical resources and technical assets, other than security classified resources and technology, are stored.

Requirement 0194 | PHYS | All entities | 31 October 2024

Facilities for Security Zones Two to Five that process, store or communicate security classified information and resources are constructed in accordance with the applicable sections of ASIO Technical Note 1/15 – Physical Security Zones, and ASIO Technical Note 5/12 – Physical Security Zones (TOP SECRET) areas.

23.4 Operate and Maintain Entity Facilities

Staying secure requires ongoing activity to keep up to date with evolving security threats and vulnerabilities. Entities need to keep their security controls up to date and ensure they remain fit for purpose for the entity's operating environment.

Requirement 0195 | PHYS | All entities | 31 October 2024

Entity facilities are operated and maintained in accordance with Security Zones and Physical Security Measures and Controls.

[17] Various state and territory Acts and Regulations set out the legal framework for design and construction of buildings in accordance with the BCA.
[18] Building hardening is the process where a building is made a more difficult or less attractive target.

23.4.1 Review or Retire Entity Facilities

Undertake regular reviews to ensure your security measures remain fit-for-purpose. Identify changes in your use of facilities, your organisation or the threat environment. Use this information to inform improvements.

23.5 International Entity Facilities (including Missions and Posts)

All Australian Government international entity facilities, including missions, posts, embassies and consulates, including both those managed by DFAT and those managed by other entities, are required to meet the PSPF requirements and be included in the managing entity's annual PSPF report on security.

DFAT is responsible for all aspects of security policy affecting Australian missions and staff attached to DFAT-managed missions. DFAT also has a broader interest in international security conditions because of the high priority attached by the Australian Government to advising Australians about the risks they might face overseas.

The managing entity of each mission/post is responsible for implementing the PSPF to ensure appropriate physical, technical, information and personnel security procedures, as well as appropriate measures and standards, and for coordinating business continuity and contingency planning at each mission/post. The managing agency is normally DFAT, though other entities can assume this responsibility where DFAT is not represented.

See Minimum Protections and Handling Requirements for use and storage arrangements in each Security Zone for physical information and mobile devices.

See Physical Security Measures and Controls and Physical Security Measures and Controls Mandatory Elements in each Security Zone.

See Secure Areas in International Entity Facilities (including Missions and Posts).

Related Standards – Physical Security Lifecycle

- Standard: ASIO Technical Notes (on GovTEAMS)

24 Security Zones

24.1 Security Zones

Security Zones define restricted access areas with increasing restrictions and access controls as the Security Zones progress from Zone One to Zone Five. Security Zones are primarily used to protect the security classified information, resources or activities that will be processed, stored or communicated in that area.

Security Zones provide a methodology for scalable physical security risk mitigation that entities apply based on their security risk assessment. Security Zones are constructed to protect against the highest risk level in accordance with the entity's security risk assessment in areas accessed by the public and authorised personnel, and where physical information and resources, other than security classified information and resources, are used, transmitted, stored or discussed.

The number and type of Security Zones required by an entity depends on the classification of information accessed, stored, processed or transmitted in the entity.

See Construct or Lease Entity Facilities for Security Zone restricted access requirements.

Table 38: Security Zones Descriptions and Restricted Access

Security Zone	Description	Security Clearance for Ongoing Access	Restricted Access
Zone One	Public area[19]	• Not required - employment screening sufficient for entity personnel.	• Unrestricted public access.
Zone Two	Entity office area	• As per highest level of security classification information/resource the individual will access in the Zone. • Temporary access may be granted to individuals without a clearance, or holding a lower security clearance if the risk of doing so is approved by the CSO, CISO, or their delegate. • If none stored, determined by entity risk assessment.	• Restricted public access. • Unrestricted access for authorised personnel. • May use single factor authentication for access control.
Zone Three	Entity restricted office area	• As per highest level of security classification information/resource the individual will access in the Zone. • Temporary access may be granted to individuals without a clearance, or holding a lower security clearance if the risk of doing so is approved by the CSO, CISO, or their delegate. • If none stored, determined by entity risk assessment.	• No public access. • Visitor access only for visitors with a need-to-know and with close escort. • Restricted access for authorised personnel. • Single factor authentication for access control.
Zone Four	Entity restricted office area	• As per highest level of security classification information/resource stored in the Zone. • Temporary access may be granted to individuals with a lower security clearance if	• No public access. • Visitor access only for visitors with a need-to-know and with close escort.

[19] The inner perimeter of Zone One may move to the building or premise perimeter out-of-hours if exterior doors are secured.

Security Zone	Description	Security Clearance for Ongoing Access	Restricted Access
		the risk of doing so is approved by the CSO, CISO, or delegate.	• Restricted access for authorised personnel with appropriate security clearance. • Single factor authentication for access control.
Zone Five	Entity highly restricted office area	• As per highest level of security classification information/resource stored in the Zone. • Temporary access may not be granted unless Exceptional Circumstances.	• No public access. • Visitor access only for visitors with a need-to-know and with close escort. • Restricted access for authorised personnel with appropriate security clearance. • Dual factor authentication for access control.

See Minimum Protections and Handling Requirements for use and storage arrangements in each Security Zone for physical information and mobile devices.

See Physical Security Measures and Controls and Physical Security Measures and Controls Mandatory Elements in each Security Zone.

24.1.1 Secure Areas in International Entity Facilities (including Missions and Posts)

The location and threat environment of some Australian Government international entity facilities (including missions and posts) necessitate more stringent protective security arrangements than entity facilities located in Australia. DFAT-managed international entity facilities use different terminology for 'Secure Areas' in place of Security Zones, most of which exceed the protections required for their Security Zone counterparts. These security areas used in some international entity facilities are described in Table 39.

Table 39: Secure Area Descriptions and Restricted Access in DFAT-managed International Entity Facilities (including Missions and Posts)

Secure Area	Security Clearance for Access	Restricted Access
Public Area	Not required.	• Public access
Controlled Access Area	Baseline security clearance (Locally engaged staff probity check)	• No public access • Visitor access only for visitors with a need-to-know and with close escort • Restricted access for authorised personnel, including locally engaged staff • Single factor authentication for access control
Restricted Area	Negative Vetting 1 or higher	• No public access • Visitor access only for visitors with a need-to-know and with close escort • Restricted access for authorised personnel with appropriate security clearance • No electronic devices permitted • Dual factor authentication for access control
Secure Area	Negative Vetting 2 or higher	• Highly restricted officer area • No public access

Secure Area	Security Clearance for Access	Restricted Access
		• No visitor access • Restricted access for authorised personnel with appropriate security clearance • No electronic devices permitted • Highly restricted dual factor authentication for access control

24.2 Security Zone Certification and Accreditation

Certification and Accreditation of Security Zones provides a level of confidence that when information is shared, other entities can and will adequately protect it.

Entities are required to certify and accredit all areas where security classified information and resources will be used, transmitted, stored or discussed, in accordance with the applicable ASIO Technical Notes and authorities.

24.2.1 Security Zone Certification Authorities

Certification of Security Zones establishes the zone's compliance with the minimum physical security requirements to the satisfaction of the relevant certification authority. See Minimum Protections and Handling Requirements for use and storage arrangements in each Security Zone for physical information and mobile devices.

See Physical Security Measures and Controls Mandatory Elements in each Security Zone.

See Secure Areas in International Entity Facilities (including Missions and Posts) for equivalent international secure areas.

For Zones One to Four, the CSO (or delegated security practitioner) may certify that the control elements have been implemented and are operating effectively.

For Zone Five areas that are used to handle TOP SECRET information or aggregated information where the aggregation of information increases its business impact level to catastrophic, ASIO-T4 is the Certification Authority.

Table 40: Certification Authority for Security Zones

	Certification Authority				
Control measure	Zone One	Zone Two	Zone Three	Zone Four	Zone Five
Entity specific threat assessments, for example police threat assessment	Chief Security Officer (or delegate) if the need is identified in the risk assessment				
Entity security risk assessment	Chief Security Officer (or delegate)				
Site security plan	Chief Security Officer (or delegate)				
SCEC-approved Type 1A security alarm system	Not applicable	Not applicable	Not applicable	SCEC-endorsed Security Zone consultant (regular servicing by authorised provider required)	
Commercial alarm system	Suitably qualified system installer or designer (regular servicing by authorised provider required)			Not applicable	Not applicable
Electronic access control system	Suitably qualified system installer or designer (current software patches and no obsolete components required)				

	Certification Authority				
Control measure	Zone One	Zone Two	Zone Three	Zone Four	Zone Five
Other zone requirements	Chief Security Officer (or delegate)				
Certification (including site inspection)	Chief Security Officer (or delegate)	Chief Security Officer (or delegate)	Chief Security Officer (or delegate)	Chief Security Officer (or delegate)	ASIO-T4

See also Technology System Authorisation.

Requirement 0196 | PHYS | All entities | 31 October 2024

Security Zones One to Four are certified by the Certification Authority in accordance with the PSPF and applicable ASIO Technical Notes before they are used operationally.

Requirement 0197 | PHYS | All entities | 31 October 2024

Security Zone Five areas that contain TOP SECRET security classified information or aggregated information where the compromise of confidentiality, loss of integrity or unavailability of that information may have a catastrophic business impact level, are certified by ASIO-T4 before they are used operationally.

24.2.2 Security Zone Accreditation Authorities

Security Zone accreditation involves compiling and reviewing all applicable certifications and other deliverables for the zone to determine and accept the residual security risks. Approval is granted for the Security Zone to operate at the desired level for a specified time.

Table 41: Accreditation Authority for Security Zones

Security Zone	Accreditation Authority
Zones One to Five	Chief Security Officer (or delegate) when the controls are certified as meeting the applicable requirements for the Security Zone
Sensitive Compartmented Information Facility (SCIF) used to secure and access TOP SECRET systems and/or sensitive compartmented information	Australian Signals Directorate

Requirement 0198 | PHYS | All entities | 31 October 2024

Security Zones One to Five are accredited by the Accreditation Authority before they are used operationally, on the basis that the required security controls are certified and the entity determines and accepts the residual risks.

Requirement 0199 | PHYS | All entities | 31 October 2024

Sensitive Compartmented Information Facility areas used to secure and access TOP SECRET systems and security classified compartmented information are accredited by the Australian Signals Directorate before they are used operationally.

24.2.3 Security Zone Recertifcation and Reaccreditation

Security Zone certification is time-limited. The assessment of compliance is specific to the role of the facility and the resources contained within the facility at the time of certification. This means that facilities may require recertification from time to time.

Security Zone recertification and reaccreditation may be triggered by circumstances including:

- expiry of the certification due to the passage of time

- changes in the assessed business impact level associated with the security classified information or resources handled or stored within the zone
- significant changes to the architecture of the facility or the physical security controls used
- any other conditions stipulated by the Accreditation Authority, such as changes to the threat level or other environmental factors of concern.

Related Standards – Security Zones

- Standard: ASIO Technical Note 1/15 – Physical Security Zones (on GovTEAMS)
- Standard: ASIO Technical Note 5/15 – Physical Security Zones (TOP SECRET areas) (on GovTEAMS)
- Standard: Annex A of ASIO Technical Note 5/12 – Compartments within Zone Five areas (on GovTEAMS)
- Standard: ASD's Information Security Manual

25 Physical Security Measures and Controls

There are a range of physical security measures that protect entity resources from being made inoperable or inaccessible, or being accessed, used or removed without proper authorisation. Entities enhance the protection of their physical resources by using successive layers or combinations of procedural and physical security measures.

Each Security Zone has individual control elements to achieve the required level of protection. These zone controls provide a level of assurance against:

- the compromise, loss of integrity or unavailability of sensitive and security classified information, and
- the compromise, loss or damage of sensitive and security classified resources.

These control elements are based on the ASIO Technical Notes for the minimum requirements to protect security classified information and assets. The physical security measures detailed in the applicable ASIO Technical Notes are designed to protect security classified information and resources from covert and surreptitious attack.

Entity specific resources may require additional security mitigation treatments based on their risk assessment.

Requirement 0200 | PHYS | All entities | 31 October 2024

Physical security measures are implemented to minimise or remove the risk of information and physical asset resources being made inoperable or inaccessible, or being accessed, used or removed without appropriate authorisation.

Requirement 0201 | PHYS | All entities | 31 October 2024

Physical security measures are implemented to protect entity resources, commensurate with the assessed business impact level of their compromise, loss or damage.

Requirement 0202 | PHYS | All entities | 31 October 2024

Physical security measures are implemented to minimise or remove the risk of harm to people.

25.1 Authorised Equipment and Commercial Services

The Security Construction and Equipment Committee (SCEC) is responsible for evaluating the suitability of security equipment for use by the Australian Government. The SCEC determines which products will be evaluated and the priority of evaluation. Evaluated security products protect classified information which would result in a business impact level of high or above if compromised.

Evaluated products are assigned a security level (SL) rating numbered 1 to 4. SL4 products offer high level security, while SL1 products offer the lowest acceptable level of security for government use. Approved items are listed in the SCEC Security Equipment Evaluated Product List (available to government personnel on GovTEAMS).

Entities may use SCEC-approved security equipment even where it is not mandated. Alternatively, entities can use suitable commercial equipment that complies with identified security related Australian and International Standards for the protection of people and information, as well as physical resources that do not have a confidentiality Business Impact Level (BIL) of medium or above. ASIO-T4 has developed the Security Equipment Guides to assist entities to select security equipment not tested by SCEC.

25.2 Security Containers, Cabinets and Rooms

Suitably assessed security containers and cabinets are used to secure information, portable and valuable assets, and money.

Requirement 0203 | PHYS | All entities | 31 October 2024

The appropriate container, safe, vault, cabinet, secure room or strong rooms is used to protect entity information and resources based on the applicable Security Zone and business impact level of the compromise, loss or damage to information or physical resources.

25.2.1 SCEC Approved Security Containers

SCEC approved security containers are for storage of security classified information and resources, and are not for the storage of other valuable, important, attractive, significant or dangerous resources. The designs of these containers provide a high level of tamper evidence of covert attack and significant delay from surreptitious attack, but provide limited protection from a forcible attack.

There are three levels of SCEC-approved containers:

- Class A—protects information that has an extreme or catastrophic business impact level in situations assessed as high risk. These containers can be extremely heavy and may not be suitable in some facilities with limited floor loadings.
- Class B—protects information that has an extreme or catastrophic business impact level in situations assessed as low risk. They are also used for information that has a high or extreme business impact level in situations assessed as higher risk. These containers are robust filing cabinets or compactuses fitted with combination locks. Class B containers size and weight needs to be considered when selecting a location. There are broadly two types of Class B containers:
    - heavy constructed models that are suitable for use where there are minimal other physical controls
    - lighter constructed models that are used in conjunction with other physical security measures.
- Class C—protects information up to an extreme business impact level in situations assessed as low risk. They are also used for information that has a medium business impact level in situations assessed as higher risk by the entity. These containers are fitted with a SCEC-approved restricted keyed lock and are of similar construction to the lighter Class B containers.

25.2.2 Commercial Safes and Vaults

Commercial safes and vaults provide a level of protection against forced entry. A vault is a secure space that is generally built in place and is normally larger than a safe. A safe is normally smaller than a vault and may be moveable. Safes and vaults provide varying degrees of protection depending on the construction and may be used to store valuable physical resources. Table 42 details the commercial safes and vaults to protect physical resources (other than classified resources) in each Security Zone.

See Minimum Protections and Handling Requirements for details of security classified information and resources that can be used and stored in each Security Zone.

Table 42: Commercial Safes and Vaults to Protect Physical Resources (other than classified resources)

Business impact level	1 Low business impact	2 Low to medium business impact	3 High business impact	4 Extreme business impact	5 Catastrophic business impact
Zone One	Determined by an entity risk assessment, locked commercial container recommended	Determined by an entity risk assessment, commercial safe or vault recommended	AS 3809 commercial safe or vault	AS 3809 high security safe or vault	Not to be held unless unavoidable
Zone Two	Determined by an entity risk assessment, locked commercial container recommended	Determined by an entity risk assessment	Commercial safe or vault	AS 3809 medium security safe or vault recommended	Not to be held unless unavoidable
Zone Three	Determined by an entity risk assessment	Determined by an entity risk assessment	Determined by an entity risk assessment, commercial safe or vault recommended	AS 3809 commercial safe or vault recommended	AS 3809 high or very high security safe or vault recommended
Zone Four	Determined by an entity risk assessment	Determined by an entity risk assessment	Determined by an entity risk assessment	Commercial safe or vault recommended	AS 3809 medium or high security safe or vault recommended
Zone Five	Determined by an entity risk assessment	Determined by an entity risk assessment	Determined by an entity risk assessment	Commercial safe or vault recommended	AS 3809 medium or high security safe or vault recommended

25.2.3 Secure Rooms and Strongrooms

Secure rooms and strongrooms may be used instead of containers to secure large quantities of official information, classified resources and valuable assets, where the compromise, loss or damage would have a moderate business impact level.

Secure rooms are designed to protect its contents from covert attack and have some degree of fire protection of the contents if the secure room is constructed properly. Secure rooms are suitable for open storage of large quantities of official information and classified resources, while maintaining the levels of protection provided by a Class A, B or C container.

Advice on construction specifications for secure rooms is detailed in the ASIO Technical notes available for Australian Government security personnel only from the protective security policy community on GovTEAMS:

- Technical Note 7-06 Class A Secure Room
- Technical Note 8-06 Class B Secure Room
- Technical Note 9-06 Class C Secure Room.

SCEC-approved commercial Class A and B doors and demountable security rooms are listed on the Security Equipment Evaluated Products List.

25.3 Perimeter Doors, Locks and Hardware for Facilities

Locks can deter or delay unauthorised access to information and physical resources. SCEC-approved locks and hardware rated to Security Level 3 are required in Security Zones Three to Five (see the Security Equipment Evaluated Product List available on GovTEAMS).

Entities may use suitable commercial locking systems in other areas.

Requirement 0204 | PHYS | All entities | 31 October 2024

Perimeter doors and hardware in areas that process, store or communicate security classified information or resources are constructed and secured in accordance with the physical security measures and controls for perimeter doors and hardware.

See Physical Security Measures and Controls Mandatory Elements

See also Table 43: Physical Security Measures and Controls – Perimeter Doors and Hardware for mandatory requirements.

25.3.1 Restricted Keying Systems

Restricted keying systems provide a level of assurance to entities that unauthorised duplicate keys have not been made. To mitigate common keying system compromises, controls include:

- legal controls, for example registered designs and patents
- levels of difficulty in obtaining or manufacturing key blanks and the machinery used to cut duplicate keys, or
- levels of protection against compromise techniques, such as picking, impressioning and decoding.

25.4 Access Control Systems

Access control is a measure or group of measures that allows authorised personnel, vehicles and equipment to pass through protective barriers while preventing unauthorised access.

Requirement 0205 | PHYS | All entities | 31 October 2024

Access by authorised personnel, vehicles and equipment to Security Zones One to Five is controlled in accordance with the physical security measures and controls for access control for authorised personnel.

See Table 38: Security Zones Descriptions and Restricted Access and Table 44: Physical Security Measures and Controls – Access Control for Authorised Personnel (including contracted and seconded staff) for mandatory requirements.

25.4.1 Identity Cards

Identity cards allow the recognition of authorised personnel in entity facilities. Identity cards are an essential access control measure and should be:

- uniquely identifiable
- include a large photo of the holder's face and large scale print of their name and surname
- worn by all authorised personnel, authorised contractors and visitors
- be clearly displayed at all times while in entity facilities (and removed outside entity facilities), and
- audited regularly in accordance with the entity's risk assessment.

Identity card-making equipment and spare, blank or returned cards should be secured within a Security Zone Two or higher zone based on the entity's security risk assessment.

25.4.2 Authentication Factors and Dual Authentication

There are three categories of authentication factors that can be used to validate identity:

- what you have (for example keys, identity cards, passes)
- what you know (for example personal identification numbers), and
- who you are (for example visual recognition, biometrics).

Dual authentication requires the use of factors from two different categories, for example an identity card and a personal identification number.

Dual authentication is required for access to Security Zone Five. Entities may use dual authentication in other circumstances where their security risk assessment identifies a need to mitigate the risk of unauthorised access.

25.4.3 Visitor Access Control

A visitor is anyone who is not authorised to have ongoing access to all or part of an entity's facilities. Visitor access control is normally an administrative process; however, this can be supported by use of electronic access control systems.

Visitor registers are used for recording visitor's name, entity or organisation, purpose of visit, date and time of arrival and departure, and visitor pass number. Visitor passes are required to be:

- visible at all times
- collected and disabled at the end of the visit, and
- audited at the end of the day.

Receptionists and guards are recommended to have:

- detailed auditable visitor control and access instructions, and
- a secure method of calling for immediate assistance if threatened.

Requirement 0206 | PHYS | All entities | 31 October 2024

Access by visitors to Security Zones One to Five is controlled in accordance with the physical security measures and controls for access control for visitors.

See Table 45: Physical Security Measures and Controls – Access Control for Visitors.

25.4.3.1. Foreign Security Assessment Visits

Some international agreements or arrangements allow security assessment visits where foreign personnel access secure areas or facilities. The purpose of these visits is to assure foreign governments of the suitability and implementation of security procedures and the protection of areas or facilities where their information or resources are stored and handled.

Foreign government personnel visitors must hold a valid level of Australian or foreign government security clearance for access to the foreign government information and resources in the facility. International agreements and arrangements commonly require that the National Security Authority or Competent Security Authority are advised of any security assessment visits. See International Information Sharing.

25.4.3.2. Event Security

Entities must consider the security of all Australian Government events they manage, plan or host, whether organised by the entity or outsourced.

The Department of Home Affairs is responsible the coordination of national security arrangements, including developing strategic security risk assessments for events that are declared by the Prime Minister as Special Events.

State or territory government agencies should seek advice from the jurisdictional police or the jurisdictional agency responsible for the event on behalf of their government.

25.4.4 Ongoing Third-party Access to Facilites

Requirement 0207 | PHYS | All entities | 31 October 2024

The Accountable Authority or Chief Security Officer approves ongoing (or regular) access to entity facilities for people who are not directly engaged by the entity or covered by the terms of a contract or agreement, on the basis that the person:

- has the required security clearance level for the Security Zone/s, and
- a business need supported by a business case and security risk assessment, which is reassessed at least every two years.

25.5 Perimeter Access Control

Perimeter access controls restrict access to entity facilities and increase the level of deterrence, detection and delay.

Types of perimeter access controls include, but are not limited to:

- fences and walls used to define and secure the perimeter
- pedestrian barriers used to restrict pedestrian access through fences or walls by installing entry and exit points, and
- vehicle security barriers.

The level of protection a fence provides depends on its height, construction, materials, access control and any additional features that increase its performance or effectiveness, for example lighting, signage or connection to an external alarm.

Entities that face significant threats and those with larger, multi-building facilities may require perimeter access controls to restrict access to their facilities.

The Security Equipment Evaluated Product List contains details on perimeter intrusion detection devices. Refer to the ASIO-T4 Security Equipment Guide SEG-003 Perimeter Security Fences, SEG-024 Access Control Portals and Turnstiles, Australian Standard AS 1725.1—Chain-link fabric security fencing and gates, and Australian Standard AS 3016—Electrical installations—Electric security fences; all available on GovTEAMS.

25.6 Security Alarm Systems

Security alarm systems (SAS) provide detection of unauthorised access to entity facilities. However, an alarm system is only effective if it is used in conjunction with other measures designed to delay and respond to unauthorised access. Where possible security alarm systems should be configured to monitor devices in high risk areas such as irregularly accessed areas, roof spaces, inspection hatches and underfloor cavities.

Alarm systems can be broadly divided into two types:

- Perimeter (or external) Intrusion Detection Systems (PIDS) or alarms – PIDS provide detection of unauthorised breaches of the perimeter and may be of value to entities that have facilities enclosed in a perimeter fence or facilities located on a large land holding.
- internal security alarm systems – a combination of SCEC-approved security alarm systems and commercial security alarm systems can be used after consideration of the zone requirements and entity security risk assessment. Security alarm systems may be single sector or sectionalised to give coverage to specific areas of risk. Sectionalised alarm systems allow greater flexibility as highly sensitive areas can remain secured when not in use and other parts of the facility are open.

Security alarm systems require periodic testing and maintenance from an authorised service provider, preferably every two years (at a minimum) to ensure the alarm system is continually operational.

Requirement 0208 | PHYS | All entities | 31 October 2024

Unauthorised access to Security Zones One to Five is controlled in accordance with the physical security measures and controls for security alarm systems.

See Table 46: Physical Security Measures and Controls – Security Alarm Systems (SAS) for mandatory elements.

25.6.1 SCEC-Approved Type 1A Security Alarm Systems

SCEC-approved Type 1A security alarm systems provide malicious insider threat protection not provided by commercial systems. SCEC-approved Type 1A security alarm systems protect SECRET, TOP SECRET and certain codeword information where the compromise, loss of integrity or unavailability of the aggregate of information would cause extreme or catastrophic damage to Australia's national security.

ASIO-T4 provides advice on SCEC Type 1A security alarm systems and may approve, other site-specific arrangements for Zones Four and Five. ASD may approve site-specific arrangements for the security of sensitive compartmented information facilities (SCIF).

SCEC Security Zone Consultant Register located in the Protective Security Policy community on GovTEAMS lists SCEC-endorsed Security Zone Consultants by state and territory.

25.6.2 Commercial Security Alarm Systems

Commercial security alarm systems are graded on the level of protection they provide. The AS/NZS 2201.1 levels of security alarm systems include:

- Class 1 or 2 are only suitable for domestic use.
- Class 3 or 4 are suitable for the protection of normal business operations in most entities.
- Class 5 is suitable for protection of information and physical resources up to an extreme business impact level.

There are a number of commercial security alarm options that may be suitable, including:

- duress alarms (or request-for-assistance devices) allow personnel to call for assistance in response to a threatening incident
- individual item alarms (or alarm circuits) provide additional protection to valuable physical resources in premises and on display, and

- vehicle alarms to remotely monitor vehicle security where the business impact level of the loss of information or physical resources in the vehicle, or the vehicle itself, is high or above. Remote vehicle alarms may also be linked to remote vehicle tracking and immobiliser systems.

25.7 Interoperability of Security Alarm Systems and External Integrated Systems

The more interoperability between security alarm systems and external integrated systems (e.g. building management systems, closed circuit television and electronic access controls systems) the greater the security alarm system vulnerabilities to unauthorised access and tampering.

Entities must ensure:

- the alarm cannot be disabled by the access control system
- there is limited one way interoperability in accordance with the Type 1A SAS for Australian Government—Product Integration specification, and
- there is limited one way interoperability in accordance with the Type 1A SAS for Australian Government—Product: Integration specification. The alarm system may disable access control system when activated.

See Table 46: Physical Security Measures and Controls – Security Alarm Systems (SAS).

25.8 Security Guards

Security guards provide deterrence against loss of information and physical resources and can provide a rapid response to security incidents. Stationary guards and guard patrols may be used separately or in conjunction with other security measures. The response time for off-site guards should be less than the delay given by the total of other controls.

Requirement 0209 | PHYS | All entities | 31 October 2024

Security guard arrangements in Security Zones One to Five are established in accordance with the physical security measures and controls for security guards.

See Table 47: Physical Security Measures and Controls – Security Guards for mandatory elements.

25.8.1 Out-of-Hours Security Guard Services

Entities may use security guard services out-of-hours in response to alarms for all Security Zones. Entities may use out-of-hours guard patrols instead of a security alarm system in Zones Two and Three. However, for Zone Three, where out-of-hours guard patrols are used instead of security alarm systems, patrols must be performed at random intervals within every four hours.

25.9 Technical Surveillance Countermeasures

Technical Surveillance Countermeasures (TSCMs) are implemented to protect security classified discussions from technical compromise. This can be achieved through real-time audio interception using electronic transmitting and receiving equipment or by a TSCM inspection that searches for surveillance devices. These countermeasures are also applicable to covert video recordings.

A TSCM inspection is a security mitigation that deters, detects and defeats covert electronic devices that may be audio, video and imaging technologies. A TSCM inspection identifies technical security weaknesses and vulnerabilities and provides a high level of assurance that an area is not technically compromised, however it is

not a guarantee. Developers of covert technology constantly update and develop new equipment and technologies to avoid detection.

Contact ASIO-T4 for advice on TSCM inspections. Requests for TSCM inspections can be made in accordance with the Protective Security Circular No 165 Facilitating TSCM inspections in Australia. See the Information Security Manual for controls to protect technology used for security classified discussions.

Requirement 0210 | PHYS | All entities | 31 October 2024

Technical surveillance countermeasures for Security Zones One to Five are established in accordance with the physical security measures and controls for technical surveillance countermeasures.

See Table 48: Physical Security Measures and Controls – Technical surveillance counter-measures (TSCM) for mandatory elements.

Related Standards – Physical Security Measures and Controls

- Standard: SCEC Security Equipment Evaluated Product List (available for Australian Government security personnel only on GovTEAMS).
- Standard: Protective Security Circular No 165 Facilitating TSCM inspections in Australia (available for Australian Government security personnel only on GovTEAMS).
- Standard: ASIO-T4 Security Equipment Guide SEG-003 Perimeter Security Fences List (available for Australian Government security personnel only on GovTEAMS).
- Standard: ASIO-T4 Security Equipment Guide SEG-024 Access Control Portals and Turnstiles List (available for Australian Government security personnel only on GovTEAMS).
- Standard: Australian Standard AS 1725.1—Chain-link fabric security fencing and gates
- Standard: Australian Standard AS 3016—Electrical installations—Electric security fences.

25.10 Physical Security Measures and Controls Mandatory Elements

Table 43: Physical Security Measures and Controls – Perimeter Doors and Hardware

Measure	Zone One	Zone Two	Zone Three	Zone Four	Zone Five
Doors	• Determined by entity risk assessment	• Constructed in accordance with ASIO Technical Note 1/15 – Physical Security Zones	• As for Zone Two	• As for Zone Two	• Constructed in accordance with ASIO Technical Note 5/12 – Physical Security Zones (TOP SECRET) areas
Locks and hardware	• Determined by entity risk assessment. (May use commercial locking systems)	• As for Zone One	• SCEC-approved Security Level 3 (SL3) locks and hardware	• As for Zone Three	• As for Zone Three
Keying systems	• Determined by entity risk assessment (SCEC-approved SL1 or SL2 keying system recommended)	• As for Zone One	• Minimum SCEC-approved SL3 keying system	• As for Zone Three	• As for Zone Three

Table 44: Physical Security Measures and Controls – Access Control for Authorised Personnel (including contracted and seconded staff)

See Security Zones for Security Clearance requirements for ongoing and temporary access.

Measure	Zone One	Zone Two	Zone Three	Zone Four	Zone Five
Access control systems	• Determined by entity risk assessment	• Determined by entity risk assessment	• Sectionalised access control system required o Electronic Assess Control Systems (EACS) is required where there are no other suitable verification and access control measures in place o Verify the identity of all personnel, including contractors, issued with EACS access cards at the time of issue (using the National Identity Proofing Guidelines to a minimum level 3)	• As Zone Three, and sectionalised access control system is: o Directly managed and controlled by the entity o Maintained by appropriately cleared contractors o Privileged operators and users are appropriately trained and security cleared to the level of the Zone	• As for Zone Four
Authentication Factors	• Determined by entity risk assessment	• Determined by entity risk assessment (Single factor authentication for access control recommended)	• Single factor authentication for access control	• Single factor authentication for access control • Dual authentication may be used where entity risk assessment identified a need to reduce risk of unauthorised access	• Dual authentication for access control
Identity cards	• Determined by entity risk assessment. (Identity cards recommended)	• Determined by entity risk assessment. (Identity cards recommended in office environments)	• Identity cards with personal identity verification required	• As for Zone Three	• As for Zone Three
Audit logs	• Determined by entity risk assessment	• Determined by entity risk assessment	• Full audit of access control systems required • Audit logs are regularly reviewed to identify unusual or prohibited activity	• As for Zone Three	• Full audit of access control systems and dual authentication required • Audit logs are regularly reviewed to identify unusual or prohibited activity

Table 45: Physical Security Measures and Controls – Access Control for Visitors

Measure	Zone One	Zone Two	Zone Three	Zone Four	Zone Five
Visitor access	• Determined by entity risk assessment	• Determined by entity risk assessment	• Yes, if visitors (and contractors) have a need-to-know	• Only visitors (and contractors) with a need-to-know, and relevant security clearance and if required, relevant compartment briefings)	• Only visitors (and contractors) with a need-to-know and relevant security clearance (and if required, relevant compartment briefings)
Visitor pass	• Determined by entity risk assessment	• Visitor pass required if no other controls in place to limit access	• Visitor pass required	• Visitor pass required	• Visitor pass required
Visitor record	• Determined by entity risk assessment	• Visitor record recommended	• Detailed auditable visitor record required	• Detailed auditable visitor record required	• Detailed auditable visitor record required

Measure	Zone One	Zone Two	Zone Three	Zone Four	Zone Five
Visitor escort	• Determined by entity risk assessment	• Visitor escort recommended in sensitive areas	• Visitor close escort required • Groups limited to 5 visitors per escort recommended	• Visitor close escort in constant line of sight required • Groups limited to 5 visitors per escort recommended	• Visitor close escort in constant line of sight required • Groups limited to 5 visitors per escort recommended

Table 46: Physical Security Measures and Controls – Security Alarm Systems (SAS)

Measure	Zone One	Zone Two	Zone Three	Zone Four	Zone Five
Out-of-hours security alarm system (SAS)	• Determined by entity risk assessment	• Determined by entity risk assessment • In an office environment, Class 3-4 SAS[20] hard wired in the zone recommended.	• Hard wired Type 1A SAS, or Class 5[20] SAS required • If no SAS, guard patrols performed at random intervals within every four hours required	• SCEC-approved Type 1A SAS required	• As for Zone Four
SAS detection devices	• Determined by entity risk assessment	• Hard wired detection service within the zone required • SCEC-approved SL2 or SL3 detection devices recommended.	• As for Zone Two	• SCEC-approved SL3 or SL4 detection devices (designed and commissioned by SCEC-endorsed Security Zone Consultants) required	• As for Zone Four
SAS contractor clearance requirements	• Determined by entity risk assessment	• Contractors who maintain these systems provided with short term access to security classified resources at the appropriate level for the information stored within the zone	• As for Zone Two	• Contractors who maintain these systems cleared at the appropriate level for the information stored within the zone	• As for Zone Four
SAS management	• Determined by entity risk assessment	• As for Zone One	• Control of alarm systems directly managed by the entity • Privileged alarm systems operators and users appropriately trained and security cleared to the level of the Security Zone • All alarm system arming and disarming personal identification numbers are secure	• As for Zone Three	• As for Zone Three
SAS monitoring and response	• All alarm systems are monitored and responded to in a timely manner • Response capability appropriate to the threat and risk	• As for Zone One	• As for Zone One	• As for Zone One	• As for Zone One
Interoperability of alarm system and other building management system	• Determined by entity risk assessment	• Determined by entity risk assessment • If a separate SAS and EACS are used, ensure the alarm cannot be disabled by the access control system	• Ensure the alarm cannot be disabled by the access control system	• Ensure limited one way interoperability in accordance with the Type 1A SAS for Australian Government—Product Integration specification	• Ensure limited one way interoperability in accordance with the Type 1A SAS for Australian Government—Product: Integration specification • The alarm system may disable access control system when activated

Table 47: Physical Security Measures and Controls – Security Guards

Measure	Zone One	Zone Two	Zone Three	Zone Four	Zone Five
Security guards and patrols	• Determined by entity risk assessment	• Determined by entity risk assessment • The response time for off-site guards is recommended to be less than the delay given by the total of other controls	• As for Zone Two	• As for Zone Two	• As for Zone Two
Out-of-hours security guard services	• Security guard services may be used out-of-hours to respond to alarms	• Out-of-hours guard patrols may be used instead of a SAS • Security guard services may be used out-of-hours to respond to alarms	• Out-of-hours guard patrols may be used instead of a SAS	• Out-of-hours guard patrols must not be used in place of a SAS • Security guard services may be used out-of-hours to respond to alarms	• Out-of-hours guard patrols must not be used in place of a SAS • Security guard services may be used out-of-hours to respond to alarms

[20] Australian Standard AS/NZS 2201.1 provides guidance on alarm systems.

Measure	Zone One	Zone Two	Zone Three	Zone Four	Zone Five
			• If no SAS, patrols must be performed at random intervals within every four hours required • Security guard services may be used out-of-hours to respond to alarms		

Table 48: Physical Security Measures and Controls – Technical surveillance counter-measures (TSCM)

Measure	Zone One	Zone Two	Zone Three	Zone Four	Zone Five
Technical surveillance counter-measures	• No requirement	• No requirement	• Determined by entity risk assessment	• As for Zone Three	• TSCM and audio security inspection: o for areas where TOP SECRET discussions are regularly held, or the compromise of other discussions may have a catastrophic business impact level o before conferences and meetings where TOP SECRET discussions are to be held o seek advice from ASIO-T4 and refer ASIO Technical Note 5/12 Physical Security of Zone Five (TOP SECRET) areas